Amended Exhibit A: Infringement Contentions for U.S. Patent No. 10,674,009 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 (corresponding to, associated with, and/or otherwise relating to, for example, voice and/or text communications), 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" further 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 claims 1-23 of U.S. Patent No. 10,674,009 (the "'009 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 '009 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 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 '009 Patent under 35 U.S.C. § 271(a).

Defendants have induced and continue to induce infringement of claims 1-23 of the '009 Patent by, with knowledge of the '009 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

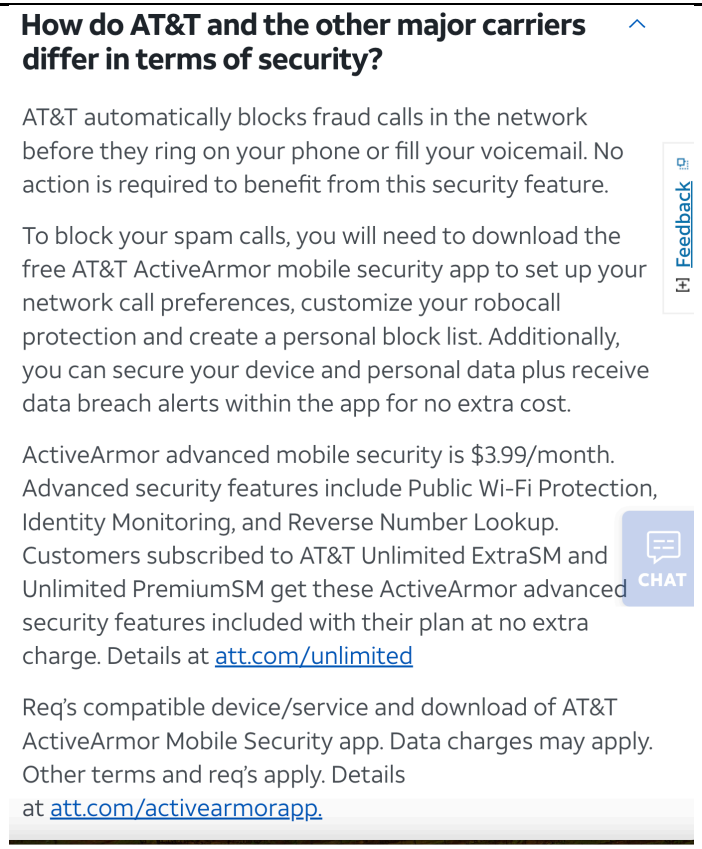
operate the Accused Instrumentalities in an infringing manner and/or preconditioning use of the Accused Instrumentalities on use in an infringing manner. Defendants further manifest this intent to induce infringement by providing support services for the Accused Instrumentalities, including providing 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 1-23 of the '009 Patent under 35 U.S.C. § 271(b).

Defendants have contributed and continue to contribute to infringement of claims 1-23 of the '009 Patent by, with knowledge of the '009 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 1-23 of the '009 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 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. 10,674,009	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) that meets the claim limitations. The Accused Instrumentalities, alone and/or in combination, comprise one or more system(s) and service(s) that are configured to determine if a given call should be blocked, connected, or if additional authentication information is required, and/or are otherwise capable of detecting, blocking, and preventing SPAM, fraudulent, and spoofed phone calls. *See, e.g.*, 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 ActiveArmor℠ 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. AT&T also 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., Stop calls with Digital Phone Call Protect*, AT&T, RQ-ATT0000137-RQ-ATT0000138 (https://www.att.com/support/article/u-verse-voice/KM1235421/):

Digital Phone Call Protect features

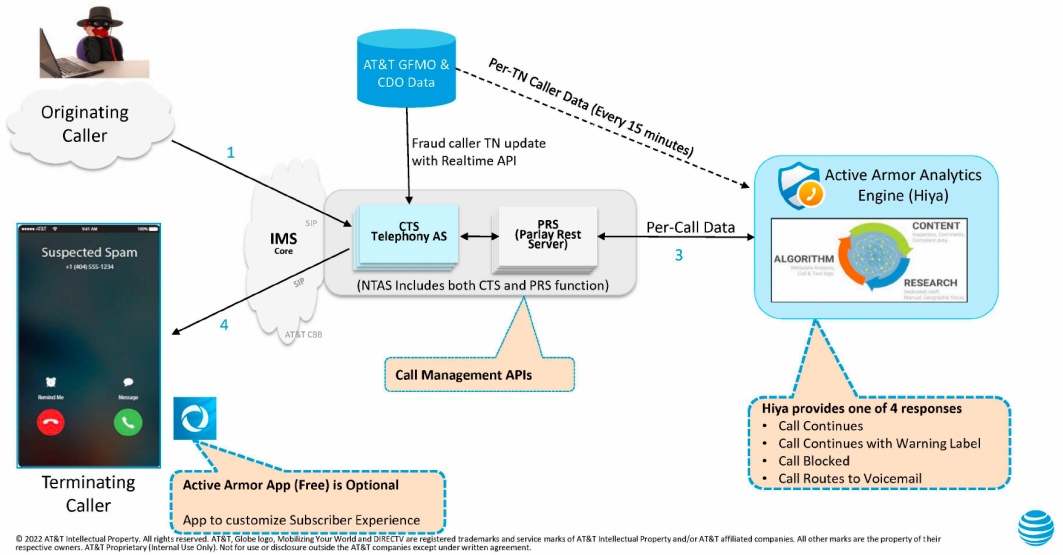
Here's what you get with Digital Phone Call Protect[1]:

- **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).

The Accused Instrumentalities are implemented, used, and/or put into service by AT&T 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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	Furthermore, 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 and/or used to, among other functions, detect spoofed, spam and/or fraudulent phone calls. *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 should be connected or blocked)): AT&T Active Armor (Call Protect) – High Level Architecture  *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/); RQ0001970 (https://sti-ga.atis.org/resources/).

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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

1[a] a verification service provider, configured to, using one or more processors:	The Accused Instrumentalities comprise a verification service provider configured to perform the limitations of the claim, using one or more processors. Within the Accused Instrumentalities, the verification service provider comprises of one or more components, implemented in hardware, software, or a combination thereof, used by, implemented in, and/or included in the Accused Instrumentalities to perform the limitations of the claim. The one or more processors are comprised of 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 verification service provider of the Accused Instrumentalities may include one or more processors located within Defendants' network, one or more third party (e.g., Hiya) processors deployed, used, and/or otherwise incorporated in the Accused Instrumentalities, or some combination thereof. *See* 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. *See, e.g.*, RQ-ATT0000024-RQ-ATT0000026 (https://about.att.com/story/2019/call_validation_displays.html):



See, e.g., 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 ActiveArmor℠ 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.

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, 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 Protect[1]:

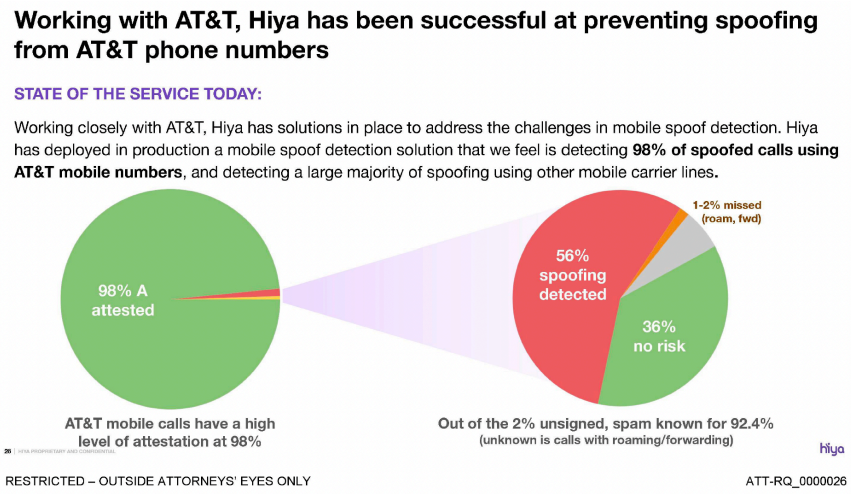
- **Call validation:** Soon you'll see a [V] on your caller ID for some calls. This means we've confirmed that the call originated from the phone registered to that number. (Remember to still be cautious when answering a call from an unknown number.)
- **Automatic fraud blocking:** Each potential fraud 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 further example, the Accused Instrumentalities are configured to implement protocols, technologies, features, and services for validating and/or verifying caller identification information, using one or more processors, 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):

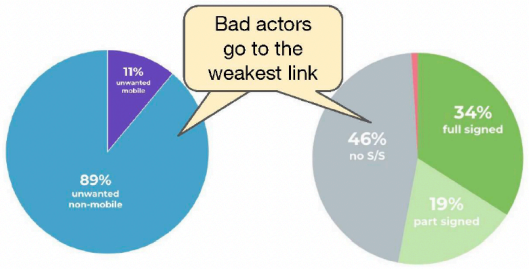


See, e.g., ATT-RQ_0000001 at 26 (showing that AT&T prevents spoofing from its own numbers on its network):



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

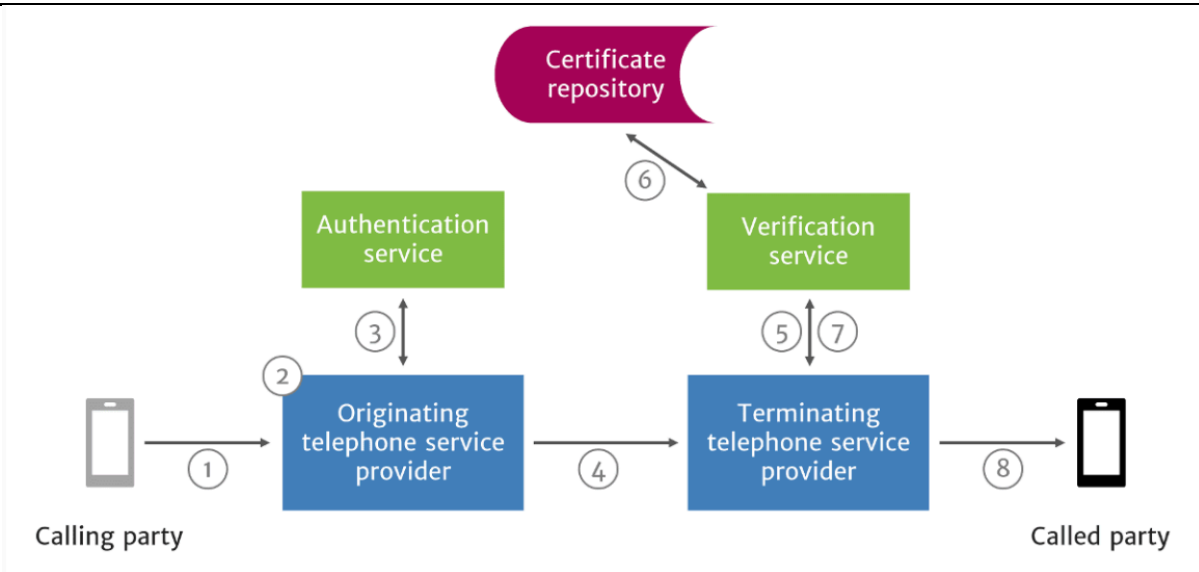
ATT-RQ_0000028

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


+1 374-425-8923
Valid number
Incoming call
Recent history
10:51 AM
Swipe an icon in any direction
Answer
Decline with message
Decline

	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 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/).



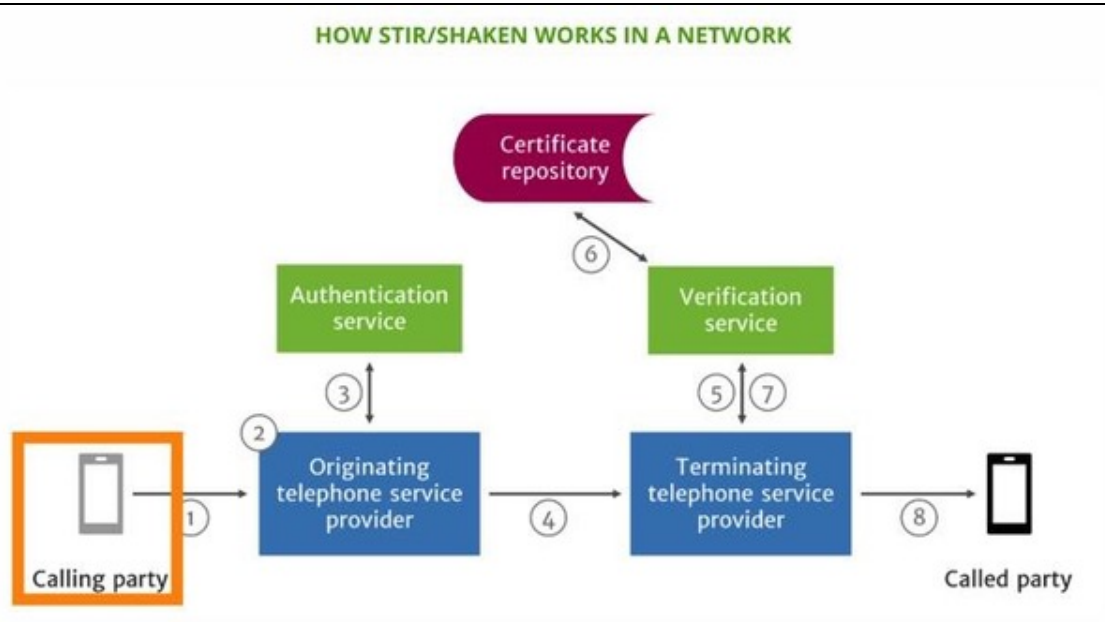
See, e.g., RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/).

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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	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[b] enroll a first device with the verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device;	The Accused Instrumentalities comprise one or more processors configured to enroll a first device with the verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device. The enrolling of the first device includes associating, by the verification service provider, the first device with a device fingerprint. RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/); RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/). The device fingerprint is generated based at least in part on a set of configuration information associated with the first device. As one example, the verification service provider enrolls a first device ("calling party", indicated with orange box). RQ0002113-RQ0002120(https://transnexus.com/whitepapers/understanding-stir-shaken/); RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).



Before Defendants determine how to attest for the validity of the calling number, Defendants' Accused Instrumentalities are configured to determine if the call should be connected. The Accused Instrumentalities, alone or in combination, enroll a first device (showing as "calling party" and identified with an orange box). Enrollment of the first device includes generation of a device fingerprint based at least in part on a set of configuration information at least a portion of which is used at least in part to perform a security determination (e.g., SIM-based, credential-based, or line-based authentication).A device fingerprint is generated based at least in part on a set of configuration information associated with the first device. Examples of such configuration information used to generate the device fingerprint include without limitation combinations of device specific data, device settings, installed applications, system or application software versions, contact list data, or other data specific to the calling device.

As one example, a device fingerprint comprises and/or is otherwise generated based at least in part on a mobile identification number ("MIN") or any derivation of a MIN or any related number. *See, e.g.*, *Mobile Identification Number*, Wikipedia, RQ0001968 (https://en.wikipedia.org/wiki/Mobile_identification_number). As another example, a device fingerprint comprises and/or is otherwise generated based at least in part on a mobile subscription

	identification number ("MSIN"). As another example, a device fingerprint comprises and/or is otherwise generated based at least in part on an international mobile subscriber identity ("IMSI") or encrypted version thereof ("TMSI"). *See, e.g.*, *International Mobile Equipment Identity*, RQ0001957-RQ0001964 (https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity); Margarethe Boggess, *What is a Mobile Identification Number (MIN)*, Cellular News (Nov. 29, 2023), RQ0002121-RQ0002123 (https://cellularnews.com/definitions/what-is-a-mobile-identification-number-min/). As one example, a device fingerprint comprises and/or is otherwise generated based at least in part on a Subscriber Module (SIM) Card serial number. *SIM card*, Wikipedia, RQ0002042-RQ0002060 (https://en.wikipedia.org/wiki/SIM_card). As one example, a device fingerprint comprises and/or is otherwise generated based at least in part on a serial number, Host Device ID, or any other unique identifier for a device (including but not limited to Android ID, UDID, IDFA, AAID). *Find the serial number or IMEI on your iPhone, iPad, or iPod touch*, Apple, RQ0001932-RQ0001939 (https://support.apple.com/en-us/108037); *Is There a Unique Android Device ID*, Saturn Cloud (Jun. 12, 2023), RQ0001965-RQ0001967 (https://saturncloud.io/blog/is-there-a-unique-android-device-id/). As one example, a device fingerprint comprises and/or is otherwise generated based at least in part on any derivation and/or combination of the above examples or any other configuration information. The Accused Instrumentalities associate the first device with a device fingerprint. *See, e.g.*, *Call Protect*, AT&T, RQ-ATT0000099-RQ-ATT0000104 (https://www.att.com/device-support/article/wireless/KM1324197/Samsung/SamsungSMG975U/):

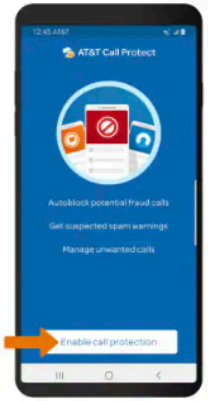
Access call protect

1. Navigate to and select the **AT&T Call Protect app**.

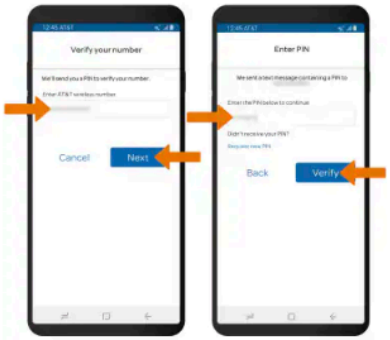
Note: AT&T Call Protect allows you to automatically block fraudulent calls, warns you about phone spam, and temporarily blocks unwanted calls.

2. Select **Enable call protection**.

*Note: Review the permissions, then select **ALLOW**.*



3. Enter your **myAT&T wireless number**, then select **Next**. Enter the **PIN** sent via text, then select **Verify**.



4. Review the Terms & Conditions, then select **I agree**. Select **Continue**.

*Note: Select **ALLOW** to give permission to the app to access your contacts.*

	For further example, AT&T collects information about equipment on the AT&T Networks, and uses it in, among other ways, "verifying your identity, detecting and preventing fraud." *See, e.g.*, *AT&T Privacy Notice*, AT&T, 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).

See also AT&T ActiveArmor Mobile Security Application and Service, AT&T, 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).

See also 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 (e.g., "Device OS", "ActiveArmor Version Information"), contact list data (TN from Device Address Book), or other data specific to the calling device):

	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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

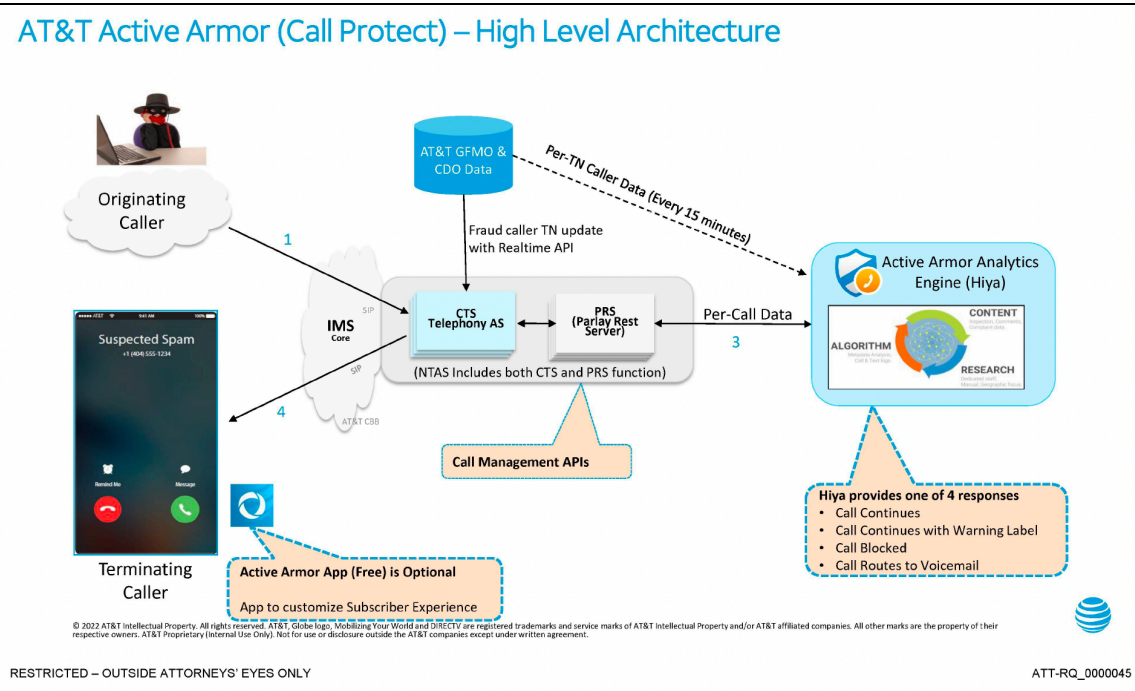
CTN (including AT&T/FN/Cricket customers)
Service tier (like Basic vs. Advanced)
Service Tags:

- 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 (AT&T GFMO and CDO Data):



See also 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.

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] store, at the verification service provider, the device fingerprint associated with the first device;	The Accused Instrumentalities comprise one or more processors configured to store, at the verification service provider, the device fingerprint associated with the first device. As one example, the one or more processors are configured to store, at the verification service provider, information associated with the first device including but not limited to the device fingerprint and/or the configuration information upon which the device fingerprint is based at least in part. For example, the Accused Instrumentalities use and store various information collected about equipment on the networks. *See, e.g.*, RQ-ATT0000070-RQ-ATT0000086 (https://about.att.com/privacy/privacy-notice.html).

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).

Data retention and security ×

We keep your information as long as we need it for business, tax or legal purposes. We set our retention periods based on things like what type of personal information it is, how long it's needed to operate the business or provide our products and services, and whether it's subject to contractual or legal obligations. These obligations might be ongoing litigation, mandatory data retention laws or government orders to preserve data for an investigation. After that, we destroy it by making it unreadable or indecipherable.

See also 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).

See also 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 (e.g., "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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

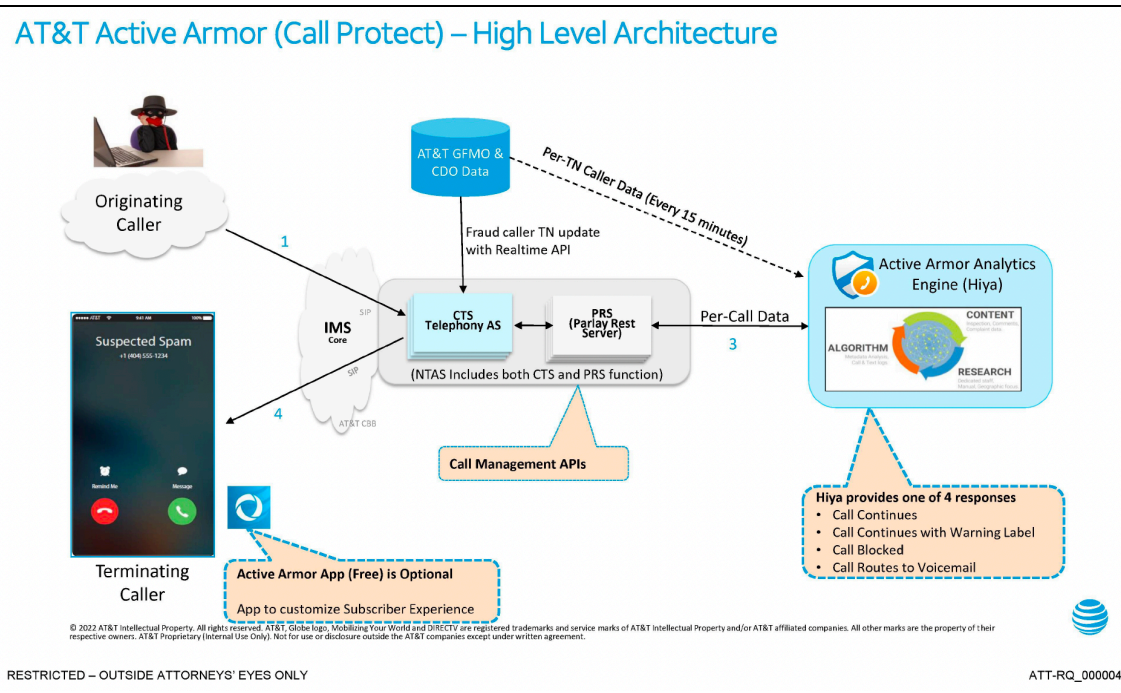
CTN (including AT&T/FN/Cricket customers)
Service tier (like Basic vs. Advanced)
Service Tags:

- 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 (storage locations, e.g., AT&T GFMO and CDO Data):



As another example, the Accused Instrumentalities are capable of storing a device fingerprint for it later to be used to check the call source against the calling number. *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/); RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/).

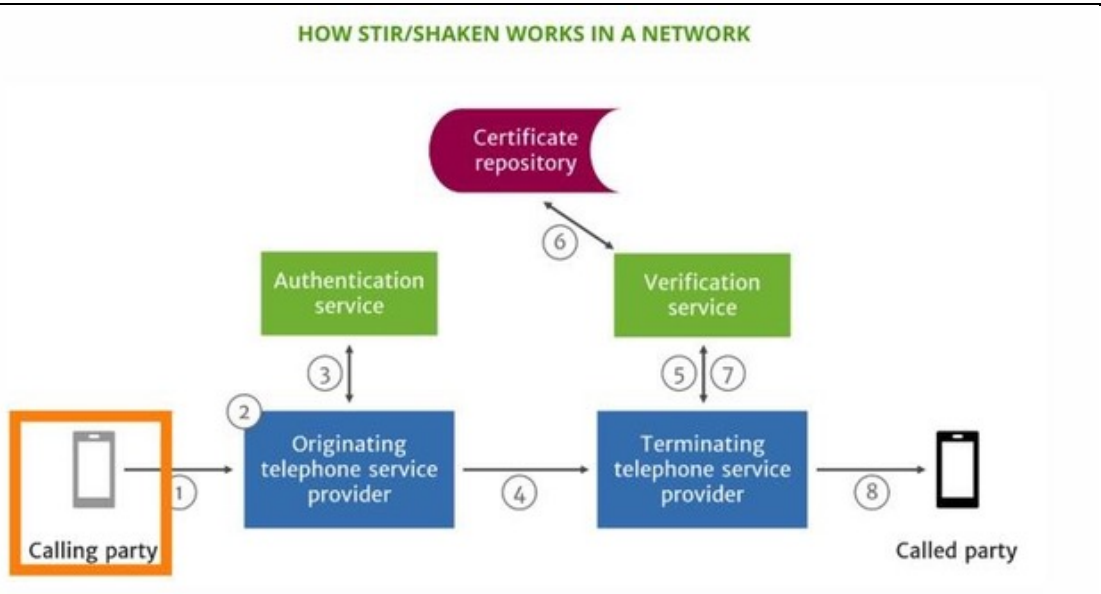
As another example, the Accused Instrumentalities are capable of storing a device fingerprint to attest for the validity of the calling number, whether it is:

(A) a subscriber registered with the originating telephone service provider's softswitch ("Full Attestation");

(B) a number behind an enterprise PBX ("Partial Attestation"); or,

(C) an identifier of from where the call was received, such as a call from an international gateway ("Gateway Attestation").

	2. The originating telephone service provider checks the call source and calling number to determine how to attest for the validity of the calling number. • **Full Attestation (A)** — The service provider has authenticated the calling party and they are authorized to use the calling number. An example of this case is a subscriber registered with the originating telephone service provider's softswitch. • **Partial Attestation (B)** — The service provider has authenticated the call origination, but cannot verify the call source is authorized to use the calling number. An example of this use case is a telephone number behind an enterprise PBX. • **Gateway Attestation (C)** — The service provider has authenticated from where it received the call, but cannot authenticate the call source. An example of this case would be a call received from an international gateway. 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[d] obtain, at the verification service provider, information transmitted by a second device associated with a communications connection;	The Accused Instrumentalities comprise one or more processors configured to obtain, at the verification service provider, information transmitted by a second device associated with a communications connection. As one example, a second device is a calling device, for example the "calling party" indicated with the orange box below. *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/); RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/).



As one example, information is transmitted by the calling party or second device to the processors, including for example a device fingerprint of and/or other information transmitted by the second device, that is obtained at the verification service provider.

An example of the obtained information transmitted by the second device associated with a communications connection includes SIP information and/or the information contained with the SIP invitation transmitted by the calling party. *SIP INVITE*, Twilio Docs, RQ0002066-RQ0002080 (https://www.twilio.com/docs/glossary/sip-invites); *SIP*, TutorialsPoint, RQ-ATT0000213-RQ-ATT0000285 (https://www.tutorialspoint.com/session_initiation_protocol/); 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).

Another example of the obtained information transmitted by the second device associated with a communications connection includes but is not limited to a mobile identification number ("MIN") or any derivation of a MIN or any related number, a mobile subscription identification number ("MSIN"), the international mobile subscriber identity ("IMSI") or encrypted version thereof ("TMSI"), Subscriber Module (SIM) Card serial number, a serial number, Host Device ID, or any

another unique identifier for a device (including but not limited to Android ID, UDID, IDFA, AAID), and/or any derivation and/or combination of the thereof.

Another example of the obtained information transmitted by the second device associated with a communications connection includes the information AT&T collects about equipment on the AT&T Networks, and uses in, among other ways, "verifying your identity, detecting and preventing fraud." *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 ×

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).

See also 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).

See also ATT-RQ_0000042, -43, -44 ("As part of the Active Armor Robocall mitigation program, data elements related to calling are shared with our 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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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.
1[e] perform, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device; and	The Accused Instrumentalities comprise one or more processors configured to perform, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device. The Accused Instrumentalities, alone and/or in combination, comprise one or more system(s) and service(s) that are configured to determine if the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint to decide if, for example, the call should be connected. *See,* 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 (e.g., "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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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:

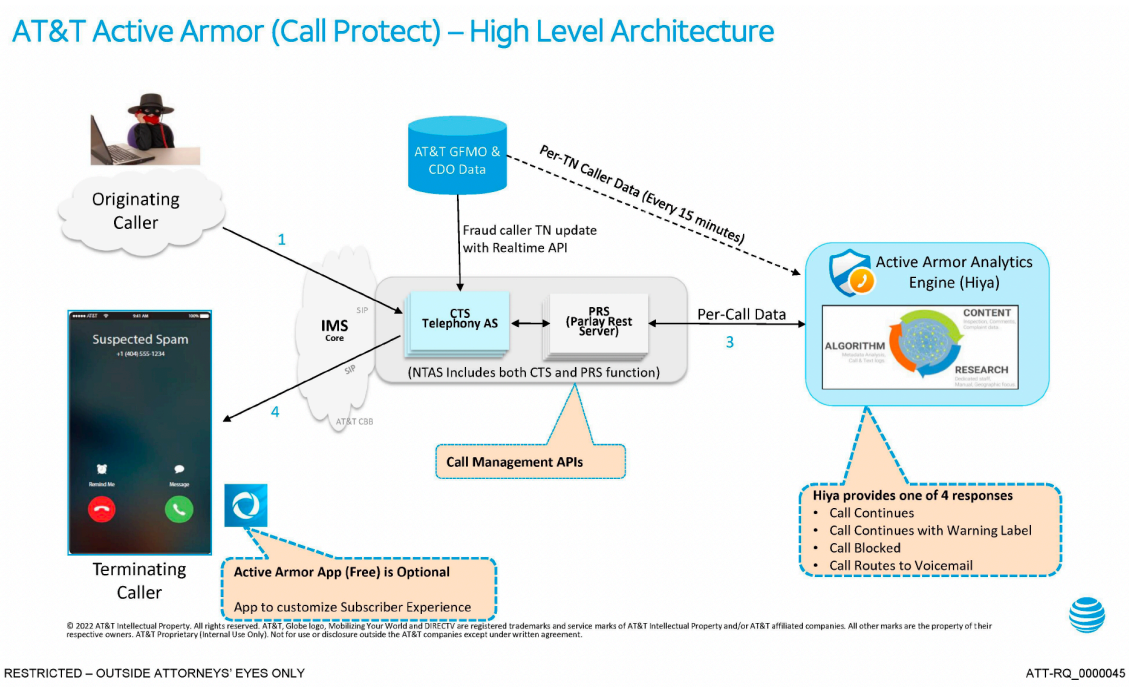
- FirstNet
- CRU
- COU
- Customers who have rate-plan-included Advanced service.
- Cricket
- Prepaid
- Wireless Home Phone

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).



Furthermore, caller identification authentication and verification technology, including without limitation STIR/SHAKEN, is technology configured and/or used to, among other functions, detect spoofed, spam and/or fraudulent phone calls.

