

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON
WIRELESS, AND NOKIA OF AMERICA CORPORATION,

Petitioner,

v.

RIGHTQUESTION, LLC,
Patent Owner.

Case IPR2025-00362
Patent 11,005,989 B1

**PATENT OWNER'S PRELIMINARY RESPONSE
TO PETITION FOR INTER PARTES REVIEW**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. FACTUAL BACKGROUND	3
A. The '989 Patent	3
B. Har	6
C. Miller	10
III. INSTITUTION SHOULD BE DENIED BECAUSE THE PETITION FAILS TO SHOW A REASONABLE LIKELIHOOD THAT THE SOLE GROUND RENDERS ANY CLAIM OBVIOUS	12
A. The Sole Ground Is Not Shown To Satisfy The “Receiving” Step. ...	14
1. The Petition Relies On An Incorrect Interpretation Of “ <i>Information Pertaining To A Call</i> ”	15
a. “ <i>Pertaining To A Call</i> ” Does Not Simply Mean That The Information is “ <i>In Response To</i> ” Initiation Of A Call.....	15
b. “ <i>Information Pertaining To A Call</i> ” is Not Met Simply By A Request Being Sent For Authentication Of A Call.....	18
2. Har’s Public And Private Key Are Not “ <i>Information Pertaining To A Call Including (1) A Value Generated Based At Least In Part On Information Associated With The Calling Device.</i> ”	20
3. Har’s Message Does Not Use Its Caller Device’s Private Key.	28

4.	Miller Does Not Add “Information Pertaining To [The] Call.”	30
5.	The Petition Fails To Show That Har/Miller Teach Receiving “ <i>Information Pertaining To The Call Including . . . (2) A Score Generated For The Calling Device, The Score Indicating A Validity Of A Phone Number</i> ”	32
a.	Har/Miller Are Not Shown To Teach That The “Score” Is “Received”.	32
b.	Har/Miller Are Not Shown To Teach Receiving <i>Both “(1) A Value Generated Based At Least In Part On Information Associated With The Calling Device, And (2) A Score Generated For The Calling Device, The Score Indicating A Validity Of A Phone Number”</i>	34
c.	Miller’s “Biometrics” Do Not Add This Limitation.	37
d.	Har/Miller Are Not Shown To Teach A “Score Indicating A Validity Of A Phone Number.”	39
B.	The Petition Fails To Show That The Sole Ground “ <i>Performs A Security Determination Based At Least In Part On The Score ... And At Least In Part By Verifying The Value</i> ”.	42
C.	Har And Miller Are Not Shown To Teach Or Suggest Any Of The Remaining Claims 2-28.	44
IV.	CONCLUSION	45

EXHIBIT LIST	
2001	Memorandum Claim Construction Opinion and Order, Civil Action Nos.: 2:24-cv-00091-JRG and 2:24-cv-00094-JRG (E.D. Tex.) [Markman-Order]
2002	Fifth Amended Docket Control Order, Civil Action Nos.: 2:24-cv-00091-JRG and 2:24-cv-00094-JRG (E.D. Tex.) [5 th -Amended-DCO]
2003	Michelle Umberger & Lissa Koop, <i>District court stays: a review of the past 12 months</i> , ManagingIP.com [2016-Stays-Report]
2004	Scott R. Boalick, USPTO Memorandum, Guidance on USPTO’s recission of “Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation” [March-24-2025-USPTO-Memorandum]
2005	U.S. District Court – Judicial Caseload Profile (Texas Eastern) [Judicial-Caseload-Profile-EDTX]
2006	<i>RightQuestion, LLC v. Verizon Communications Inc., et al.</i> , No. 2:24-cv-00091-JRG, Docket Control Order (June 14, 2024) [June-14-2024-DCO]
2007	<i>USPTO rescinds memorandum addressing discretionary denial procedures</i> , USPTO (Feb. 28, 2025), https://www.uspto.gov/about-us/news-updates/uspto-rescinds-memorandum-addressing-discretionary-denial-procedures [Feb.-28-2025-Recission-Update]
2008	“DEFENDANTS’ P.R. 3-3, 3-4, AND 3-6(b) AMENDED INVALIDITY CONTENTIONS AND SUBJECT MATTER ELIGIBILITY CONTENTIONS,” served Nov. 14, 2024 in <i>RightQuestion, LLC v. Verizon Business Network Services LLC, et al.</i> , No. 2:24-cv-00091-JRG [Amended-Invalidity-Contentions]

2009	L. Hall, “Relentless robocalls anger consumers,” Consumer Action News (Spring 2019) [Relentless-Robocalls]
2010	[reserved]
2011	Merriam-Webster Dictionary – definition & meaning – <i>pertain</i> ; <i>pertained</i> ; <i>pertaining</i> ; <i>pertains</i>

I. INTRODUCTION

The Petition should be denied because it fails to demonstrate a reasonable likelihood that any challenged claim will be found unpatentable if institution review is granted. The Petition relies on a single ground (“Har” in view of “Miller”) to challenge claims 1-28 under 35 U.S.C. § 103. Har and Miller, however, fail to teach or suggest multiple limitations of each independent claim. Furthermore, although the Petition argues that it would have been obvious to modify Har in combination with Miller to add missing limitations, it fails to substantiate any reason for the ordinary artisan in the art at the time of the invention to add the missing limitations necessary to meet the claims.

First, the sole ground is not shown to satisfy the “*receive*” limitations. The Petition repeatedly relies on unsupportably broad interpretations of the claim language to stretch the disclosures of Har and Miller in the direction of the materially different claimed invention. The Petition also mischaracterizes the intrinsic evidence to suggest that servers’ encryption keys and users’ signature keys necessarily “pertain[] to” particular phone calls, even though these static keys in the cited art are not like the unpredictable or unique call information described in the patent pertaining to the call, such as timestamps and phone numbers.

The Petition also fails to show that the sole proposed combination, Har/Miller, discloses the claimed “score indicating a validity of a phone number.”

The combination does not “receive” any such score: Miller is shown only to teach that its score is generated anew *in situ* for each alleged security determination. Furthermore, the proposed combination would receive a “value” and “score” both based on the same redundant information—one being a scoring of the other—and the Petition offers no reason that the ordinary artisan would have thought such redundancy tolerable, let alone obvious. The Petition’s alternative proposed modification, to use “biometrics” like face size for this value, would impose a kind of additional security barrier to network access, again without any showing that this would be considered welcome or tolerable, let alone obvious. Finally, the combination’s “score” is not shown to be “indicating the validity of a [phone] number” as the patent discloses and the claims require.

Second, the Petition fails to show the claimed “*security determination*” based on both the “*value*” and “*score*” above, for many of the same reasons.

In addition, the Board should exercise its discretion to deny the Petition for the reasons stated in Patent Owner’s Brief in Support of Discretionary Denial (Paper 8) filed on June 16, 2025, which is incorporated herein by reference.

This response is timely under 35 U.S.C. § 313 and 37 C.F.R. § 42.107(b), because it is filed within three months of the April 15, 2025, Notice of Filing Date Accorded to Petition and Time for Filing Patent Owner Preliminary Response. Paper 7.

This Preliminary Response raises only selected arguments sufficient to support denial of review. Patent Owner reserves all rights to present additional arguments and evidence to the extent necessary if institution is granted.

II. FACTUAL BACKGROUND

To orient the Board regarding the petitioned ground, this Section describes certain background facts concerning the patented invention and alleged prior art relevant to the arguments raised in this Preliminary Response.

A. The '989 Patent

U.S. Patent No. 11,005,989, entitled Validating Automatic Number Identification Data and filed on February 7, 2020, is a continuation and claims the benefit of the filing date of an application filed November 5, 2018, and further claims the benefit of the filing date provisional application No. 61/901,322 filed on November 7, 2013.

The invention of the '989 patent provides a solution to the problem of spoofing, as well as other fraudulent call practices like scams, spam, robocalls and the like. Spoofing can occur when a bad actor intentionally falsifies (“spoofs”) the identity of another caller’s device, thereby disguising the fraudulent caller’s true identity. *See, e.g.*, Ex. 1001 [’989 Pat.], 2:43-46, 10:14-20.

