

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 IPR2025-00361
Patent 11,856,132 B1

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

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. FACTUAL BACKGROUND.....	4
A. The '132 Patent	5
B. Har	7
C. Miller.....	11
III. INSTITUTION SHOULD BE DENIED BECAUSE THE PETITION FAILS TO SHOW A REASONABLE LIKELIHOOD THAT THE SOLE GROUND RENDERS ANY CLAIM OBVIOUS....	13
A. Har alone or in combination with Miller is not shown to teach or suggest receiving all three types of information pertaining to a call, as required by the claims.	14
1. Har alone or in combination with Miller is not shown to teach or suggest receiving the claimed phone number associated with a callee device.	14
a) Har is not shown to teach or suggest receiving a callee device's phone number as information pertaining to a call.....	15
b) The addition of Miller does not fill the gap in Har's disclosure.	17
2. Har alone or in combination with Miller is not shown to teach or suggest receiving information pertaining to a call that includes a cryptographic element associated with a caller device.	21
a) Har does not teach or suggest receiving a cryptographic element associated with a caller device.....	23
b) The addition of Miller does not fill the gaps in Har's disclosure.	27
B. Har in Combination With Miller Does Not Disclose Performing A Security Determination Based On The Claimed Cryptographic Element.....	30
C. The Petition fails to establish that a person of ordinary skill in the art would have been motivated to combine Miller with Har.	36

D. Har in combination with Miller does not teach or suggest any
of the remaining claims 2-19.....39

IV. CONCLUSION40

EXHIBIT LIST	
2001	Memorandum Claim Construction Op. & 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)
2006	<i>RightQuestion, LLC v. Verizon Commun’ns Inc., et al.</i> , No. 2:24-cv-00091-JRG, Dkt. 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 [New]	L. Hall, “Relentless robocalls anger consumers,” Consumer Action News (Spring 2019) [Relentless-Robocalls]
2010 [New]	<i>eSignature</i> , docusign, https://www.docusign.com/products/electronic-signature (last accessed July 15, 2025) [docusign-eSignature]

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 the sole independent claim under 35 U.S.C. §103. This combination fails for at least three reasons.

First, neither Har alone, nor the combination of Har with Miller, teaches or suggests the first step in the claimed process: receiving information pertaining to a call, wherein the information includes a *phone number associated with a callee device and a cryptographic element associated with a caller device*.

Har discloses receiving information about a *callee* in an authentication request, not information about the callee’s *device* (such as the device’s phone number). While the Petition argues that it would be obvious to include the callee device’s phone number, Har teaches away from this rationale. The Petition also attempts to equate the claimed phone number to a previously received phone number kept in data storage. But this argument fails because the claimed phone number must be received as *information pertaining to a call initiated by a calling device*; it cannot be something that is merely previously stored before the call.

The Petition’s addition of Miller also fails to teach or suggest receiving the callee’s phone number as information pertaining to a call. The Petition’s

combination relies on the assertion that Miller's service provider 14 is a device. But, as is commonly understood and confirmed by the disclosures of both Miller and the '132 patent, a service provider is not a device as claimed. Rather, a "device" indicates a communication device used by a user (or a client device), and a "service provider," indicates an entity that provides a service to a client device.

Similarly, the Petition fails to establish that Har alone or in combination with Miller teaches or suggests receiving information pertaining to a call that includes *a cryptographic element associated with a caller device*. The Petition relies on Har's disclosure that an authentication request can be encrypted and digitally signed by a user. But the Petition fails to establish that any element used in either of these processes is a cryptographic element associated with a caller device.

Furthermore, the Petition's combination of Miller with Har also fails to teach or suggest receiving a cryptographic element as information pertaining to a call. The Petition relies on Miller's disclosure of a key created by a computer 18 as part of a challenge-response process. But this key is a unique identifier for computer 18, not a cryptographic element as claimed in the patent.

Second, the combination of Har and Miller does not teach or suggest *performing a security determination based at least in part on the cryptographic element* received in the first step of the claim. Because the Petition fails to establish that the combination of Har with Miller teaches the claimed step of receiving a

cryptographic element related to a caller device, it follows that the combination cannot perform the claimed security determination based on this missing cryptographic element.

Moreover, the combination fails for the independent reason that it relies on a flawed analysis of Miller's calculation of a score as part of its authentication process. As described by Miller, a score is based on changes in individual values of computer minutia. But neither computer minutia, nor changes in computer minutia, is a cryptographic element. The Petition also fails to explain how calculating a score, without more, is performing a security determination as recited by the claims. For both reasons, Miller's calculation of a score is not performing the claimed security determination based on a cryptographic element.