As one example, a security determination is performed at the verification service provider to "check[] the call source and calling number to determine how to attest for the validity of the calling number." *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/); RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

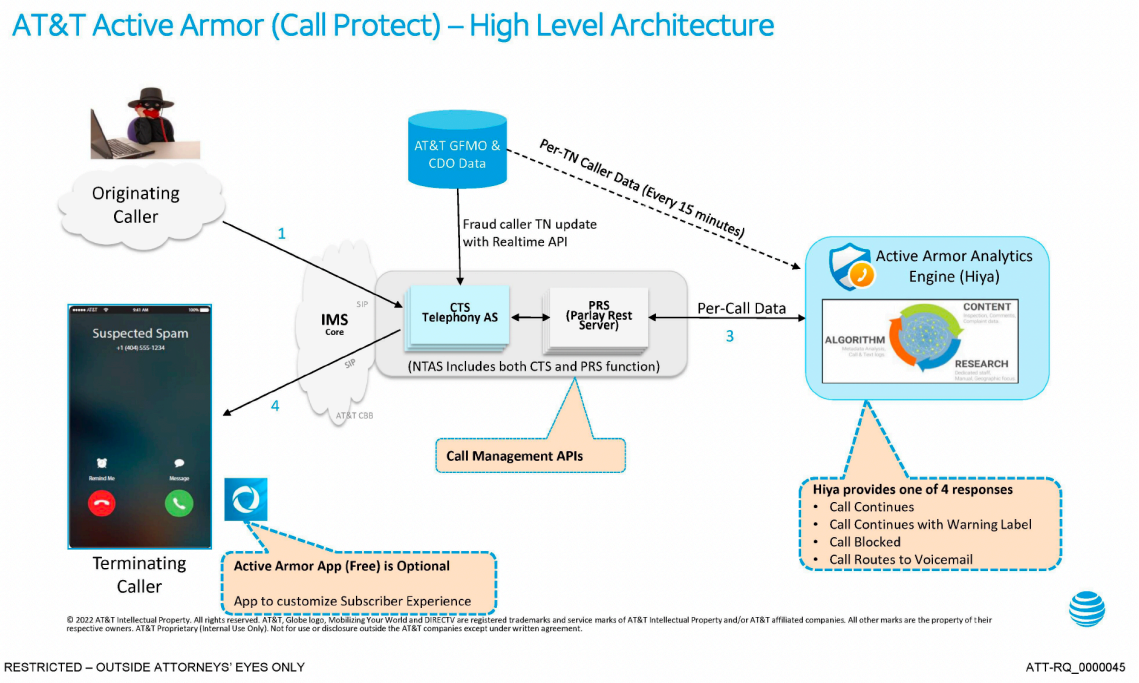
As another example, a security determination is performed at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device to determine how to attest for the validity of the calling

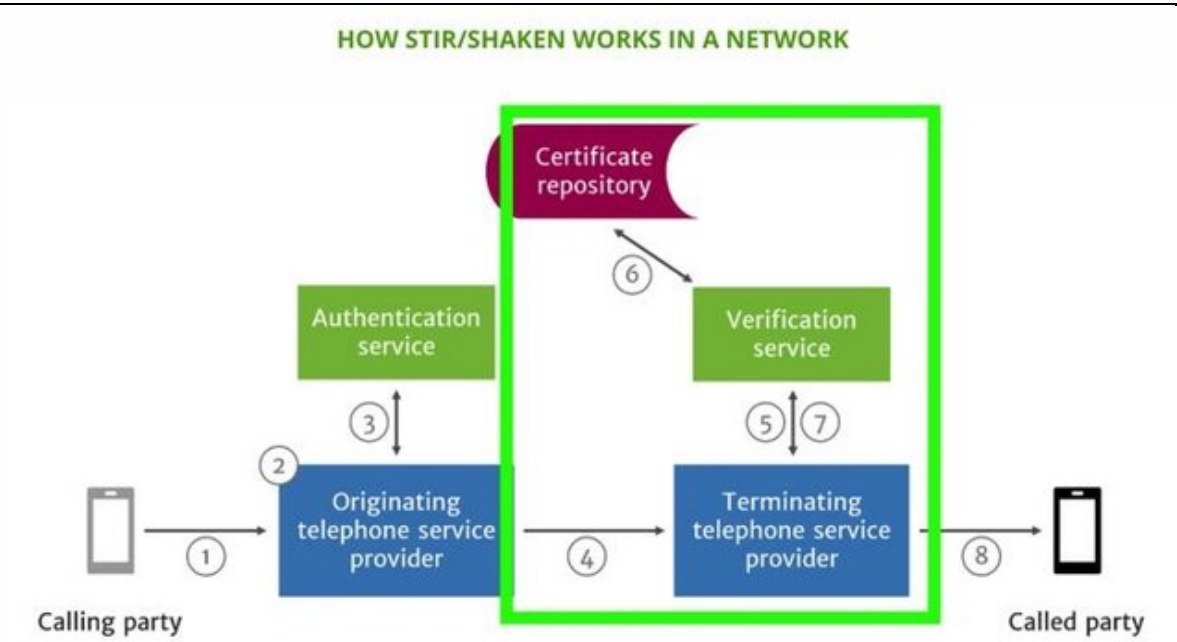
	number. *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/): 2. The originating telephone service provider checks the call source and calling number to determine how to attest for the validity of the calling number. • **Full Attestation (A)** — The service provider has authenticated the calling party and they are authorized to use the calling number. An example of this case is a subscriber registered with the originating telephone service provider's softswitch. • **Partial Attestation (B)** — The service provider has authenticated the call origination, but cannot verify the call source is authorized to use the calling number. An example of this use case is a telephone number behind an enterprise PBX. • **Gateway Attestation (C)** — The service provider has authenticated from where it received the call, but cannot authenticate the call source. An example of this case would be a call received from an international gateway. As one example, the SIP Identity header comprises information based on and/or reflecting performance of a security determination. *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/):

	3. The originating telephone service provider uses the authentication service to create a SIP Identity header. The authentication service could be a third-party service hosted in the cloud a software application integrated with the telephone service provider's softswitch or Session Border Controller (SBC). The SIP Identity header contains the following data: • Calling number • Called number(s) • Current timestamp • Attestation level • Origination identifier 4. The SIP INVITE with the SIP Identity header is sent to the terminating telephone service provider. In addition, the Identity token may be sent across the internet, out-of-band, to the terminating provider's Call Placement Service 5. The SIP INVITE with Identity header is passed to the verification service.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

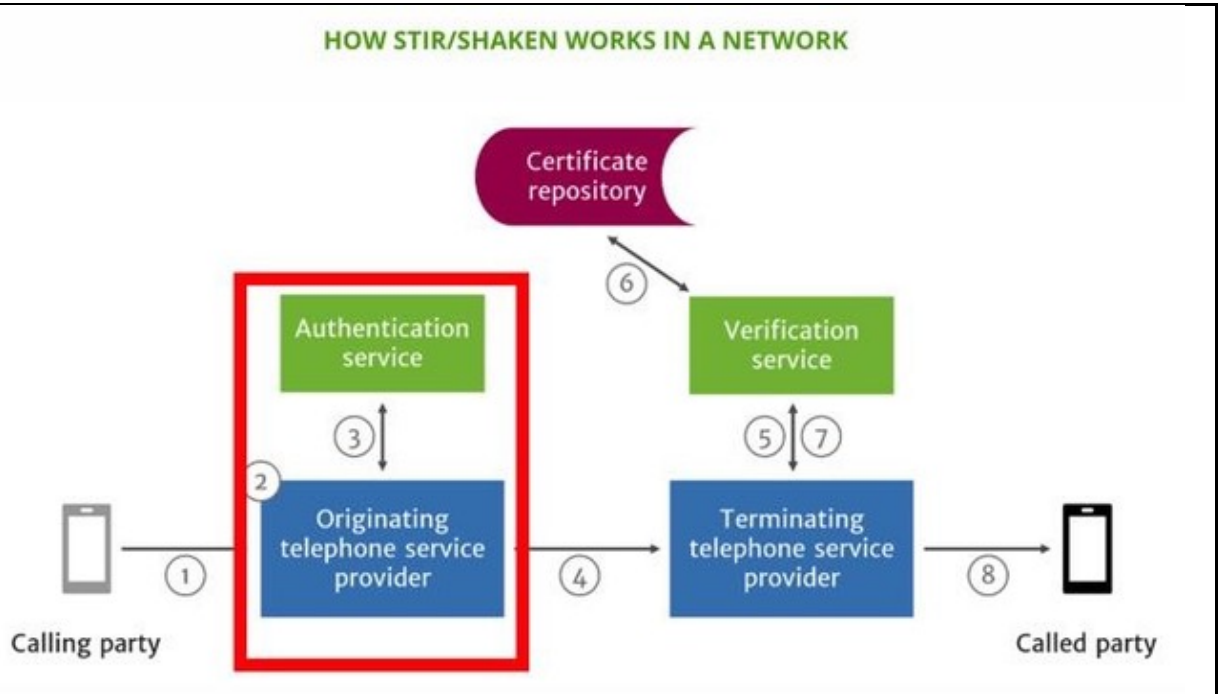
	6. The verification service obtains the digital certificate of the originating telephone service provider from the public certificate repository and begins a multi-step verification process. If all verification steps are successful, then the calling number has not been spoofed. • The SIP Identity header is base64 URL decoded and the details are compared to the SIP INVITE message. • The public key of the certificate is used to verify the SIP Identity header signature. • The certificate chain of trust is verified. 7. The verification service returns the results to the terminating service provider's softswitch or SBC. 8. The call is completed to the called party. 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[f] based at least in part on the security determination, select an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication.	The Accused Instrumentalities comprise one or more processors configured to, based at least in part on the security determination, select an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication. For example, AT&T's Robocall Mitigation system(s), Call Protect system(s) and service(s), ActiveArmor, the ActiveArmor mobile application, and Defendants' use of STIR/SHAKEN, alone and/or in combination, are configured to determine if a given call should be blocked, connected, or

	if additional authentication information is required. *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 should be connected or blocked)):  As one example, the one or more processors are capable of selecting an action based on the SIP Identity header. As one example, the action may be selected using the components, functionality, and/or processes indicated by the green box below:



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

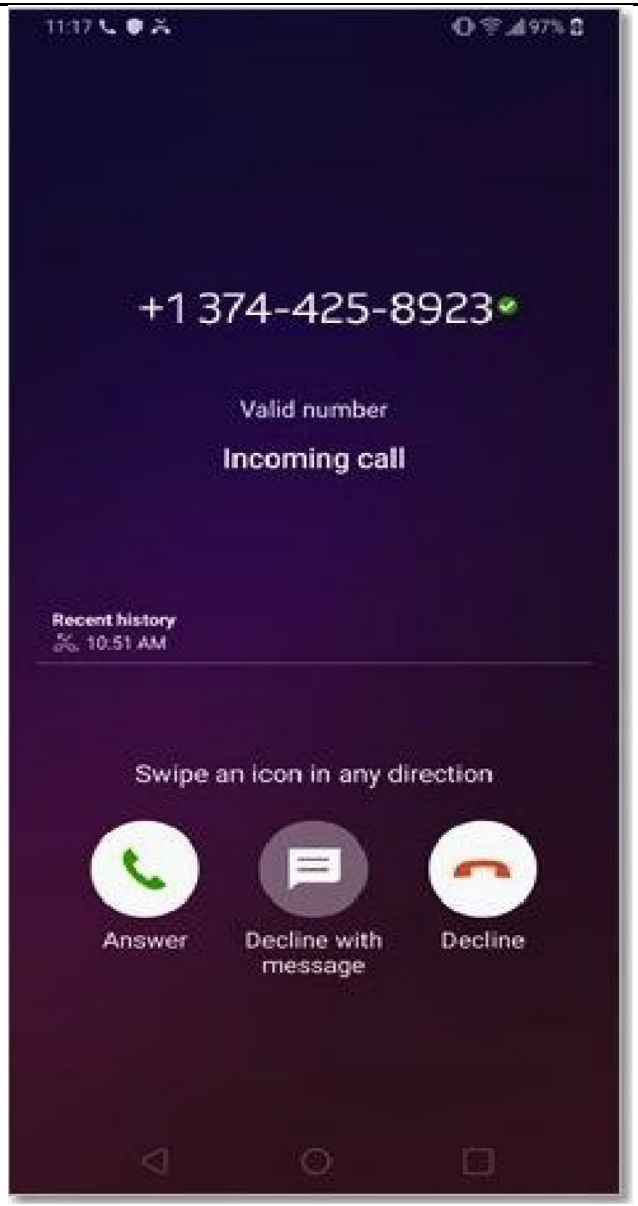
As another example, the one or more processors are capable of selecting an action based on the SIP Identity header. As one example, the action may be selected using the components, functionality, and/or processes indicated by the red box below:



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

The action capable of selection comprises at least one of blocking the communication, requesting additional verification, and permitting the communication:

	6. The verification service obtains the digital certificate of the originating telephone service provider from the public certificate repository and begins a multi-step verification process. If all verification steps are successful, then the calling number has not been spoofed. • The SIP Identity header is base64 URL decoded and the details are compared to the SIP INVITE message. • The public key of the certificate is used to verify the SIP Identity header signature. • The certificate chain of trust is verified. 7. The verification service returns the results to the terminating service provider's softswitch or SBC. 8. The call is completed to the called party. As one example, the communication is permitted in Step 8 above. *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/). For example, the Accused Instrumentalities permit the call or permit the call and convey an assurance to a callee associated with the call. *See, e.g.*, RQ-ATT0000024-RQ-ATT0000026 (https://about.att.com/story/2019/call_validation_displays.html):

	 +1 374-425-8923 Valid number Incoming call Recent history 10:51 AM Swipe an icon in any direction Answer Decline with message Decline

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.

Furthermore, caller identification authentication and verification technology, including without limitation AT&T's Robocall Mitigation system(s), Call Protect system(s) and service(s), ActiveArmor, and the ActiveArmor mobile application are capable of detecting, blocking and preventing SPAM, fraudulent and spoofed phone calls.

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 also Apple iPhone 13, AT&T, RQ-ATT0000161-RQ-ATT0000163 (https://www.att.com/device-support/article/wireless/KM1403775/Apple/iPhone13/).

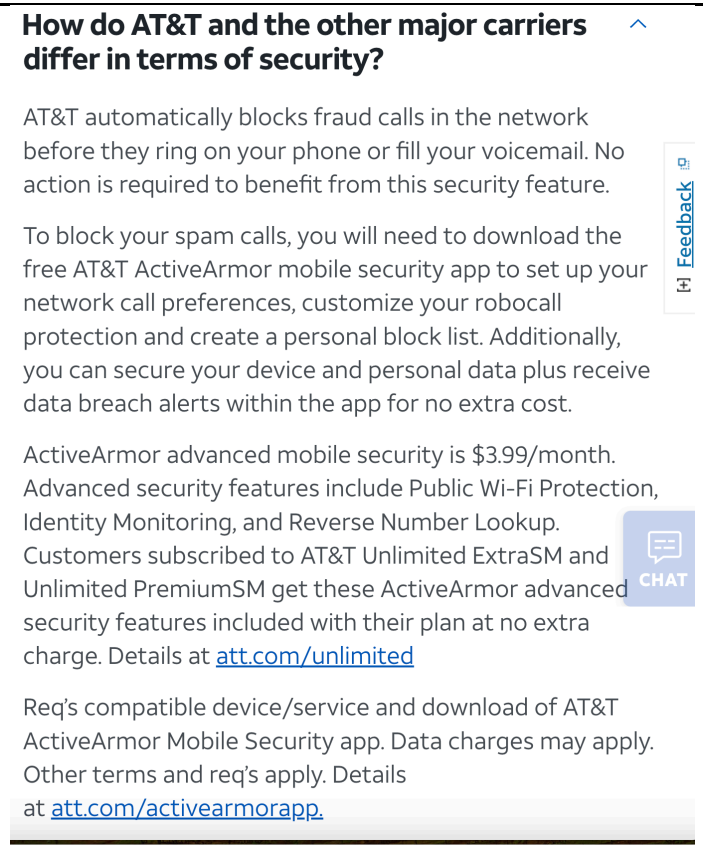
As another example, based at least in part on the security determination, the Accused Instrumentalities indicate a failure to confirm to the callee the identity of the caller and/or block the call. *See, e.g.*, *AT&T Community Forums*, AT&T (Jan. 2, 2023), RQ-ATT0000095-RQ-ATT0000098 (https://forums.att.com/conversations/account-features/blocking-unknown-numbers/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 you 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

	As one example of an action, based at least in part on the security determination, the Accused Instrumentalities block a call. *See, e.g.*, *What is AT&T ActiveArmor mobile security?*, AT&T, RQ-ATT0000153-RQ-ATT0000160 (https://www.att.com/wireless/what-is-activearmor-security/): **What are the benefits of AT&T ActiveArmor?** Customers should download the free AT&T ActiveArmor mobile security app to customize their robocall protection, manage nuisance calls, and create their own personal block list. Additionally, with AT&T ActiveArmor advanced, customers can secure their devices and personal data plus receive data breach alerts within the app. Download to activate the free app and services for an extra layer of protection that helps you easily secure your data, manage nuisance calls, and more. • **24/7 automatic fraud call blocking:** Detects and blocks calls from likely fraudsters before they reach you. • **Spam call blocking:** Blocks or sends calls to voicemail if identified as a Spam Risk. • **Nuisance call alerts:** Labels potential nuisance calls from telemarketers, surveys, and more. • **Spam call routing:** Choose call categories to accept, block, or send to voicemail. • **Unknown calls to voicemail:** Automatically sends callers to voicemail if they're not in your address book and blocks other numbers in your personal block list. • **Block all texts from email:** Block all email-originated texts from your phone. • **Personal block list:** Add individual unwanted callers to your own block list. • **Device security:** Helps protect your data from mobile threats. • **System update:** Keep up to date with operating system changes with reminders. • **Breach reports:** Get alerts about company data breaches, along with helpful tips. *See also* RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/):



See also., RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/):



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

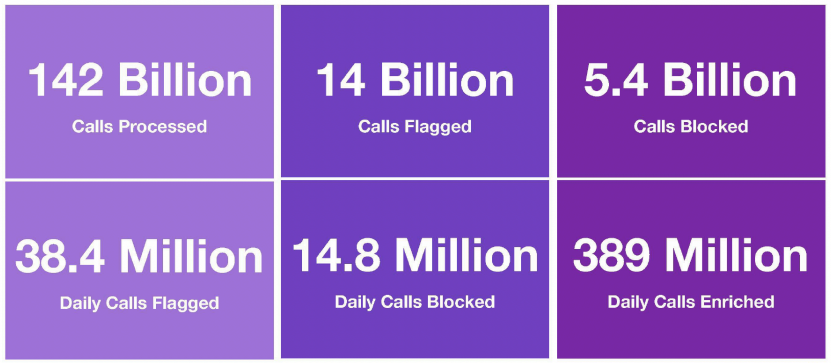
Digital Phone Call Protect features

Here's what you get with Digital Phone Call Protect[1]:

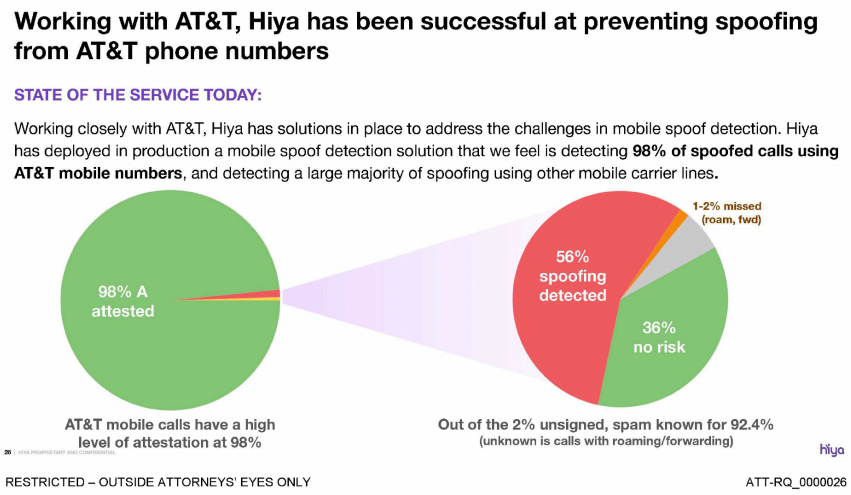
- **Call validation:** Soon you'll see a [V] on your caller ID for some calls. This means we've confirmed that the call originated from the phone registered to that number. (Remember to still be cautious when answering a call from an unknown number.)
- **Automatic fraud blocking:** Each potential fraud 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).

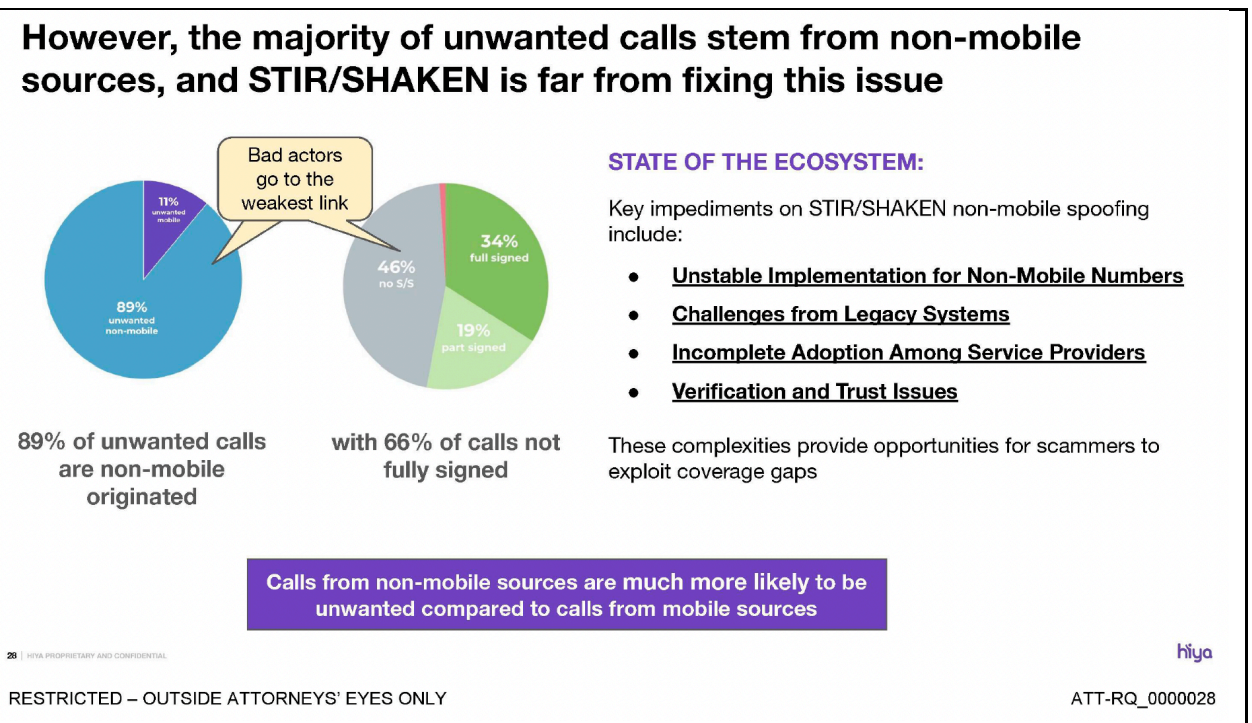
See, e.g., ATT-RQ_0000001 at 3, showing volume of blocks calls necessitating the use of computer systems with processors to make the determination to block or connect an outgoing or incoming call:

Hiya-AT&T Call Protect 2023 Summary

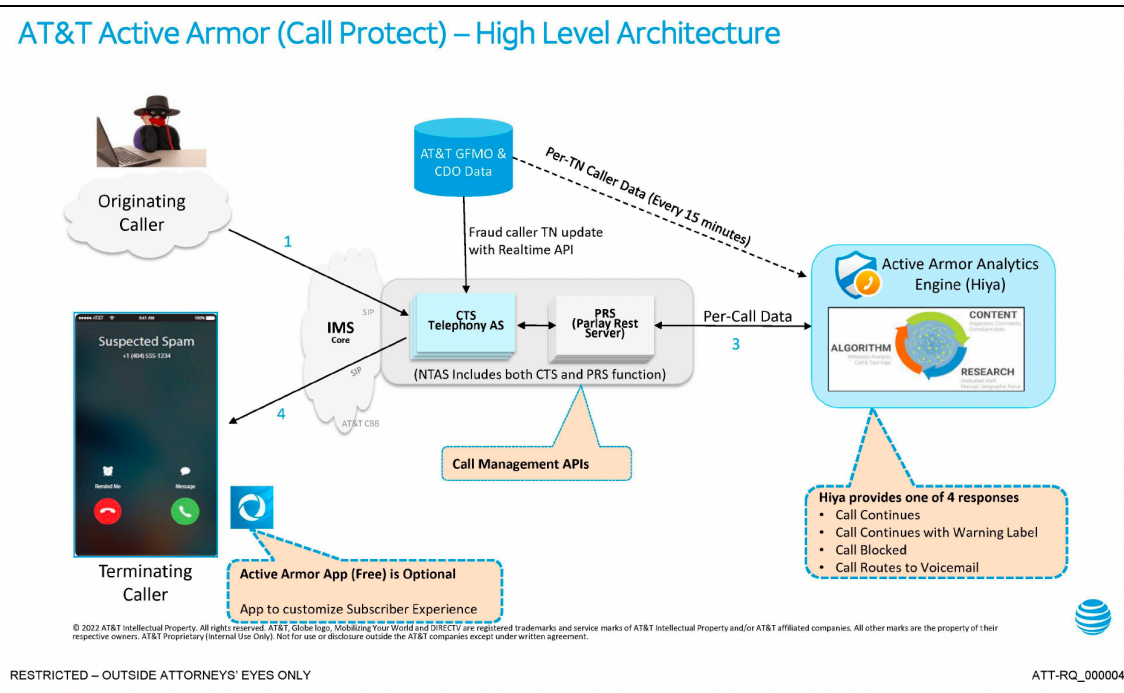


RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY ATT-RQ_0000003

	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. 98% A attested AT&T mobile calls have a high level of attestation at 98% 56% spoofing detected 1-2% missed (roam, fwd) 36% no risk Out of the 2% unsigned, spam known for 92.4% (unknown is calls with roaming/forwarding) 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.



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 should be connected or blocked)):

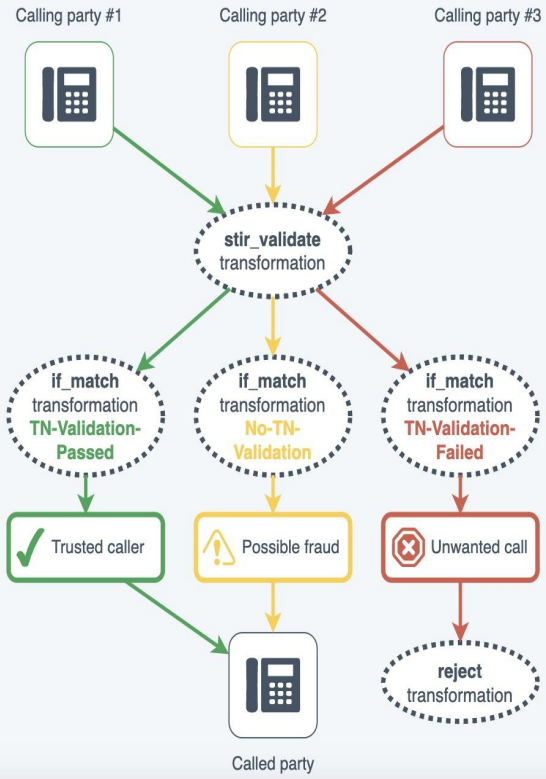


See also Verification Examples, CarrierX, RQ0001940-RQ0001955 (https://www.carrierx.com/documentation/how-it-works/stir-shaken#verification-examples):

Verification Examples

The `stir_validate` transformation is normally not used all by itself. You can use it to verify the call signature and then use the output data with other transformations to manage the further call behavior.

An example of such a behavior can look like this:



See also RQ-ATT0000135-RQ-ATT0000136 (https://about.att.com/story/2021/robocalls.html):

	AT&T's approach works for business and consumer lines – wired or wireless. We're on track to *double* last year's numbers because of our *triple*-barreled protection: 1. AT&T Call Protect gives wireless customers automatic fraud blocking and suspected spam alerts. 2. Our global fraud team runs an additional program that blocks fraud calls to every type of AT&T phone service. 3. STIR/SHAKEN, a new call authentication technology, is now boosting both programs with extra data for detection and accuracy. 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 2. The system of claim 1, wherein the information transmitted by the second device is obtained via a backchannel that is different from the communications connection.	Within the Accused Instrumentalities the information transmitted by the second device is obtained via a backchannel that is different from the communications connection. As an example, the information transmitted by the second device is obtained via a connection or channel that uses the same type of path as the communications connection but different protocols. As another example, the information transmitted by the second device is obtained via a channel or connection that follows a different route and/or data flow as the communications connection. As another example, the information transmitted by the second device is encoded within the same type of path as a communications connection or the information transmitted by the second device is not encoded and is obtained via an encoded primary communication channel. As another example, the information transmitted by the second device is obtained via a communications connection. As an example, the Accused Instrumentalities use other backchannel methods, such as SMS, WiFi, or Internet data in the verification service. For example, the communication includes a component that is difficult to predict by a potential attacker, such as a serial number, a counter, a pseudo-random

	or random number, a number specific to the session or the phone, or any other appropriate component value. As yet another example, the AT&T networks use an encoded primary communication channel so that the backchannel is not a separate channel. As one example, the AT&T Networks rely on an encoded primary channel included in the SIP Identity header. As a separate example, this encoded primary channel is accomplished with an AT&T mobile application, such as the ActiveArmor mobile application. RQ-ATT0000139-150 (https://www.att.com/legal/terms.activeArmorMobileSecurity.html). For example, in the Accused Instrumentalities, one communication channel can be used by the calling party device to make the call and a different communication channel, including for example a second communication channel accomplished with, initiated by, or used by the calling party's device, the called party's device, and/or an AT&T mobile application on the calling party's and/or called party's device, such as the ActiveArmor mobile application, can be used to obtain the information transmitted by the second device. RQ-ATT0000139-RQ-ATT0000150 (https://www.att.com/legal/terms.activeArmorMobileSecurity.html). For example, ATT discloses that it keeps information transmitted by the second device confidential and/or obtains information from third parties. *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 ×

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).

See also 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).

See, ATT-RQ_0000042, -43, -44 (evidencing information such as 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 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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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:

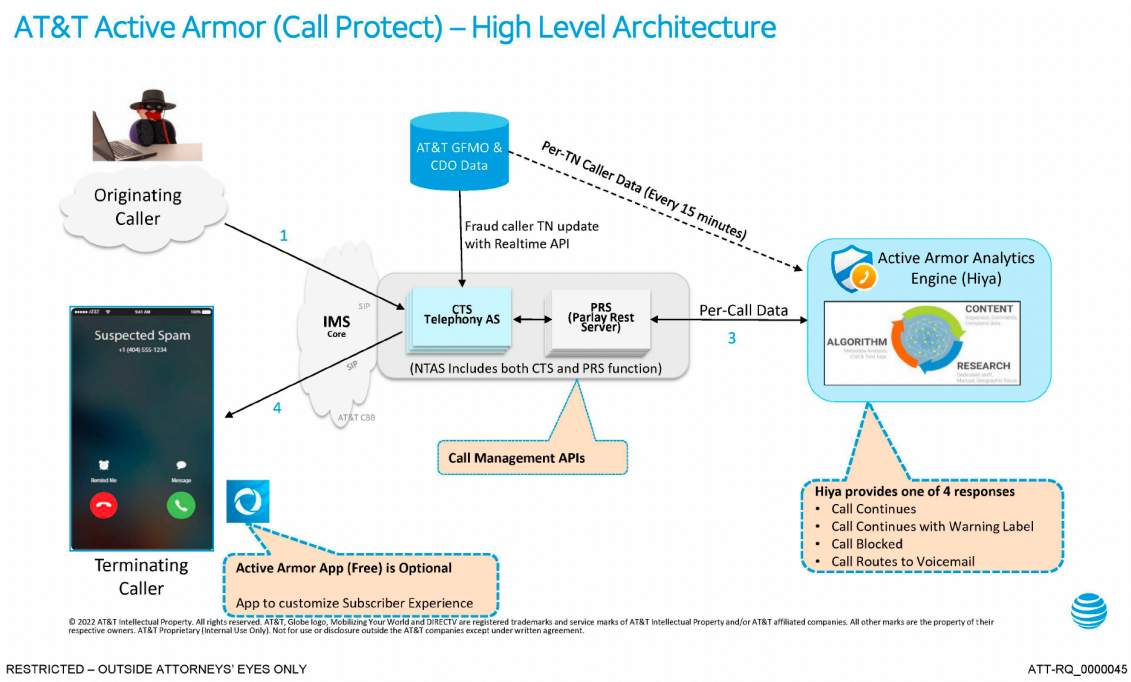
- FirstNet
- CRU
- COU
- Customers who have rate-plan-included Advanced service.
- Cricket
- Prepaid
- Wireless Home Phone

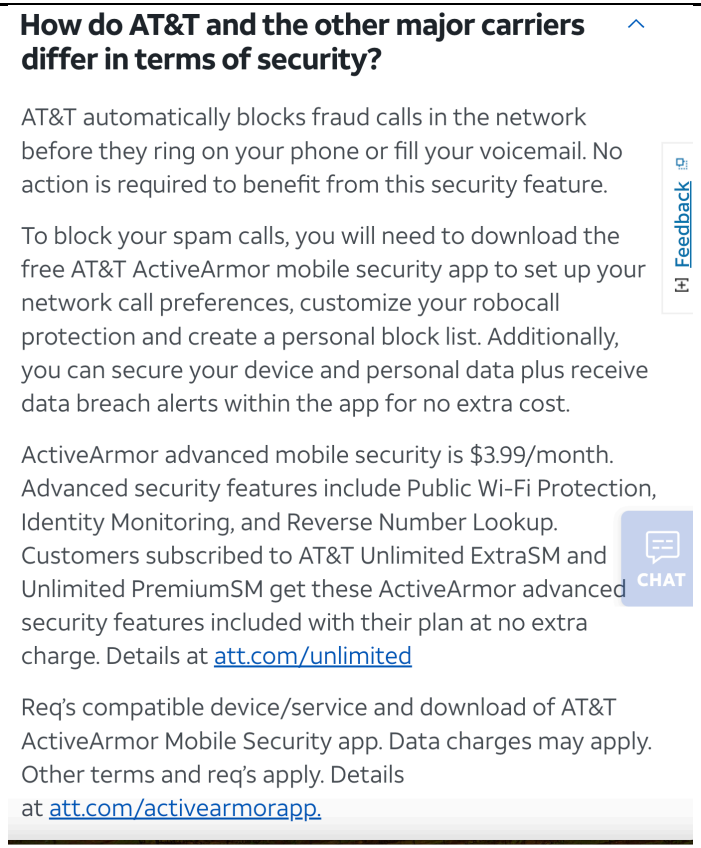
ActiveArmor Application Data

TN from Device Address Book - Hashed (shared only with explicit subscriber consent)
Device OS
ActiveArmor Version Information

See, e.g., 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. 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 of claim 1, wherein based at least in part on the security determination, the verification service provider is further configured to convey an assurance to a recipient associated with the communications connection.	Within the Accused Instrumentalities, based at least in part on the security determination, the verification service provider is further configured to convey an assurance to a recipient associated with the communications connection. *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 should be connected or blocked)):  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/).



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

As one example, based at least in part on the security determination associated with the inter-network and intra-network call, the Accused Instrumentalities convey and/or are configured to 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):

	 +1 374-425-8923 Valid number Incoming call Recent history 10:51 AM Swipe an icon in any direction Answer Decline with message Decline

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.

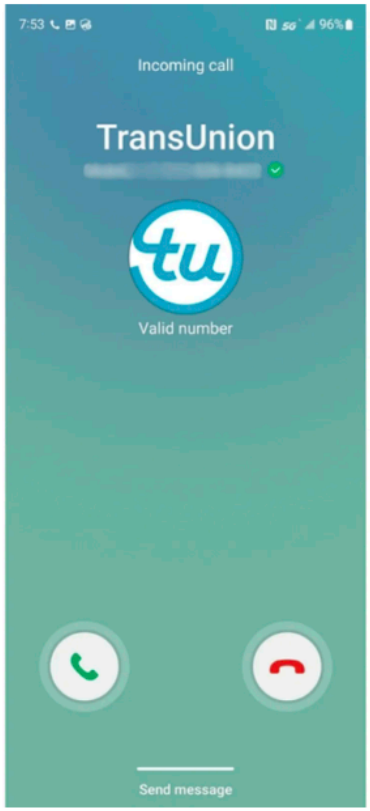
This strategy will give a multiplier effect to call protection: A "valid number" on an AT&T device means the incoming call has been authenticated by SHAKEN/STIR *and* passed through AT&T Call Protect screening.

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 also 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.

See also RQ-ATT0000161-RQ-ATT0000163 (https://www.att.com/device-support/article/wireless/KM1403775/Apple/iPhone13/).

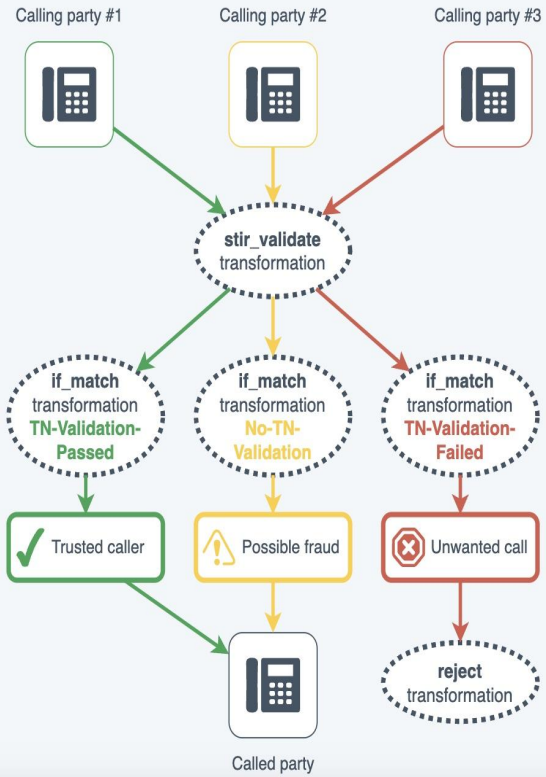
As another example, based at least in part on the security determination, the Accused Instrumentalities convey and/or are configured to convey a failure to confirm to the callee associated with the call, including but not limited by conveying "Unknown caller," any indication of a potential spoofed, spam, or fraudulent call, such as "suspected spam" or "suspected fraud," any indication a call was blocked, and/or by not conveying with an allowed communication an assurance such as a

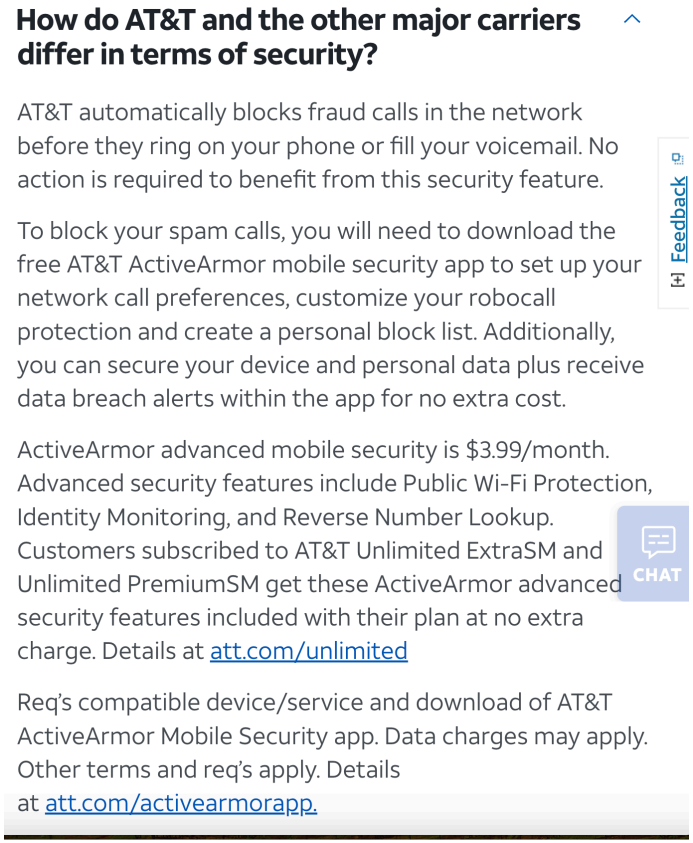
	green check, “valid number,” or “[V]”, a brand logo, contact/caller name, or providing a call log, report, or other indication reflecting confirmation. *See, e.g.*, RQ-ATT0000095-RQ-ATT0000098 (https://forums.att.com/conversations/account-features/blocking-unknown-numbers/63b33783c1c54d548b8bbe5b). Hey, 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 you 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.*, *AT&T Text-Blocking Sets a Record*, 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. *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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	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. *See, e.g.*, RQ0001940-RQ0001955 (https://www.carrierx.com/documentation/how-it-works/stir-shaken#verification-examples):

	Verification Examples The `stir_validate` transformation is normally not used all by itself. You can use it to verify the call signature and then use the output data with other transformations to manage the further call behavior. An example of such a behavior can look like this:  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 of claim 1, wherein the communications	Within the Accused Instrumentalities, the communications connection is associated with at least

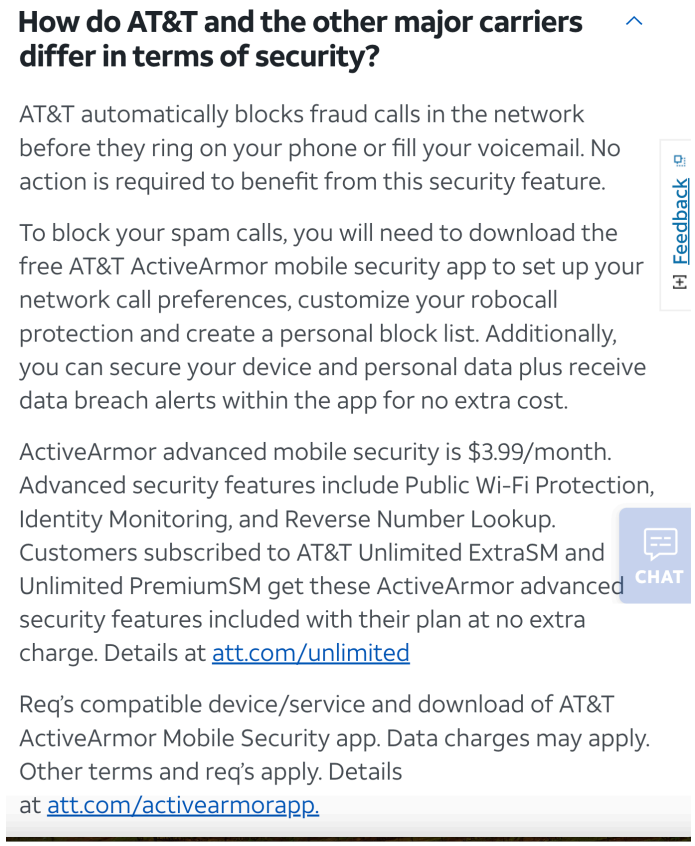
connection is associated with at least one of email, SMS, instant message, and a phone call.	one of email, SMS, instant message, and a phone call. For example, within the Accused Instrumentalities the communication connection is associated with a phone call. AT&T advertises: "AT&T automatically blocks 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/).  *See also* RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security).