Spoofing is a pervasive problem. Americans received more than 47 billion robocalls in 2018 alone, many of which involved spoofed numbers. Ex. 2009

[Relentless-Robocalls] 1. Spoofing makes robocalls harder to detect and more likely to deceive. People are more inclined to answer a call that appears to come from their local area code, a known business, or even their own number. *Id.* Traditional call-blocking techniques, which often relied on blacklists or pattern recognition, could not keep pace with spoofers who frequently changed numbers or mimicked trusted sources.

As explained in the Background of the Invention of the '989 patent, “[d]etermining the trustworthiness of information used to identify entities involved in communications such as text messages (e.g., SMS), email, calls, and instant messaging can be challenging. For example, information such as Automated Number Identification (ANI) information can be spoofed by unscrupulous entities, making it difficult for caller identity information to be trusted [by callees]. As a result, organizations [and individuals] face high fraud risks, or employ resource-intensive measures in order to identify callers and senders of messages.” Ex. 1001 [’989 patent], 1:23-32.

The ’989 patent specification provides several examples of how to make a security determination. The claims of the patent describe a particular implementation in which one or more processors receive information pertaining to the call, including a value generated based at least in part on information associated with the calling device, and a score generated for the calling device, the

score indicating a validity of a phone number. *Id.*, e.g., 8:61-9:6, 9:34-37, 12:10-23.

FIG. 12 of the '989 patent shows an example environment of the claimed invention. As described, a phone call (1214) to a callee or relying party (1212) is initiated by a communication unit (1208). In the example shown, once the relying party (1212) answers the call (1214), the communication unit (1208) sends information to the relying party about the call, including, for example, one or more of a device identifier, call start time, and number called. Figure 2A also shows an example environment of the invention, in which contact (204) in the form of a call is initiated to a callee/relying party, and the callee receives the call and observes ANI or caller ID information that is used to verify the call made to the callee. *Id.*, 15:60-16:2. A security determination is made based on the validation of the information received. *Id.*, e.g., 16:6-10.

In an embodiment of the claimed invention, the system performs a security determination based at least in part on verifying the value included in the information pertaining to the call, and based at least in part on the score generated for the calling device. *Id.*, e.g., 10:6-20, 16:7-10; *see id.* at, e.g., 8:55-9:6. Based at least in part on the security determination, the system then, for example, conveys either an assurance or a failure to confirm to the callee associated with the call. *Id.*, e.g., 10:57-11:6; *see id.*, e.g., 10:21-25, 16:11-18.

The benefits of the claimed invention are significant. For example, by enabling real-time verification of caller ID information, the claimed invention helps restore confidence in answering phone calls. *Id.*, *e.g.*, 9:6-10, 12:3-9. Consumers can better trust that the number they see on their screen is accurate, and telecom providers can better filter out suspicious or fraudulent calls before they reach users. *Id.*, *see id.*, *e.g.*, 1:30-32, 10:66-11:6.

B. Har

The Petition relies on U.S. Patent Publication No. 2012/0144198, entitled User Authentication In A Mobile Environment, to challenge the claims of the '989 patent as obvious in combination with Miller. Pet., 5-6.

The relied-upon disclosures in Har and the '989 patent disclose different problems and solutions. Har does not mention spoofing: rather, Har states that it addresses security risks in a mobile environment where a mobile device user receives a call from someone who “identif[ies] himself,” but “there is no guarantee that the caller is who he says he is,” or when, on the other hand, a call is made by a genuine service provider but “it is difficult for a caller who calls a user to know if the person who answers the call is the person the caller is calling,” since the person “who answered the call” might be either “the account holder or someone else.” Ex. 1004 [Har], [0011]. Har teaches that such verifications (either of the calling or receiving person) are to be accomplished in one of two ways: either by successful

decryption of a sent message using a shared key, or, alternatively, by successful verification of a digital “signature” using a “private key.”

Har teaches that users may also volunteer other information, such as the user’s identity, to Har’s authentication server. *Id.*, [0018]. However, Har does not teach that such information may be used as an alternative method of authentication aside from either successful decryption or successful digital signature verification. Rather, “[i]f authentication of the user being authenticated was successful, the identity of the user being authenticated, any other information about the user in the authentication server’s data store and any information volunteered by the user requesting authentication can be sent to the user receiving the verification.” *Id.* (emphasis added); *see id.*, [0015]-[0016].

“For example,” Har explains, “a caller may identify himself as a service provider, offering a new service or a current promotion,” and “request sensitive personal information.” *Id.*, [0011].¹ To address such situations, Har’s objective is to use an authentication server to authenticate a first user to a second user, by authenticating a transmission by the first user to the authentication server by either

¹ In these examples set out in Har, any impersonation would be of a “service provider.” *Id.* Such situations may differ from “spoofing” of users or phone numbers addressed in the ’989 patent as discussed above. *See supra* Section II.A.

encryption using a secret, private key, or a signature such as using a digital certificate. *Id.*, [0012]-[0017], [0026]. The user to be authenticated may be prompted “for credentials,” the specific prompted credentials mentioned being “a password or personal identification number (PIN) code.” *Id.*, [0002], [0012]-[0019].

All embodiments of Har depend for authentication, for both **the person** making the call and **the person** receiving the call, on either decryption of the incoming message using a known key, or in the alternative, verification of a digital signature using known information about the user’s signature. *Id.*, *e.g.*, [0026], [0028]-[0030]. For example, Har expressly teaches that if its system is used to attempt to authenticate a sender’s transmission for a receiving party,

[i]f the decryption fails, the authentication of the sender’s transmission (and thus authentication of the identity of the sender) fails. If the digital signature cannot be verified, the authentication of the sender’s transmission fails.

Id., [0026]. And if Har’s system is used to attempt to authenticate as “a trusted third party” the authentication server providing the key or signature information,

[i]f the decryption fails, the authentication of the authentication server fails. If the digital signature cannot be verified, the authentication of the authentication server fails.

Id., [0028]. Finally, if Har's system is used to attempt to authenticate the user who received the call by authenticating a confirmation message from the receiving user,

[i]f the decryption fails, the authentication of the of the *[sic]* second user fails. If the digital signature cannot be verified, the authentication of the of the *[sic]* second user fails.

Id., [0030]. A successful validation of the authentication of the conformation message, too, requires either a successful decryption using the key, or a verification of the digital signature:

If the decryption fails, the authentication of the authentication server confirmation message fails. If the digital signature cannot be verified, the authentication of the authentication server confirmation message fails.

Id., [0032]. Every embodiment disclosed by Har requires either such a successful decryption or such a successful verification of the digital signature, "in accordance with" the above teachings. *Id.*, Figure 2, [0033]-[0035]. While some of the claims of Har merely refer to "authentication" without specifically stating that success of either Har's key-based decryption or Har's key-based signature verification is required for authentication, *see id.*, claims 1-5, 7, the only two authentication alternatives that Har discloses or teaches are key-based decryption of the message

or key-based verification of the digital signature. *See generally id.*; *accord id.*, claims 6, 8-20 (expressly requiring encryption/decryption).

C. Miller

The Petition also relies on U.S. Patent Publication No. 2012/0201381, entitled Cryptographic Security Functions Based on Anticipated Changes in Dynamic Minutiae, (“Miller”) to challenge the claims of the ’989 patent in combination with Har.

Miller and the ’989 patent solve different problems, using different solutions. As explained above in Section II.A, the ’989 patent describes and claims an invention to, for example, validate a phone number associated with a calling device in order to prevent spoofing. Miller’s objective is to authenticate a user before allowing the user to access a service.

As stated by Miller, “[o]ne or more embodiments of the present invention, methods and systems for dynamic key cryptography ... can be used for authenticating users to services.” Ex. 1021 [Miller], [0012]. Figure 1 of Miller is a system illustrating communication and security between a client (Service User 20), client device (Computer 18), and a Service Provider (14), facilitated by a Dynamic Key Crypto Provider (10) (“DKCP”). *Id.*, [0017].

The described DKCP performs a “challenge, response and validation sequence” in order to authenticate “a specific computer 18 and service user 20.”

Id., [0050]. This process is based on “minutiae” collected about the user and the user’s computer. Minutiae is “any piece of information that can be definitively associated with the computer and its user, including information from the general categories of what the user or computing device has, what the user knows, and what the user is.” *Id.*, [0030].