Third, the petition fails to establish a motivation to combine Har with Miller. The Petition's proposed combination purportedly augments Har's user authentication by adding Miller's device authentication. According to the Petition, a motivation to make this combination can be found within the references themselves, which allegedly suggest that the combination would create a more secure system. The Petition does not, however, identify any disclosure in either reference that supports this conclusion. If anything, Har teaches away from using device-based authentication.

The Petition alternatively argues that a person of ordinary skill in the art would be motivated to create a combined system because it would be more efficient. But once again, if anything, the references suggest the opposite: that the proposed combination creates a more complicated system without any corresponding benefit over the results that can be achieved by Har alone.

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), as 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 '132 Patent

U.S. Patent No. 11,856,132, entitled Validating Automatic Number Identification Data, was filed on April 12, 2021, and claims priority to provisional application No. 61/901,322 filed on November 7, 2013.

The invention of the '132 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.

Spoofing is a pervasive problem. Americans received more than 47 billion robocalls in 2018 alone, many of which involved spoofed numbers. *See*, Ex. 2009 [Relentless-Robocalls]. Spoofing makes robocalls harder to detect and more likely to be deceptive. 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 spoofer who frequently changed numbers or mimicked trusted sources.

As explained in the Background of the Invention of the '132 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 [’132 patent], at 1:27-36.

The ’132 patent specification provides several examples of how to make a security determination, including using a cryptographic element associated with a calling device. As explained by the ’132 patent, a device can use a unique temporary identifier either as a secret key or to compute a secret key. *Id.*, at 12:44-46. Exemplary methods of computing a secret key include the well-known Diffie-Hellman key exchange or RSA key transport, where the enrolling device uses a public key associated with the verification service provider to compute an encrypted key, which is then sent to the verification service provider in an encrypted manner. *Id.*, at 12:46-51.

A verification service provider and the calling device can both store this key. *Id.*, at 12:53-56; *see, also*, 3:34-35 (device 102 can store a secret key in storage 114). In this example, the key is symmetric, which means that the encrypting and decrypting devices both use the same key.

When the device initiates a call to another device, the caller device “securely conveys information about the call to a verification service via a message encrypted with the symmetric key.” *Id.*, at 12:59-67. In addition, the called device captures the ANI data of the caller device and queries the verification service provider about the call. *Id.*, at 13:1-3. The verification service provider then compares the information received from the caller device with the request from the called device and returns a verification result. *Id.*, at 13:3-5.

The information received by the verification service provider about the call, and used to determination a verification result, can include “at least one of a timestamp, a unique identifier, a symmetric key, and device information, which is passed to the Verification Service to prevent, for example, attempts to spoof the legitimate device.” *Id.*, at 9:20-26.

The benefits of the claimed invention are significant. By enabling real-time verification of caller ID information, the claimed invention helps restore confidence in answering phone calls. 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.

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 ’132

patent as obvious in combination with Miller. Unlike the '132 patent, Har is not trying to solve the problem of spoofing a phone number. Rather, Har's objective is to identify a caller.

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] at [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. Ex. 1004 [Har] at [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], [0018].

For example, a caller may identify himself as a service provider, offering a new service or a current promotion,” and “request sensitive personal information.” *Id.*, [0011]. 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 encryption using a secret, private key, or a signature such as using a digital certificate. *Id.* at [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.” Ex. 1004 [Har], at [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. Ex. 1004 [Har] at, *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.

Ex. 1004 [Har] [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.

Ex. 1004 [Har] at [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.

Ex. 1004 [Har] at [0030]. Finally 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.

Ex. 1004 [Har] at [0031]. 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. Ex. 1004 [Har] at 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* Ex. 1004 [Har] at 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* Ex. 1004 [Har]; *accord id.*, claims 6, 8-20 (expressly requiring encryption/decryption).

C. Miller

The Petition relies on combining Har with 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 ’132 patent.

Miller and the ’132 patent solve different problems using different solutions. As previously explained, the ’132 patent describes how to 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. 1022 [Miller], at [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.*, at [0017].

Miller’s described DKCP performs a “challenge, response and validation sequence” in order to authenticate “a specific computer 18 and service user 20.” *Id.*, at [0050]. This process is based on “minutiae” collected about the user and the user’s computer. Minutia may be “any piece[s] 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.*, at [0030].

Miller’s Figure 2 shows the “challenge, response and validation process performed by the system of Figure 1.” *Id.*, at [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.*, at [0062]. The challenge asks the service user’s computer to send back a response using particular minutiae selected by the DKCP. *Id.*, at [0065]. Miller’s 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 dynamic key crypto provider 10 to determine if there is a match.” *Id.*, at [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.*, at [0069]. Miller's service provider then decides how to respond to the failure, which can include denying the user's service request. *Id.*, at [0118].