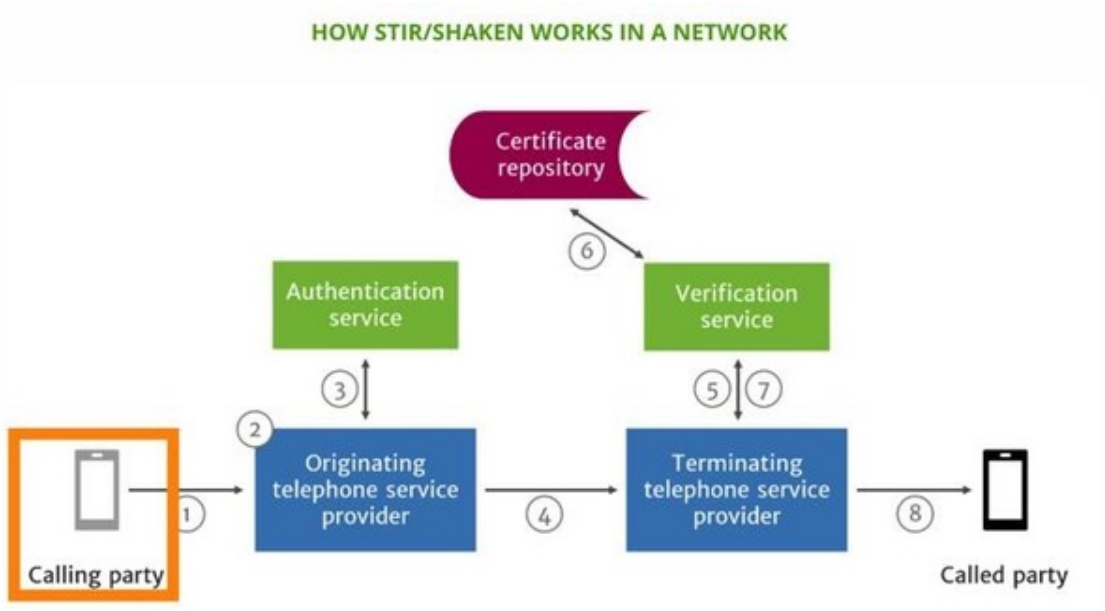
For another example, within the Accused Instrumentalities the communication connection is associated with SMS and/or instant message. *See, e.g.*, RQ-ATT0000046-RQ-ATT0000048 (https://about.att.com/blogs/2023/activearmor-text-blocking.html):

> *AT&T ActiveArmor Offers New Text-Filtering Features for Even More Protection*
>
> We know that spam texts and robocalls are a pain. That's why we're pleased to give important updates on our spam-fighting AT&T ActiveArmor℠.
>
> Our new and better network filters **blocked more than 1 billion spam text messages** from reaching customers in July – our highest-ever total. Every month since then, customers have collectively reported one-third fewer spam texts getting through to their phones.
>
> We block spam texts for everyone on our network – you don't have to do a thing. But if you download the free AT&T ActiveArmor mobile security app, you can now get even more control of incoming text messages:
>
> - **You can block email-to-text messages** – a consistent source of spam. These are texts that appear to come from an email address.[1] Just review the terms and toggle a switch on the ActiveArmor app.

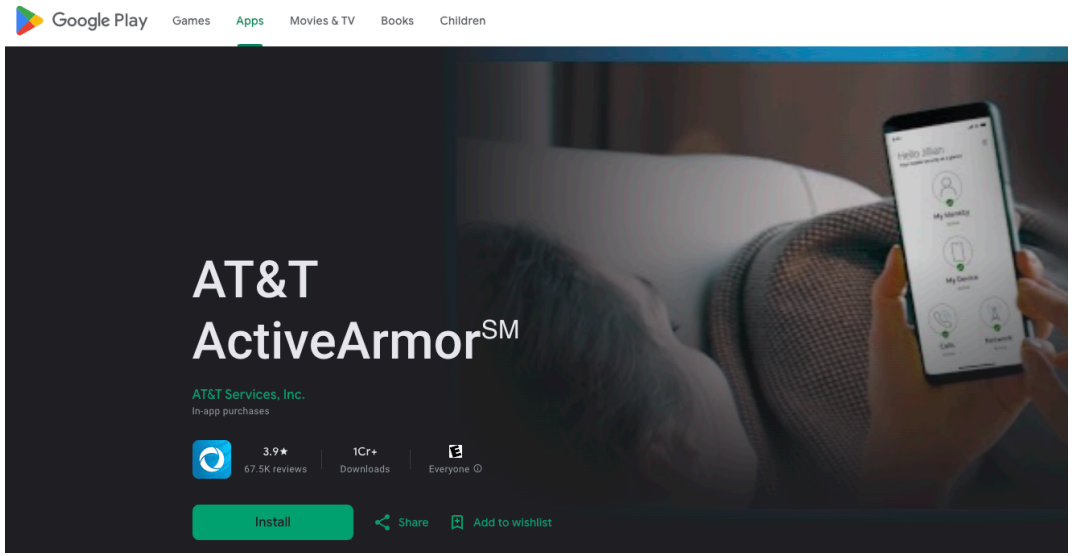
As one example, within the Accused Instrumentalities, the verification service provider verifies the corresponding communication identifiers for the email, SMS, instant message, or phone call respectively. As another example, the initial communication path used by the device to contact a verification service includes channels such email and SMS, instead of a phone call. *SMS*, Wikipedia, RQ0002081-RQ0002100 (https://en.wikipedia.org/wiki/SMS). In such a scenario, the verification service does not verify the Automatic Number Identification (ANI) of the device, and instead verifies the corresponding communication identifiers associated with the initial communication path. Automatic number identification, *Wikipedia*, RQ0001664-RQ0001665 (https://en.wikipedia.org/wiki/Automatic_number_identification).

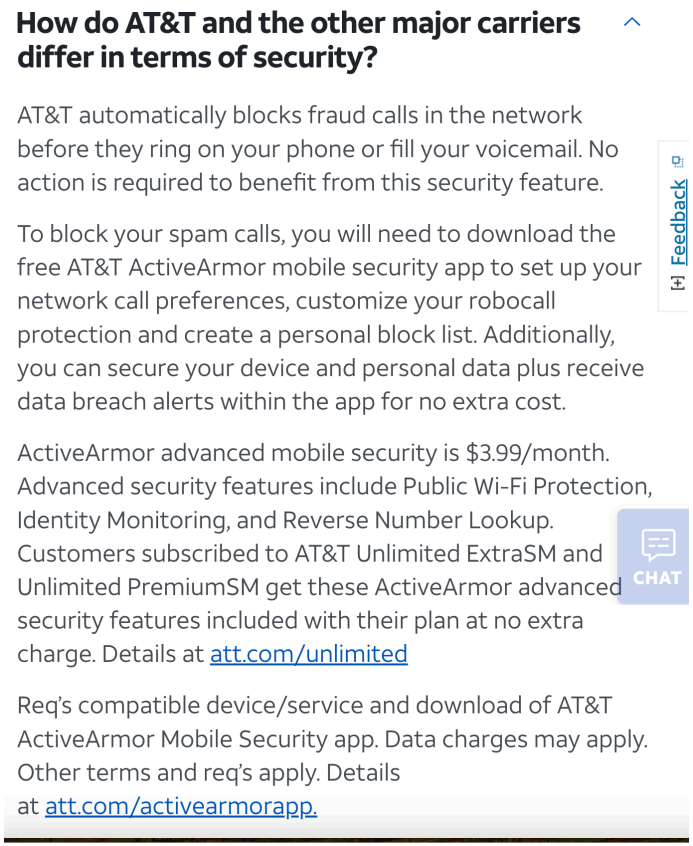
An analysis of proprietary backend systems and/or source code may be necessary to fully and

	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 of claim 1, wherein the first device comprises at least one of a smartphone, a tablet, a PC, a phablet, and a wearable device.	Within the Accused Instrumentalities the first device comprises at least one of a smartphone, a tablet, a PC, a phablet, and a wearable 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/). 

	See also RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the first device ("calling party", indicated with orange box below) comprises at least one of a smartphone, a tablet, a PC, a phablet, and a wearable device. *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/); RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).  For example, within the Accused Instrumentalities, the first device comprises but is not limited to the following smartphones, smartwatches, and/or tablets. *See, e.g.*, RQ-ATT0000105-RQ-ATT0000117 (https://www.att.com/scmsassets/support/wireless/devices-working-on-att-network.pdf); *see also* RQ-ATT0000118-RQ-ATT0000119 (https://www.att.com/support/how-to/wireless/esim-get-started/). As another example, within the Accused Instrumentalities, the first device comprises but is not limited to a PC. For example, AT&T advertises providing instant messaging, Voice over IP (VOIP) calling, as well as other features, on a desktop computer. *See, e.g.*, *AT&T Collaborate app for Desktop*, RQ-ATT0000180-RQ-ATT0000206

	(https://asecare.att.com/tutorials/att-collaborate-app-desktop). As another example, AT&T discloses that the Accused Instrumentalities, including but not limited to AT&T ActiveArmor, are compatible with at least smartphones, wearable devices (including but not limited to Apple smartwatches), and iPod Touch. *See* RQ-ATT0000049-RQ-ATT0000050 (https://apps.apple.com/us/app/at-t-activearmor/id1218465964): **Information** Seller AT&T Services, Inc. Size 138.1 MB Category Utilities Compatibility **iPhone** Requires iOS 13.0 or later. **iPod touch** Requires iOS 13.0 or later. Languages English Age Rating 4+ Copyright ©2024 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property. All other marks are the property of their respective owners. Price Free In-App Purchases 1. Plus *See* RQ-ATT0000007-RQ-ATT0000011 (https://www.att.com/device-support/article/wireless/000092356/Apple/WatchSeries8/): WIRELESS SUPPORT / DEVICE SUPPORT / AT&T ActiveArmor Mobile Security Apple Watch Series 8 Change device Share **AT&T ActiveArmor Mobile Security** Use AT&T ActiveArmor to automatically block fraudulent calls, warn about phone spam, and temporarily block unwanted calls. *See* RQ-ATT0000001-RQ-ATT0000006 (https://www.att.com/device-support/article/wireless/000092356/Apple/WatchSE44mm/):

	 *See* RQ-ATT0000042-RQ-ATT0000045 AT&T ActiveArmor on Google Play Store  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 of claim 1, wherein enrolling the first device is based at least in part on at least one of PIN verification, password	Within the Accused Instrumentalities enrolling the first device is based at least in part on at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address,

verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number.	and a 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/).  *See also* RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). For example, the Accused Instrumentalities use PIN verification, including in activating and/or

assessing the Accused Instrumentalities . *See, e.g.*, RQ-ATT0000099-RQ-ATT0000104:

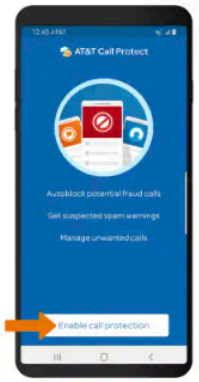
Access call protect

1. Navigate to and select the **AT&T Call Protect app**.

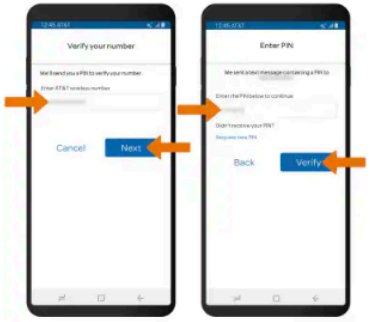
Note: AT&T Call Protect allows you to automatically block fraudulent calls, warns you about phone spam, and temporarily blocks unwanted calls.

2. Select **Enable call protection**.

*Note: Review the permissions, then select **ALLOW**.*



3. Enter your **myAT&T wireless number**, then select **Next**. Enter the **PIN** sent via text, then select **Verify**.



4. Review the Terms & Conditions, then select **I agree**. Select **Continue**.

*Note: Select **ALLOW** to give permission to the app to access your contacts.*

	For further example, the Accused Instrumentalities collect and use password verification, knowledge-based authentication, geolocation information, credit card information validation, and/or a check of a least one of a name, an address, and a phone number, including for enrolling a first device. *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.

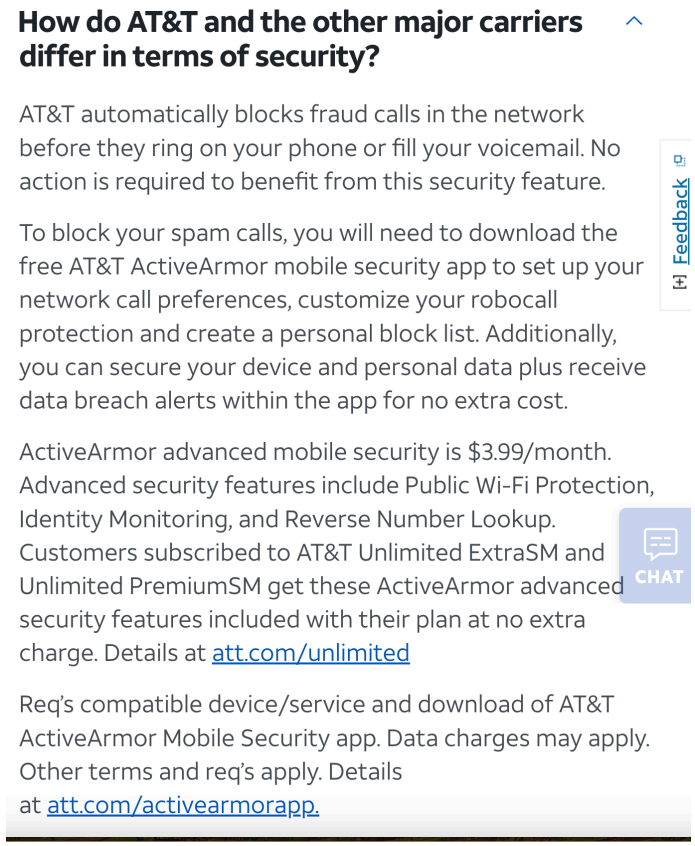
How we use your information ×

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).

See also RQ-ATT0000139-RQ-ATT0000150 (https://www.att.com/legal/terms.activeArmorMobileSecurity.html):

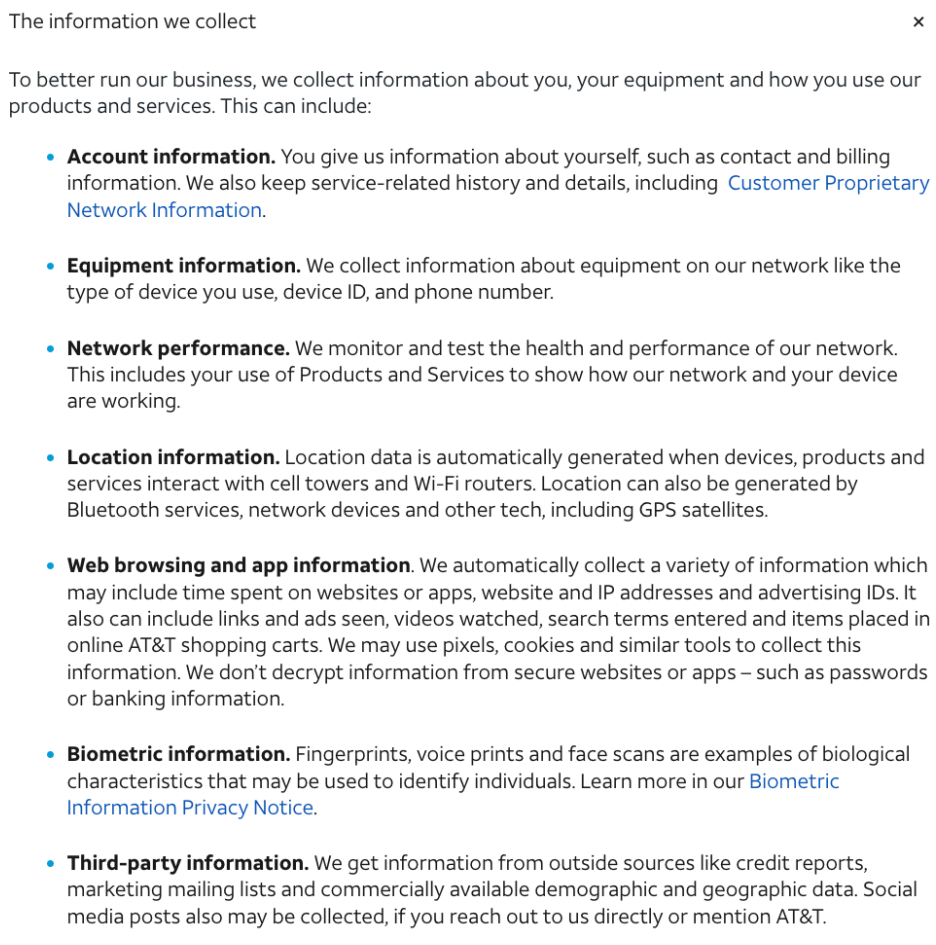
	In order to perform the functions of the Service including but not limited to its Call Features, AT&T may use and/or disclose or allow the disclosure to our third-party vendor(s) of Your personal information, including without limitation mobile number, contacts/address book in order to populate detail 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). As one example, enrolling of a first device is based in part or in whole on PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and/or a check of at least one of a name, an address, and a phone number. As yet another example, enrolling of a first device is based upon information that is included 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 7. The system of claim 1,	Within the Accused Instrumentalities the additional authentication comprises at least one of PIN

wherein the additional authentication comprises at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number.	verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a 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/). 

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

As one example, requested additional authentication comprises PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and/or a check of at least one of a name, an address, and a phone number.

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 ×

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).

See also 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).

As another example, additional authentication comprises of information that is included in the SIP INVITE. *See, e.g.,* RQ0002066-RQ0002080 (https://www.twilio.com/docs/glossary/sip-invites); RQ-ATT0000213-RQ-ATT0000285(https://www.tutorialspoint.com/session_initiation_protocol/); RQ0001666-RQ0001671(https://telnyx.com/resources/the-beginners-guide-to-sip-headers).

As another example, the Accused Instrumentalities are configured to implement PIN verification, including for example in enrolling a first device and/or for additionally authenticating, including but not limited to password, fingerprint, and/or Face ID. *See, e.g.,* RQ-ATT0000099-RQ-ATT0000104 (https://www.att.com/device-support/article/wireless/KM1324197/Samsung/SamsungSMG975U/):

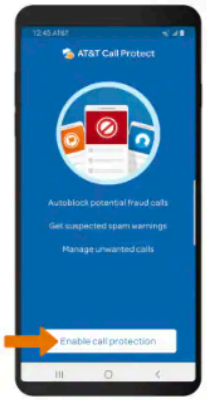
Access call protect

1. Navigate to and select the **AT&T Call Protect app**.

Note: AT&T Call Protect allows you to automatically block fraudulent calls, warns you about phone spam, and temporarily blocks unwanted calls.

2. Select **Enable call protection**.

*Note: Review the permissions, then select **ALLOW**.*



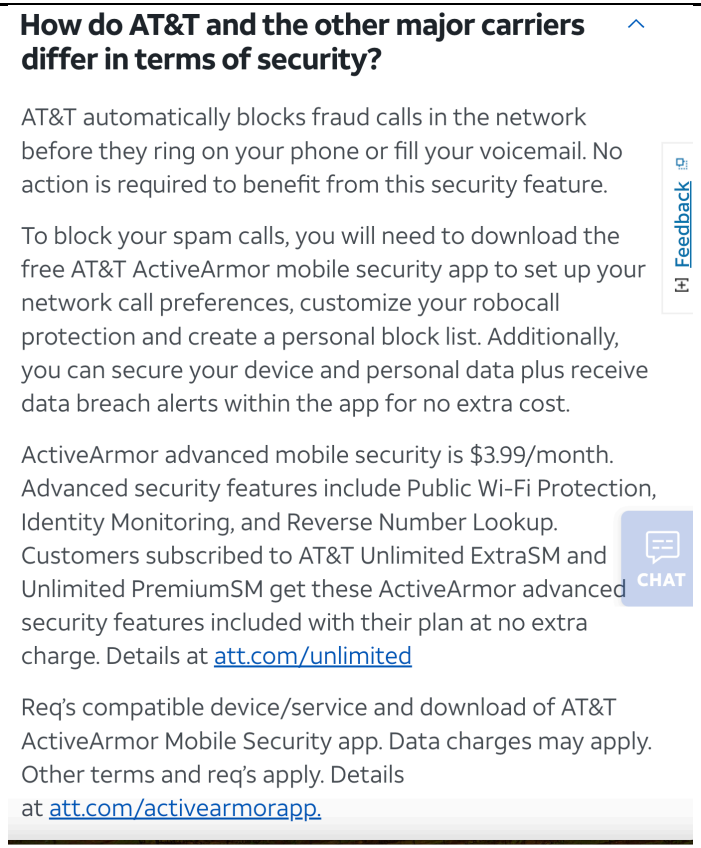
3. Enter your **myAT&T wireless number**, then select **Next**. Enter the **PIN** sent via text, then select **Verify**.



4. Review the Terms & Conditions, then select **I agree**. Select **Continue**.

*Note: Select **ALLOW** to give permission to the app to access your contacts.*

	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 of claim 1, wherein the set of configuration information comprises at least one of a set of device settings, a set of installed applications, system version information, application software version information, and a contact list associated with the first device.	Within the Accused Instrumentalities the set of configuration information comprises at least one of a set of device settings, a set of installed applications, system version information, application software version information, and a contact list associated with the first 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/).



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

For example, the Accused Instrumentalities collect and use the following information which comprises a set of device settings, a set of installed applications, system version information, application software version information, and/or a contact list associated with the first device. *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 ×

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).

See also 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")

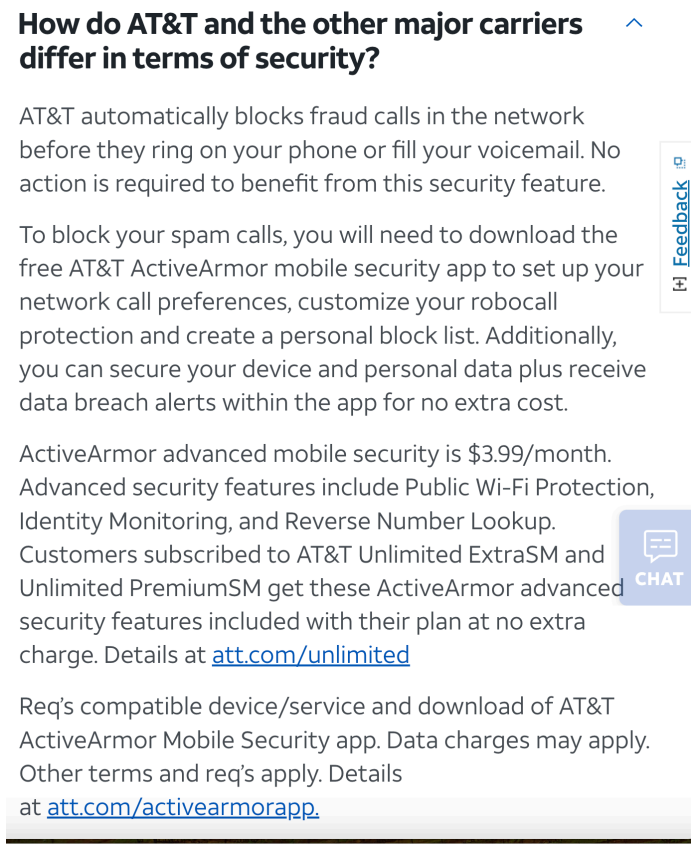
In order to perform the functions and to improve the effectiveness of the Service including but not limited to its Data Features for all users, AT&T, its pertinent suppliers and their subsidiaries, agents and subcontractors may collect, maintain, process, use, and disclose diagnostic, technical, usage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

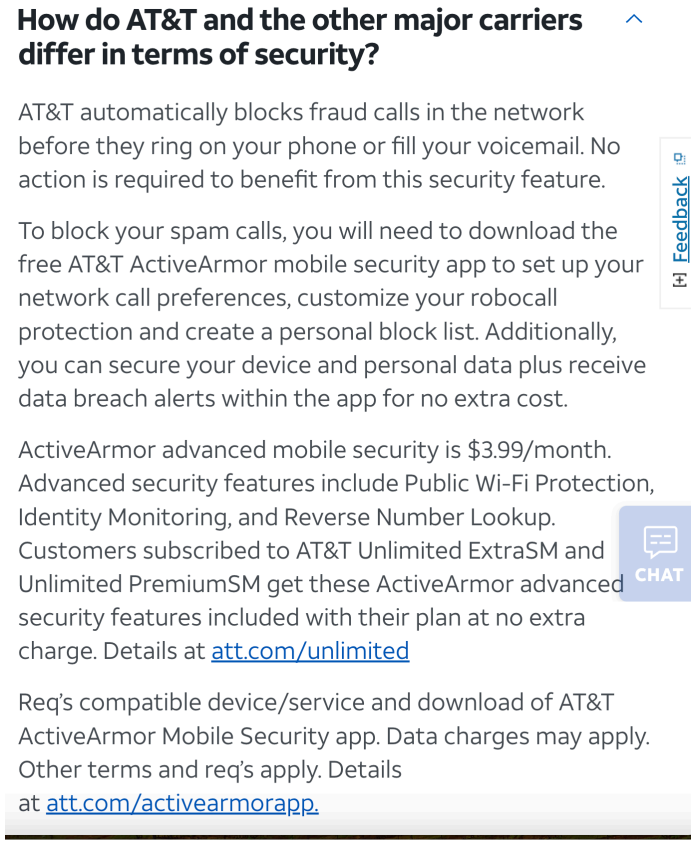
This set of configuration information is associated with the device. For instance, the device settings are associated with the device. Also, the set of installed applications are associated with the device. Also, the system version information will be associated with the device. As another example, the Accused Instrumentalities use installed applications, such as ActiveArmor. As another example, the Accused Instrumentalities use application software version information, such as ActiveArmor version information. As yet another example, the list of contacts on the device may be included in the configuration information associated with the 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 9. The system of claim 1, wherein the verification service provider is further configured to re-enroll the first device in response to a determination of a change in the device fingerprint.	Within the Accused Instrumentalities the verification service provider is further configured to re-enroll the first device in response to a determination of a change in the device fingerprint. 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/). 

	See also RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security). As one example, the verification service provider is further configured to re-enroll the first device in response to a determination of a change in the device fingerprint, including a change in the information used at least in part to generate the device fingerprint. Before Defendants determine how to attest for the validity of the calling number, Defendants' Accused Instrumentalities are configured to determine if the call should be connected. The Accused Instrumentalities, alone or in combination, enroll and/or re-enroll a first device. Re-enrollment of the first device includes generation of a device fingerprint based at least in part on a set of configuration information at least a portion of which is used at least in part to perform a security determination (e.g., SIM-based, credential-based, or line-based authentication). As one example, a device fingerprint is generated based at least in part on a mobile identification number ("MIN") or any derivation of a MIN or any related number. *See, e.g.*, RQ0001968 (https://en.wikipedia.org/wiki/Mobile_identification_number). As another example, a device fingerprint is generated based at least in part on a mobile subscription identification number ("MSIN"). As another example, a device fingerprint comprises the international mobile subscriber identity ("IMSI") or encrypted version thereof ("TMSI"). *See, e.g.*, RQ0001957-RQ0001964 (https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity); RQ0002121-RQ0002123 (https://cellularnews.com/definitions/what-is-a-mobile-identification-number-min/). As one example, a device fingerprint is generated based at least in part on Subscriber Module (SIM) Card serial number. RQ0002042-RQ0002060 (https://en.wikipedia.org/wiki/SIM_card). As one example, a device fingerprint is generated based at least in part on a serial number, Host Device ID, or any another unique identifier for a device (including but not limited to Android ID, UDID, IDFA, AAID). RQ0001932-RQ0001939 (https://support.apple.com/en-us/108037); RQ0001965-RQ0001967 (https://saturncloud.io/blog/is-there-a-unique-android-device-id/). As one example, a device fingerprint is generated based at least in part on any derivation and/or combination of the above example or any other configuration 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 10 [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.. *See, e.g.*, 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 ActiveArmor℠ 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/).



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

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

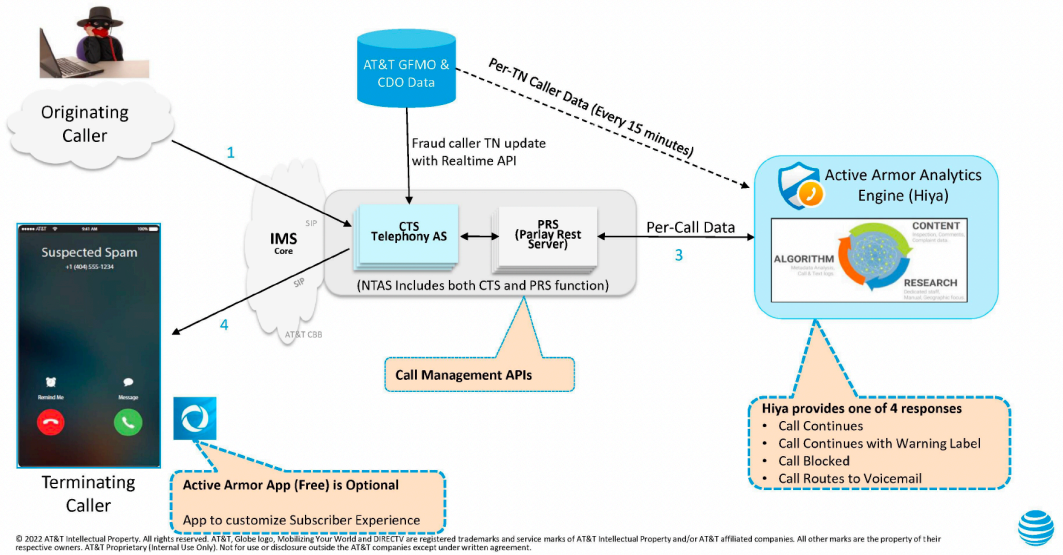
Here's what you get with Digital Phone Call Protect[1]:

- **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).

As another example, the Accused Instrumentalities are used and/or otherwise performed by AT&T 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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	Furthermore, caller identification authentication and verification technology, including without limitation &T's Robocall Mitigation system(s), Call Protect system(s) and service(s), ActiveArmor, the ActiveArmor mobile application, and STIR/SHAKEN, is technology configured and/or used to, among other functions, detect spoofed, spam and/or fraudulent phone calls. *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 should be connected or blocked)): AT&T Active Armor (Call Protect) – High Level Architecture  *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.
10[a] enrolling a first device with a verification service provider, wherein enrolling the first device includes associating, by the	The Accused Instrumentalities enroll a first device with the verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device;	The verification service provider may be located within Defendants' network directly, operated by a third party (e.g., Hiya), or some combination thereof. *See* 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. *See, e.g.*, RQ-ATT0000024-RQ-ATT0000026 (https://about.att.com/story/2019/call_validation_displays.html):

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC


+1 374-425-8923
Valid number
Incoming call
Recent history
10:51 AM
Swipe an icon in any direction
Answer
Decline with message
Decline

	See also 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): **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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

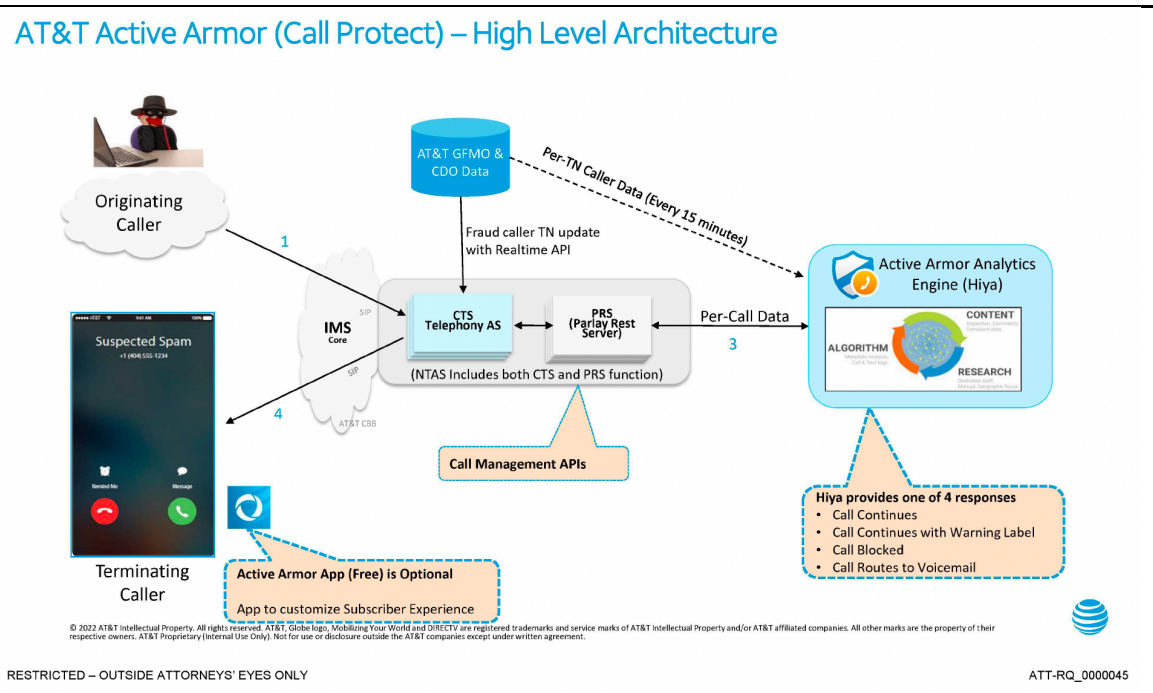
CTN (including AT&T/FN/Cricket customers)
Service tier (like Basic vs. Advanced)
Service Tags:

- 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

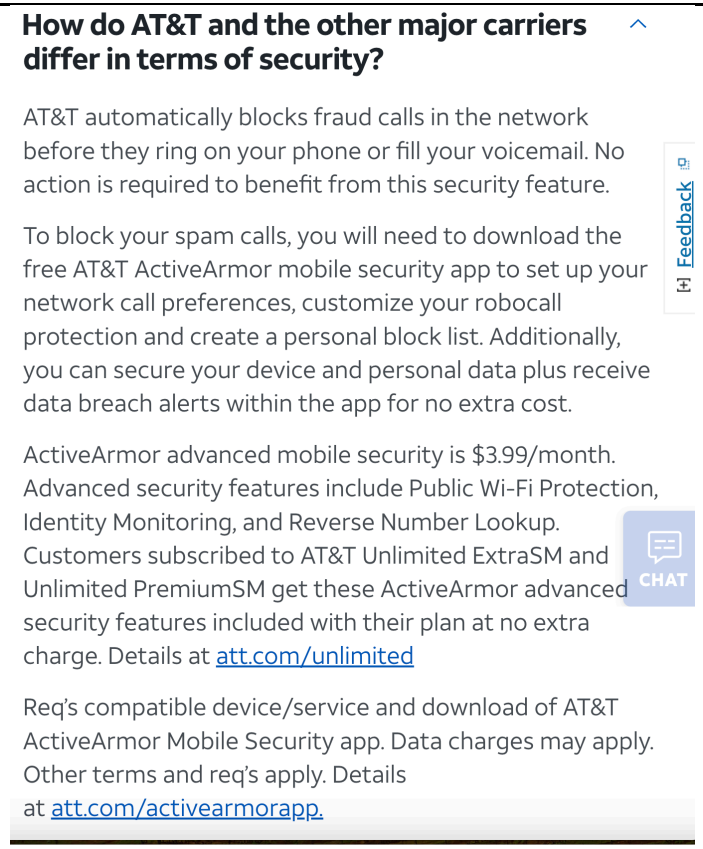
See, e.g., ATT-RQ_0000045 (AT&T GFMO and CDO Data):



The verification service provider is comprised of one or more components, implemented in hardware, software, or a combination thereof, used by, implemented in, and/or included in the Accused Instrumentalities that function in the manner described herein. *See, e.g.*, RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security):

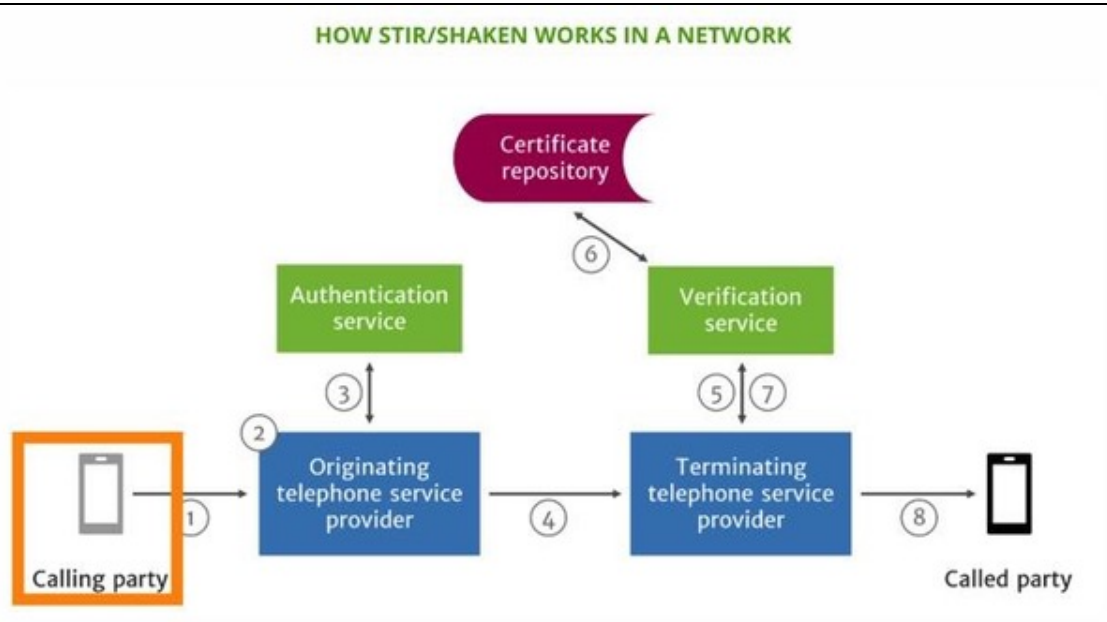
- **Robocall Scam Identification & Mitigation:** AT&T has established mechanisms to identify illegal robocall campaigns and help to mitigate them.
  - Through the complementary programs listed below, AT&T has blocked or labeled billions of unwanted robocalls.
    - AT&T ActiveArmor℠ automatically blocks 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.