Figure 2 shows the “challenge, response and validation process performed by the system of FIG. 1.” *Id.*, [0018]. In step 116, the DKCP formulates a “challenge” and then sends the challenge, at step 118, to the service user’s computer 18. *Id.*, [0062]. The challenge asks the service user’s computer to send back a response using particular minutiae selected by the DKCP. *Id.*, [0065]. The DKCP then validates this response at step 120, by “comparing the actual response received from the computer 18 to the allowable responses that are pre-processed by the dynamic key crypto provider 10 to determine if there is a match.” *Id.*, [0066]. If the response is not as expected, then a validation failure process alerts the service provider 14 that the validation has failed, as shown in Figure 6B. *Id.*, [0069]. The service provider then decides how to respond to the failure, which can include denying the user’s service request. *Id.*, [0118].

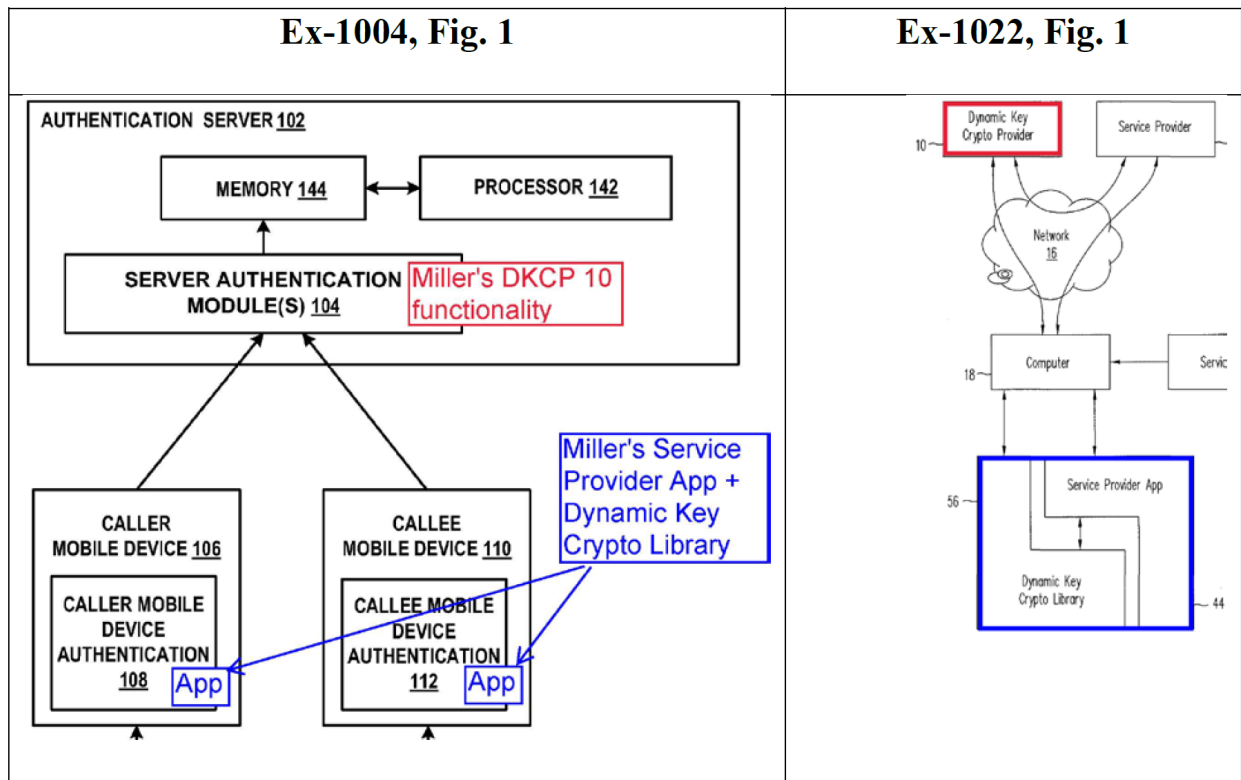
The DKCP can also calculate a “score” for the response received from the service user’s computer. *Id.*, Figure 6, [0104]. The compute score process 144 shown in Miller’s Figure 6A computes a heuristic and probabilistic scoring based

on the returned minutiae and then compares the resulting score against a threshold defined by the service provider. *Id.*, [0105], [0111]. If the score meets the threshold, the DKPC sends the score to the service provider. *Id.*, [0111]. The service provider then decides whether to grant the user access to the service. *Id.*, [0119].

If the score is below the threshold, then the DKPC performs an additional authentication process, called a “step-up request.” *Id.*, [0112]. As part of this process, the DKCP formulates and sends a new challenge to the service user’s computer, and the challenge-response-validation process repeats. *Id.*, [0114].

III. INSTITUTION SHOULD BE DENIED BECAUSE THE PETITION FAILS TO SHOW A REASONABLE LIKELIHOOD THAT THE SOLE GROUND RENDERS ANY CLAIM OBVIOUS

The Petition’s sole ground depends on a proposed, allegedly obvious combination that modifies Har in numerous ways to provide “augmentation” by adding aspects “of Miller’s authentication system specific to device authentication” to the system that Har teaches. Pet., 15. The Petition illustrates its proposed combination as shown below.



Pet., 15.

The Petition relies on a flawed analysis and should be denied because it fails to demonstrate a reasonable likelihood that Har and Miller, combined as proposed, teach or suggest multiple limitations of each of the independent claims. While the Petition attempts to stretch the language of the claims beyond their plain and ordinary meaning, to stretch the disclosures of the references toward the claimed invention, and to bend the prosecution history of the '989 patent in the direction of its desired result, a perusal of the patent, the claims, and the asserted prior art makes clear that the claimed invention is not shown to be met by the proposed combination in the sole ground of the Petition. **First**, the proposed combination is

not shown to receive the required “information pertaining to a call.” Contrary to the Petition, it is not enough that the information is “in response to” initiation of a call or a requesting authentication of a call. Har’s keys are not “information pertaining to a call . . . including . . . a value generated based at least in part on information associated with the calling device”; the mere alleged fact that a key generating the “value” is stored in memory associated with the calling device does not satisfy this limitation, the prosecution history says nothing to the contrary, and Miller’s minutia are not shown to fill this gap. Moreover, the combination is not shown to receive the claimed “score,” and the proposed combination would receive a “value” and “score” that are both based on the same redundant information for no substantiated reason, regardless whether the combination is additionally modified as proposed to use biometrics, like face size. Finally, the alleged “score” is not shown to be “indicating a validity of a [phone] number” as claimed. *Second*, the Petition fails to show the claimed “security determination” based on both the “value” and “score” above, for many of the same reasons.

A. The Sole Ground Is Not Shown To Satisfy The “Receiving” Step.

Claim 1 requires a system comprising one or more processors configured to “receive information pertaining to a call initiated by a calling device, the information pertaining to the call including: (1) a value generated based at least in part on information associated with the calling device, and (2) a score generated

for the calling device, the score indicating a validity of a phone number.” Ex. 1001 [’989 Patent], 22:48-55; *see also id.*, 24:27-32 (claim 27), 24:45-49 (claim 28).

The Petition fails to show that this limitation is met.

1. The Petition Relies On An Incorrect Interpretation Of
“Information Pertaining To A Call”

a. “Pertaining To A Call” Does Not Simply Mean
That The Information is “In Response To”
Initiation Of A Call.

The Petition asserts that the claims’ requirement that the “receive[d] information” be information “pertaining to a call” is satisfied “because” the alleged “received information” in the Har/Miller system “is received in response to the authentication process resulting from Har recognizing that a call has been initiated.” Pet., 26. Specifically, the Petition asserts:

The Har/Miller system discloses this limitation and describes processor(s) configured to “receive information pertaining to a call” as detailed below. Moreover, as detailed below, the received information is “pertaining to the *[sic]* call” ***because it is received in response to the authentication process resulting from Har recognizing that a call has been initiated.***

Pet., 26 (emphasis and “[sic]” added). Thus, the Petition asserts, “pertaining to a call” is satisfied when the information is received “in response to” or “in connection with” a call, regardless whether the information itself specifically

describes or relates to the call. This broad interpretation of the claim language is inconsistent with both its plain meaning and the intrinsic record.