The DKCP can also calculate a "score" for the response received from the service user's computer. *Id.*, at Fig. 6 and [0104]. Miller's compute score process 144, shown in its 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.*, at [0105], [0111]. If the score meets the threshold, the DKPC sends the score to the service provider. *Id.*, at [0111]. Miller's service provider then decides whether to grant the user access to the service. *Id.*, at [0119].

If the score is below the threshold, then the DKPC performs an additional authentication process, called a "step-up request." *Id.*, at [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.*, at [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 relies on a flawed analysis and should be denied for at least three reasons. *First*, the Petition fails to demonstrate a reasonable likelihood that Har alone or in combination with Miller teaches or suggests the claimed step of receiving

three types of information pertaining to a call initiated by a caller device. *Second*, the Petition fails to demonstrate a reasonable likelihood that Har alone or in combination with Miller teaches or suggests the claimed step of making a security determination using the claimed cryptographic element. *Third*, a person of ordinary skill in the art would not be motivated to combine Har with Miller.

A. Har alone or in combination with Miller is not shown to teach or suggest receiving all three types of information pertaining to a call, as required by the claims.

The first step of claim 1 requires “receiving information pertaining to a call initiated by a caller device, wherein the information pertaining to the call comprises data related to (1) a phone number associated with a callee device, (2) device information associated with the caller device, and (3) a cryptographic element associated with the caller device.” Ex. 1001 [’132 Patent], at 22:55-60 (claim 1). Har in combination with Miller is not shown to teach or suggest receiving either a phone number associated with a callee device, or a cryptographic element associated with a caller device, as information pertaining to a call.

1. Har alone or in combination with Miller is not shown to teach or suggest receiving the claimed phone number associated with a callee device.

Har, either alone or in combination with Miller, is not shown to teach or suggest receiving a callee device’s phone number as information pertaining to a call. Har teaches that an authentication request can include information about the callee,

not about the callee's device (such as its phone number). The Petition's addition of Miller fails to fill this gap, at least because it relies on a flawed assumption that Miller's service provider 14 is a "device" as claimed.

a) Har is not shown to teach or suggest receiving a callee device's phone number as information pertaining to a call.

For the claimed step of receiving a callee phone number, the Petition relies on Har's disclosure of an authentication server receiving an authentication request, which includes "information identifying the *callee*." Pet. at 29 (citing Ex. 1004 [Har], at [0023] (emphasis added)). But Har does not disclose including the callee's phone number as identification information about the callee, so the Petition argues that it would be obvious to do so for several reasons. Pet. at 30. None is substantiated.

The Petition first argues that it would be obvious because "Har teaches that 'user information ... includes the mobile telephone number of users,'" providing no citation for this quoted language. *Id.* Relatedly, the Petition argues that "it is also obvious, and well-known, that information related to a call includes the recipient's phone number." *Id.* Even assuming that both these statements are true, they do not lead to the conclusion that it would be obvious for Har's authentication request to include this particular piece of information, out of all the available information about a callee, in an authentication request, as required to meet the claims.

The Petition tries to rationalize including the callee's phone number in an authentication request "so that the authentication server could identify the callee device and communicate with it." *Id.* Similarly, the Petition argues that Har's disclosure of "information identifying the callee" teaches or suggests "data related to" the callee's phone number "because the callee is contacted and identified by using the phone number." *Id.*

But Har provides a contrary teaching for how to contact a callee. According to Har, the authentication server may have a data store of user information that includes the mobile telephone numbers of users. Ex. 1004 [Har] at [0018]. If the authentication server wants to communicate with the callee, Har teaches that the "authentication server can look up in its data store, the mobile telephone number of the user to whom the authentication information will be sent (the second user)." *Id.* Har therefore teaches using a previously stored phone number, not a phone number received in an authentication request, to contact the callee.

Relatedly, the Petition also argues that Har's authentication server performs the claimed step of "receiving" the callee's telephone number when it builds this data store, such as through a registration process. Pet. at 30. But creating the data store, which is described by Har as including multiple types of information for multiple users, *see* Ex. 1004 [Har] at [0018], presumably occurs before a particular call is initiated for which a particular Har user's authentication is requested. As

such, when Har's authentication server receives information for its data store, it is not shown to be *receiving information pertaining to a call initiated by a caller device*, as required by the claims.

Finally, the Petition claims, without explanation, that Har's disclosure of user credentials such as PINs or passwords sent in a message digitally signed by the callee somehow meets the claim language of receiving information pertaining to a call, including "a phone number associated with a callee device." Pet. at 30-31. Such an unsupported and unexplained assertion is not entitled to any weight. Such user credentials would, as far as the record goes, apply to the user generally, not to any particular call.

b) The addition of Miller does not fill the gap in Har's disclosure.