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



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 Protect[1]: • **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* RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/); RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/). The enrolling of the first device includes associating, by the verification service provider, the first device with a device fingerprint. *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/); RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/). The device fingerprint is generated based at least in part on a set of configuration information associated with the first device. As one example, the verification service provider enrolls a first device ("calling party", indicated with orange box). *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/); RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).



Before Defendants determine how to attest for the validity of the calling number, Defendants' Accused Instrumentalities determine if the call should be connected. The Accused Instrumentalities, alone or in combination, enroll a first device (showing as "calling party" and identified with an orange box). Enrollment of the first device includes generation of a device fingerprint based at least in part on a set of configuration information at least a portion of which is used at least in part to perform a security determination (e.g., SIM-based, credential-based, or line-based authentication).

A device fingerprint is generated based at least in part on a set of configuration information associated with the first device. Examples of such configuration information used to generate the device fingerprint include without limitation combinations of device specific data, device settings, installed applications, system or application software versions, contact list data, or other data specific to the calling device.

As one example, a device fingerprint comprises and/or is otherwise generated based at least in part on a mobile identification number ("MIN") or derivation. *See, e.g.*, RQ0001968 (https://en.wikipedia.org/wiki/Mobile_identification_number). As another example, a device fingerprint comprises and/or is otherwise generated based at least in part on a mobile subscription identification number ("MSIN"). As another example, a device fingerprint comprises and/or is

	otherwise generated based at least in part on the international mobile subscriber identity ("IMSI") or encrypted version thereof ("TMSI"). *See, e.g.*, RQ0001957-RQ0001964 (https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity); RQ0002121-RQ0002123 (https://cellularnews.com/definitions/what-is-a-mobile-identification-number-min/). As one example, a device fingerprint comprises and/or is otherwise generated based at least in part on a Subscriber Module (SIM) Card serial number. RQ0002042-RQ0002060 (https://en.wikipedia.org/wiki/SIM_card). As one example, a device fingerprint comprises and/or is otherwise generated based at least in part on a serial number, Host Device ID, or any other unique identifier for a device (including but not limited to Android ID, UDID, IDFA, AAID). RQ0001932-RQ0001939 (https://support.apple.com/en-us/108037); RQ0001965-RQ0001967 (https://saturncloud.io/blog/is-there-a-unique-android-device-id/). As one example, a device fingerprint comprises and/or is otherwise generated based at least in part on any derivation and/or combination of the above examples or any other configuration information. The Accused Instrumentalities associate the first device with a device fingerprint. *See, e.g.*, RQ-ATT0000099-RQ-ATT0000104 (https://www.att.com/device-support/article/wireless/KM1324197/Samsung/SamsungSMG975U/):

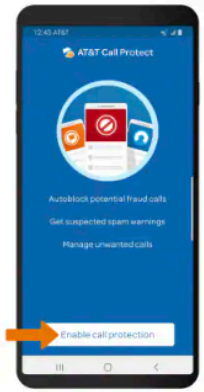
Access call protect

1. Navigate to and select the **AT&T Call Protect app**.

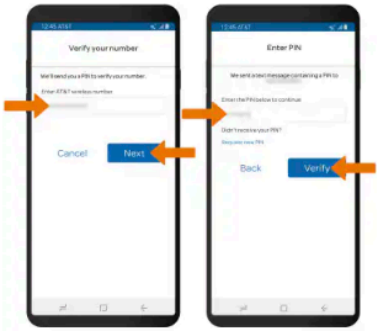
Note: AT&T Call Protect allows you to automatically block fraudulent calls, warns you about phone spam, and temporarily blocks unwanted calls.

2. Select **Enable call protection**.

*Note: Review the permissions, then select **ALLOW**.*



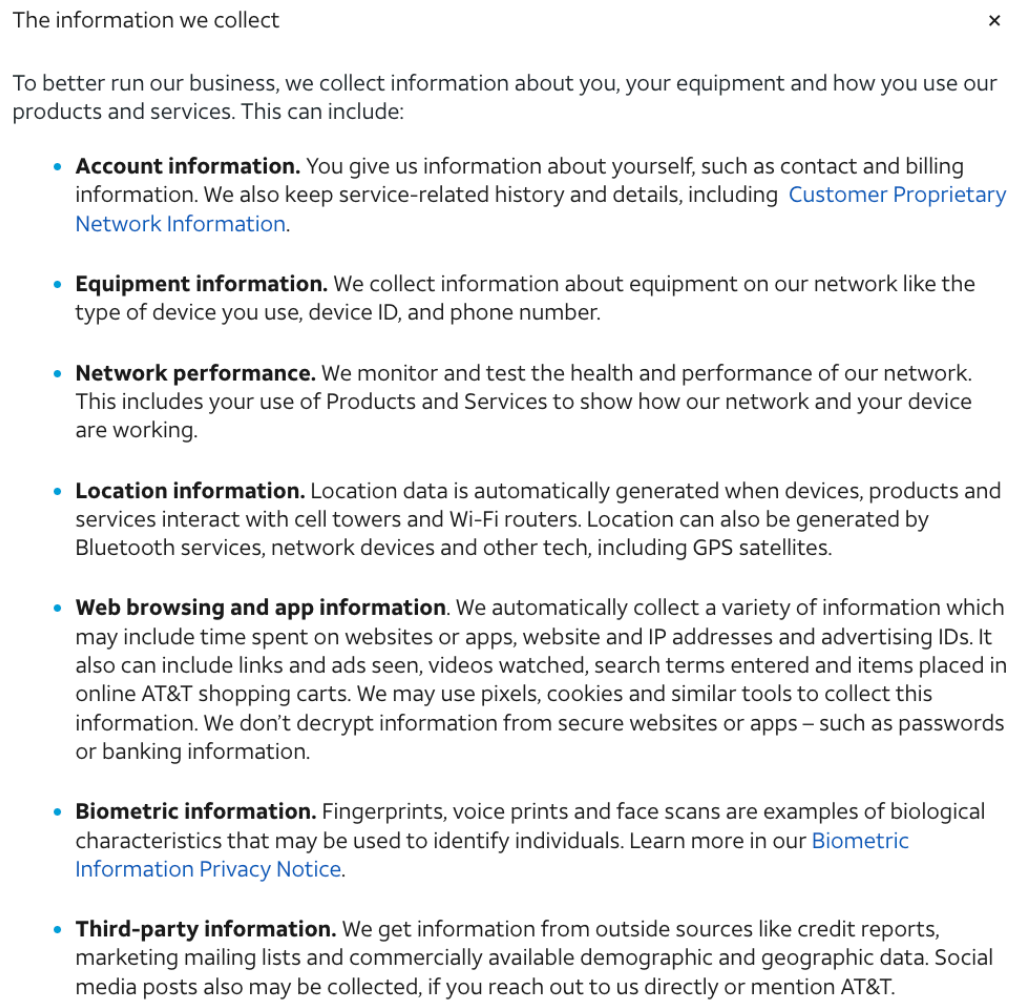
3. Enter your **myAT&T wireless number**, then select **Next**. Enter the **PIN** sent via text, then select **Verify**.



4. Review the Terms & Conditions, then select **I agree**. Select **Continue**.

*Note: Select **ALLOW** to give permission to the app to access your contacts.*

Further, for example, AT&T collects information about equipment on the AT&T Networks, and uses it in, among other ways, "verifying your identity, detecting and preventing fraud." *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 ×

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).

See also 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).

See also 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 (e.g., "Device OS", "ActiveArmor Version Information"), contact list data (TN from Device Address Book), or other data specific to the calling device):

	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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

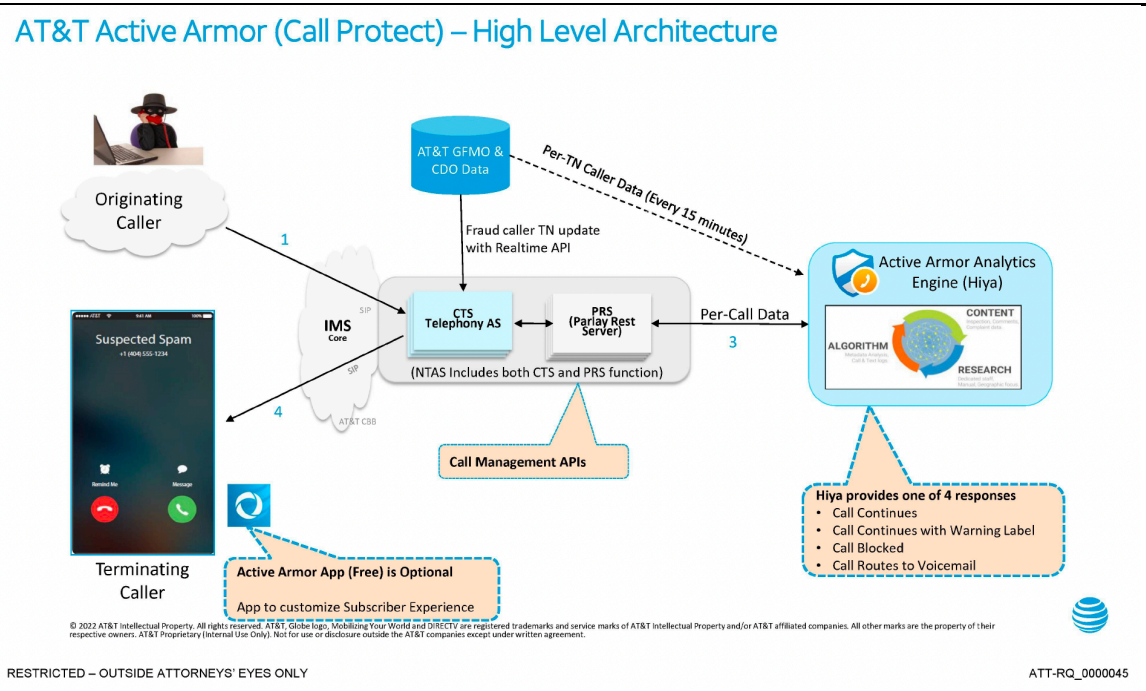
CTN (including AT&T/FN/Cricket customers)
Service tier (like Basic vs. Advanced)
Service Tags:

- 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 (AT&T GFMO and CDO Data):



See also 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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	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.
10[b] storing, at the verification service provider, the device fingerprint associated with the first device;	The Accused Instrumentalities store, at the verification service provider, the device fingerprint associated with the first device. As one example, Accused Instrumentalities store, at the verification service provider information associated with the first device including but not limited to the device fingerprint and/or the configuration information upon which the device fingerprint is based at least in part. For example, the Accused Instrumentalities use and store various information collected about equipment on the networks. *See, e.g.*, RQ-ATT0000070-RQ-ATT0000086 (https://about.att.com/privacy/privacy-notice.html).

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).

Data retention and security ×

We keep your information as long as we need it for business, tax or legal purposes. We set our retention periods based on things like what type of personal information it is, how long it's needed to operate the business or provide our products and services, and whether it's subject to contractual or legal obligations. These obligations might be ongoing litigation, mandatory data retention laws or government orders to preserve data for an investigation. After that, we destroy it by making it unreadable or indecipherable.

See also 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).

	See also ATT-RQ_0000042, -43, -44 (evidencing fingerprint information such as device specific data, device settings, installed applications (e.g., Active Armor), 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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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:

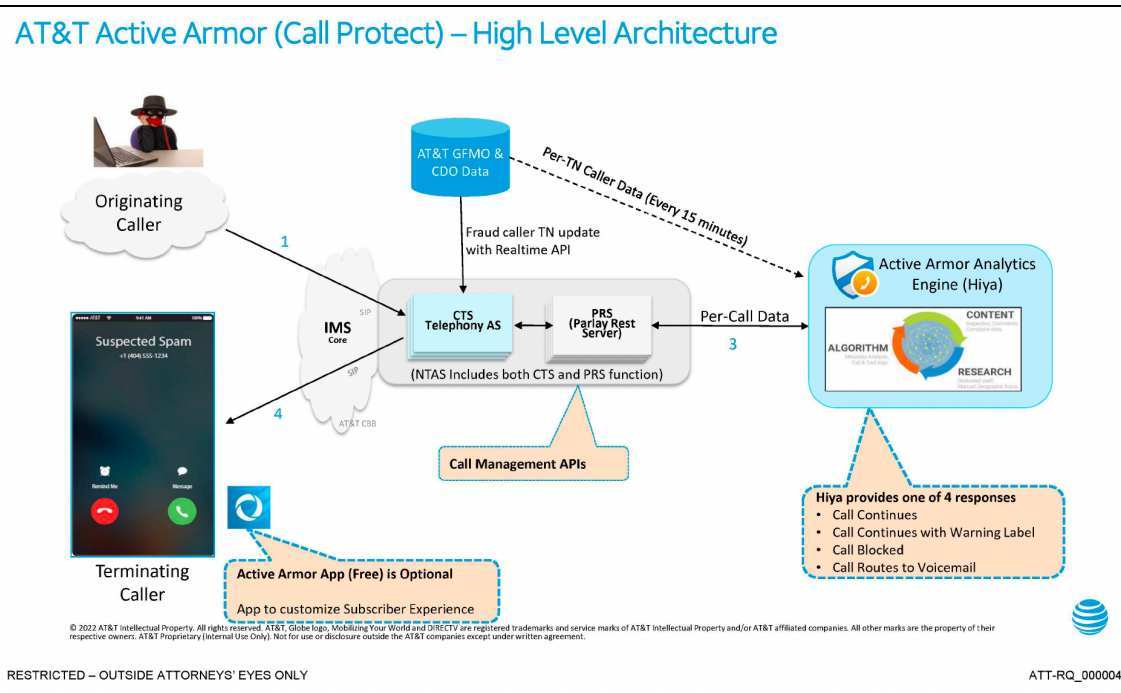
- FirstNet
- CRU
- COU
- Customers who have rate-plan-included Advanced service.
- Cricket
- Prepaid
- Wireless Home Phone

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 (storage locations, e.g., AT&T GFMO and CDO Data):

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC



As another example, the Accused Instrumentalities store a device fingerprint for it later to be used to check the call source against the calling number. *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/); RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/).

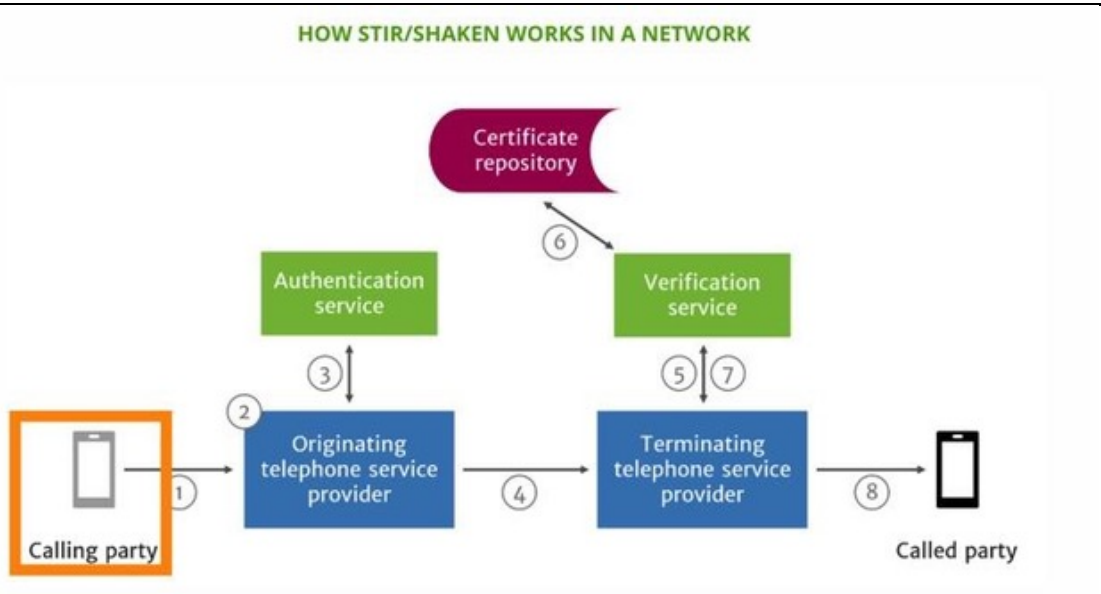
As another example, the Accused Instrumentalities store a device fingerprint to attest for the validity of the calling number, whether it is:

(A) a subscriber registered with the originating telephone service provider's softswitch ("Full Attestation");

(B) a number behind an enterprise PBX ("Partial Attestation"); or,

(C) an identifier of from where the call was received, such as a call from an international gateway ("Gateway Attestation").

	2. The originating telephone service provider checks the call source and calling number to determine how to attest for the validity of the calling number. • **Full Attestation (A)** — The service provider has authenticated the calling party and they are authorized to use the calling number. An example of this case is a subscriber registered with the originating telephone service provider's softswitch. • **Partial Attestation (B)** — The service provider has authenticated the call origination, but cannot verify the call source is authorized to use the calling number. An example of this use case is a telephone number behind an enterprise PBX. • **Gateway Attestation (C)** — The service provider has authenticated from where it received the call, but cannot authenticate the call source. An example of this case would be a call received from an international gateway. 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.
10[c] obtaining, at the verification service provider, information transmitted by a second device associated with a communications connection;	The Accused Instrumentalities obtain, at the verification service provider, information transmitted by a second device associated with a communications connection. As one example, a second device associated with a communications connection is a calling device, for example the "calling party" indicated with the orange box below. *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/); RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/).



As one example, information is transmitted by a calling party or second device, including for example a device fingerprint of and/or other information transmitted by the second device, that is obtained at the verification service provider.

An example of the obtained information transmitted by the second device associated with a communications connection includes SIP information and/or the information contained with the SIP invitation transmitted by the calling party. *See, e.g.,* RQ0002066-RQ0002080 (https://www.twilio.com/docs/glossary/sip-invites); RQ-ATT0000213-RQ-ATT0000285 (https://www.tutorialspoint.com/session_initiation_protocol/); RQ0001666-RQ0001671(https://telnyx.com/resources/the-beginners-guide-to-sip-headers).

Another example of the obtained information transmitted by the second device associated with a communications connection includes but is not limited to a mobile identification number ("MIN") or any derivation of a MIN or any related number, a mobile subscription identification number ("MSIN"), the international mobile subscriber identity ("IMSI") or encrypted version thereof ("TMSI"), Subscriber Module (SIM) Card serial number, a serial number, Host Device ID, or any another unique identifier for a device (including but not limited to Android ID, UDID, IDFA, AAID), and/or any derivation and/or combination of the thereof.

	Another example of the obtained information transmitted by the second device associated with a communications connection includes the information AT&T collects about equipment on the AT&T Networks, and uses in, among other ways, "verifying your identity, detecting and preventing fraud." *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 ×

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).

See also 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).

See also ATT-RQ_0000042, -43, -44 ("As part of the Active Armor Robocall mitigation program, data elements related to calling are shared with our 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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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.
10[d] performing, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device;	The Accused Instrumentalities perform, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device. The Accused Instrumentalities, alone and/or in combination, comprise one or more system(s) and service(s) that are configured to determine if the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint to decide if, for example, the call should be connected. *See,* 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 (e.g., "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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

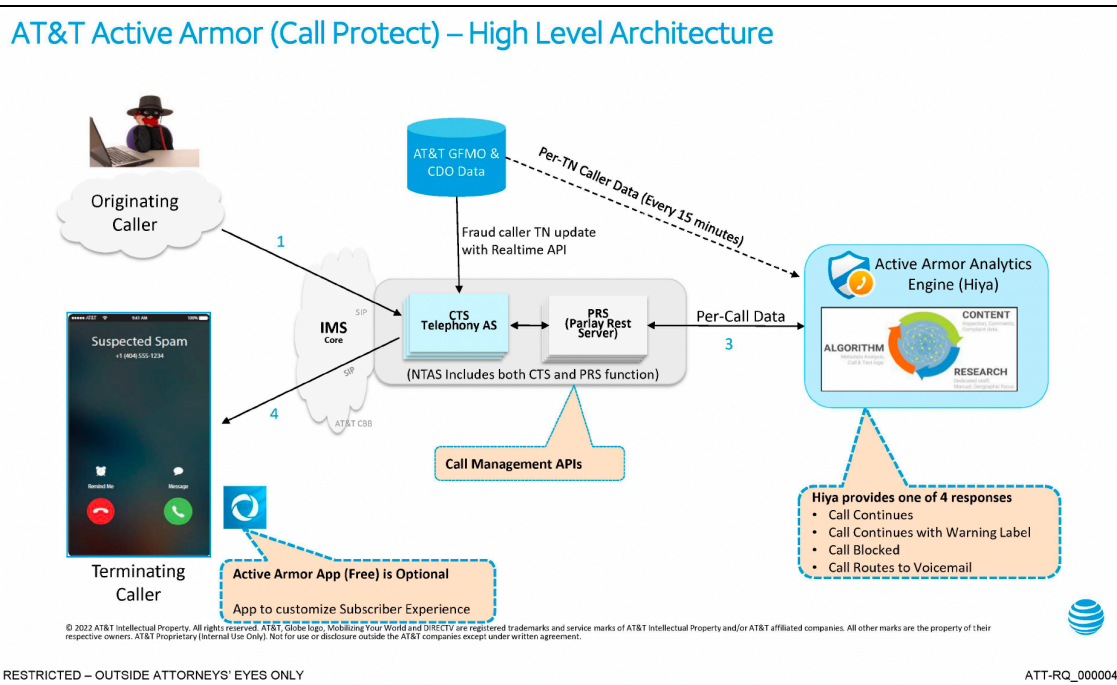
CTN (including AT&T/FN/Cricket customers)
Service tier (like Basic vs. Advanced)
Service Tags:

- 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).



Furthermore, caller identification authentication and verification technology, including without limitation STIR/SHAKEN, is technology configured and/or used to, among other functions, detect spoofed, spam and/or fraudulent phone calls.

As one example, a security determination is performed at the verification service provider to "check[] the call source and calling number to determine how to attest for the validity of the calling number." *See, e.g.,* RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/); RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

As another example, a security determination is performed at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device to determine how to attest for the validity of the calling number. *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/):

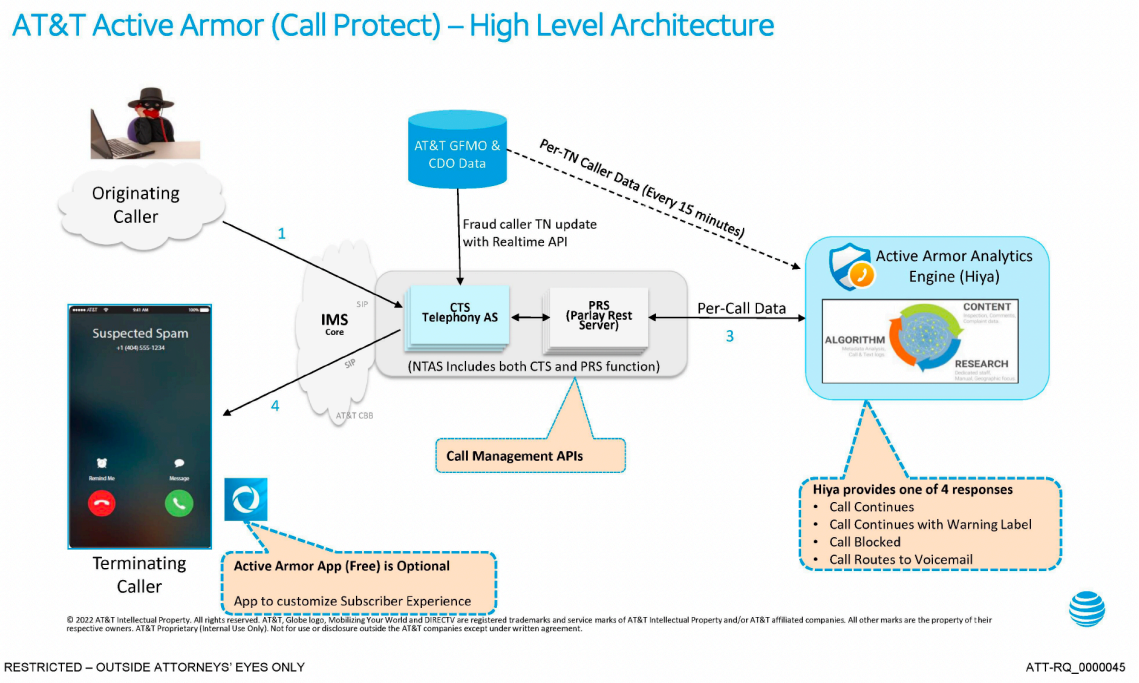
	2. The originating telephone service provider checks the call source and calling number to determine how to attest for the validity of the calling number. • **Full Attestation (A)** — The service provider has authenticated the calling party and they are authorized to use the calling number. An example of this case is a subscriber registered with the originating telephone service provider's softswitch. • **Partial Attestation (B)** — The service provider has authenticated the call origination, but cannot verify the call source is authorized to use the calling number. An example of this use case is a telephone number behind an enterprise PBX. • **Gateway Attestation (C)** — The service provider has authenticated from where it received the call, but cannot authenticate the call source. An example of this case would be a call received from an international gateway. As one example, the SIP Identity header comprises information based on and/or reflects performance of a security determination:

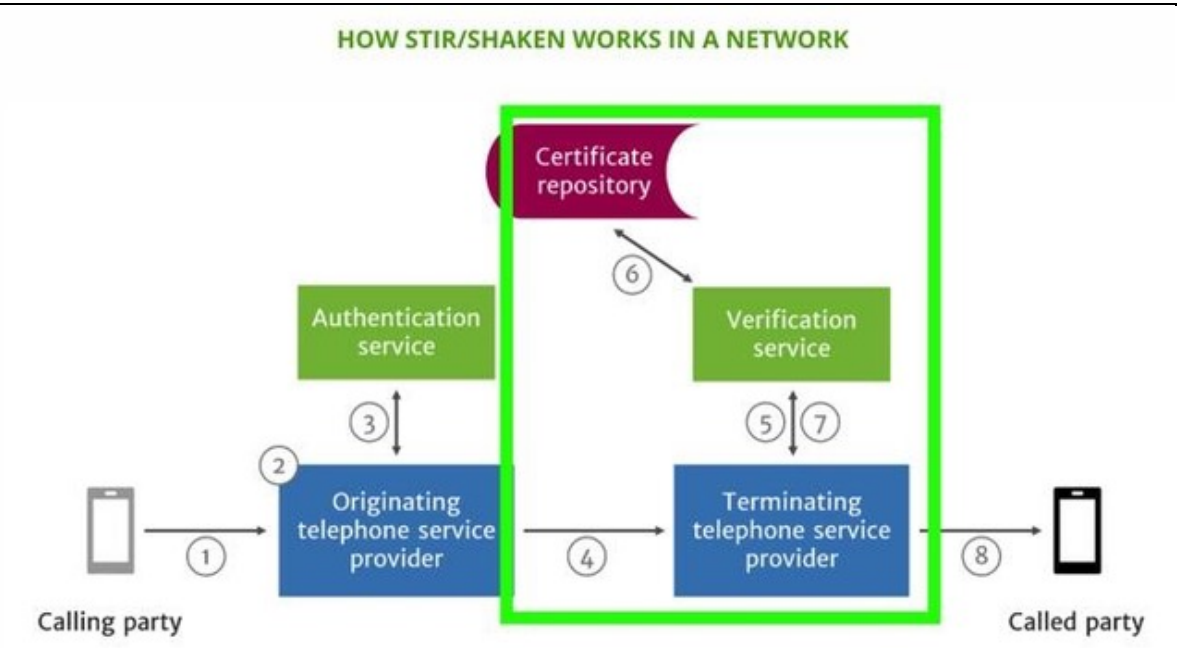
EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	3. The originating telephone service provider uses the authentication service to create a SIP Identity header. The authentication service could be a third-party service hosted in the cloud a software application integrated with the telephone service provider's softswitch or Session Border Controller (SBC). The SIP Identity header contains the following data: • Calling number • Called number(s) • Current timestamp • Attestation level • Origination identifier 4. The SIP INVITE with the SIP Identity header is sent to the terminating telephone service provider. In addition, the Identity token may be sent across the internet, out-of-band, to the terminating provider's Call Placement Service 5. The SIP INVITE with Identity header is passed to the verification service.

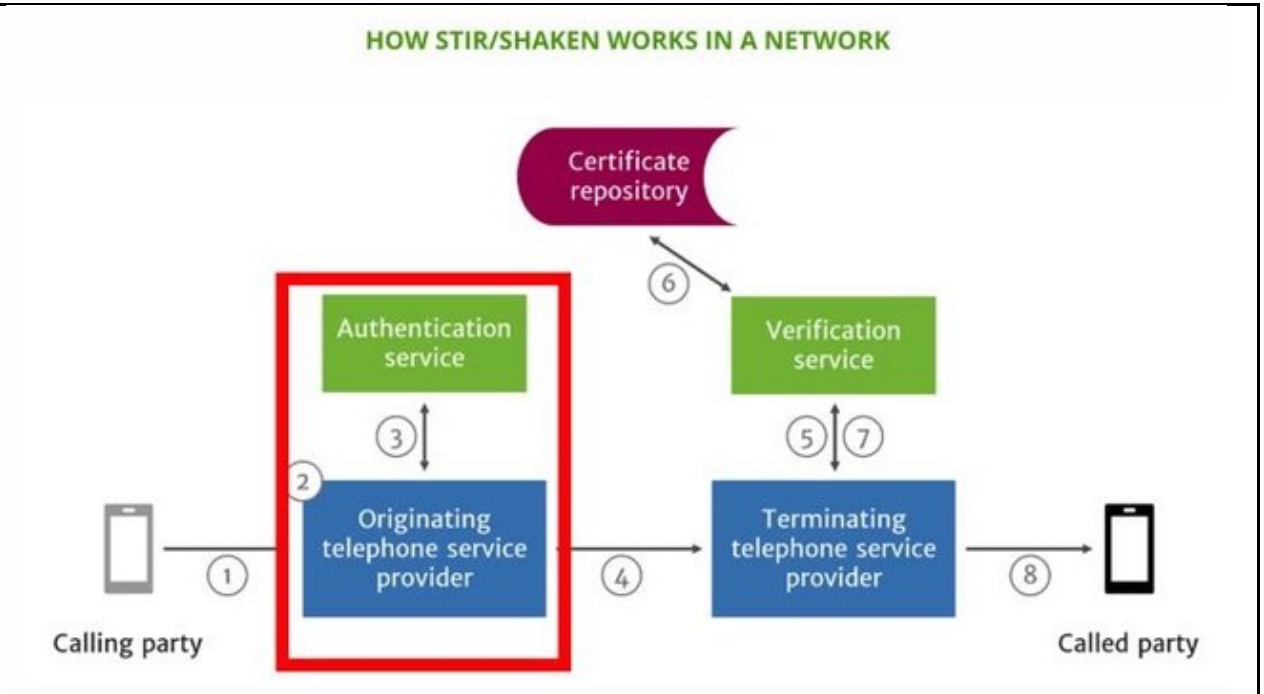
EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	6. The verification service obtains the digital certificate of the originating telephone service provider from the public certificate repository and begins a multi-step verification process. If all verification steps are successful, then the calling number has not been spoofed. • The SIP Identity header is base64 URL decoded and the details are compared to the SIP INVITE message. • The public key of the certificate is used to verify the SIP Identity header signature. • The certificate chain of trust is verified. 7. The verification service returns the results to the terminating service provider's softswitch or SBC. 8. The call is completed to the called party. 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.
10[e] and based at least in part on the security determination, selecting, at the verification service provider, an action comprising at least one of blocking the communication, requesting additional	The Accused Instrumentalities, based at least in part on the security determination, select an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication. For example, AT&T's Robocall Mitigation system(s), Call Protect system(s) and service(s), ActiveArmor, the ActiveArmor mobile application, and Defendants' use of STIR/SHAKEN, alone and/or in combination, are configured to determine if a given call should be blocked, connected, or

authentication, and permitting the communications.	if additional authentication information is required. *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 should be connected or blocked)):  As one example, the Accused Instrumentalities select an action based on the SIP Identity header. As one example, the action may be selected in the steps indicated by the green box below. *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/).