The limitation that the “receive[d] information” be “information pertaining to a call initiated by a calling device” requires receiving information specific to the initiated call, not merely information transmitted in response to the call. Because the Petition relies on the incorrect meaning of the limitation, it has not shown that its proposed combination discloses this limitation. In the claims, the plain and ordinary meaning of “information pertaining to a call” requires that the information be specific to or referring to the call, such as, for example, an attribute or feature of that specific call or having reference to that call, not merely that the information be sent in response to, or contemporaneously with, the call. *See, e.g.*, Ex. 2011 [Merriam-Webster Dictionary] (showing that ordinary meaning of “pertaining to” includes, *e.g.*, “to belong as an attribute, feature” to or “to have reference” to).

The specification of the '989 patent confirms that the claim language does not mean simply information sent in response to, or contemporaneously with, the call, as the Petition suggests. Pet., 26. As the specification explains, in the invention, the message may include components “specific to the” call that vary with the call and are “difficult (if not impossible) to predict,” such as “a number specific to the session or the phone.” Ex. 1001 ['989 Pat.], 4:49-50. For example, in some embodiments, the information can include a timestamp of the call itself.

Id., 8:40-42 (“In some embodiments, the message includes a timestamp of the call, such that the message cannot be replayed later.”); 8:55-60 (similar); 14:54-57 (“When the relying party observes the incoming ANI and Caller ID, it decodes the one time code based on the symmetric key for the account associated with the user and validates the timestamp.”).

In some embodiments, the message may include phone number identification data for the call. *Id.*, 8:67. As another example, the specification explains, in some embodiments the information “includes or is associated with the number to which the phone call is placed.” *Id.*, 8:42-44; *see also id.*, 2:52-55, 2:64-3:4 (“When contacting callee 118, automatic number identification (ANI) data, such as caller id, for the calling device 102 is presented to the callee.”). As yet another example, the information may include a “counter,” which appears to increase the count with every call. *Id.*, 8:44-48, 17:6. The specification further discloses other such “call information” varying with the call, such as “the call start time,” whether the call comes from an “invalid number” or an “unknown number,” “and a score indicating the validity of the number.” *Id.*, 8:64-9:1.

The specification does not suggest that “information” is “pertaining to [the] call” merely because it is sent in response to or roughly contemporaneously with the call. To the contrary, the patent specifically discloses advantages of the invention’s use of this “difficult . . . to predict” information varying with the call

for verification rather than information that is *not* specific to the call. *Id.*, 4:49-50. For example, the patent discloses that when “the message sent to the verification service includes a timestamp,” it “can be used to prevent a replay attack,” “such that the message cannot be replayed later.” *Id.*, 8:40-57. If the timestamp of the call is “old or aged,” that fact “can be used by the verification service to score the validity of the communication,” since “an old or aged timestamp may be indicative of an attack.” *Id.*, 8:57-60; *see also, e.g., id.*, 4:46-50, 7:51-58 (further examples). The disclosure of the invention in the specification thus confirms that the ordinary artisan in the art at the time of the invention would understand that the received information is not “pertaining to [the] call,” as the claim requires, merely “*because*” it is “received in response to the authentication process resulting from Har recognizing that a call has been initiated,” Pet., 26 (emphasis added).

In light of the Petition’s express reliance on this incorrect interpretation of “information *pertaining to [the] call*,” *see id.*, the Petition fails to establish that Har and Miller discloses or renders obvious this limitation.

b. “Information Pertaining To A Call” is Not Met Simply By A Request Being Sent For Authentication Of A Call.

To the extent that the Petition further argues that the mere existence of Har’s “authentication request” satisfies the requirement to “receive information

pertaining to a call,” the Petition’s interpretation of the claim is contrary to the claim language and intrinsic evidence for further reasons, as explained below.

Although the Petition’s discussion of this limitation (at 27-30) is convoluted and unclear, it seems to suggest that the sending and receipt of Har’s “authentication request” must meet the requirement to “receive information pertaining to a call” because Har’s “request” is sent by “the caller” to “the server” and is “requesting the server to authenticate the identity of the first user.” Pet., 27 (citing “Ex-1004, [0014-0015]. Ex-1003, ¶89”). However, the mere fact that a transmission constitutes an authentication request by the recipient of a call for authentication of the identity of the initiator of the call does not satisfy the claims’ requirement that the transmission include information “pertaining to [the] call.” That would contradict the patent, which, for example, distinguishes expressly between, on the one hand, the “request” for verification for the call, and on the other hand, the “information associated with the call” or “about the call” or “indicated by the call,” that the service provider may, in the “request,” ask to be verified. Ex. 1001 [’989 Pat.], at, *e.g.*, 3:9-12 (“callee 118 sends a request (128) for . . . verification of ANI data indicated by the call”), 5:26-29, 6:17-36; *see also*,

e.g., id., 4:41-67. The information that an authentication request is asking to be authenticated, and the authentication request itself, are not the same thing.²

Thus, the fact that in Har an “authentication request” is received does not show that the prior art meets the claims’ limitation requiring receiving “information pertaining to a call” as claimed.

2. Har’s Public And Private Key Are Not “Information Pertaining To A Call Including (1) A Value Generated Based At Least In Part On Information Associated With The Calling Device.”

Next, the Petition argues that Har’s authentication message, because it is encrypted and signed using a public and private key, necessarily satisfies the first of the two specific elements recited in the claims as “includ[ed]” in the

² The ’989 Patent discloses that, in some embodiments of the claimed invention, “sending a message” for “validation of caller ID or ANI data” may be performed by sending and receipt of “information associated with the call” in such a way that “the message is implicit in the information associated with the call.” Ex. 1001 [’989 Pat.], 6:17-36. In such embodiments, the validation request may thus, in the context of the invention, be implicit in information pertaining to the call. However, the Petition does not point to any such teaching in the prior art. And innovations disclosed by the patent, as opposed to the prior art, cannot be used to find the patent’s own claims obvious.

“information pertaining to a call”: namely, “(1) a value generated based at least in part on information associated with the calling device.” Pet., 26-31. The Petition argues that the Board must make this finding, and cannot find otherwise, because during prosecution of the ’989 patent the applicant supposedly stated to the Office that such use of a “key” satisfied this limitation. *Id.* The Petition is wrong. Har’s keys are for Har’s authentication server and Har’s user, and are not specific to any call. The Petition’s argument is built on literally rewriting the prosecution history—misleadingly omitting, and replacing with ellipses, the critical words cited in the prosecution. The Board should reject the Petition’s misleading characterizations.

The Petition points to Har’s alleged disclosure that a user can send an authentication “message encrypted using the server’s public key . . . and signed using the private key . . . of the first user.” Ex. 1004 [Har] [0016] (cited by Pet., 28). However, this information, even if it is sent in response to the call, is not shown to be information “pertaining to [the] call.” Pet., 26. As the Petition tacitly concedes, the “public key” is the public key for Har’s *authentication server*, and the private key is that of Har’s *user*, and neither is described as being specific to any call. Ex. 1004 [Har] [0016]; Pet., 28-29. So far as Har discloses or the Petition argues, Har’s server always uses its key, and Har’s user always uses its key: the keys are not specific to the call. Contrast these keys in Har with the types

of information pertaining to the specific call that is disclosed in the '989 patent: depending on the embodiment, the patent discloses receiving information such as “the number to which the phone call is placed,” “a timestamp of the call,” “a counter” of the call, “the incoming ANI and Caller ID,” or other “number[s] specific to the session” Ex. 1001 [’989 Pat.] 4:49-50, 8:40-54, 14:54-57. Such information, may unpredictably vary for specific calls—a fact that the patent, but not the cited prior art, discloses to be advantageous for purposes of call verification, as already noted above. *Id.*, *e.g.*, 8:40-60. Har’s keys, which are not shown to vary with the call, are not shown to be like the information pertaining to the call described in the patent. Thus, Har’s use of its keys are not shown to satisfy “information pertaining to [the] call” as claimed.

The Petition points (at 27-31) to the '989 Patent’s disclosure of using a “key” to encrypt its message, and argues that “Har’s usage of encryption keys to encrypt and sign Har’s authentication request” “correspond directly” to this aspect of the invention as described in the patent and cited in the prosecution history in support of this limitation—and that the Board therefore supposedly must find that Har’s use of keys equally satisfies this limitation of receiving “information pertaining to [the] call.” That is not correct. The Petition misapprehends or mischaracterizes the patent’s disclosure and the prosecution history citing it.