As another example, the one or more processors are capable of selecting an action based on the SIP Identity header. As one example, the action may be selected using the components, functionality, and/or processes indicated by the red box below:



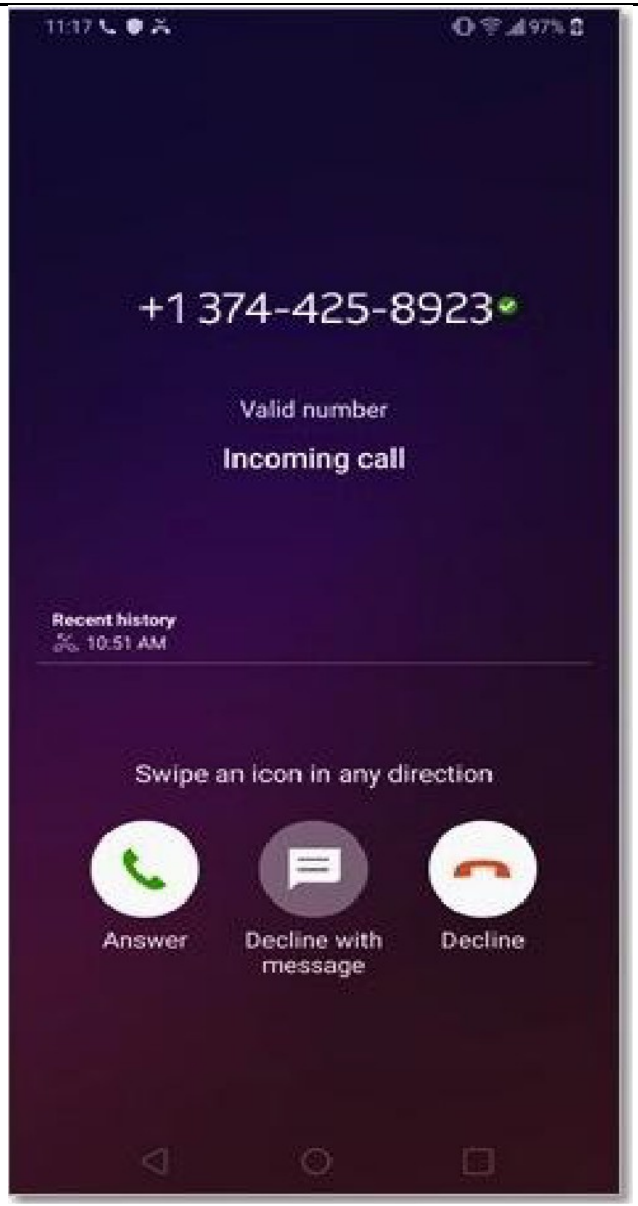
See, e.g., RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/) (modified).

The action selected comprises at least one of blocking the communication, requesting additional verification, and permitting the communication:

6. The verification service obtains the digital certificate of the originating telephone service provider from the public certificate repository and begins a multi-step verification process. If all verification steps are successful, then the calling number has not been spoofed.
   - The SIP Identity header is base64 URL decoded and the details are compared to the SIP INVITE message.
   - The public key of the certificate is used to verify the SIP Identity header signature.
   - The certificate chain of trust is verified.
7. The verification service returns the results to the terminating service provider's softswitch or SBC.
8. The call is completed to the called party.

As one example, the communication is permitted in Step 8 above. *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/).

For example, the Accused Instrumentalities permit the call or permit the call and convey an assurance to a callee associated with the call. *See, e.g.*, RQ-ATT0000024-RQ-ATT0000026 (https://about.att.com/story/2019/call_validation_displays.html):

	 +1 374-425-8923 Valid number Incoming call Recent history 10:51 AM Swipe an icon in any direction Answer Decline with message Decline

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.

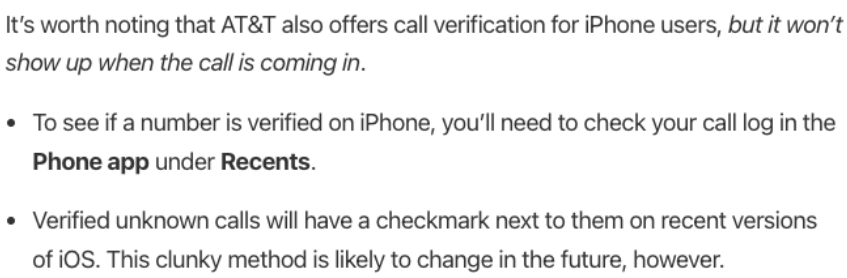
Here are some other key points:

- 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.

Furthermore, caller identification authentication and verification technology, including without limitation AT&T's Robocall Mitigation system(s), Call Protect system(s) and service(s), ActiveArmor, and the ActiveArmor mobile application are capable of detecting, blocking and preventing SPAM, fraudulent and spoofed phone calls.

See also RQ-ATT0000088-RQ-ATT0000090 (https://www.idropnews.com/news/fast-tech/att-will-

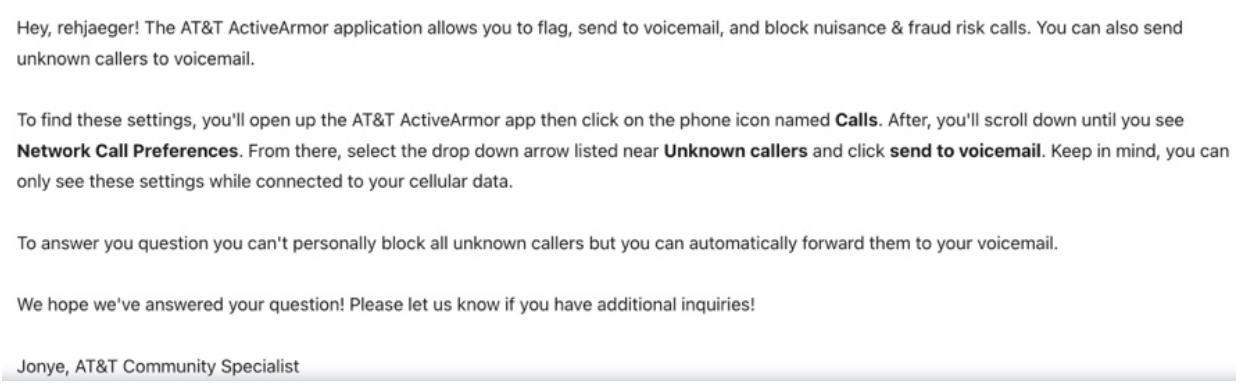
warn-you-of-incoming-robocalls-but-not-on-iphone/125657/):



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 also RQ-ATT0000161-RQ-ATT0000163 (https://www.att.com/device-support/article/wireless/KM1403775/Apple/iPhone13/). As another example, based at least in part on the security determination, the Accused Instrumentalities indicate a failure to confirm to the callee the identity of the caller and/or block the call. *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 you 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

As one example, based at least in part on the security determination associated with the inter-network and intra-network call, the Accused Instrumentalities block a call. *See, e.g.*, RQ-ATT0000153-RQ-ATT0000160 (https://www.att.com/wireless/what-is-activearmor-security/):

What are the benefits of AT&T ActiveArmor?

Customers should download the free AT&T ActiveArmor mobile security app to customize their robocall protection, manage nuisance calls, and create their own personal block list. Additionally, with AT&T ActiveArmor advanced, customers can secure their devices and personal data plus receive data breach alerts within the app.

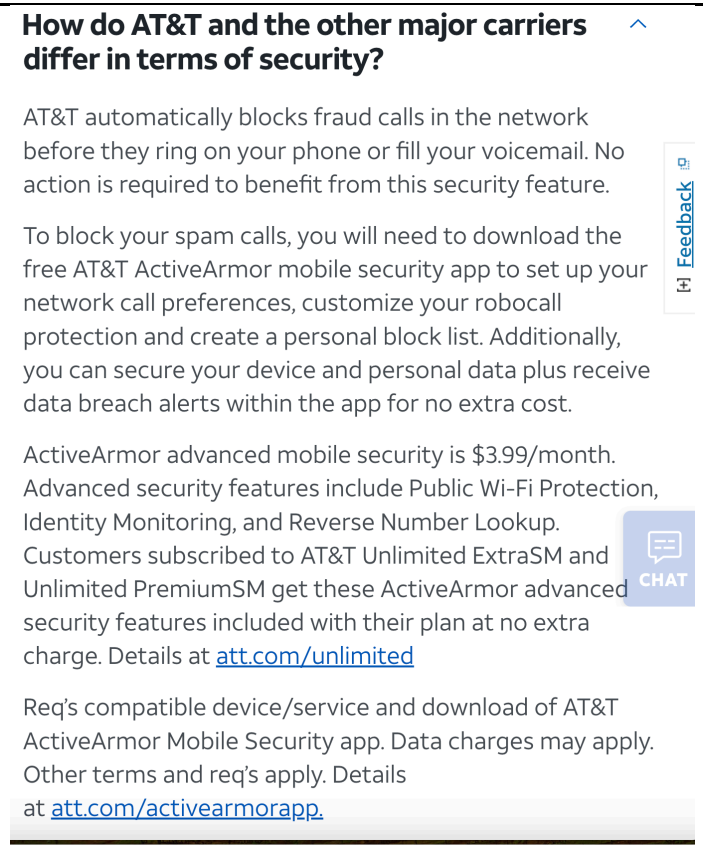
Download to activate the free app and services for an extra layer of protection that helps you easily secure your data, manage nuisance calls, and more.

- **24/7 automatic fraud call blocking:** Detects and blocks calls from likely fraudsters before they reach you.
- **Spam call blocking:** Blocks or sends calls to voicemail if identified as a Spam Risk.
- **Nuisance call alerts:** Labels potential nuisance calls from telemarketers, surveys, and more.
- **Spam call routing:** Choose call categories to accept, block, or send to voicemail.
- **Unknown calls to voicemail:** Automatically sends callers to voicemail if they're not in your address book and blocks other numbers in your personal block list.
- **Block all texts from email:** Block all email-originated texts from your phone.
- **Personal block list:** Add individual unwanted callers to your own block list.
- **Device security:** Helps protect your data from mobile threats.
- **System update:** Keep up to date with operating system changes with reminders.
- **Breach reports:** Get alerts about company data breaches, along with helpful tips.

See also RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/):



See also 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-ATT0000137-RQ-ATT0000138 (https://www.att.com/support/article/u-verse-voice/KM1235421/):

Digital Phone Call Protect features

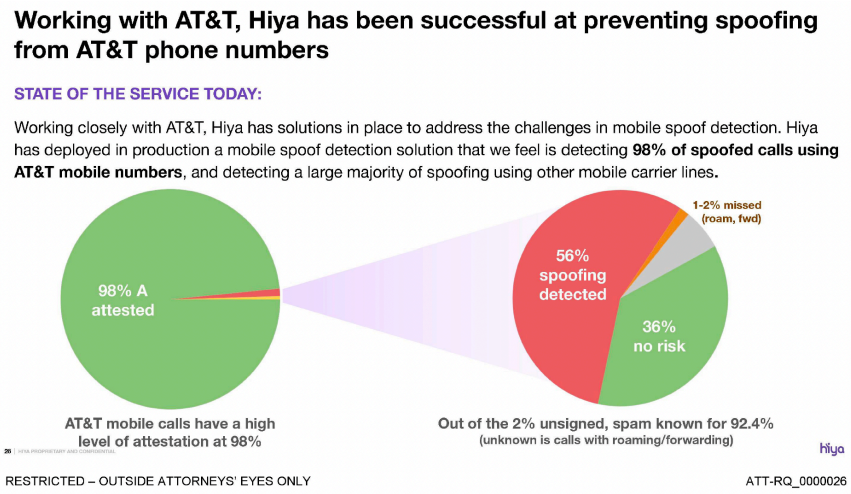
Here's what you get with Digital Phone Call Protect[1]:

- **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).

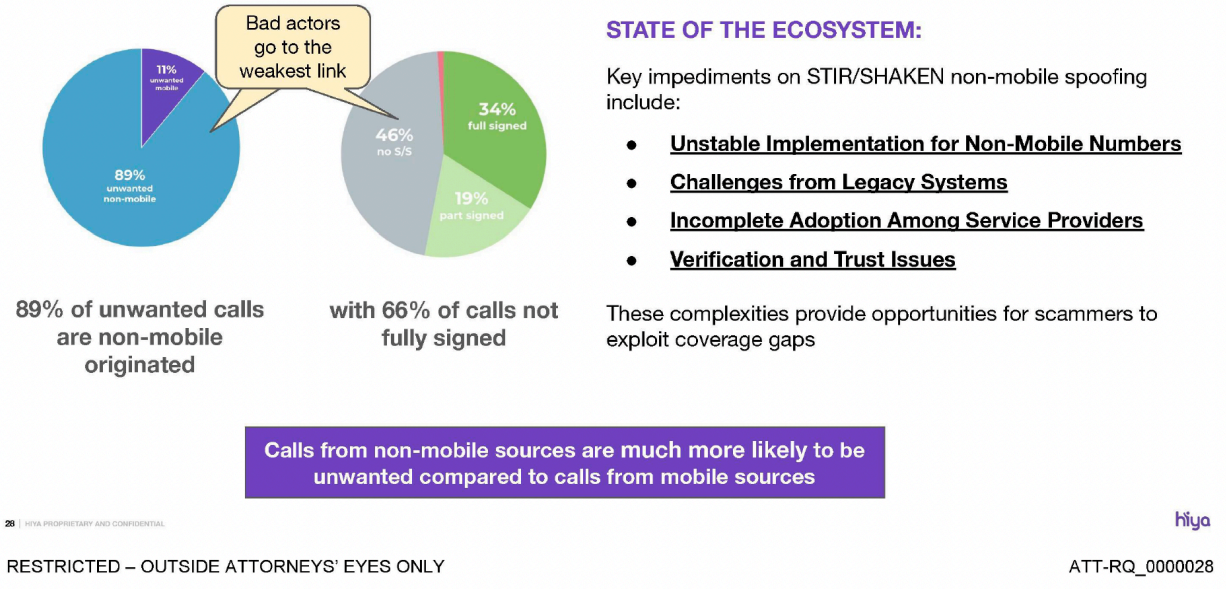
See, e.g., ATT-RQ_0000001 at 3, showing volume of blocks calls necessitating the use of computer systems with processors to make the determination to block or connect an outgoing or incoming call:



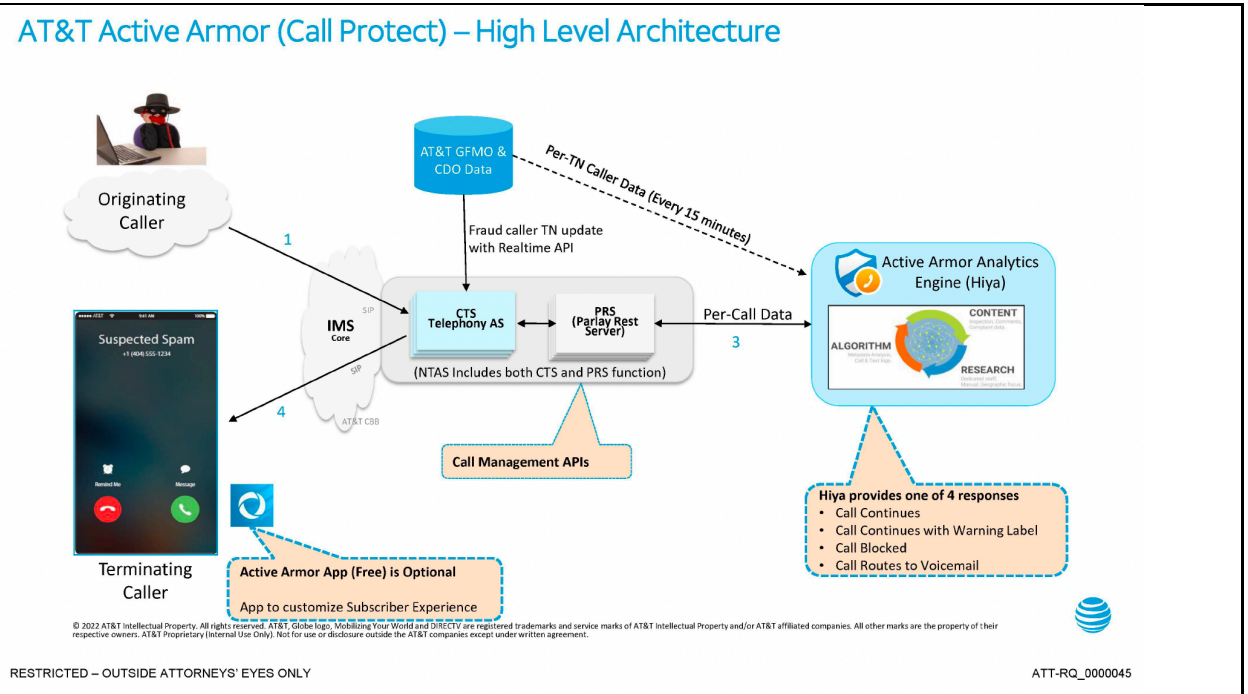
See, e.g., ATT-RQ_0000001 at 26, showing that AT&T prevents spoofing from its own numbers on its network:



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.



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 should be connected or blocked)):

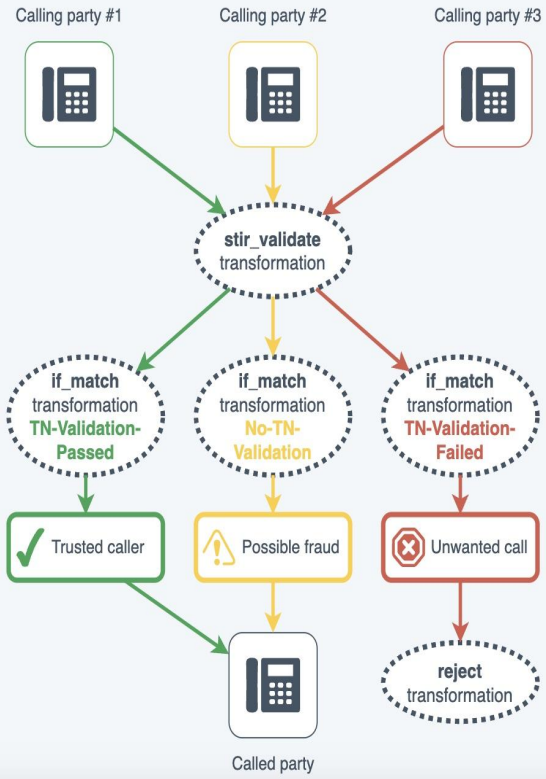


See also RQ0001940-RQ0001955 (https://www.carrierx.com/documentation/how-it-works/stir-shaken#verification-examples):

Verification Examples

The `stir_validate` transformation is normally not used all by itself. You can use it to verify the call signature and then use the output data with other transformations to manage the further call behavior.

An example of such a behavior can look like this:



See also RQ-ATT0000135-RQ-ATT0000136 (https://about.att.com/story/2021/robocalls.html):

	AT&T's approach works for business and consumer lines – wired or wireless. We're on track to *double* last year's numbers because of our *triple*-barreled protection: 1. AT&T Call Protect gives wireless customers automatic fraud blocking and suspected spam alerts. 2. Our global fraud team runs an additional program that blocks fraud calls to every type of AT&T phone service. 3. STIR/SHAKEN, a new call authentication technology, is now boosting both programs with extra data for detection and accuracy. 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 method of claim 10, wherein the information transmitted by the second device is obtained via a backchannel that is different from the communications connection.	Within the Accused Instrumentalities the information transmitted by the second device is obtained via a backchannel that is different from the communications connection. As an example, the information transmitted by the second device is obtained via a connection or channel that uses the same type of path as the communications connection but different protocols. As another example, the information transmitted by the second device is obtained via a channel or connection that follows a different route and/or data flow as the communications connection. As another example, the information transmitted by the second device is encoded within the same type of path as a communications connection or the information transmitted by the second device is not encoded and is obtained via an encoded primary communication channel. As another example, the information transmitted by the second device is obtained via a communications connection. As an example, the Accused Instrumentalities use other backchannel methods, such as SMS, WiFi, or Internet data in the verification service. For example, the communication includes a component

	that is difficult to predict by a potential attacker, such as a serial number, a counter, a pseudo-random or random number, a number specific to the session or the phone, or any other appropriate component value. As yet another example, the AT&T networks use an encoded primary communication channel so that the backchannel is not a separate channel. As one example, the AT&T Networks rely on an encoded primary channel included in the SIP Identity header. As a separate example, this encoded primary channel is accomplished with an AT&T mobile application, such as the ActiveArmor mobile application. RQ-ATT0000139-150 (https://www.att.com/legal/terms.activeArmorMobileSecurity.html). For example, in the Accused Instrumentalities, one communication channel can be used by the calling party device to make the call and a different communication channel, including for example a second communication channel accomplished with, initiated by, or used by the calling party's device, the called party's device, and/or an AT&T mobile application on the calling party's and/or called party's device, such as the ActiveArmor mobile application, can be used to obtain the information transmit by the second device. RQ-ATT0000139-RQ-ATT0000150 (https://www.att.com/legal/terms.activeArmorMobileSecurity.html). For example, ATT discloses that it keeps information transmitted by the second device confidential and/or obtains information from third-parties. *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 ×

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).

See also 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).

See, ATT-RQ_0000042, -43, -44 (evidencing information such as 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 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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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., 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.

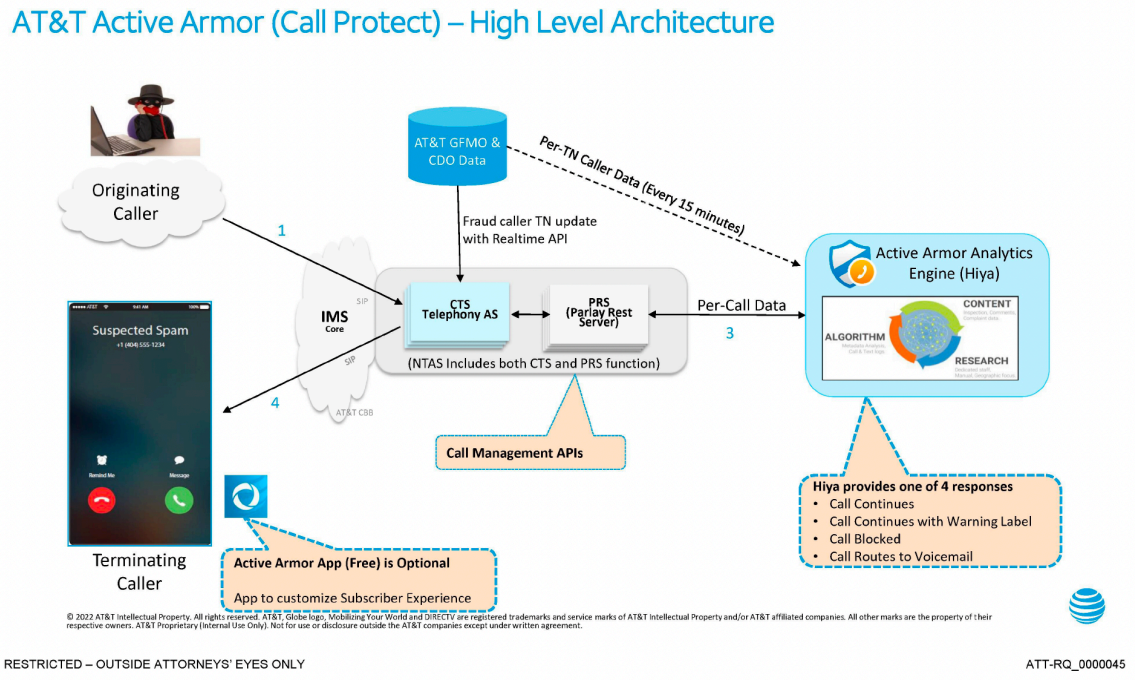
For example, a call that is illegally "spoofed" – or shows a faked number – will fail the SHAKEN/STIR Caller ID verification and will not be marked as verified. By contrast, verification will confirm that a call is really coming from the identified number or entity. More calls will be verified over time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

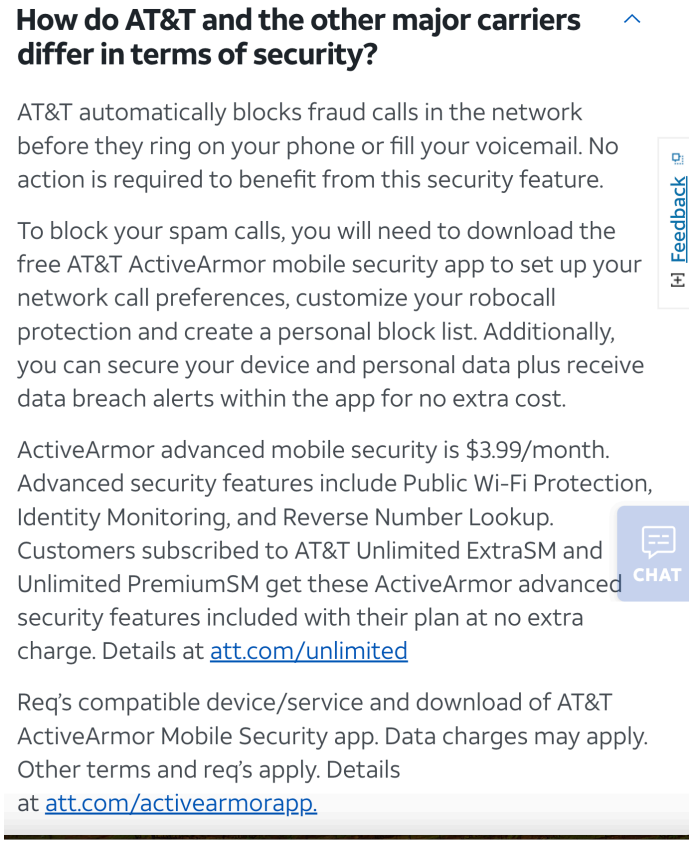
The FCC has recommended SHAKEN/STIR standards to digitally validate phone calls. The acronym stands for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR).

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.

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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
Claim 12. The method of claim 10, wherein based at least in part on the security determination, the verification service provider is further configured to convey an assurance to a recipient associated with the communications connection.	Within the Accused Instrumentalities, based at least in part on the security determination, the verification service provider is further configured to convey an assurance to a recipient associated with the communications connection. *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 should be connected or blocked)):  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, based at least in part on the security determination associated with the inter-network and intra-network call, the Accused Instrumentalities convey and/or are configured to 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.

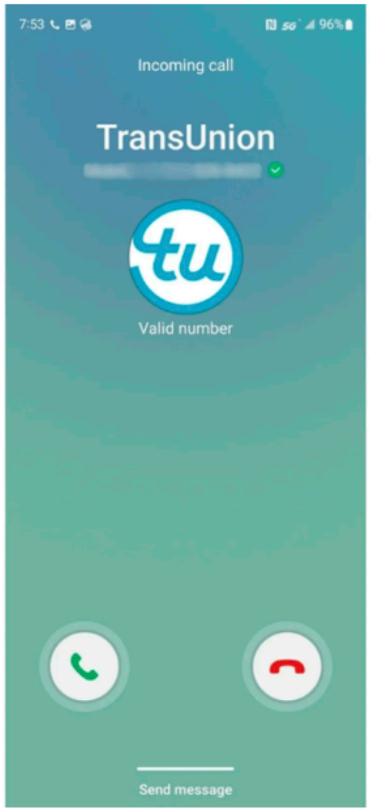
Phone service providers have jointly developed a technology – the SHAKEN/STIR standards – to digitally validate calls. This won't solve the problem of unwanted robocalls by itself. But it can give consumers greater confidence and control over the calls they answer.

"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 also* 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.

See also RQ-ATT0000161-RQ-ATT0000163 (https://www.att.com/device-support/article/wireless/KM1403775/Apple/iPhone13/).

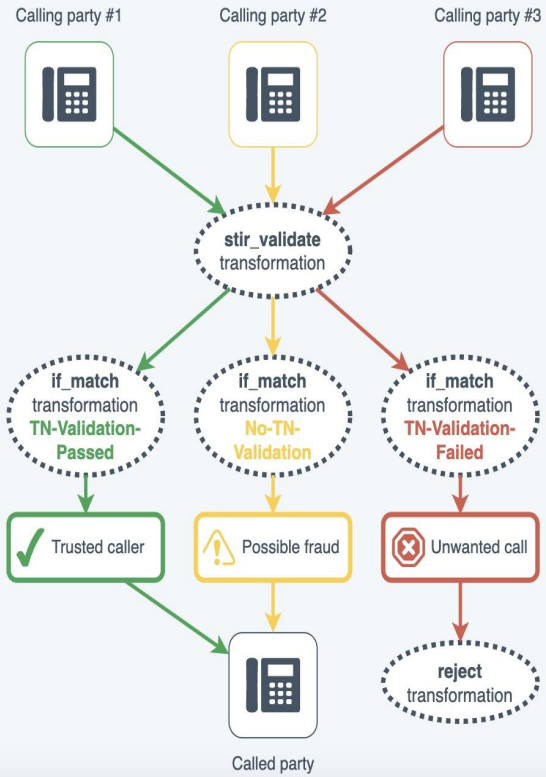
As another example, based at least in part on the security determination, the Accused Instrumentalities convey and/or are configured to convey a failure to confirm to the callee associated with the call, including but not limited by conveying "Unknown caller," any indication of a potential spoofed, spam, or fraudulent call, such as "suspected spam" or "suspected fraud," any indication a call was blocked, and/or by not conveying with an allowed communication an assurance such as a

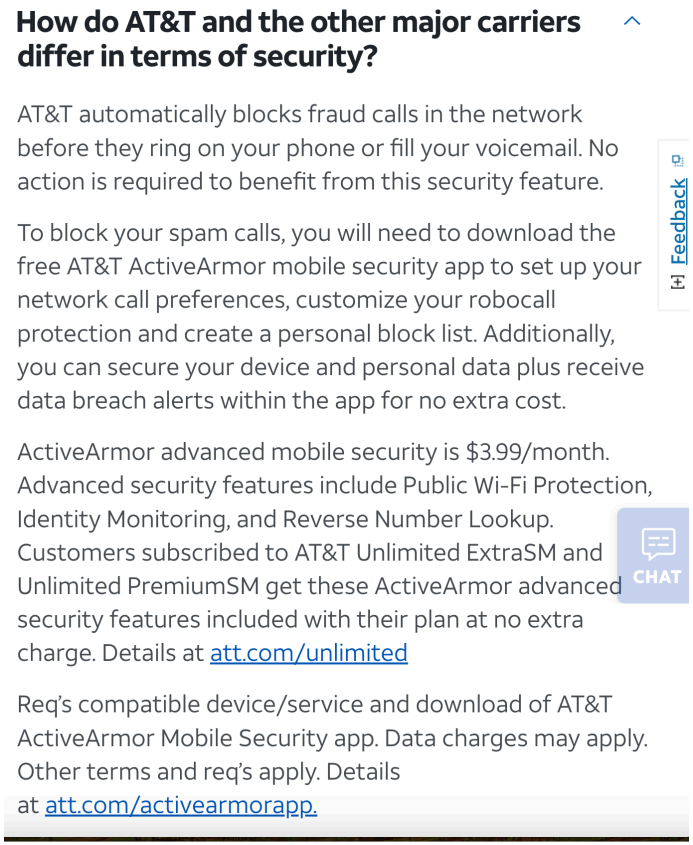
	green check, “valid number,” or “[V]”, a brand logo, contact/caller name, or providing a call log, report, or other indication reflecting confirmation. *See, e.g.*, RQ-ATT0000095-RQ-ATT0000098 (https://forums.att.com/conversations/account-features/blocking-unknown-numbers/63b33783c1c54d548b8bbe5b). Hey, 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 you 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.

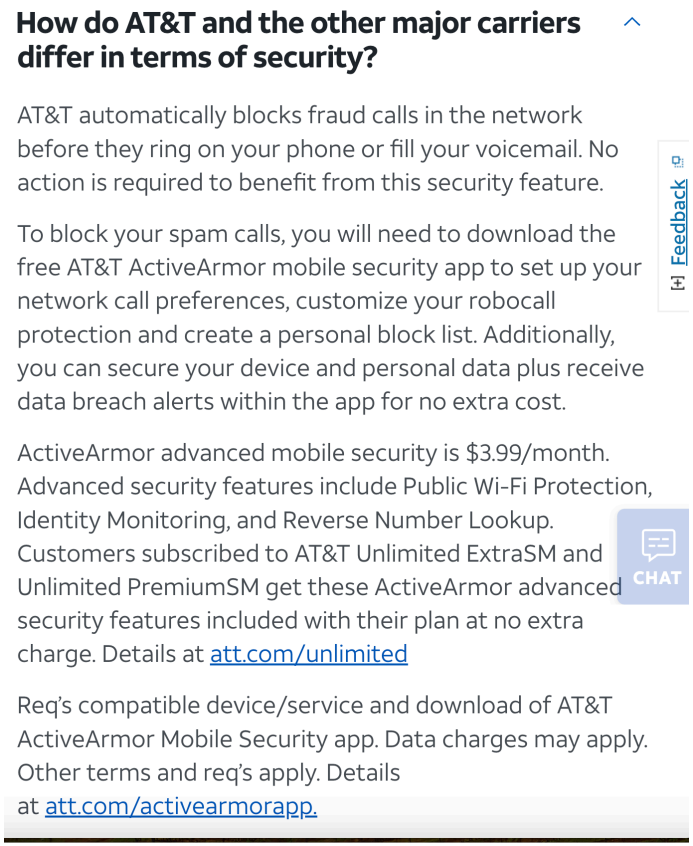
EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

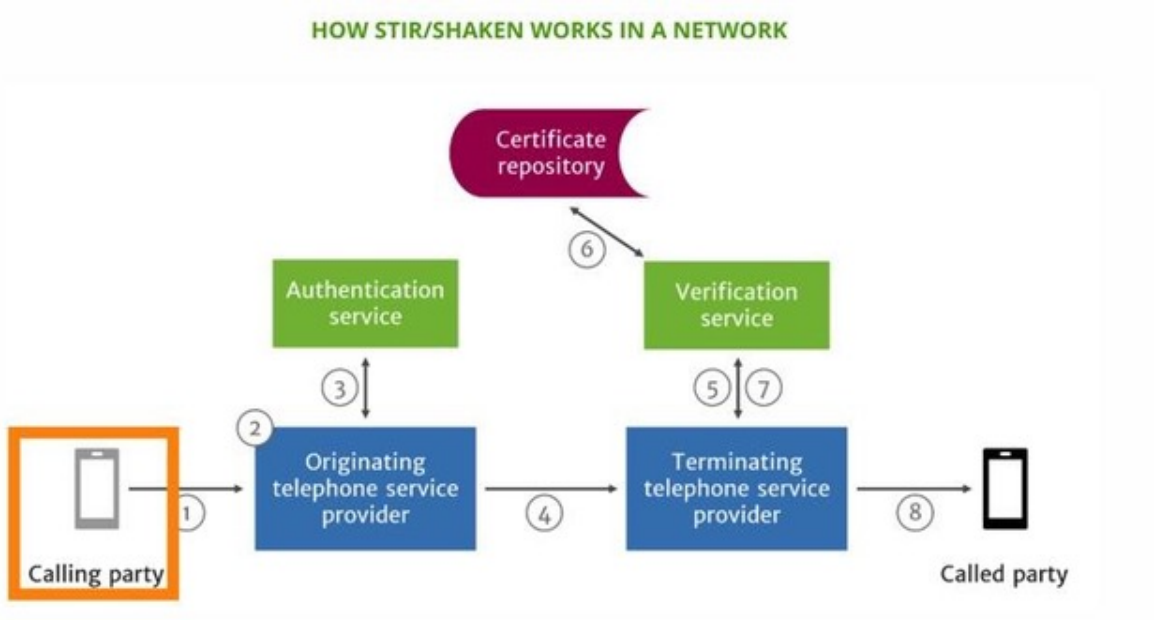
	See also RQ0001970 (https://sti-ga.atis.org/resources/). The terminating network conveys the verification result to the called user by including a "verstat" parameter in the From and/or P-Asserted-Identity header fields of the INVITE request sent to the called endpoint device, as defined in [TS 24.229]. • 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. *See, e.g.*, RQ0001940-RQ0001955 (https://www.carrierx.com/documentation/how-it-works/stir-shaken#verification-examples):

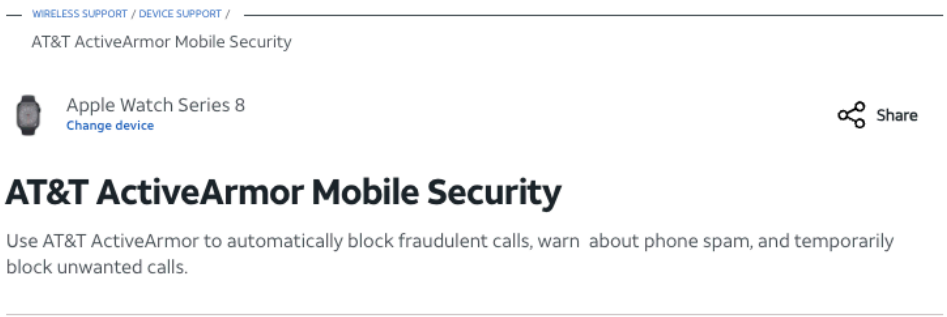
	Verification Examples The `stir_validate` transformation is normally not used all by itself. You can use it to verify the call signature and then use the output data with other transformations to manage the further call behavior. An example of such a behavior can look like this:  An analysis of proprietary 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 method of claim 10, wherein the communications	Within the Accused Instrumentalities, the communications connection is associated with at least

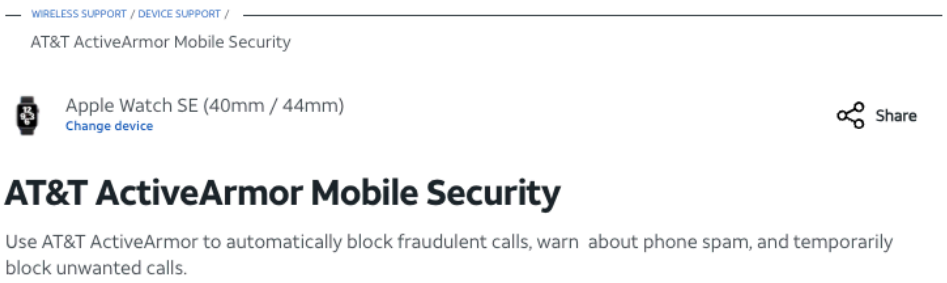
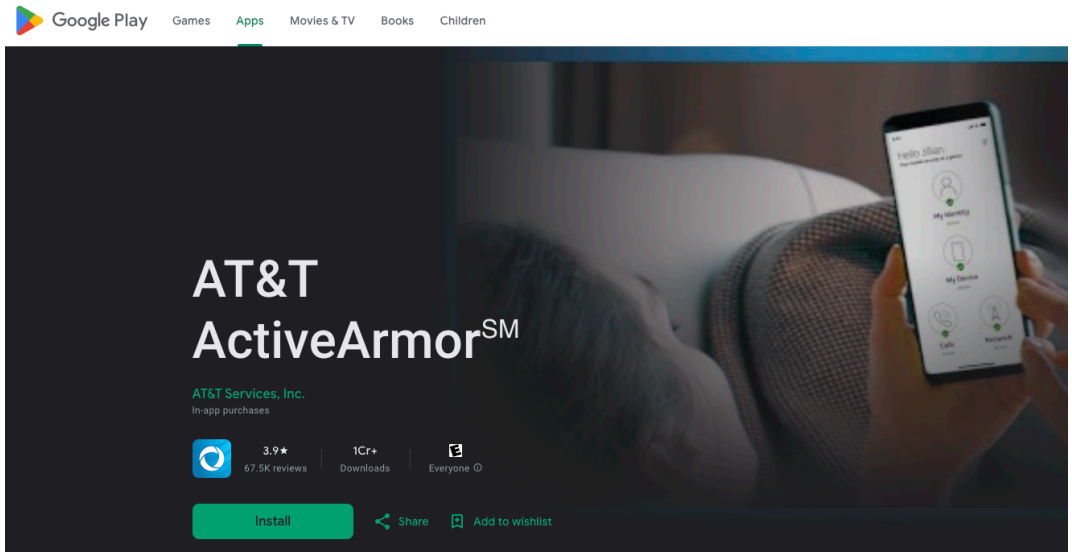
connection is associated with at least one of email, SMS, instant message, and a phone call.	one of email, SMS, instant message, and a phone call. For example, within the Accused Instrumentalities the communication connection is associated with a phone call. AT&T advertises: "AT&T automatically blocks 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/).  *See also* RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security).

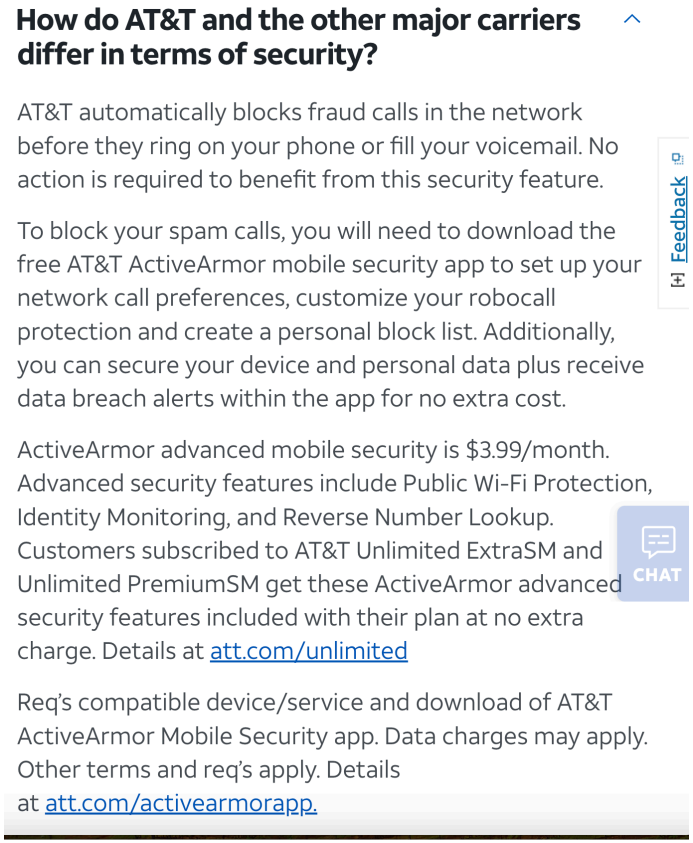
	For another example, within the Accused Instrumentalities the communication connection is associated with SMS and/or instant message. *See, e.g.*, RQ-ATT0000046-RQ-ATT0000048 (https://about.att.com/blogs/2023/activearmor-text-blocking.html): *AT&T ActiveArmor Offers New Text-Filtering Features for Even More Protection* We know that spam texts and robocalls are a pain. That's why we're pleased to give important updates on our spam-fighting AT&T ActiveArmor℠. Our new and better network filters **blocked more than 1 billion spam text messages** from reaching customers in July – our highest-ever total. Every month since then, customers have collectively reported one-third fewer spam texts getting through to their phones. We block spam texts for everyone on our network – you don't have to do a thing. But if you download the free AT&T ActiveArmor mobile security app, you can now get even more control of incoming text messages: • **You can block email-to-text messages** – a consistent source of spam. These are texts that appear to come from an email address.[1] Just review the terms and toggle a switch on the ActiveArmor app. As one example, within the Accused Instrumentalities, the verification service verifies the corresponding communication identifiers for the email, SMS, instant message, or phone call respectively. As another example, the initial communication path used by the device to contact a verification service includes channels such email and SMS, instead of a phone call. In such a scenario, the verification service does not verify the ANI of the device, and instead verifies the corresponding communication identifiers associated with the initial communication path. 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 method of claim 10, wherein the first device	Within the Accused Instrumentalities the first device comprises at least one of a smartphone, a

comprises at least one of a smartphone, a tablet, a PC, a phablet, and a wearable device.	tablet, a PC, a phablet, and a wearable 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/).  *See also* RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security).

	As one example, the first device ("calling party", indicated with orange box below) comprises at least one of a smartphone, a tablet, a PC, a phablet, and a wearable device. *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/); RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).  For example, within the Accused Instrumentalities, the first device comprises but is not limited to the following smartphones, smartwatches, and/or tablets. *See, e.g.*, RQ-ATT0000105-RQ-ATT0000117 (https://www.att.com/scmsassets/support/wireless/devices-working-on-att-network.pdf); *see also* RQ-ATT0000118-RQ-ATT0000119 (https://www.att.com/support/how-to/wireless/esim-get-started/). As another example, within the Accused Instrumentalities, the first device comprises but is not limited to a PC. For example, AT&T advertises providing instant messaging, Voice over IP (VOIP) calling, as well as other features, on a desktop computer. *See, e.g.*, RQ-ATT0000180-RQ-ATT0000206 (https://asecare.att.com/tutorials/att-collaborate-app-desktop). As another example, AT&T discloses that the Accused Instrumentalities, including but not limited to AT&T ActiveArmor, are compatible with at least smartphones, wearable devices

	(including but not limited to Apple smartwatches), and iPod Touch. *See* RQ-ATT0000049-RQ-ATT0000050 (https://apps.apple.com/us/app/at-t-activearmor/id1218465964): **Information** Seller AT&T Services, Inc. Size 138.1 MB Category Utilities Compatibility **iPhone** Requires iOS 13.0 or later. **iPod touch** Requires iOS 13.0 or later. Languages English Age Rating 4+ Copyright ©2024 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property. All other marks are the property of their respective owners. Price Free In-App Purchases 1. Plus *See* RQ-ATT0000007-RQ-ATT0000011 (https://www.att.com/device-support/article/wireless/000092356/Apple/WatchSeries8/)  *See* RQ-ATT0000001-RQ-ATT0000006 (https://www.att.com/device-support/article/wireless/000092356/Apple/WatchSE44mm/):

	 *See* RQ-ATT0000042-RQ-ATT0000045 *AT&T ActiveArmor on Google Play Store*  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 method of claim 10, wherein enrolling the first	Within the Accused Instrumentalities enrolling the first device is based at least in part on at least one of PIN verification, password verification, knowledge-based authentication, geolocation

device is based at least in part on at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number.	information, credit card information validation, and a check of at least one of a name, an address, and a 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/).  *See also* RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security).

	For example, the Accused Instrumentalities use PIN verification, including as part of activating and/or accessing the Accused Instrumentalities, including but not limited to password, fingerprint, and/or Face ID. *See, e.g.*, RQ-ATT0000099-RQ-ATT0000104 (https//www.att.com/device-support/article/wireless/KM1324197/Samsung/SamsungSMG975U/):

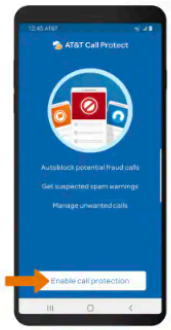
Access call protect

1. Navigate to and select the **AT&T Call Protect app**.

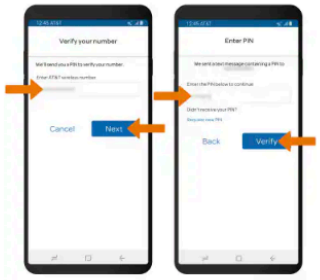
Note: AT&T Call Protect allows you to automatically block fraudulent calls, warns you about phone spam, and temporarily blocks unwanted calls.

2. Select **Enable call protection**.

*Note: Review the permissions, then select **ALLOW**.*



3. Enter your **myAT&T wireless number**, then select **Next**. Enter the **PIN** sent via text, then select **Verify**.



4. Review the Terms & Conditions, then select **I agree**. Select **Continue**.

*Note: Select **ALLOW** to give permission to the app to access your contacts.*

	For further example, the Accused Instrumentalities collect and use password verification, knowledge-based authentication, geolocation information, credit card information validation, and/or a check of a least one of a name, an address, and a phone number, including for enrolling a first device. *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.

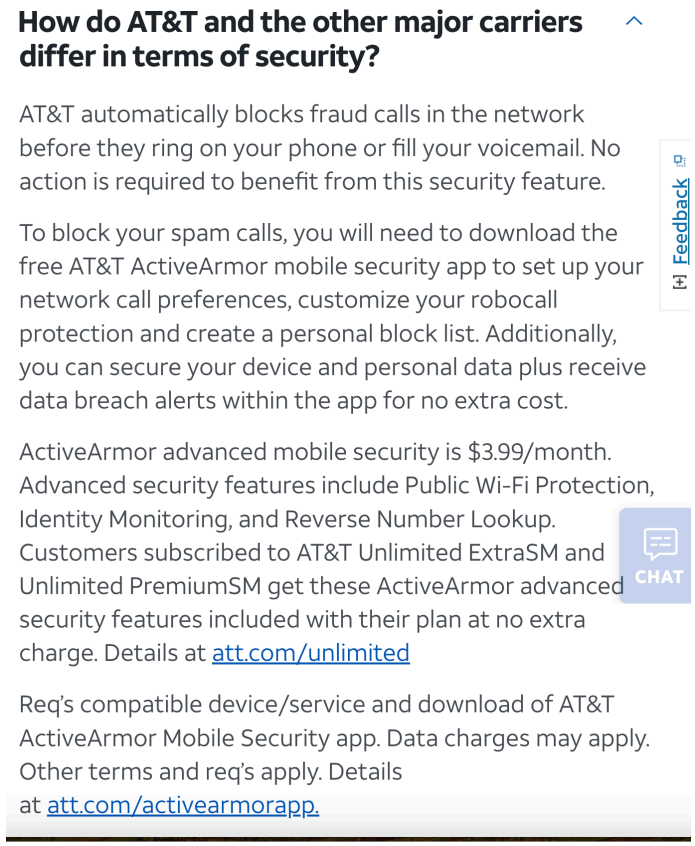
How we use your information ×

We rely on the information we collect to support our business functions, power our services and improve your experience, such as when we:

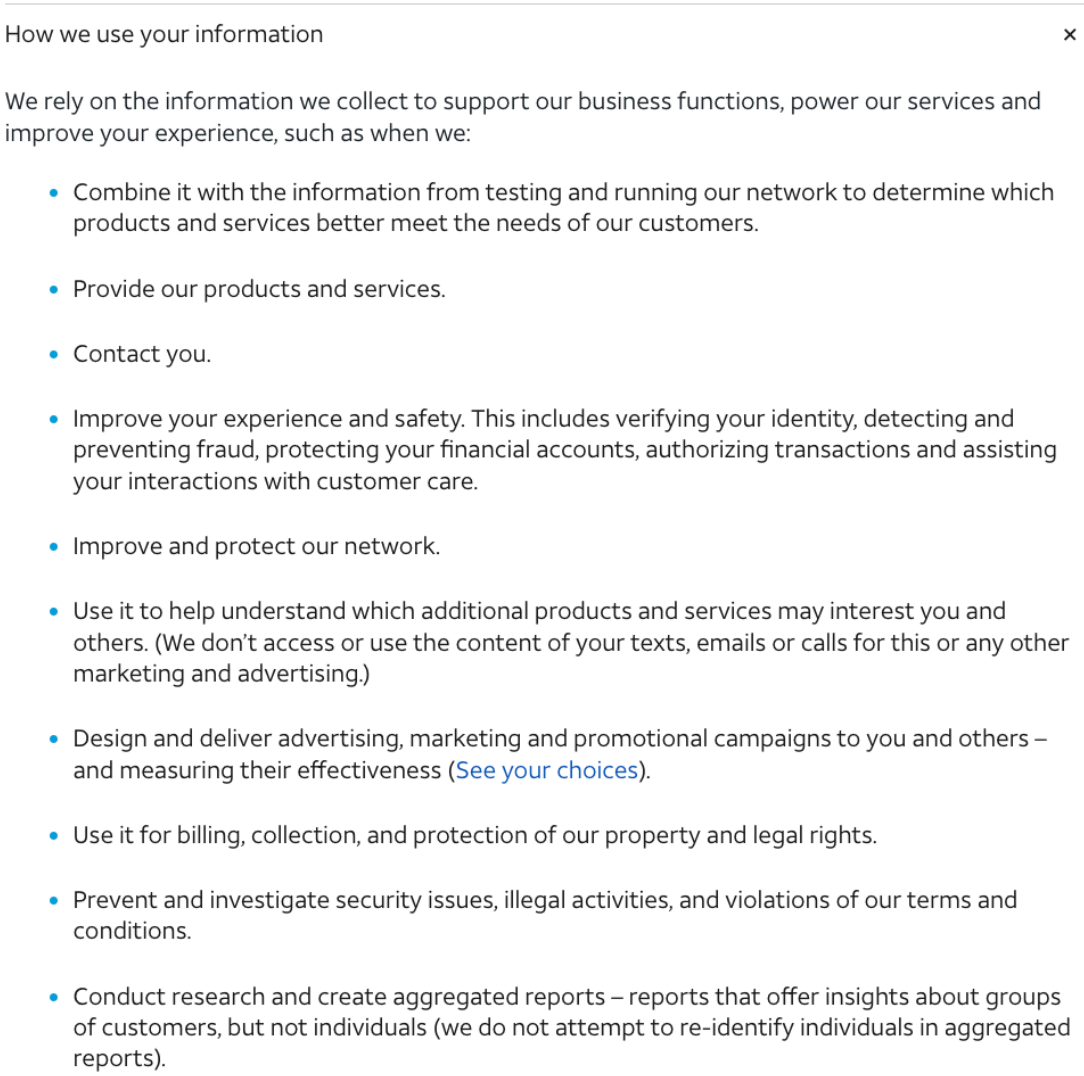
- Combine it with the information from testing and running our network to determine which products and services better meet the needs of our customers.
- Provide our products and services.
- Contact you.
- Improve your experience and safety. This includes verifying your identity, detecting and preventing 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).

See also RQ-ATT0000139-RQ-ATT0000150:

	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, enrolling of a first device is based in part or in whole on PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and/or a check of at least one of a name, an address, and a phone number. As yet another example, enrolling of a first device is based upon information that is included 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 16. The method of claim	Within the Accused Instrumentalities the additional authentication comprises at least one of PIN

10, wherein the additional authentication comprises at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number.	verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a 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/).  *See also* RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security).

	As one example, requested additional authentication comprises PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and/or a check of at least one of a name, an address, and a phone number. As another example, additional authentication comprises of information that is included in the SIP INVITE. *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.



See also 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).

As another example, the Accused Instrumentalities are configured to implement PIN verification, including for enrolling a first device, for additionally authenticating, and/or other services, including but not limited to password, fingerprint, and/or Face ID.

See, e.g., RQ-ATT0000099-RQ-ATT0000104 (https//www.att.com/device-support/article/wireless/KM1324197/Samsung/SamsungSMG975U/):

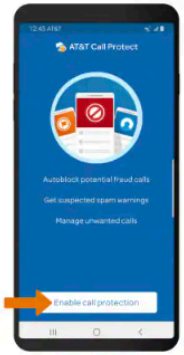
Access call protect

1. Navigate to and select the **AT&T Call Protect app**.

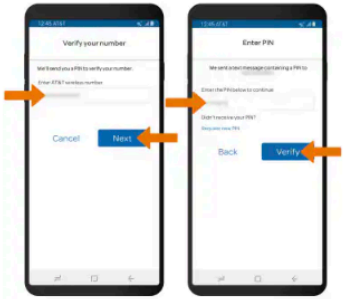
Note: AT&T Call Protect allows you to automatically block fraudulent calls, warns you about phone spam, and temporarily blocks unwanted calls.

2. Select **Enable call protection**.

*Note: Review the permissions, then select **ALLOW**.*



3. Enter your **myAT&T wireless number**, then select **Next**. Enter the **PIN** sent via text, then select **Verify**.

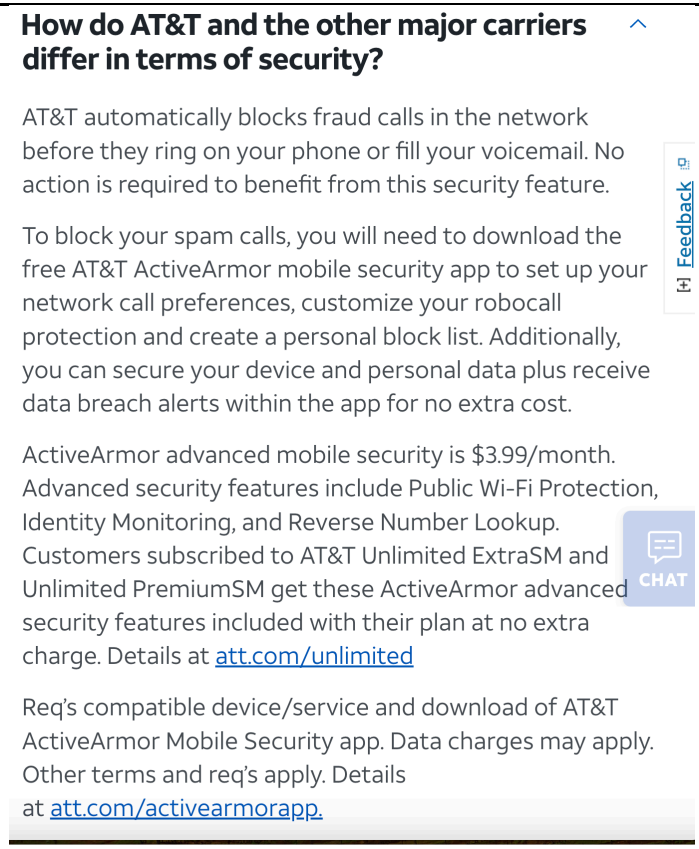


4. Review the Terms & Conditions, then select **I agree**. Select **Continue**.

*Note: Select **ALLOW** to give permission to the app to access your contacts.*

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. [pre] A computer program product embodied in a tangible and 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 comprising 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 determine if a given call should be blocked, connected, or if additional authentication information is required, and/or are otherwise capable of detecting, blocking, and preventing SPAM, fraudulent, and spoofed phone calls. *See, e.g.*, 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 ActiveArmor℠ 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/).



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

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 Protect[1]:

- **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).

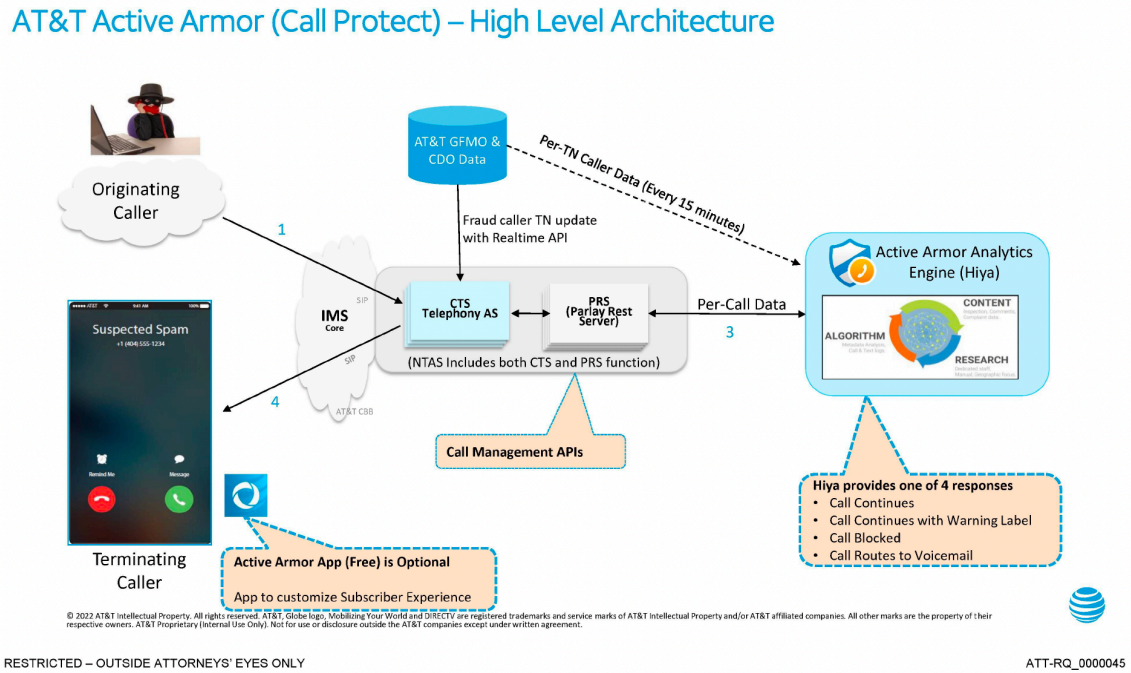
As another example, the Accused Instrumentalities are implemented, used, and/or put into service by AT&T in cross-network communications. *See e.g.*, RQ-ATT0000051-RQ-ATT0000053 (https://about.att.com/story/2019/att_tmo_call-authentication.html).

	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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

Furthermore, 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 and/or used to, among other functions, detect spoofed, spam and/or fraudulent phone calls.

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 should be connected or blocked)):



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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

17[a] enrolling a first device with a verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device;	The Accused Instrumentalities comprise computer instructions for enrolling a first device with the verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device. The verification service provider may be located within Defendants' network directly, operated by a third party (e.g., Hiya), or some combination thereof. *See* 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. *See, e.g.*, RQ-ATT0000024-RQ-ATT0000026 (https://about.att.com/story/2019/call_validation_displays.html):



See also 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: **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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

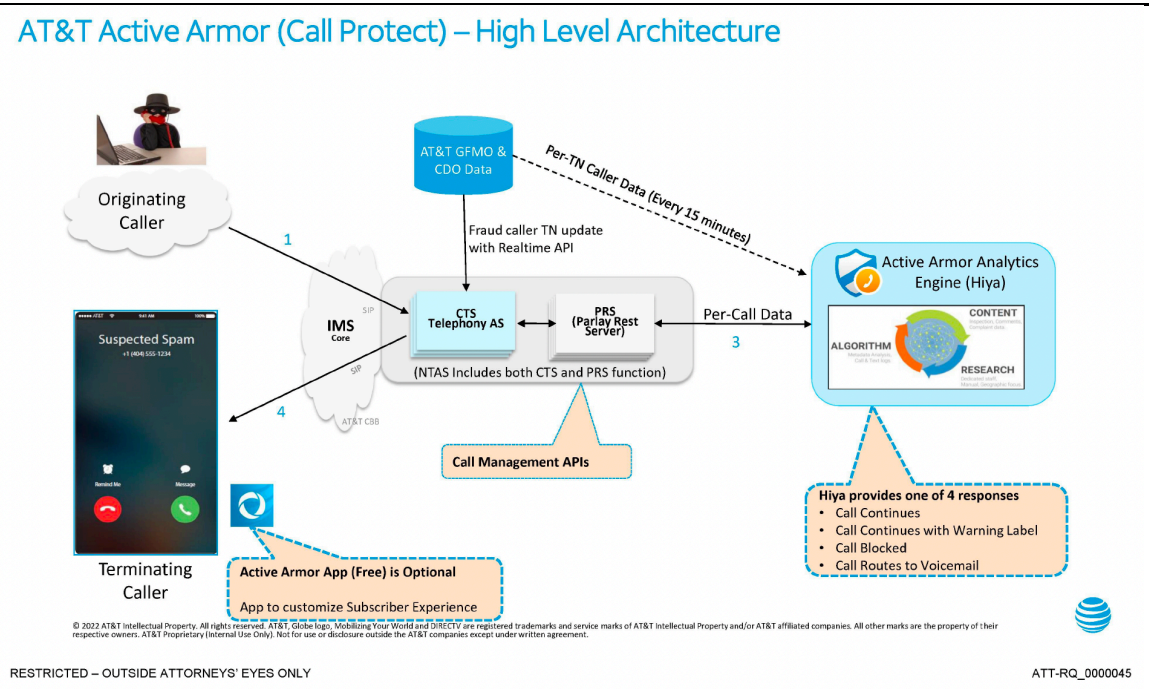
CTN (including AT&T/FN/Cricket customers)
Service tier (like Basic vs. Advanced)
Service Tags:

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

ActiveArmor Application Data

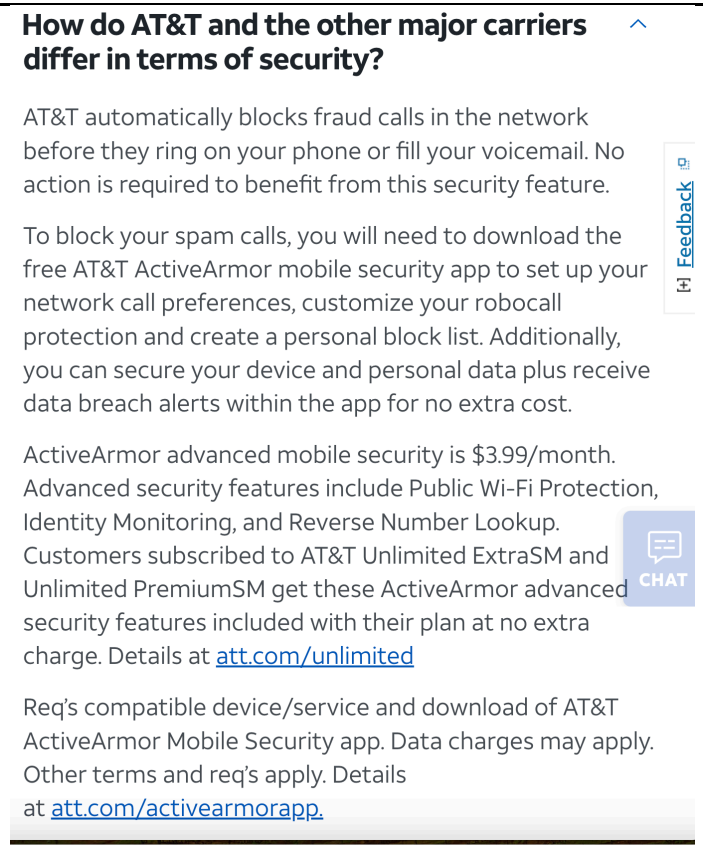
TN from Device Address Book - Hashed (shared only with explicit subscriber consent)
Device OS
ActiveArmor Version Information

See, e.g., ATT-RQ_0000045 (AT&T GFMO and CDO Data):



The verification service provider is comprised of one or more components, implemented in hardware, software, or a combination thereof, used by, implemented in, and/or included in the Accused Instrumentalities that function in the manner described herein. *See, e.g.*, 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 ActiveArmor℠ 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. *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.

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 Protect[1]:

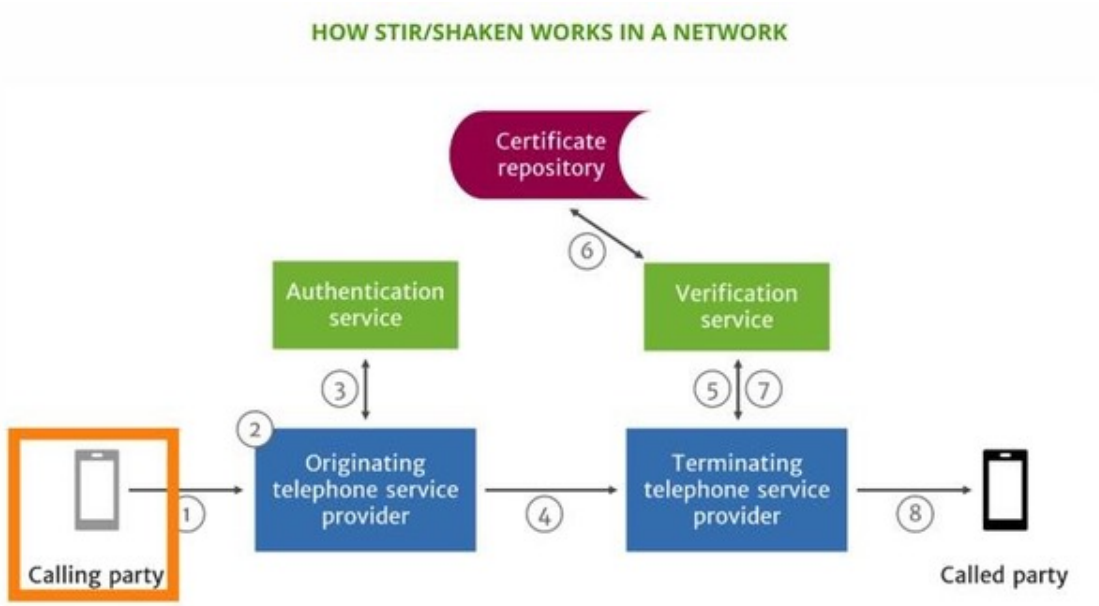
- **Call validation:** Soon you'll see a [V] on your caller ID for some calls. This means we've confirmed that the call originated from the phone registered to that number. (Remember to still be cautious when answering a call from an unknown number.)
- **Automatic fraud blocking:** Each potential fraud 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 RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/); RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

The enrolling of the first device includes associating, by the verification service provider, the first device with a device fingerprint. *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/); RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/). The device fingerprint is generated based at least in part on a set of configuration information associated with the first device.

The Accused Instrumentalities comprise a computer program product that has instructions for caller identification validation and/or verification technology, including without limitation ActiveArmor, the ActiveArmor mobile application, and STIR/SHAKEN.

As one example, the verification service provider enrolls a first device ("calling party", indicated with orange box). *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/); RQ-ATT0000035-RQ-

	ATT0000041 (https://www.att.com/security/).  Before Defendants determine how to attest for the validity of the calling number, Defendants' Accused Instrumentalities are configured to determine if the call should be connected. The Accused Instrumentalities, alone or in combination, enroll a first device (showing as "calling party" and identified with an orange box). Enrollment of the first device includes generation of a device fingerprint based at least in part on a set of configuration information at least a portion of which is used at least in part to perform a security determination (e.g., SIM-based, credential-based, or line-based authentication). A device fingerprint is generated based at least in part on a set of configuration information associated with the first device. Examples of such configuration information used to generate the device fingerprint include without limitation combinations of device specific data, device settings, installed applications, system or application software versions, contact list data, or other data specific to the calling device.

	As one example, a device fingerprint comprises and/or is otherwise generated based at least in part on a mobile identification number ("MIN") or derivation. *See, e.g.*, RQ0001968 (https://en.wikipedia.org/wiki/Mobile_identification_number). As another example, a device fingerprint comprises and/or is otherwise generated based at least in part on a mobile subscription identification number ("MSIN"). As another example, a device fingerprint comprises and/or is otherwise generated based at least in part on the international mobile subscriber identity ("IMSI") or encrypted version thereof ("TMSI"). *See, e.g.*, RQ0001957-RQ0001964 (https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity); RQ0002121-RQ0002123 (https://cellularnews.com/definitions/what-is-a-mobile-identification-number-min/). As one example, a device fingerprint comprises and/or is otherwise generated based at least in part on a Subscriber Module (SIM) Card serial number. RQ0002042-RQ0002060 (https://en.wikipedia.org/wiki/SIM_card). As one example, a device fingerprint comprises and/or is otherwise generated based at least in part on a serial number, Host Device ID, or any other unique identifier for a device (including but not limited to Android ID, UDID, IDFA, AAID). RQ0001932-RQ0001939 (https://support.apple.com/en-us/108037); RQ0001965-RQ0001967 (https://saturncloud.io/blog/is-there-a-unique-android-device-id/). As one example, a device fingerprint comprises and/or is otherwise generated based at least in part on any derivation and/or combination of the above examples or any other configuration information. The Accused Instrumentalities associate the first device with a device fingerprint. *See, e.g.*, RQ-ATT0000099-RQ-ATT0000104 (https://www.att.com/device-support/article/wireless/KM1324197/Samsung/SamsungSMG975U/):

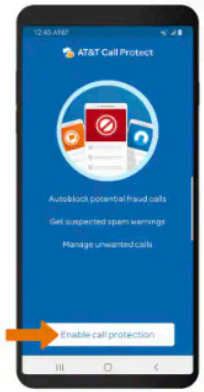
Access call protect

1. Navigate to and select the **AT&T Call Protect app**.

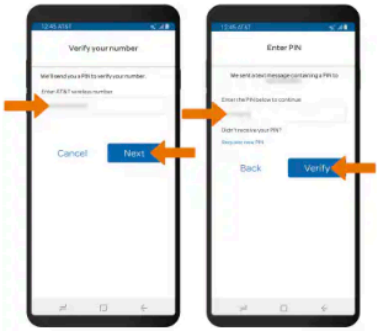
Note: AT&T Call Protect allows you to automatically block fraudulent calls, warns you about phone spam, and temporarily blocks unwanted calls.

2. Select **Enable call protection**.

*Note: Review the permissions, then select **ALLOW**.*



3. Enter your **myAT&T wireless number**, then select **Next**. Enter the **PIN** sent via text, then select **Verify**.



4. Review the Terms & Conditions, then select **I agree**. Select **Continue**.

*Note: Select **ALLOW** to give permission to the app to access your contacts.*

Further, for example, AT&T collects information about equipment on the AT&T Networks, and uses it in, among other ways, "verifying your identity, detecting and preventing fraud." *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 ×

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).

See also 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).

See also 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 (e.g., "Device OS", "ActiveArmor Version Information"), contact list data (TN from Device Address Book), or other data specific to the calling device):

	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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

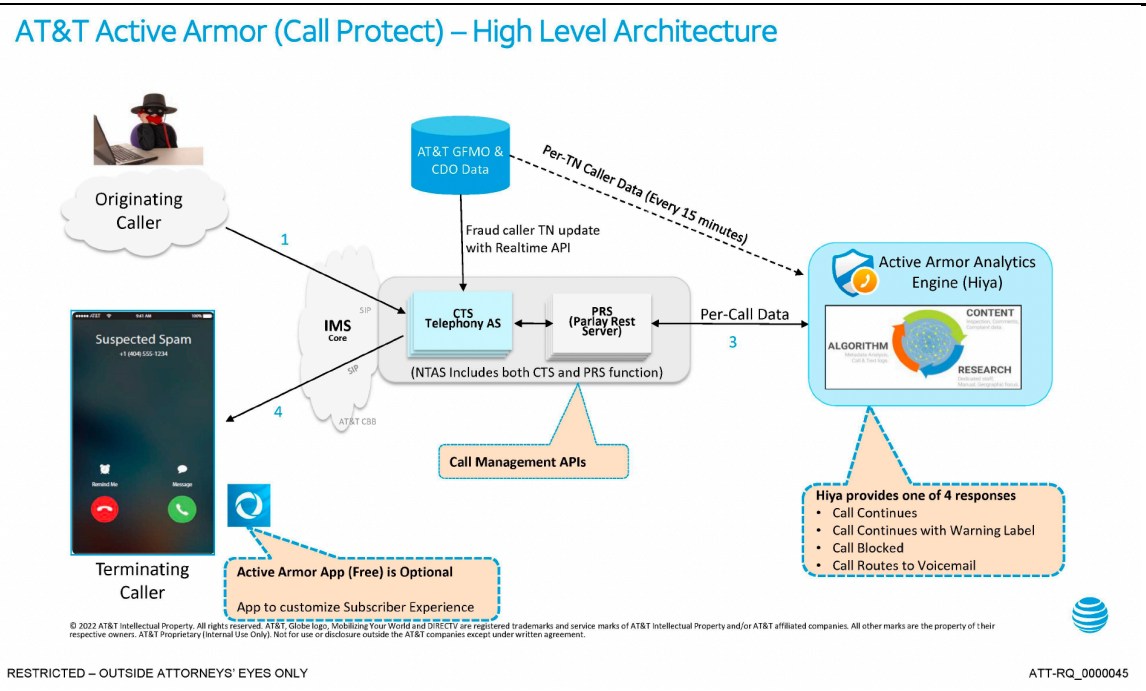
CTN (including AT&T/FN/Cricket customers)
Service tier (like Basic vs. Advanced)
Service Tags:

- 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 (AT&T GFMO and CDO Data):



See also 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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	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.
17[b] storing, at the verification service provider, the device fingerprint associated with the first device;	The Accused Instrumentalities comprise computer instructions for storing, at the verification service provider, the device fingerprint associated with the first device. As one example, the computer instructions instruct how to store, at the verification service provider the configuration information associated with the first device. As one example, Accused Instrumentalities store, at the verification service provider information associated with the first device including but not limited to the device fingerprint and/or the configuration information upon which the device fingerprint is based at least in part. For example, the Accused Instrumentalities use and store various information collected about equipment on the networks. *See, e.g.*, RQ-ATT0000070-RQ-ATT0000086 (https://about.att.com/privacy/privacy-notice.html).