According to the Petition, the '989 patent specification says that *all that is required* to meet the “information pertaining to the call including (1) a value generated based at least in part on information associated with the calling device” is that the verification request include “an additional value” that is “pseudo-randomly generated ... using a key that is stored on the device.” Pet., 27-28. The Petition’s argument is reproduced below, with all alteration marks and emphases unchanged:

Har’s usage of encryption keys to encrypt and sign Har’s authentication request is a “*value generated...*” because the keys correspond directly to the ‘989 specification portions identified by the applicant to the Examiner for this element.

The applicant amended the claims to recite:

Receive information ...including: (1) a [[code]] value generated based at least in part on information associated with the calling device...

Ex-1002, 0197. “Support for the amendments ... may be found ... in Paragraphs [0046] and [0048]-[0049]....” Ex-1002, 0195. Paragraph [0046] in the ‘989 application recites that the “*value generated*” may use a “key” that is “stored in a memory associated with the device” (and therefore “*based at least in part on information associated with the calling device*” according to the applicant):

the verification processing resident on the device ... generates a message based on a value stored in a memory associated with the device, ... One example implementation is for the message to be a message

authentication code on the phone number called, where the message authentication code is at least one of ... an additional value that may be pseudo-randomly generated ... using a **key that is stored on the device**

Ex-1002, 0041 (corresponding to Ex-1001, 8:31-52); Ex-1003, ¶91.

Har's "authentication request" with its encryption and digital signature disclose what the applicant told the Examiner was the claimed "value" (which corresponds to the authentication request as the encrypted message and/or the digital signature).

Pet., 27-28 (all emphases by Petitioner).

This argument is wrong on multiple levels, and is presented in a way that is affirmatively misleading.

First, the Petition does not explain why the mere use of a "key that is stored on the device" to generate a value in the message would satisfy the claims' requirement that the information be "information *pertaining to [the] call.*" The Petition is apparently relying on an unstated premise that any information that constitutes "*a value generated based at least in part on information associated with the calling device*" inherently satisfies the claims' separately recited requirement that the information that "includ[es]" this value be "*information pertaining to [the] call.*" That is not true. A value may be pseudo-randomly generated based at least in part on information associated with the calling device, and yet still not pertain to a particular call.

But the more specific premise of the Petition’s argument is also wrong—and involves a misleading elision by the Petitioner of part of the patent’s disclosure raised in the prosecution history. Contrary to the Petition’s false suggestion, the ’989 Patent does **not** disclose, nor did “the applicant t[e]l[l] the Examiner,” that the mere inclusion of any “value . . . pseudo-randomly generated using a key that is stored on the device” necessarily satisfies the requirement of “*information pertaining to the call including (1) a value generated based at least in part on information associated with the calling device.*” Pet., 27. Rather, in language elided using ellipses from the Petition’s quotation of the patent, the ’989 specification discloses using such a generated “value” when it is an authentication code “*associated with the number to which the phone call is placed*”—a materially different, narrower proposition that makes the “value” one that is expressly about “*the phone call*”, and therefore **does** plainly satisfy the claim language’s requirement of “*pert[[in]e]n[ce] to the call,*” unlike Har’s mere use of its server’s and user’s keys to encrypt and digitally certify. Ex. 1001 [’989 pat.] 8:42-52.

As the Petition (at 27) notes, when this limitation was amended to its present form during prosecution, the applicant cited for support paragraphs of the application, including paragraph [0046] corresponding to column 8, lines 31-51 of the issued ’989 patent. Pet., 27-28; Ex. 1002, [0041].

However, contrary to the Petition, the applicant did **not** thereby “t[e]l[l] the Examiner” that all that was necessary to satisfy this limitation was that “that the ‘value generated’ . . . use a ‘key’ that is ‘stored in a memory associated with the device.’” Pet., 27. Rather, what the applicant pointed out to the Examiner was merely disclosure in the specification of a value that was an “authentication code” **“associated with the number to which the phone call is placed.”** Ex. 1001 [’989 pat.] 8:42-52. The key language bolded in the previous sentence is misleadingly omitted from the Petitioner’s partial reproduction of this portion of the patent specification. Here is the Petition’s expurgated partial reproduction of this cited portion of the specification, next to what the specification actually says:

Petition	Specification
the verification processing resident on the device ... generates a message based on a value stored in a memory associated with the device, ...	the verification processing resident on the device determines that a phone call is placed, generates a message based on a value stored in a memory associated with the device, and transmits the generated message to a verification service provider at the time that the phone call is made. In some embodiments, the determination is performed, for example, by subscribing to relevant events, or by modifying the interrupt or event handlers, the phone number selection, the phone number entry, the operating system, or one or more drivers. In some embodiments, the message includes a timestamp of the call, such that the message cannot

One example implementation is for the message to be a message authentication code on the phone number called, where the message authentication code is at least one of ... an additional value that may be pseudo-randomly generated ... using a key that is stored on the device Pet., 28 (quoting Ex. 1002, 0041 “corresponding to Ex-1001, 8:31-52”) (alteration marks in original)	be replayed later. In some embodiments, the message includes or is associated with the number to which the phone call is placed. One example implementation is for the message to be a message authentication code on the phone number called, where the message authentication code is at least one of a counter value and an additional value that may be pseudo-randomly generated, for example, using a key that is stored on the device Ex. 1001 [’989 pat.], 8:31-52 (emphasis added)
---	---

As seen above, the specification states: “In some embodiments, the message *includes or is associated with the number to which the phone call is placed.*” Ex. 1001 [’989 pat.], 8:42.44. The very next sentence gives an “example” of this very sort of message associated with this very number: “One example implementation is for the message to be a message authentication code *on the phone number called*, where the message authentication code is at least one of a counter value and an additional value that may be pseudo-randomly generated, for example, using a key that is stored on the device” *Id.*, 8:44-49 (emphasis added).

In sum, nothing in either the specification or the prosecution history is shown to support the Petition’s argument. When the Petition’s misleading

omissions and convoluted rewriting of the written description of the invention are rejected, there is no support for the Petition's assertion that Har's mere use of its keys satisfies this limitation.

3. Har's Message Does Not Use Its **Caller Device's** Private Key.

Alternatively, the Petition argues that "Har teaches, or renders obvious that the 'private key' is associated with the caller device." Pet., 30. As noted, the Petition takes the position that "Har's 'device generates a message' using two 'keys ... stored on the device:' (1) the 'server's public key' and (2) the 'private key' stored in the device," and immediately quotes Har's unambiguous statement that this private key is "the private key (also called the private certificate) of the first user." Pet., 28 (ellipsis by Petitioner) (quoting Ex. 1004 [Har] [0016]). What the Petition appears to be arguing is that, *if* the "private key" used in Har's relied-on message were the key of Har's caller device instead of Har's user, it would mean that Har's message would include "*information pertaining to [the] call*" as claimed. Pet., 30. However, the Petition fails to show that Har discloses that this key, which Har expressly says is the key of the "**user**," is actually the key of the **device**, or that it would have been obvious to change this key from a user key to a device key in Har/Miller.

Contrary to the Petition (at 30-31), Har does not teach that its "private key" is associated with Har's **caller device**. First, Har does not disclose any such thing.

The Petition argues that because Har teaches a “server’s private key” and Har’s “server” is a “device,” Har therefore “teaches such keys are associated with devices.” Pet., 30. That does not follow. To seek to meet this limitation, the Petition is expressly relying on a *different* private key, which Har expressly describes as “the private key (also called the private certificate) of the first *user*.” Ex. 1004 [Har], [0016] (quoted at Pet., 28). The fact that the *server* may have a separate private key—on which the Petition is not relying to meet this limitation—is beside the point.

As if tacitly conceding this difficulty, the Petition mainly, but vainly, argues that “it would be an obvious *variation* [from Har and Miller’s actual teachings] to use a private key associated with the caller device to digitally sign the communication from the caller device to the authentication server” because supposedly such a private key for the caller device could be stored on the device and “[s]uch a usage would effectuate the goals of both Har and Miller to ensure correct authentication.” Pet., 30. But that just begs the question. The Petition does not even attempt to show that the ordinary artisan would have reason to conclude that the proposed combination does not *already* “ensure correct authentication.” Har, for example, teaches that its required encryption and digital certification already do, without any modification whatsoever. Ex. 1004 [Har] at, e.g., [0002], Abstract. And, to the extent that Har and Miller teach call

authentication, they teach authentication using encryption, digital certification, and trusted information that does not vary with specific calls, as demonstrated above.