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).

Data retention and security ×

We keep your information as long as we need it for business, tax or legal purposes. We set our retention periods based on things like what type of personal information it is, how long it's needed to operate the business or provide our products and services, and whether it's subject to contractual or legal obligations. These obligations might be ongoing litigation, mandatory data retention laws or government orders to preserve data for an investigation. After that, we destroy it by making it unreadable or indecipherable.

See also 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).

	See also 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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

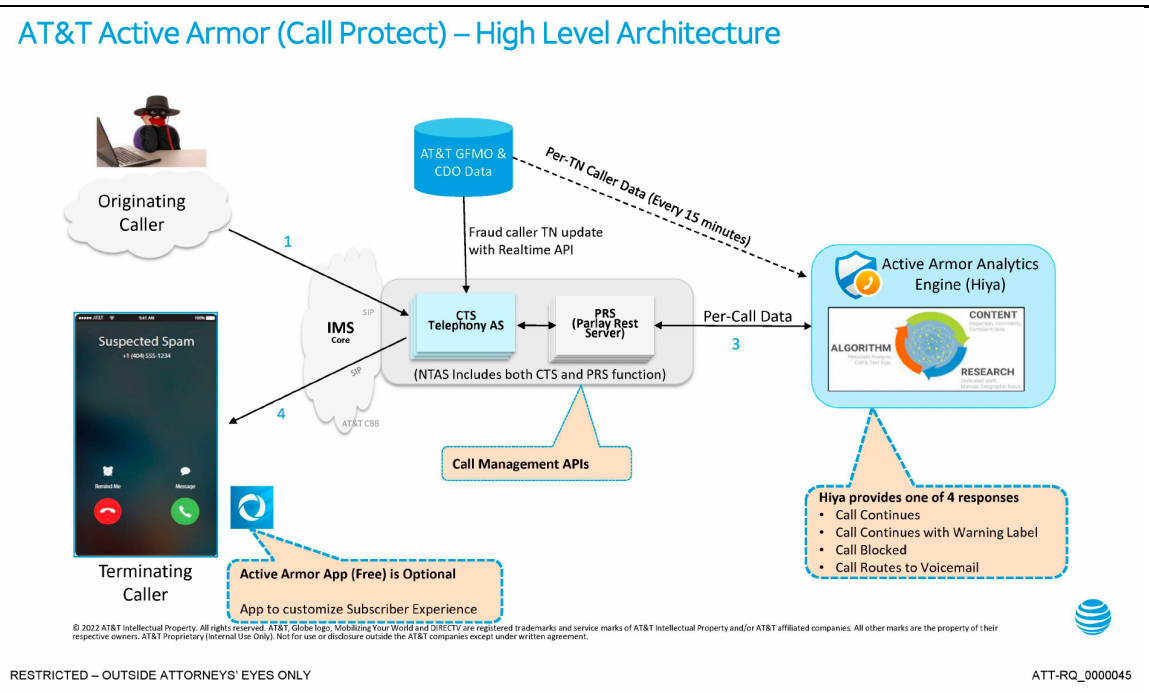
CTN (including AT&T/FN/Cricket customers)
Service tier (like Basic vs. Advanced)
Service Tags:

- 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 (storage locations, e.g., AT&T GFMO and CDO Data):



As another example, the Accused Instrumentalities store a device fingerprint for it later to be used to check the call source against the calling number. *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/); RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/).

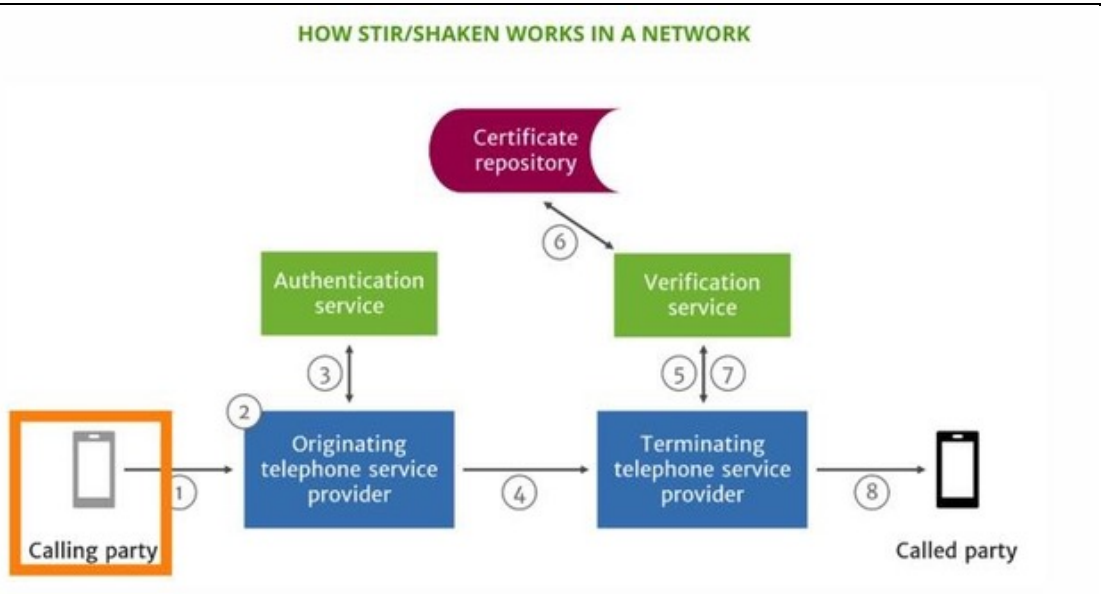
As another example, the Accused Instrumentalities store a device fingerprint to attest for the validity of the calling number, whether it is:

(A) a subscriber registered with the originating telephone service provider's softswitch ("Full Attestation");

(B) a number behind an enterprise PBX ("Partial Attestation"); or,

(C) an identifier of from where the call was received, such as a call from an international gateway ("Gateway Attestation").

	2. The originating telephone service provider checks the call source and calling number to determine how to attest for the validity of the calling number. • **Full Attestation (A)** — The service provider has authenticated the calling party and they are authorized to use the calling number. An example of this case is a subscriber registered with the originating telephone service provider's softswitch. • **Partial Attestation (B)** — The service provider has authenticated the call origination, but cannot verify the call source is authorized to use the calling number. An example of this use case is a telephone number behind an enterprise PBX. • **Gateway Attestation (C)** — The service provider has authenticated from where it received the call, but cannot authenticate the call source. An example of this case would be a call received from an international gateway. 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.
17[c] obtaining, at the verification service provider, information transmitted by a second device associated with a communications connection;	The Accused Instrumentalities comprise computer instructions for obtaining, at the verification service provider, information transmitted by a second device associated with a communications connection. As one example, a second device associated with a communication connection is a calling device, for example the "alling party" indicated with the orange box below. *See, e.g.*, RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/); RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/).



As one example, information is transmitted by a calling party or second device, including for example a device fingerprint of and/or other information transmitted by the second device, that is obtained at the verification service provider.

An example of the obtained information transmitted by the second device associated with a communications connection includes SIP information and/or the information contained with the SIP invitation transmitted by the calling party. *See, e.g.,* RQ0002066-RQ0002080 (https://www.twilio.com/docs/glossary/sip-invites); RQ-ATT0000213-RQ-ATT0000285 (https://www.tutorialspoint.com/session_initiation_protocol/); RQ0001666-RQ0001671(https://telnyx.com/resources/the-beginners-guide-to-sip-headers).

Another example of the obtained information transmitted by the second device associated with a communications connection includes but is not limited to a mobile identification number ("MIN") or any derivation of a MIN or any related number, a mobile subscription identification number ("MSIN"), the international mobile subscriber identity ("IMSI") or encrypted version thereof ("TMSI"), Subscriber Module (SIM) Card serial number, a serial number, Host Device ID, or any another unique identifier for a device (including but not limited to Android ID, UDID, IDFA,

	AAID), and/or any derivation and/or combination of the thereof. Another example of the obtained information transmitted by the second device associated with a communications connection includes the information AT&T collects about equipment on the AT&T Networks, and uses in, among other ways, "verifying your identity, detecting and preventing fraud." *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 ×

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).

See also 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). 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.
17[d] performing, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored	The Accused Instrumentalities comprise computer instructions for performing, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device.

device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device;	The Accused Instrumentalities, alone and/or in combination, comprise one or more system(s) and service(s) that are configured to determine if the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint to decide if, for example, the call should be connected. *See,* 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 (e.g., "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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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

callInfoLocation
callInfoPurpose
callInfoType
callInfoConfidence
callInfoSource
callInfoOrigin

AT&T Account Services

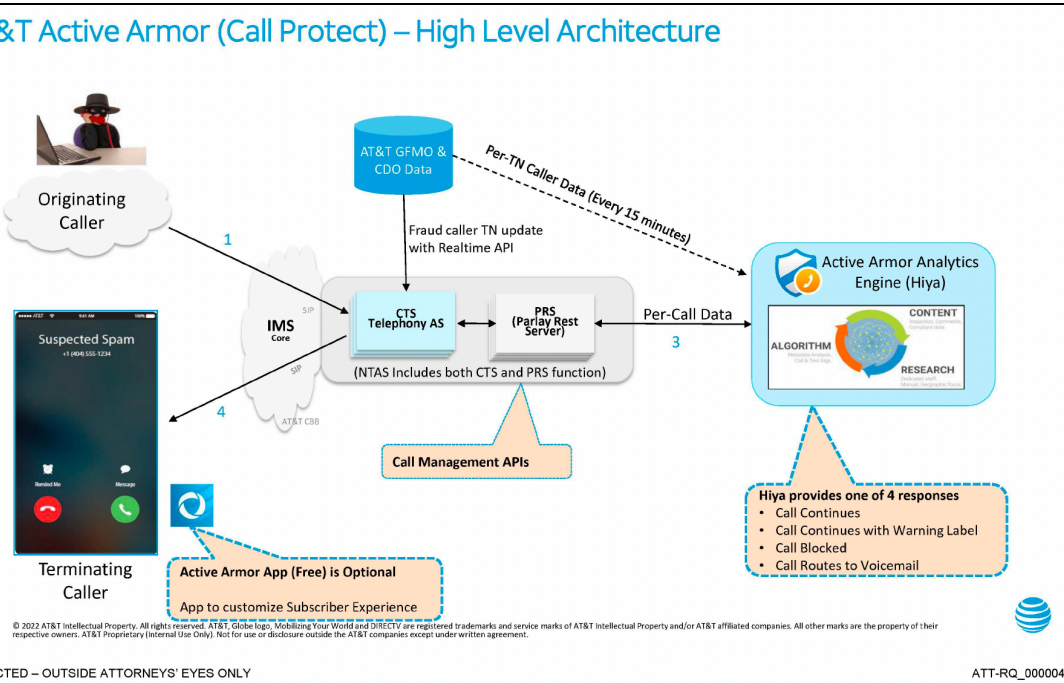
CTN (including AT&T/FN/Cricket customers)
Service tier (like Basic vs. Advanced)
Service Tags:

- 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).



Furthermore, caller identification authentication and verification technology, including without limitation STIR/SHAKEN, is technology configured and/or used to, among other functions, detect spoofed, spam and/or fraudulent phone calls.

As one example, a security determination is performed at the verification service provider to "check[] the call source and calling number to determine how to attest for the validity of the calling number." *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/); RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).

As another example, a security determination is performed at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device to determine how to attest for the validity of the calling number. *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/):

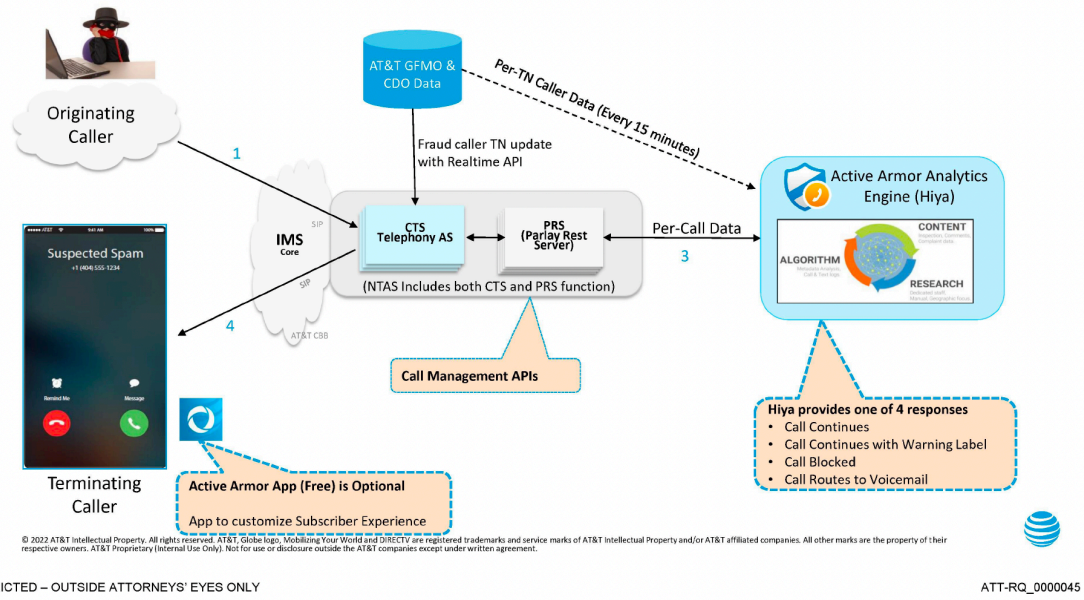
	2. The originating telephone service provider checks the call source and calling number to determine how to attest for the validity of the calling number. • **Full Attestation (A)** — The service provider has authenticated the calling party and they are authorized to use the calling number. An example of this case is a subscriber registered with the originating telephone service provider's softswitch. • **Partial Attestation (B)** — The service provider has authenticated the call origination, but cannot verify the call source is authorized to use the calling number. An example of this use case is a telephone number behind an enterprise PBX. • **Gateway Attestation (C)** — The service provider has authenticated from where it received the call, but cannot authenticate the call source. An example of this case would be a call received from an international gateway. As one example, the SIP Identity header comprises information based on and/or reflects a security determination:

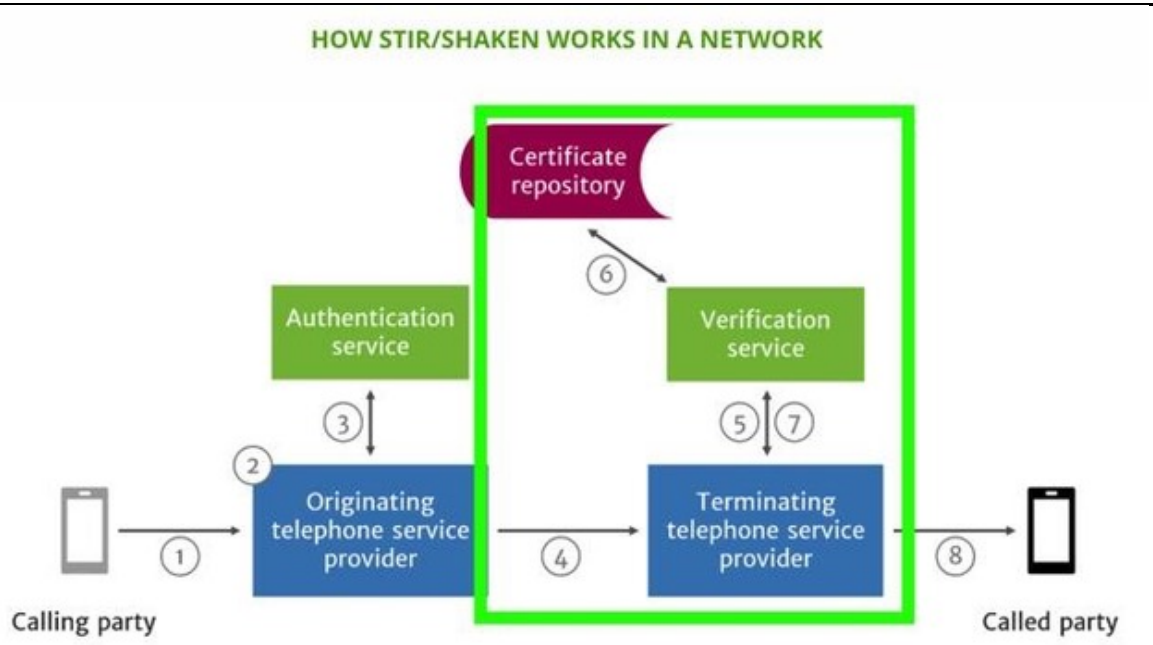
EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

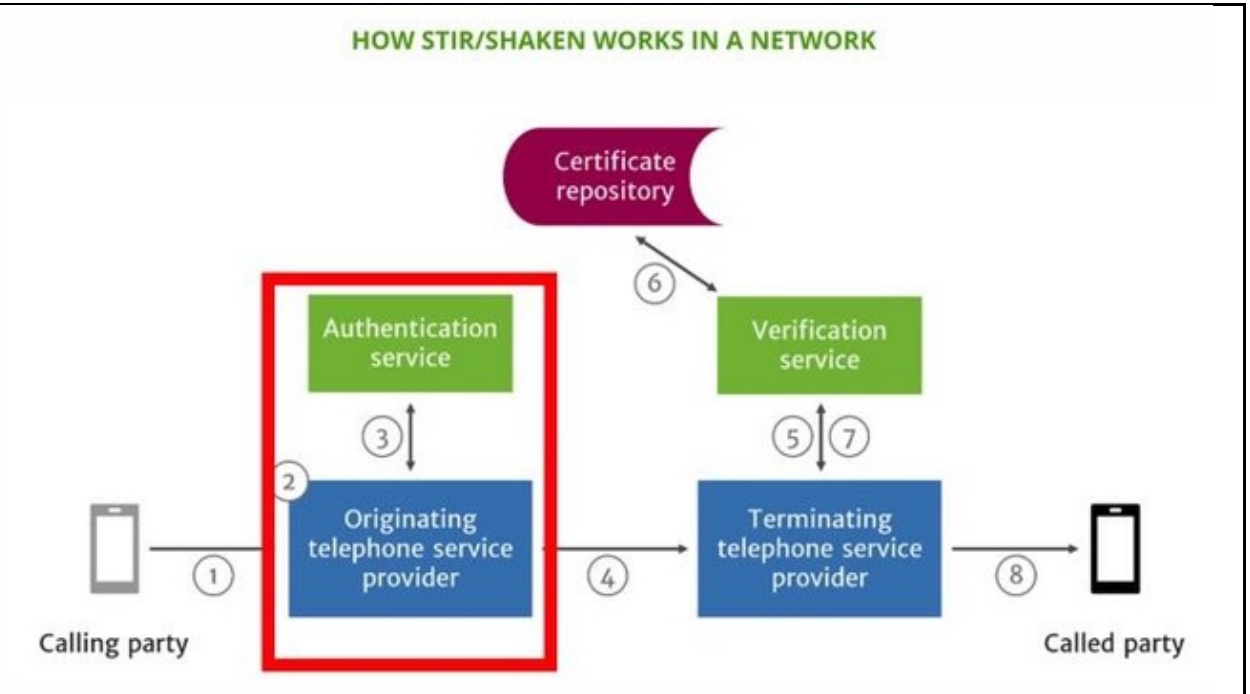
	3. The originating telephone service provider uses the authentication service to create a SIP Identity header. The authentication service could be a third-party service hosted in the cloud a software application integrated with the telephone service provider's softswitch or Session Border Controller (SBC). The SIP Identity header contains the following data: • Calling number • Called number(s) • Current timestamp • Attestation level • Origination identifier 4. The SIP INVITE with the SIP Identity header is sent to the terminating telephone service provider. In addition, the Identity token may be sent across the internet, out-of-band, to the terminating provider's Call Placement Service 5. The SIP INVITE with Identity header is passed to the verification service.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	6. The verification service obtains the digital certificate of the originating telephone service provider from the public certificate repository and begins a multi-step verification process. If all verification steps are successful, then the calling number has not been spoofed. • The SIP Identity header is base64 URL decoded and the details are compared to the SIP INVITE message. • The public key of the certificate is used to verify the SIP Identity header signature. • The certificate chain of trust is verified. 7. The verification service returns the results to the terminating service provider's softswitch or SBC. 8. The call is completed to the called party. 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.
17[e] and based at least in part on the security determination, selecting, at the verification service provider, an action comprising at least one of blocking the communication, requesting additional	The Accused Instrumentalities comprise computer instructions instruct for, based at least in part on the security determination, selecting an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication. For example, AT&T's Robocall Mitigation system(s), Call Protect system(s) and service(s), ActiveArmor, the ActiveArmor mobile application, and Defendants' use of STIR/SHAKEN, alone and/or in combination, are configured to determine if a given call should be blocked, connected, or

authentication, and permitting the communication.	if additional authentication information is required. *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 should be connected or blocked)): AT&T Active Armor (Call Protect) – High Level Architecture  As one example, the Accused Instrumentalities comprise computer instructions for selecting an action based on the SIP Identity header. As one example, the action may be selected in the steps indicated by the green box below. *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/):

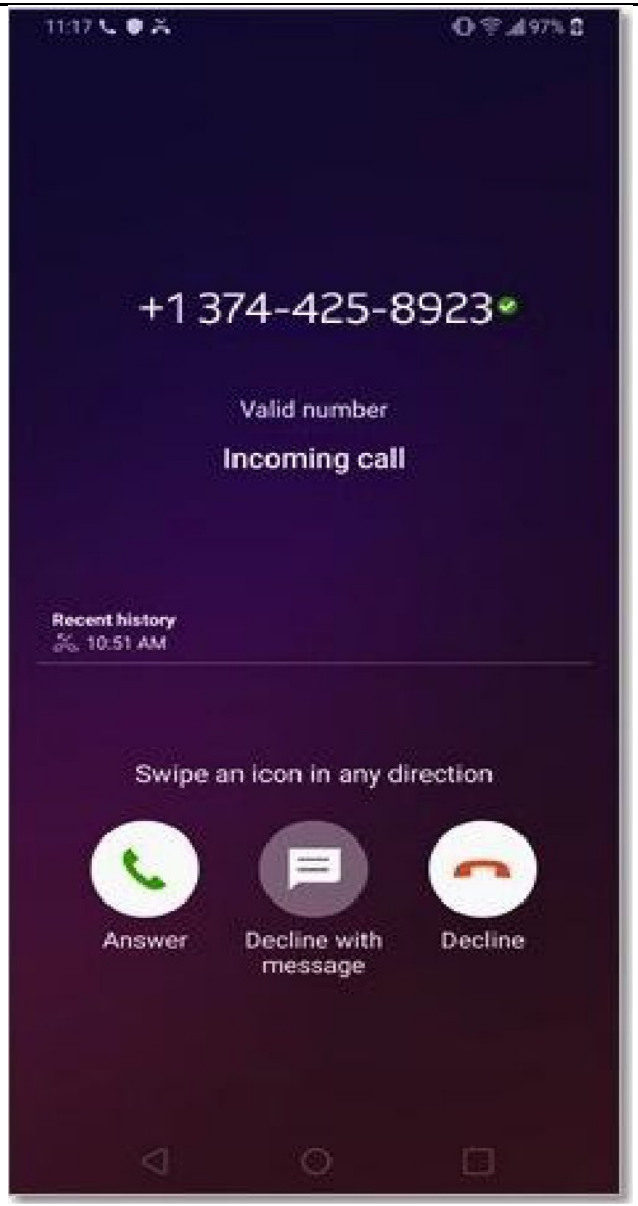
	 As another example, the Accused Instrumentalities are capable of selecting an action based on the SIP Identity header. As one example, the action may be selected using the components, functionality, and/or processes indicated by the red box below:



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

The action selected comprises at least one of blocking the communication, requesting additional verification, and permitting the communication:

	6. The verification service obtains the digital certificate of the originating telephone service provider from the public certificate repository and begins a multi-step verification process. If all verification steps are successful, then the calling number has not been spoofed. • The SIP Identity header is base64 URL decoded and the details are compared to the SIP INVITE message. • The public key of the certificate is used to verify the SIP Identity header signature. • The certificate chain of trust is verified. 7. The verification service returns the results to the terminating service provider's softswitch or SBC. 8. The call is completed to the called party. As one example, the communication is permitted in Step 8 above. *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/). As another example, the Accused Instrumentalities permit the call or permit the call and convey an assurance to a callee associated with the call. *See, e.g.*, RQ-ATT0000024-RQ-ATT0000026 (https://about.att.com/story/2019/call_validation_displays.html):

	 +1 374-425-8923 Valid number Incoming call Recent history 10:51 AM Swipe an icon in any direction Answer Decline with message Decline

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.

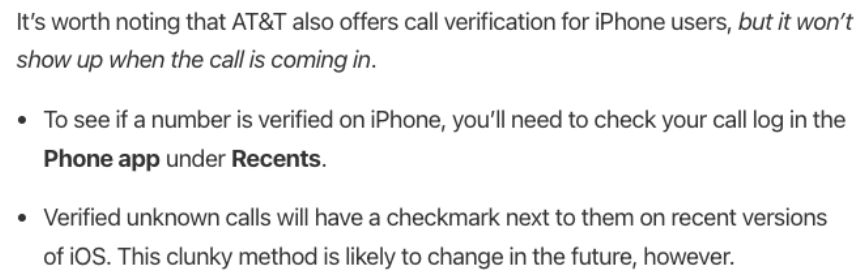
Here are some other key points:

- 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.

Furthermore, caller identification authentication and verification technology, including without limitation AT&T's Robocall Mitigation system(s), Call Protect system(s) and service(s), ActiveArmor, and the ActiveArmor mobile application are capable of detecting, blocking and preventing SPAM, fraudulent and spoofed phone calls.

See also RQ-ATT0000088-RQ-ATT0000090 (https://www.idropnews.com/news/fast-tech/att-will-

warn-you-of-incoming-robocalls-but-not-on-iphone/125657/):

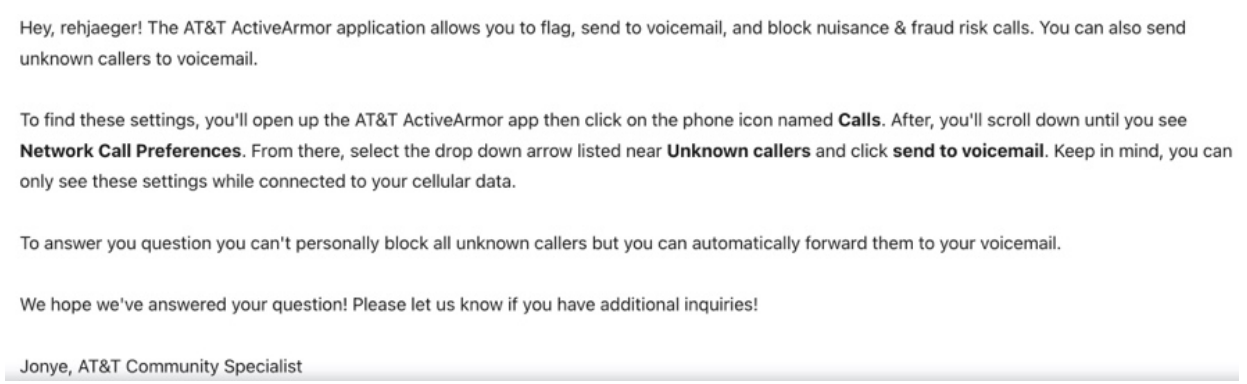


It's worth noting that AT&T also offers call verification for iPhone users, *but it won't show up when the call is coming in*.

- 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 also RQ-ATT0000161-RQ-ATT0000163 (https://www.att.com/device-support/article/wireless/KM1403775/Apple/iPhone13/).

As another example, based at least in part on the security determination the Accused Instrumentalities indicate a failure to confirm to the callee the identity of the caller and/or blocks the call. *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 you 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

As one example of an action, based at least in part on the security determination associated with the inter-network and intra-network call, the Accused Instrumentalities block a call. *See, e.g.*, RQ-

ATT0000153-RQ-ATT0000160 (https://www.att.com/wireless/what-is-activearmor-security/):

What are the benefits of AT&T ActiveArmor?

Customers should download the free AT&T ActiveArmor mobile security app to customize their robocall protection, manage nuisance calls, and create their own personal block list. Additionally, with AT&T ActiveArmor advanced, customers can secure their devices and personal data plus receive data breach alerts within the app.

Download to activate the free app and services for an extra layer of protection that helps you easily secure your data, manage nuisance calls, and more.

- **24/7 automatic fraud call blocking:** Detects and blocks calls from likely fraudsters before they reach you.
- **Spam call blocking:** Blocks or sends calls to voicemail if identified as a Spam Risk.
- **Nuisance call alerts:** Labels potential nuisance calls from telemarketers, surveys, and more.
- **Spam call routing:** Choose call categories to accept, block, or send to voicemail.
- **Unknown calls to voicemail:** Automatically sends callers to voicemail if they're not in your address book and blocks other numbers in your personal block list.
- **Block all texts from email:** Block all email-originated texts from your phone.
- **Personal block list:** Add individual unwanted callers to your own block list.
- **Device security:** Helps protect your data from mobile threats.
- **System update:** Keep up to date with operating system changes with reminders.
- **Breach reports:** Get alerts about company data breaches, along with helpful tips.

See also RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/):



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

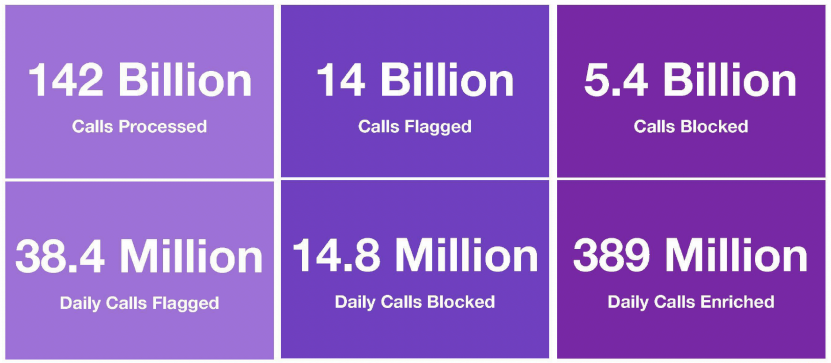
Digital Phone Call Protect features

Here's what you get with Digital Phone Call Protect[1]:

- **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, 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

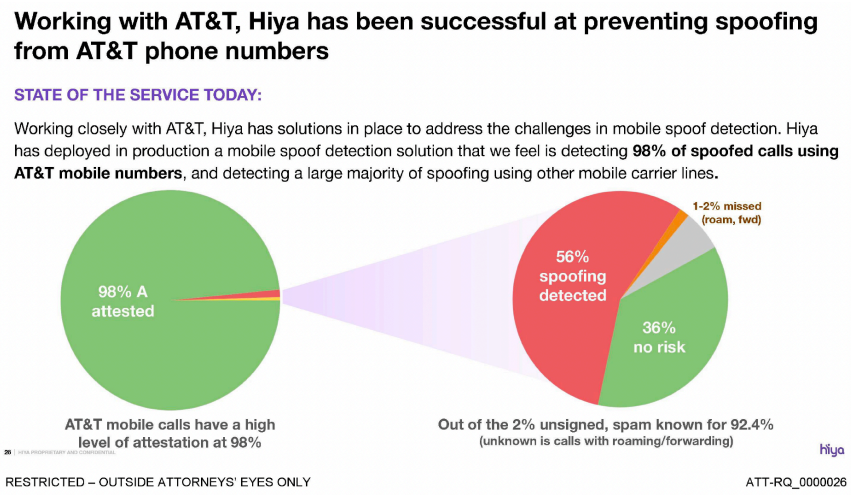


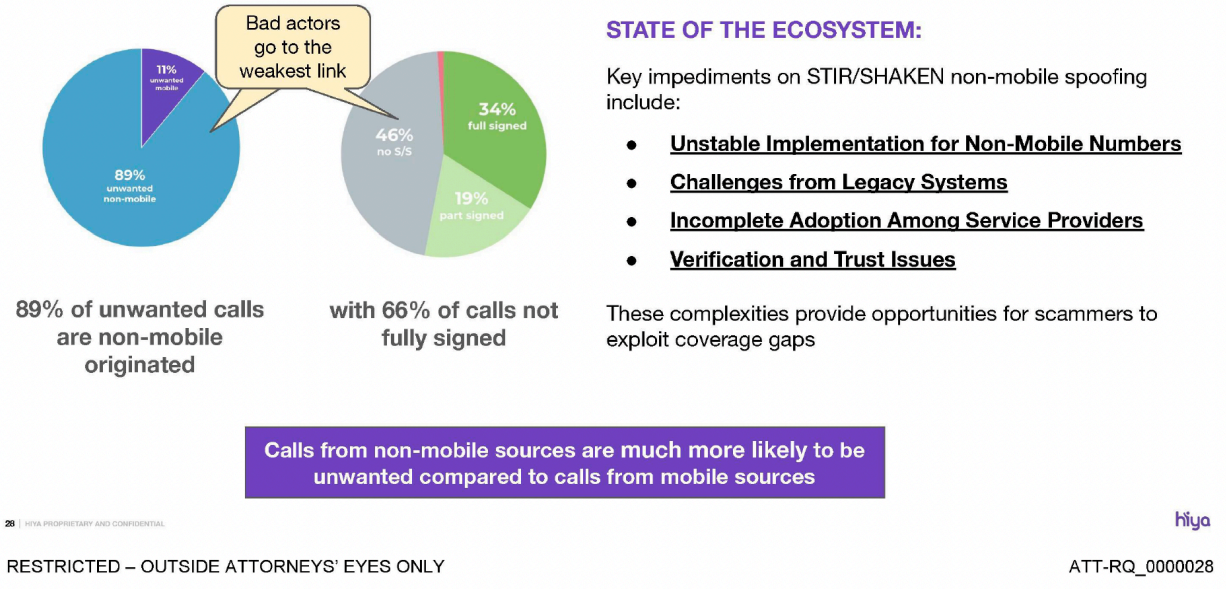
3 | HIYA PROPRIETARY AND CONFIDENTIAL

Hiya

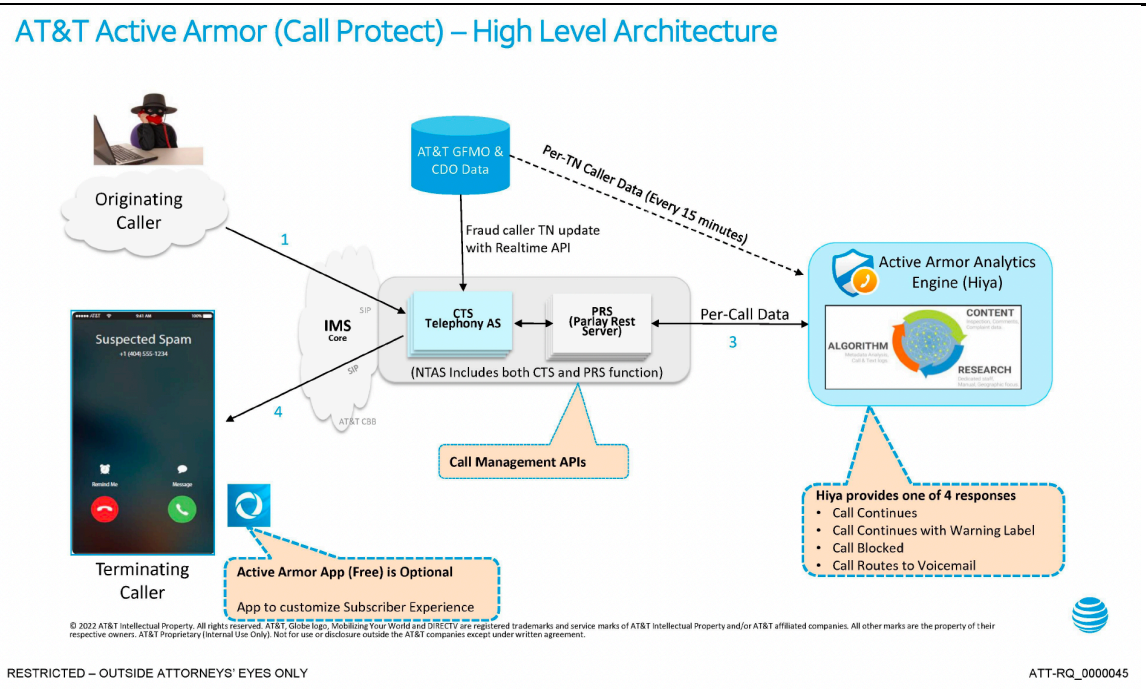
RESTRICTED – OUTSIDE ATTORNEYS' EYES ONLY

ATT-RQ_0000003

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



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 should be connected or blocked)):

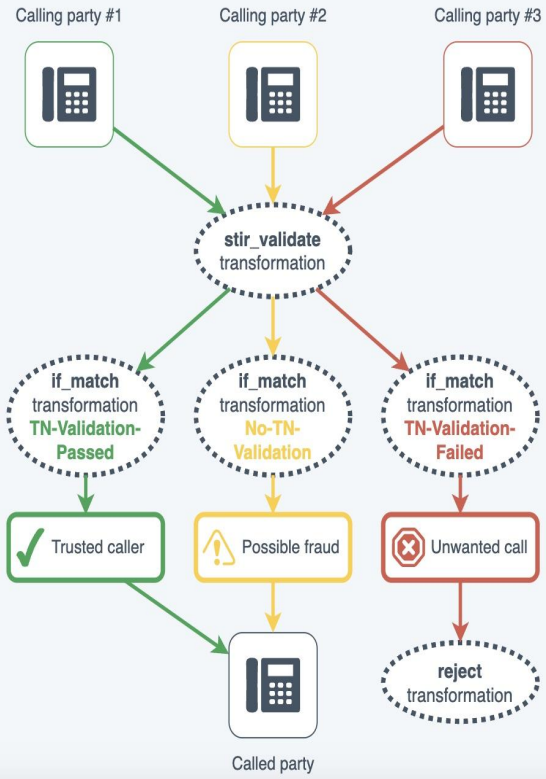


See also RQ0001940-RQ0001955 (https://www.carrierx.com/documentation/how-it-works/stir-shaken#verification-examples):

Verification Examples

The `stir_validate` transformation is normally not used all by itself. You can use it to verify the call signature and then use the output data with other transformations to manage the further call behavior.

An example of such a behavior can look like this:



See also RQ-ATT0000135-RQ-ATT0000136 (https://about.att.com/story/2021/robocalls.html):

	AT&T's approach works for business and consumer lines – wired or wireless. We're on track to *double* last year's numbers because of our *triple*-barreled protection: 1. AT&T Call Protect gives wireless customers automatic fraud blocking and suspected spam alerts. 2. Our global fraud team runs an additional program that blocks fraud calls to every type of AT&T phone service. 3. STIR/SHAKEN, a new call authentication technology, is now boosting both programs with extra data for detection and accuracy. 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 computer program product of claim 17, wherein the information transmitted by the second device is obtained via a backchannel that is different from the communications connection.	Within the Accused Instrumentalities the information transmitted by the second device is obtained via a backchannel that is different from the communications connection. As an example, the information transmitted by the second device is obtained via a connection or channel that uses the same type of path as the communications connection but different protocols. As another example, the information transmitted by the second device is obtained via a channel or connection that follows a different route and/or data flow as the communications connection. As another example, the information transmitted by the second device is encoded within the same type of path as a communications connection or the information transmitted by the second device is not encoded and is obtained via an encoded primary communication channel. As another example, the information transmitted by the second device is obtained via a communications connection. As an example, the Accused Instrumentalities use other backchannel methods, such as SMS, WiFi, or Internet data in the verification service. For example, the communication includes a component

	that is difficult to predict by a potential attacker, such as a serial number, a counter, a pseudo-random or random number, a number specific to the session or the phone, or any other appropriate component value. As yet another example, the AT&T networks use an encoded primary communication channel so that the backchannel is not a separate channel. As one example, the AT&T Networks rely on an encoded primary channel included in the SIP Identity header. As a separate example, this encoded primary channel is accomplished with an AT&T mobile application, such as the ActiveArmor mobile application. RQ-ATT0000139-150 (https://www.att.com/legal/terms.activeArmorMobileSecurity.html). For example, in the Accused Instrumentalities, one communication channel can be used by the calling party device to make the call and a different communication channel, including for example a second communication channel accomplished with, initiated by, or used by the calling party's device, the called party's device, and/or an AT&T mobile application on the calling party's and/or called party's device, such as the ActiveArmor mobile application, can be used to obtain the information transmitted by the second device. RQ-ATT0000139-RQ-ATT0000150 (https://www.att.com/legal/terms.activeArmorMobileSecurity.html). For example, ATT discloses that it keeps information transmitted by the second device confidential and/or obtains information from third-parties. *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 ×

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).

See also 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).

See, ATT-RQ_0000042, -43, -44 (evidencing information such as 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 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

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

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:

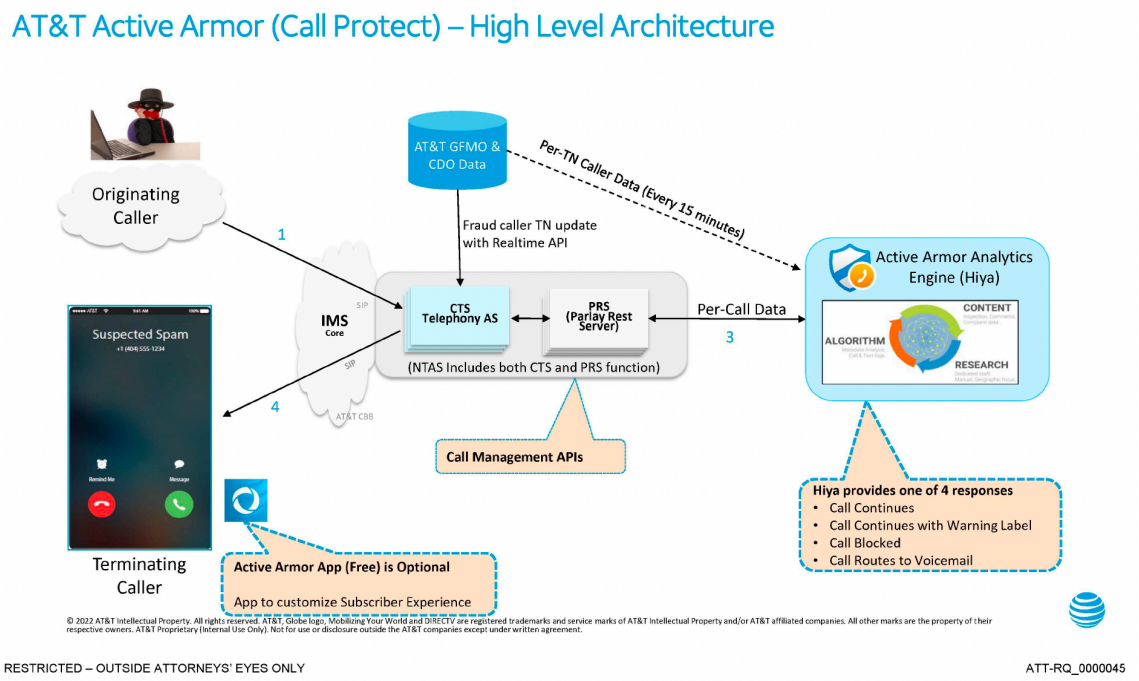
- FirstNet
- CRU
- COU
- Customers who have rate-plan-included Advanced service.
- Cricket
- Prepaid
- Wireless Home Phone

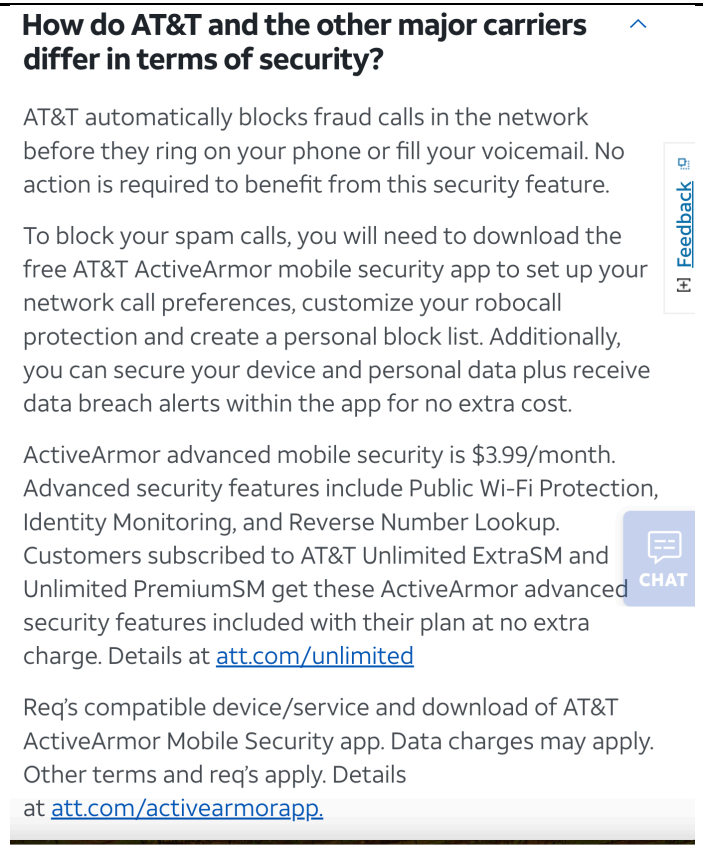
ActiveArmor Application Data

TN from Device Address Book - Hashed (shared only with explicit subscriber consent)
Device OS
ActiveArmor Version Information

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

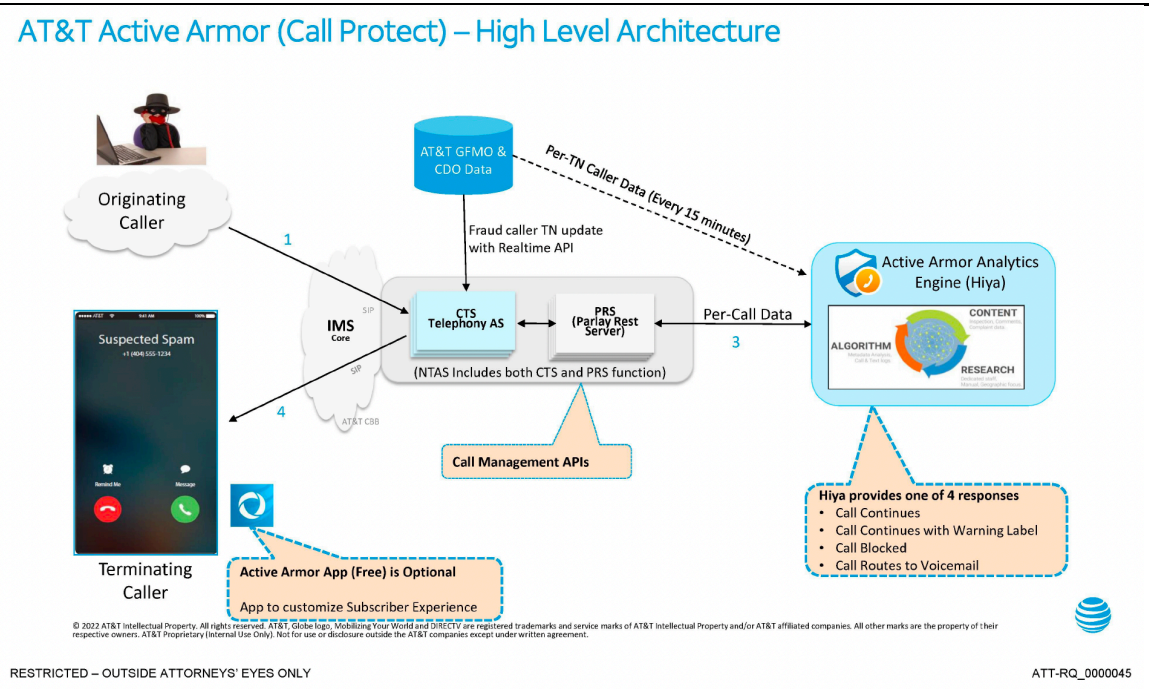
	AT&T* and T-Mobile today began rollout of cross-network call authentication based on SHAKEN/STIR standards – another big step toward protecting consumers from unwanted robocalls. SHAKEN/STIR technology lets consumers know that an incoming call is really coming from the number listed on the caller ID 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. 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 computer program product of claim 17, wherein based at least in part on the security determination, the verification service provider is further configured to convey an assurance to a recipient associated with the communications channel.	Within the Accused Instrumentalities, based at least in part on the security determination, the verification service provider is further configured to convey an assurance to a recipient associated with the communications channel. *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 should be connected or blocked)):  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/).



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

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 should be connected or blocked)):



As one example, based at least in part on the security determination associated with the inter-network and intra-network call, the Accused Instrumentalities convey and/or are configured to 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):

	 +1 374-425-8923 Valid number Incoming call Recent history 10:51 AM Swipe an icon in any direction Answer Decline with message Decline

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.

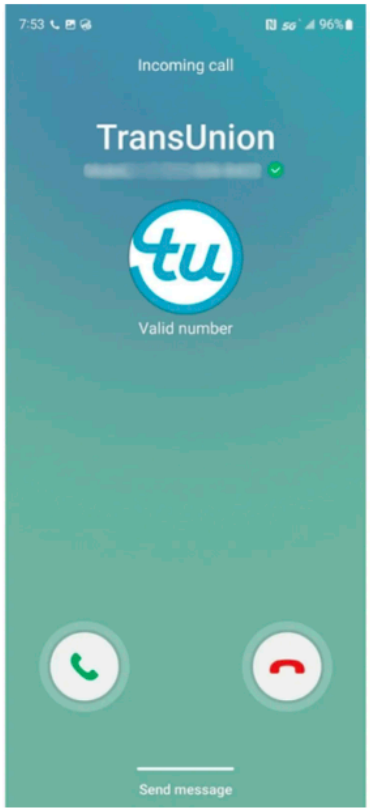
"This is another step to tame annoying, unwanted robocalls," said Kevin Petersen, AT&T senior vice president, Postpaid Wireless Products. "In the coming year, we'll continue to take more steps and put more pressure on the bad guys."

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.

EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

	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 also* 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.

See also RQ-ATT0000161-RQ-ATT0000163 (https://www.att.com/device-support/article/wireless/KM1403775/Apple/iPhone13/).

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 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 not conveying with an allowed communication 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. *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 you 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.

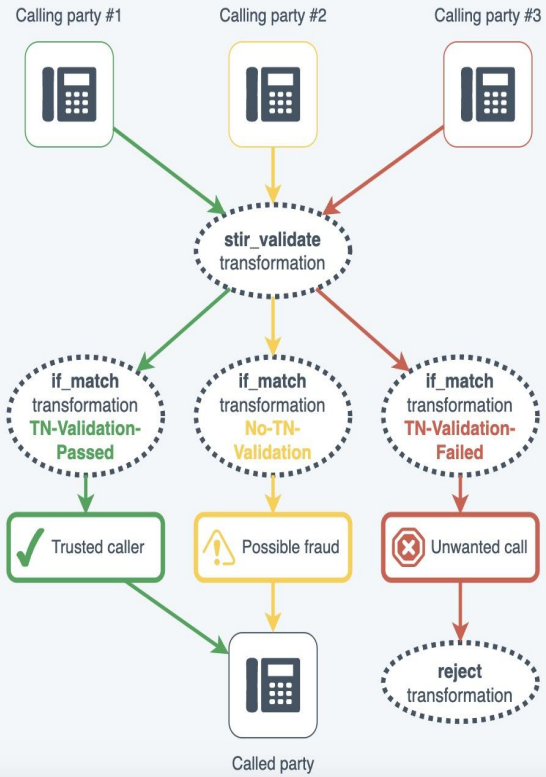
For example, a call that is illegally "spoofed" – or shows a faked number – will fail the SHAKEN/STIR Caller ID verification and will not be marked as verified. By contrast, verification will confirm that a call is really coming from the identified number or entity. More calls will be verified over time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

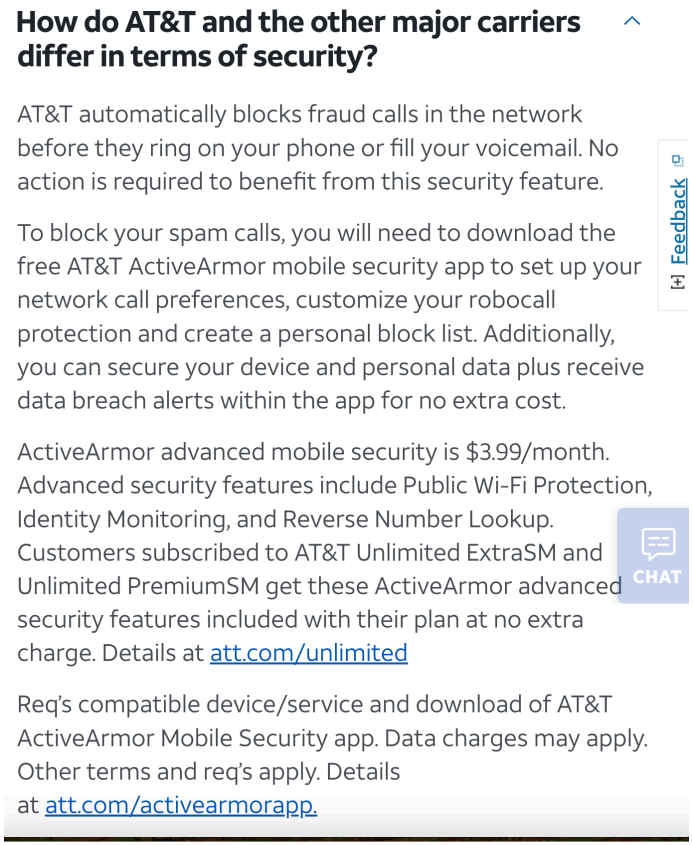
The FCC has recommended SHAKEN/STIR standards to digitally validate phone calls. The acronym stands for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR).

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.

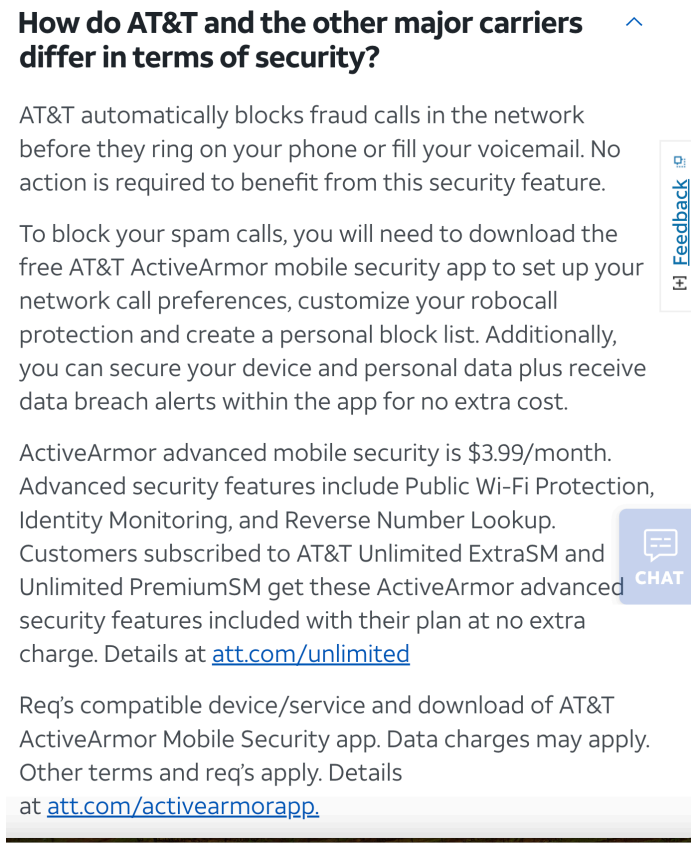
EX-1007
AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
AND NOKIA OF AMERICA CORPORATION v RIGHTQUESTION, LLC

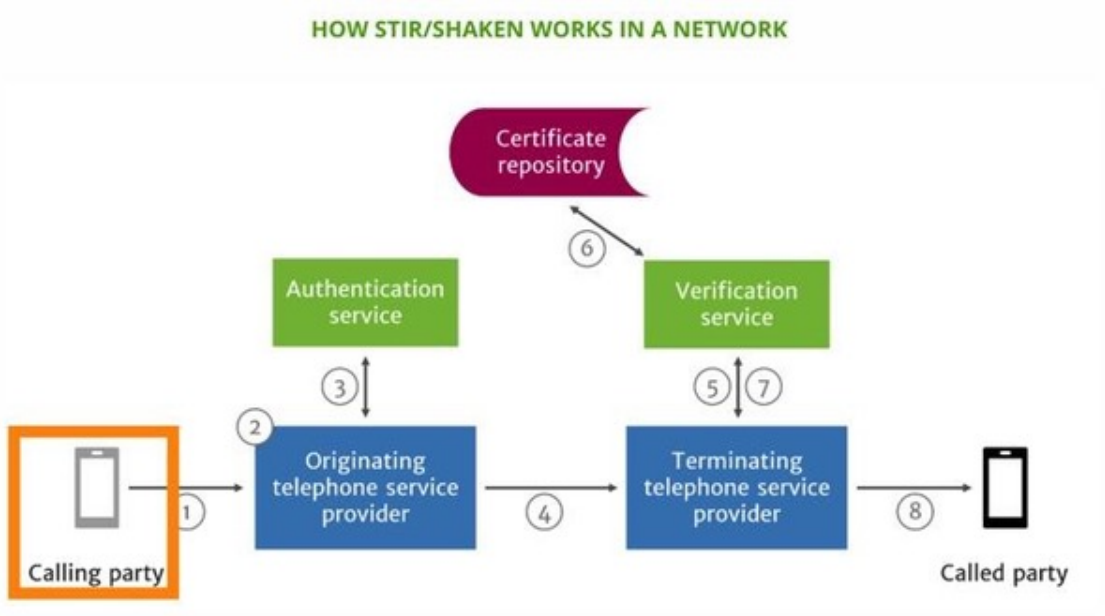
	See also RQ0001970 (https://sti-ga.atis.org/resources/). The terminating network conveys the verification result to the called user by including a "verstat" parameter in the From and/or P-Asserted-Identity header fields of the INVITE request sent to the called endpoint device, as defined in [TS 24.229]. • 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. *See, e.g.*, RQ0001940-RQ0001955 (https://www.carrierx.com/documentation/how-it-works/stir-shaken#verification-examples):

	Verification Examples The `stir_validate` transformation is normally not used all by itself. You can use it to verify the call signature and then use the output data with other transformations to manage the further call behavior. An example of such a behavior can look like this:  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 computer program product of claim 17, wherein the	Within the Accused Instrumentalities the information transmitted by the second device is obtained

communications connection is associated with at least one of email, SMS, instant message, and a phone call.	via a backchannel that is different from the communications connection. For example, within the Accused Instrumentalities the communication connection is associated with a phone call. 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/).  *See also* RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security).

	For another example, within the Accused Instrumentalities the communication connection is associated with SMS and/or instant message. *See, e.g.*, RQ-ATT0000046-RQ-ATT0000048 (https://about.att.com/blogs/2023/activearmor-text-blocking.html): *AT&T ActiveArmor Offers New Text-Filtering Features for Even More Protection* We know that spam texts and robocalls are a pain. That's why we're pleased to give important updates on our spam-fighting AT&T ActiveArmor℠. Our new and better network filters **blocked more than 1 billion spam text messages** from reaching customers in July – our highest-ever total. Every month since then, customers have collectively reported one-third fewer spam texts getting through to their phones. We block spam texts for everyone on our network – you don't have to do a thing. But if you download the free AT&T ActiveArmor mobile security app, you can now get even more control of incoming text messages: • **You can block email-to-text messages** – a consistent source of spam. These are texts that appear to come from an email address.[1] Just review the terms and toggle a switch on the ActiveArmor app. As one example, the verification service verifies the corresponding communication identifiers for the email, SMS, instant message, or phone call respectively. As another example, the initial communication path used by the device to contact a verification service includes channels such email and SMS, instead of a phone call. 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 computer program product of claim 17, wherein the first device comprises at least one of a smartphone, a tablet, a PC, a phablet, and a wearable device.	Within the Accused Instrumentalities the information transmitted by the second device is obtained via a backchannel that is different from the communications connection. 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/).  *See also* RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security).

	As one example, the first device ("calling party", indicated with orange box below) comprises at least one of a smartphone, a tablet, a PC, a phablet, and a wearable device. *See, e.g.*, RQ0002113-RQ0002120 (https://transnexus.com/whitepapers/understanding-stir-shaken/); RQ-ATT0000035-RQ-ATT0000041 (https://www.att.com/security/).  For example, within the Accused Instrumentalities, the first device comprises but is not limited to the following smartphones, smartwatches, and/or tablets. *See, e.g.*, RQ-ATT0000105-RQ-ATT0000117 (https://www.att.com/scmsassets/support/wireless/devices-working-on-att-network.pdf); *see also* RQ-ATT0000118-RQ-ATT0000119 (https://www.att.com/support/how-to/wireless/esim-get-started/). As another example, within the Accused Instrumentalities, the first device comprises but is not limited to a PC. For example, AT&T advertises providing instant messaging, Voice over IP (VOIP) calling, as well as other features, on a desktop computer. *See, e.g.*, RQ-ATT0000180-RQ-ATT0000206 (https://asecare.att.com/tutorials/att-collaborate-app-desktop). As another example, AT&T discloses that the Accused Instrumentalities, including but not limited to AT&T ActiveArmor, are compatible with at least smartphones, wearable devices (including but not limited to Apple smartwatches), and iPod Touch. *See* RQ-ATT0000049-RQ-ATT0000050 (https://apps.apple.com/us/app/at-t-activearmor/id1218465964):

Information

Seller
AT&T Services, Inc.

Size
138.1 MB

Category
Utilities

Compatibility
iPhone
Requires iOS 13.0 or later.

iPod touch
Requires iOS 13.0 or later.

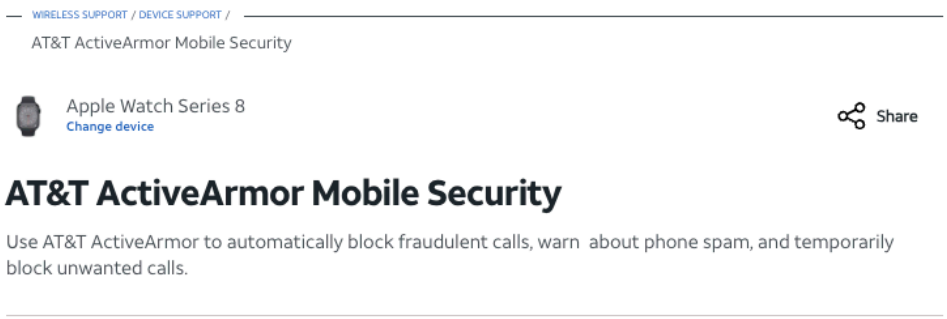
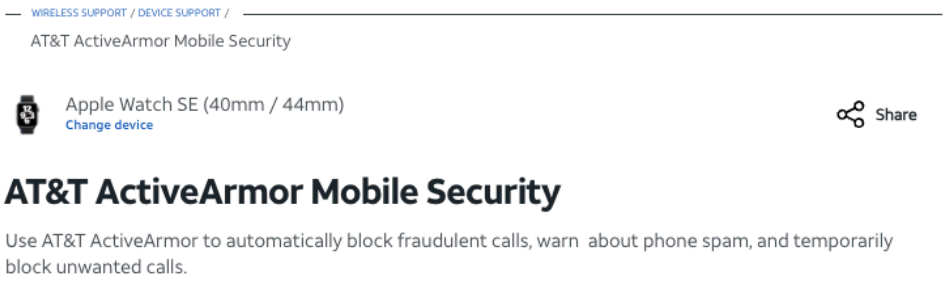
Languages
English

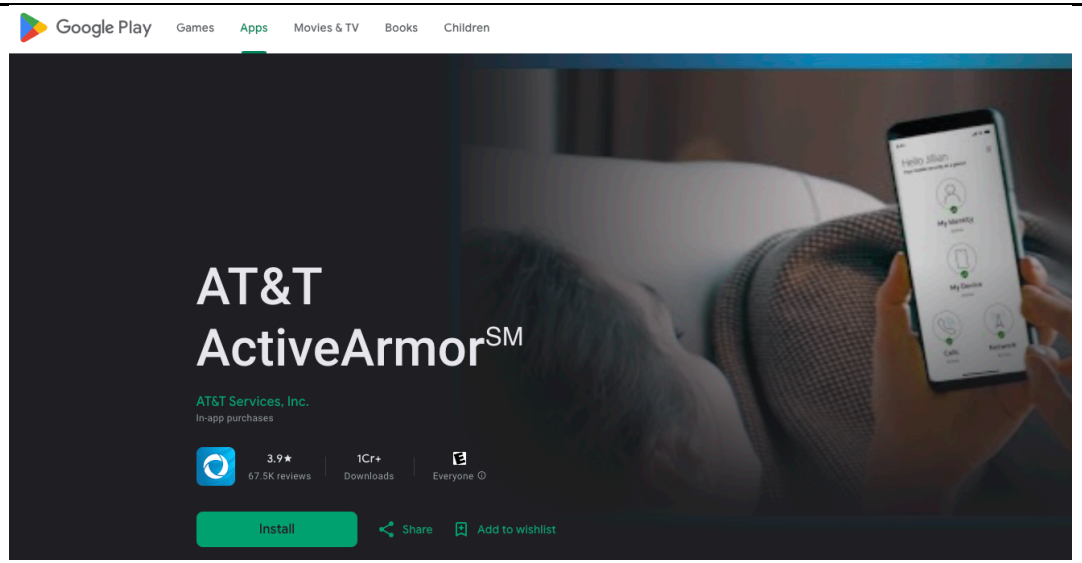
Age Rating
4+

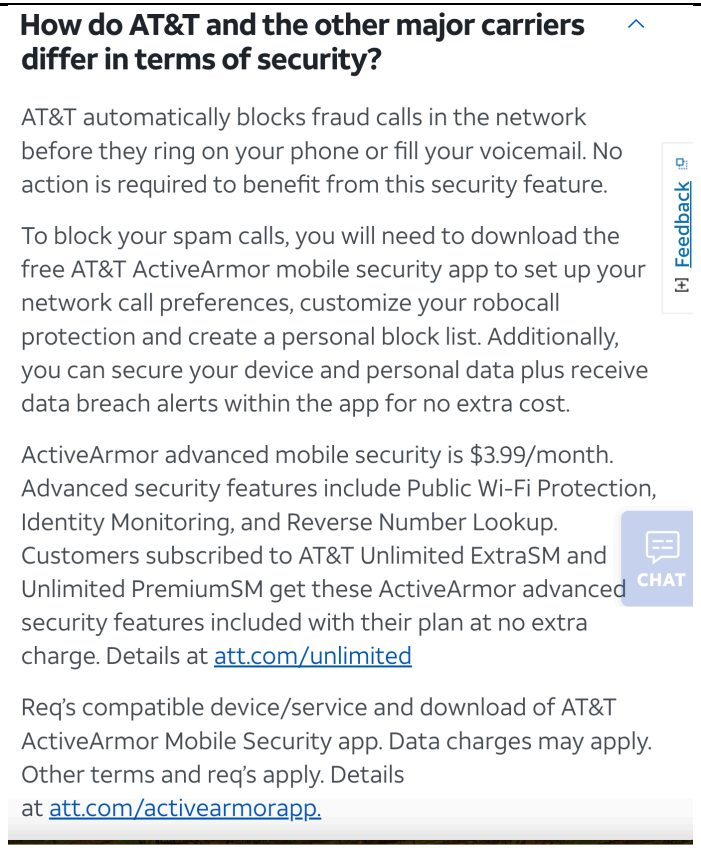
Copyright
©2024 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property. All other marks are the property of their respective owners.

Price
Free

In-App Purchases
1. Plus

	See RQ-ATT0000007-RQ-ATT0000011 (https://www.att.com/device-support/article/wireless/000092356/Apple/WatchSeries8/):  *See* RQ-ATT0000001-RQ-ATT0000006 (https://www.att.com/device-support/article/wireless/000092356/Apple/WatchSE44mm/):  *See* RQ-ATT0000042-RQ-ATT0000045 *AT&T ActiveArmor on Google Play Store*

	 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 computer program product of claim 17, wherein enrolling the first device is based at least in part on at least one of PIN verification, password verification, knowledge based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number	Within the Accused Instrumentalities enrolling the first device is based at least in part on at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a 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/).



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

For example, the Accused Instrumentalities use PIN verification, including as part of activating and/or accessing the Accused Instrumentalities, including but not limited to password, fingerprint, and/or Face ID. *See, e.g.*, RQ-ATT0000099-RQ-ATT0000104 (https//www.att.com/device-support/article/wireless/KM1324197/Samsung/SamsungSMG975U/):

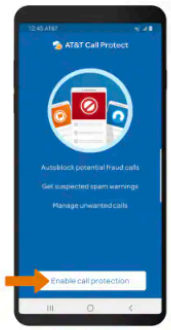
Access call protect

1. Navigate to and select the **AT&T Call Protect app**.

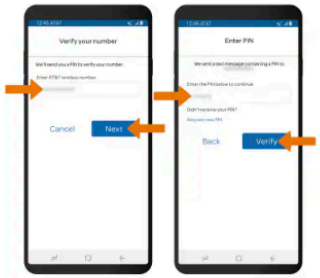
Note: AT&T Call Protect allows you to automatically block fraudulent calls, warns you about phone spam, and temporarily blocks unwanted calls.

2. Select **Enable call protection**.

*Note: Review the permissions, then select **ALLOW**.*



3. Enter your **myAT&T wireless number**, then select **Next**. Enter the **PIN** sent via text, then select **Verify**.



4. Review the Terms & Conditions, then select **I agree**. Select **Continue**.

*Note: Select **ALLOW** to give permission to the app to access your contacts.*

For further example, the Accused Instrumentalities collect and use password verification, knowledge-based authentication, geolocation information, credit card information validation, and/or a check of a least one of a name, an address, and a phone number, including for enrolling a first device. *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.

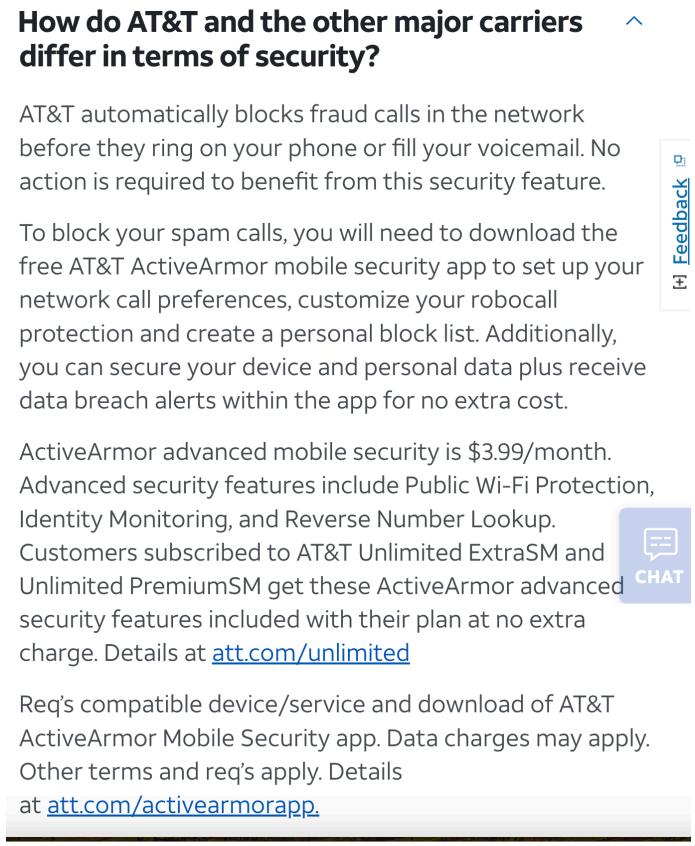
How we use your information ×

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).

See also 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). As one example, enrolling a first device is based in part or in whole on PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and/or a check of at least one of a name, an address, and a phone number. As yet another example, enrolling is based upon information that is included 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 23. The computer program	Within the Accused Instrumentalities the additional authentication comprises at least one of PIN

product of claim 17, wherein the additional authentication comprises at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number.	verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a 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/).  *See also* RQ-ATT0000012-RQ-ATT0000023 (https://sustainability.att.com/priority-topics/network-data-security).

	As one example, requested additional authentication comprises PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and/or a check of at least one of a name, an address, and a phone number. As another example, additional authentication comprises of information that is included in the SIP INVITE. As another example, the initial enrollment of a device by a relying party or the verification service, as well as occasional re-enrollments sessions, are combined with one or more additional authentication tools including PIN verification, password verification, Knowledge Based Authentication, geolocation information, or verification tools such as Name+Address+Phone checks or credit card information validation. Such additional authentication can also be combined with an ANI verification session. 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.