See supra § II.B-C, III.A.1. The Petition establishes no reason or teaching to depart from Har’s and Miller’s existing teachings and begin using information that does, rather than doesn’t, vary with a call for validation or authentication purposes.

Moreover, even if it were obvious to make the private key used in Har’s message the key of the caller device, the Petition fails to show that use of the device’s private key would render the message “information pertaining to [the] call” as claimed. As already noted above, the Petition fails to show that such keys would be specific to any particular call. *See supra* § III.A.1. And that means that such keys, as also already noted above, would lack the patent’s disclosed advantages of using information that varies with the call in the verification process, which, for example, can help prevent illicit “replay” of valid messages by spoofers, which is not true of the key. *See id.*

4. Miller Does Not Add “Information Pertaining To [The] Call.”

In the alternative, after its arguments based on Har, the Petition next argues that adding Miller to the proposed Har/Miller supplies this missing limitation of “information pertaining to the call including: (1) a value generated based at least in part on information associated with the calling device” through its use of “computer minutia.” But it does not. Miller is even farther afield than Har—

indeed, it generally does not even relate to phone calls at all. And its “computer minutia” are not information pertaining to any specific call.

As explained above, *supra* § II.C, Miller relates to “authentication between a client electronic device and a service provider,” where “[t]he standard method for identifying a user to an online service is by entering a username and password.” Ex. 1022 [Miller] [0003], [0010]. Miller seeks to improve the traditional username/password methods by “uniquely identifying a user’s computer or other electronic device based on (1) the electronic device itself, e.g., a mobile phone or personal computing device, and using a very wide range of hardware, firmware, and software minutia found on the computer; (2) secrets a user of the computer knows; and (3) biometric information the computer might collect from the user.” *Id.*, [0026].

Petitioner relies on Miller’s “computer minutia,” Pet., 32–33, but these cited “computer minutia” are static device characteristics, such as serial numbers or software IDs, which are not shown to relate in any way to the call or to vary with the call. Pet., 32-36.³

³ The Petition again argues that the use of a “key” somehow satisfies the requirement of “information pertaining to [the] call,” but fails to show that this is true for Miller’s keys any more than for Har’s. *See, e.g., supra* § III.A.3.

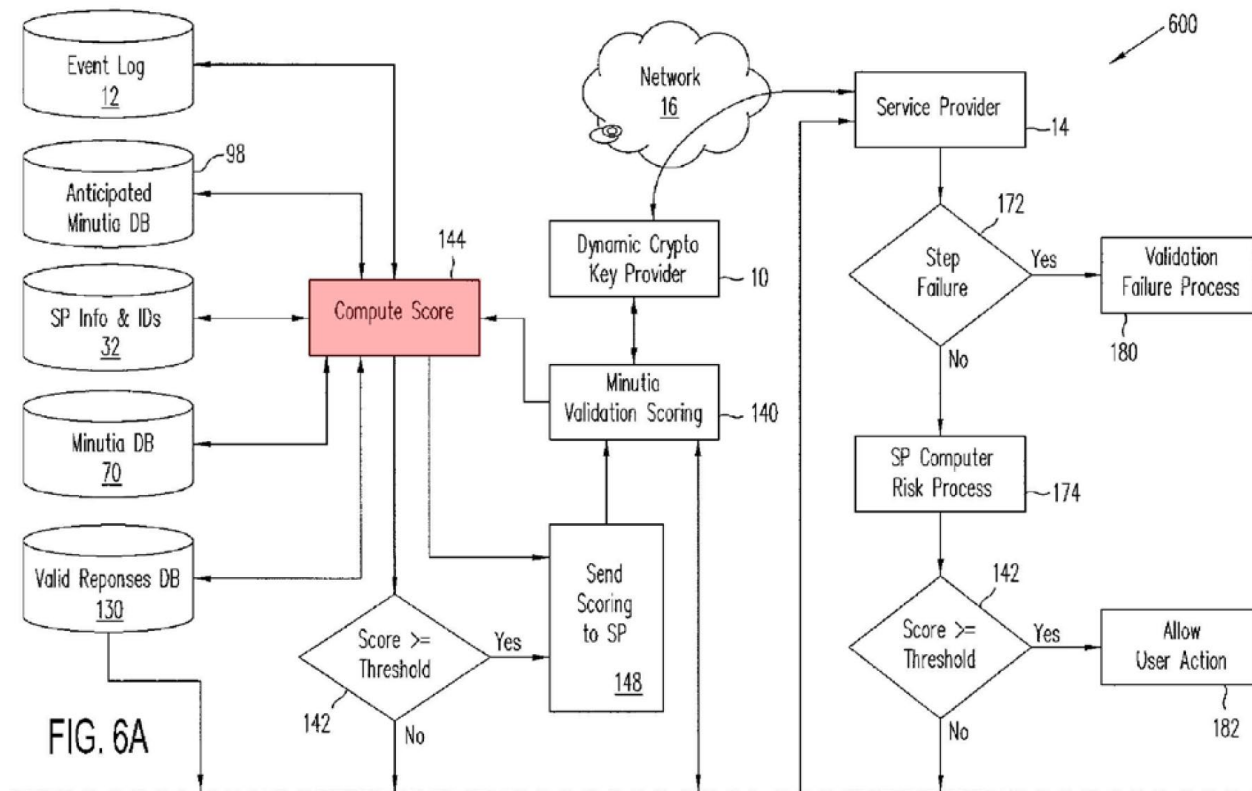
5. The Petition Fails To Show That Har/Miller Teach Receiving “Information Pertaining To The Call Including . . . (2) A Score Generated For The Calling Device, The Score Indicating A Validity Of A Phone Number”.

Claim 1 recites that the processor “receive ... (1) a value generated based at least in part on information associated with the calling device, and (2) a score generated for the calling device.” Petitioner relies, in the alternative, on Miller’s “score” and on Miller’s use of “user biometrics” as allegedly disclosing the claimed “score” in the claims. Pet., 36. Both of these alternatives for the claimed “score” fail to show disclosure or obviousness of the claim as a whole.

a. Har/Miller Are Not Shown To Teach That The “Score” Is “Received”.

The Petition fails to show that the alleged “score” is “receive[d]” in the proposed Har/Miller combination, as required by the claims. It also fails to show that such a modification of Har/Miller would have been obvious to an ordinary artisan at the time of the invention.

For the claimed “score,” the Petition relies on “the ‘compute score 144’ functionality” illustrated in Miller’s Figure 6A:



Ex. 1022 [Miller], Figure 6A (annotation by Petitioner); Pet., 36-37.

The Petition fails to show, however, that this functionality satisfies the “receive” limitation of the claims. Miller’s score in Compute Score 144 is generated *each time* a security determination is requested, at the alleged verification service performing the security determination. Ex. 1022 [Miller], [0104]-[0105], [0111]-[0120]; Pet., 40-43, 45. Thus, so far as is shown, Miller teaches that its “score” is generated afresh *in situ* for each security determination. Ex. 1022 [Miller], [0104]-[0105].

The Petition attempts to manufacture a disclosure in Miller of transmission of Miller’s score based solely on Miller’s boilerplate statement that it can use more

than one processor, and the annotation of Miller's drawings with Petitioner's own arrows. Pet., 40-43. But the Petition points to no specific teachings; it just spins imagined disclosures or obvious modifications based solely on this brief boilerplate. The Petition also fails to show that it would have been obvious to modify Miller (or Har/Miller) specifically to meet the claims, in the absence of the teachings of the claimed invention in the '989 patent. Boilerplates may be useful, but without more they do not constitute a specific boiler.

The Petition fails to show that Har/Miller "receive" the "score."

- b. Har/Miller Are Not Shown To Teach Receiving **Both** "(1) A Value Generated Based At Least In Part On Information Associated With The Calling Device, **And** (2) A Score Generated For The Calling Device, The Score Indicating A Validity Of A Phone Number".

Even if Miller's alleged "score" were being "receive[d]" as claimed in Har/Miller, the proposed combination separately relies on Miller's computer minutia to satisfy the "*value*" limitation, but the Petition fails to articulate, let alone show, any reason that the ordinary artisan at the time of the invention would have modified Har in light of Miller to incorporate Miller's "score" while also retaining Miller's separate transmission of device minutia.

For the claimed "*score*," the Petition relies on Miller's "score." Pet., 42. At the same time, for the claimed "*value*," the Petition relies on Miller's device

“minutia.” Pet., 31-36. However, as the Petition acknowledge, Miller’s “score” is itself computed from these same device minutia. As the Petition concedes, for example, “Miller generates a ‘score’ by combining available factors, *including minutia*.” Pet., 38; *see also, e.g.*, Ex. 1022 [Miller], [0105] (“The compute score 144 process computes a heuristic and probabilistic scoring of the minutia and minutia values used in the validated response”).

What is more, as noted above, *supra* § III.A.1-3, the Petition relies in the alternative on Har, in particular on Har’s digital signature, for the claimed “*value*.” Pet., 27-31. For this purpose at least, Har’s digital signature, generated using a private key that is not disclosed to change, is materially indistinguishable from “minutia” as Miller discloses and uses that term. Ex. 1022 [Miller], [0050-0060] (“showing different minutia,” in the Petition’s words); Pet., 32.⁴

Assuming for the sake of argument that both, or either, Har and Miller’s alleged “*value*” met the “*value*” limitation, the Petition’s proposed combination results in duplicative data being transmitted and received, with no reason given why the ordinary artisan would have done so.

⁴ No modification is proposed of the static nature of Har’s private key associated with Har’s digital signature.

First, the proposed combination would redundantly send minutia and a score based on the minutia. The claim requires “*receiv[ing]*” **both** (1) the “*value*,” **and** (2) the “*score*.” So in the proposed combination, both the raw minutia (the alleged “*value*”) **and** the “*score*” derived from those minutia must be received. *See, e.g.,* Pet., 36 (conceding that Miller’s alleged claimed “*score*” is “based upon the ‘minutia’ discussed in” connection with Miller’s alleged “*value*”). But there is no showing or argument why the ordinary artisan at the time of the invention would have possibly been motivated to create such redundant transmissions. *See generally* Pet., 26-44. The Petition is, in effect, proposing that it would be obvious to modify the teachings of the art to receive both information and a scoring of that information, without explaining why.

Notably, the proposed combination would differ in this respect from the invention described and claimed in the ’989 patent, which does not disclose such duplication. In the embodiments of the claimed invention disclosed in the ’989 patent specification, the “*value*” and the “*score*” do not convey the same information. In the ’989 patent’s embodiments, the “*score*” is focused on behavioral and historical factors rather than physical device criteria. *See, e.g.,* Ex. 1001 [’989 pat.] 12:17-23 (“In some embodiments, input from a relying party provides feedback on a particular phone call that indicates a problem with the user’s device, such as a stolen device, possible spoof attempt, fraud related to a

device, or a verification that subsequently proved to be errant. This information can then be incorporated into an overall reputation score of a caller's device.”); 8:58-60 (“the timestamp can be used by the verification service to score the validity of the communication, where an old or aged timestamp may be indicative of an attack.”). In contrast, Miller’s alleged “score” is more focused on device minutia that are—in the words of the Petition—“specifically associated with” a “device.” Pet., 32-33; Ex. 1022 [Miller] [0039], [0050]-[0060], [0094].

Thus, the Petition fails to show that Har/Miller disclose or render obvious receiving both the “value” and the “score” required by the claims.

c. Miller’s “Biometrics” Do Not Add This Limitation.

Petitioner’s brief obviousness argument relying in the alternative on Miller’s “user biometrics” to meet the claimed “*score*” is similarly flawed. Pet., 36, 43-44.

First, the claims require that the “*score*” be “*generated for the calling device,*” “*indicat[e] a validity of a phone number,*” and be received as part of “*information pertaining to a call.*” Petitioner does not explain why the ordinary artisan at the time of the invention would have had a reason to modify the prior art to adapt Miller’s biometric login methods—which are designed to replace passwords for web-based service access, *see, e.g.*, Ex. 1022 [Miller], [0010], [0028], [0031]—for use in authenticating telephone calls. Petitioner does not show

why, in a world where computer passwords are already considered frustrating, the ordinary artisan would have considered the addition of biometric security barriers to making calls to be a good idea, let alone an idea that would be acceptable to users. To the contrary, the potential downsides to such biometric barriers to system access amounted to a standing joke among office workers at the time. Petitioner offers no countervailing evidence that it would have been obvious to modify Miller, or Har/Miller, to use Miller's biometric measures as the basis for this security instead of the information that Har and Miller already disclosed.

Second, the Petition does not show that use of “user biometrics” as taught by Miller generates a “*score*” as claimed, and its short argument that it would have been obvious relies on yet another unsupportably broad understanding of the claim language. The Petition argues that “[i]t would be obvious to a POSA that the collection/usage of such biometrics involves generating a ‘score’ to reduce these characteristics to values usable in computers.” Pet., 44. Thus, the Petition's argument relies on an implicit understanding of the claimed “*score*” as being satisfied by, for example, mere numerical encodings of physical measurements “to reduce” these physical measurements “to values usable in computers.” *Id.* This unsupportably broad understanding of “*score*” does not comport with the '989 patent's usage of that term. In the context of the patent, the “*score*” is the result of some assessment—hence the term “score”—and is not merely any numerical

encoding of a physical measurement. *See, e.g.*, Ex. 1001 ['989 Pat.] 9:37-39 (“In some embodiments, the verification service creates a verification score for a device when a call is initiated.”).

The Petition has not shown that Har/Miller taught or rendered obvious the modification of Har/Miller to use biometrics to meet the claimed “*score*.”

d. Har/Miller Are Not Shown To Teach A “Score Indicating A Validity Of A Phone Number.”

The claimed “score” is required by the claims to be a “score indicating a validity of a phone number.” Miller’s score, relied on by Petitioner for this limitation, is not shown to be “indicating a validity of a phone number.”

The Petition relies on Miller’s score, and argues that Miller’s disclosure of its score “mirrors” the patent’s disclosure of its claimed “*score*” cited by the applicant to the Examiner as support for the “score” element of the claims in the course of prosecution. Pet., 37. But that is not correct, and the Petition again misapprehends or mischaracterizes the ’989 patent specification.

The Petition points to statements in the ’989 specification at 9:1 and 9:38-45 (which Petitioner asserts “correspond[] to” the portions of the application cited as support for the “score” limitation during prosecution) teaching “‘a score indicating the validity of the [phone] number’ ([0048]) and that ‘the verification score [of the ’989 patent] is created using a variety of approaches that include one or more of

combining the available factors to create a score by applying relative weighting to each of the available factors’ ([0049]).” Pet., 37-38. According to the Petition, this means that “*“a score indicating a validity of a phone number...”* encompasses combining various information (‘available factors’) about the call / communication and the related devices to calculate the score,” and Har/Miller performs authentication “using the caller’s identification to ‘vouch for’ the caller,” and so therefore, because “Miller generates a ‘score’ by combining available factors, including minutia” such as even the phone number itself, and “the caller’s device phone number is one form of identification,” the claimed “*score indicating a validity of a phone number*” is supposedly met by Miller simply because Miller generates a score by combining various unspecified minutia, potentially iterating to emphasize or “isolat[e]” “particular minutia,” and Har/Miller vouches for the caller. Pet., 38-40.

The Petition’s arguments do not hold water. **First**, the fact that the ’989 patent says its “*score*” may be generated from various “available factors” (Ex. 1001, [0049]) does not mean that the “*score*” indicates the validity of a phone number whenever it is generated from various available factors. A score could be tailored to indicate many different things. The ’989 patent, unlike Har or Miller, expressly discloses creating a “*score*” that is “a score indicating the validity of the [phone] number.” Ex. 1001 [’989 pat.], 8:64-9:1 (“In various embodiments, the

call information includes one or more of: invalid number, unknown number, no call in progress, the call start time (if there is a call in progress), the phone number for the current call, and a score indicating the validity of the number.”). Miller, or Har/Miller, contain no such disclosure, and are at most shown to be capable of iterating the score to isolate certain unspecified factors. And while Miller indicates that the phone number may sometimes form one of the many minutia it uses, Miller is not shown to make any particular mention of indicating the validity of the phone number by the score; the mere fact that the phone number is one of the many minutia does not mean that Miller contemplates indicating whether the phone number is valid. Pet., 38-39.⁵ Finally, the Petition seems to contend that Miller’s score, by allegedly indicating the validity of a device, effectively also indicates the validity of an associated phone number. Pet., 38. However, that is not necessarily so, nor is it shown to be obvious in the context of the invention. In the absence of any specific teaching in Miller, or Har/Miller, of generating a score

⁵ As noted above, the Petition argues in the alternative that Miller may use biometrics, such as “retinal scan” and “facial geometry,” but these biometric facts have nothing inherently to do with the validity of a phone number, any more than other non-call-related indicia. Pet. 36-44.

that is “indicating a validity of a phone number,” these generic disclosures fail to show that this limitation is met.

*

*

*

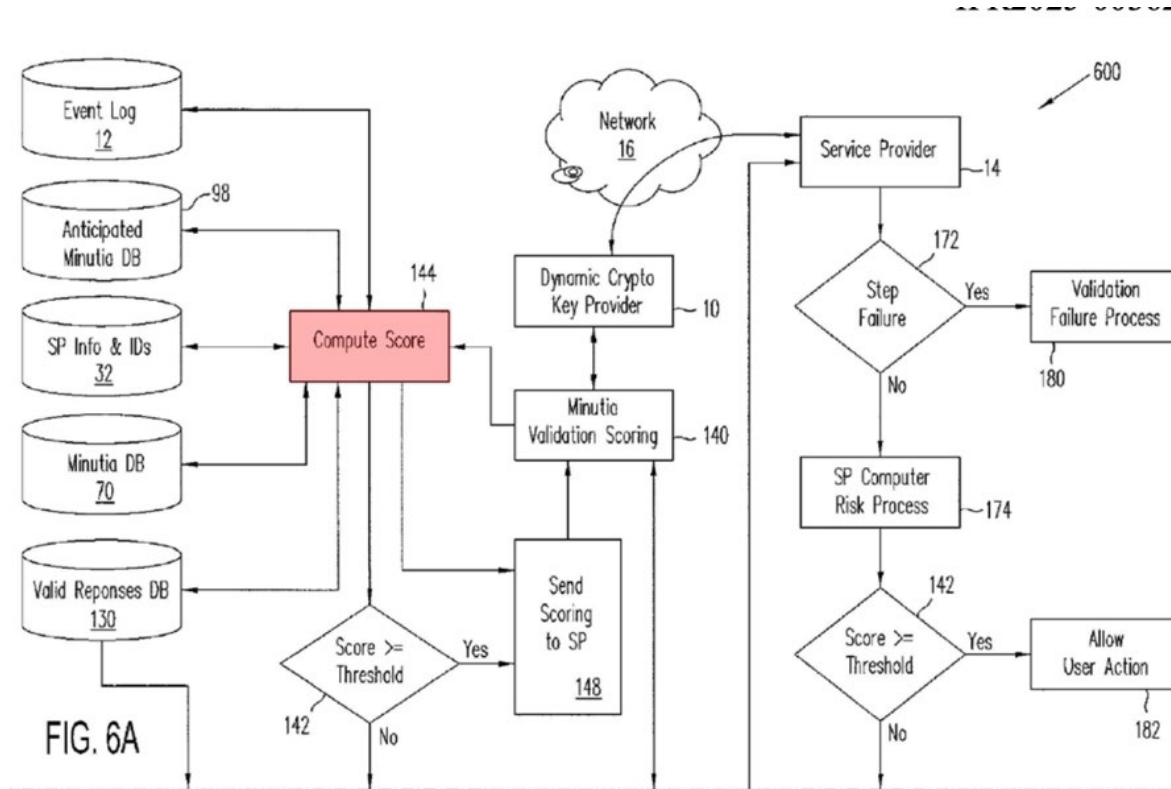
Accordingly, Har and Miller do not disclose or teach the “*information pertaining to a call, including*” the (1) “*value*” and (2) “*score*” claimed.

B. The Petition Fails To Show That The Sole Ground “*Performs A Security Determination Based At Least In Part On The Score ... And At Least In Part By Verifying The Value*”.

In addition to the missing limitations above, the Petition fails to establish that the proposed Har/Miller combination performs a “*security determination*” based at least in part on both (1) a “*score*” and (2) verification of a “*value*,” as expressly required by claim 1.

The claim language recites that the determination be made “*based at least in part on the score generated for the calling device, and at least in part by verifying the value included in the information pertaining to the call.*” Ex. 1001, 22:56-59, 24:33-36, 24:51-54. For similar reasons to why the combination of Har/Miller is not shown to receive both of the claimed “*value*” and the claimed “*score*,” Petitioner also fails to show performing a security determination based on both values.

For example, as already noted above, *supra* § III.A.4, Petitioner relies on Miller’s Figure 6A, showing box 144 creating a “compute score”:



Pet., 37 (annotation Petitioner's).

As is clear from the figure above, Miller's "compute score" generated in box 144 is compared to a "threshold" in box 142. *Accord, e.g.*, Pet., 45. As previously explained, *supra* § III.A.4, Miller's "compute score" that is generated in box 144 already includes various computer minutia. Petitioner does not show any reason why the ordinary artisan in this art at the time of the invention would, in addition to using this score, *also* separately verify the same underlying minutia or a digital signature derived from it. As shown above, Miller itself does not disclose or suggest such a two-part evaluation. It teaches the compute score as a singular basis

for determining trustworthiness, and that score already reflects an internal assessment of device identity. Pet., *e.g.*, 25. No reason is shown, in the absence of hindsight, why the ordinary artisan would have found it obvious to redundantly re-verify the same device minutia after having already scored them.

Accordingly, Petitioner fails to show how the combined system would perform, or suggest to the ordinary artisan that it be modified to perform, a “*security determination*” based independently on both a score and on verifying a value, as required by the claims.

C. Har And Miller Are Not Shown To Teach Or Suggest Any Of The Remaining Claims 2-28.

The analysis presented above with respect to claim 1 applies equally to independent claims 27 and 28. With respect to the patentability of those claims, the Petition asserts only that they are “method and computer program product claims corresponding to claim 1 and invalid for the same reasons.” Pet., 75. As well, because Har and Miller are not shown to teach or suggest each and every element of any independent claim, they do not teach or suggest each and every element of any of dependent claims 2-26.

IV. CONCLUSION

For the reasons described herein, the Petition fails to demonstrate a reasonable likelihood of success as to any of the challenged claims. The Petition should be denied.

Respectfully submitted,

/ Sal Lim /

Sal Lim (Reg. No. 45,706)
KRAMER ALBERTI LIM & TONKOVICH LLP
Kenneth J. Weatherwax (Reg. No. 54,528)
LOWENSTEIN & WEATHERWAX LLP

Date: July 15, 2025

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITS

This Patent Owner Preliminary Response (the “POPR”) consists of 9860 words, excluding table of contents, table of authorities, certificate of service, this certificate, or table of exhibits. The POPR complies with the type-volume limitation of 14,000 words as mandated in 37 C.F.R. § 42.24. In preparing this certificate, counsel has relied on the word count of the word-processing system used to prepare the paper (Microsoft Word).

Respectfully submitted,

/ Kenneth J. Weatherwax /

Date: July 15, 2025

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the following documents were served
by electronic service, by agreement between the parties, on the date below:

**PATENT OWNER'S PRELIMINARY RESPONSE
EXHIBITS 2009-2010**

The names and addresses of the parties being served are as follows, pursuant
to their agreement to electronic service (*see* 00360 Pet., 82; 00361 Pet., 81; 00362
Pet., 81):

AT&T Services Inc.,
Cellco Partnership d/b/a Verizon Wireless, and
Nokia Of America Corporation,

by and through their counsel:

Kevin Anderson	KPAnderson@duanemorris.com
Patrick D. McPherson	PDMcPherson@duanemorris.com
Glenn D. Richeson	GDRicheson@duanemorris.com
Brian H. Pandya	BHPandya@duanemorris.com

/ Abbie Neufeld /

Date: July 15, 2025