The Petition next asserts that it would be obvious for an authentication server that combines the functions of Har and Miller to receive a callee's phone number. Pet. at 31. According to the Petition, this is so because it would be obvious for Har's authentication server to implement the purported ability of Miller's DKCP to communicate with a callee device. *Id.* This combination fails for at least two reasons.

First, this combination appears clearly contrary to Har's explicit teaching, explained above, that its authentication server contacts a callee by using a previously

stored phone number. The Petition provides no explanation for why a person of ordinary skill in the art would need or want to contact a callee in any other way.

Next, the combination is premised on the flawed assumption that Miller's service provider is a callee device. *Id.* (“Miller's DKCP communicates with the callee device (e.g., Miller's ‘service provider’).”). But a service provider is not a device, as those terms are ordinarily understood and used by both Miller and the '132 patent.

The '132 patent describes a device as a communication device that is used by an end user (also called a client device). *See, e.g.,* Ex. 1001 ['132 Patent], at 2:46-56 (“Described herein are techniques for ascertaining the identity of a device....example techniques disclosed herein include a client-side (e.g., end-user phone-side) agent....”). Referring to the system shown in Figure 1, the '132 patent defines “client device 102” as “a device with telephonic capabilities that is used, by a user, to contact callee 118 (e.g., a bank).” *Id.* at 2:66-3:1. Specific examples of a device include a phone (Fig. 1, 102), telephonic device (Fig. 3B, 322, 328), or smartphone (Figs. 4-14). *Id.*, at Figs. 1, 3B and 4-14.

Miller uses the term device in the same way, to mean a communication device used by a user (or client device). For example, Miller states that “[d]ynamic key cryptography in accordance with one or more embodiments ... provide authentication between a client electronic computer and a service provider”). Ex.

1022 [Miller], at [0026]. Miller further refers to identifying a “user’s computer or other electronic device,” which can be “e.g., a mobile phone or personal computing device.” *Id.*, at [0026]. Miller and the ’132 patent together demonstrate that the ordinary meaning of device, as understood in the context of their technology, indicates a communication device used by an end user (or client device).

According to the Petition, Miller’s service provider 14 is the claimed device. Pet. at 31. (“the callee device (e.g., Miller’s ‘service provider’)”). But this conclusion is not shown to be supported by Miller. Nor is it shown to be supported by the ordinary meanings of device and service provider.

Miller states that service provider 14 “is a customer receiving services from dynamic key crypto provider 10....Examples of a service provider 14 include but are not limited to social networking websites, corporate IT services, and online banking, healthcare, and travel services.” Ex. 1022 [Miller] at [0049]. None of these examples is a client device.

The record shows that a service provider would have been, and is, commonly understood to be an entity that offers services to users. A typical service provider is hosted by one or more servers, most likely a bank of servers, none of which is a device as that term is used by either Miller or the ’132 patent. Here again, Miller and the ’132 patent demonstrate a consistent understanding of the terminology. Miller describes a service provider as providing “social networking websites,

corporate IT services, and online banking, healthcare, and travel services.” Ex. 1022 [Miller] at [0049]. The ’132 patent identifies a service provider as a bank or other entity, Ex. 1001 [’132 Patent], at 4:44, and includes an extensive description of a verification service provider as an entity that provides identification services. *See, e.g.*, Ex. 1001 [’132 Patent], Figs. 1, 2A and 2B and accompanying descriptions.

In addition, a service provider would have been commonly understood to have greater processing power and storage capabilities than a user device. Miller demonstrates this ordinary understanding. As described by Miller, the DKCP may be a “web service capable of securely manipulating and analyzing large amounts of data” and it may be “cloud-based so it can have sufficient computational speed and power to off-load intensive computational efforts from a sometimes resource constrained computer 18.” Ex. 1022 [Miller], at [0049]. The Petition provides no explanation or evidence to overcome this ordinary understanding that a computationally powerful service provider is not the equivalent of a less powerful and less capable user device.

As Miller and the ’132 patent both demonstrate, a service provider is an entity that provides a service, and a device is a client device used by an end user. Miller does not teach that its service provider 14 is a device, as that term is used by the ’132 patent or as understood by a person of ordinary skill in the art.

The Petition's proposed combination of Miller and Har therefore fails because it is based on functionality that does not exist in Miller. For this additional reason, the combination does not teach or suggest the claimed step of receiving information pertaining to a call initiated by a caller device, including the callee device's phone number.

2. Har alone or in combination with Miller is not shown to teach or suggest receiving information pertaining to a call that includes a cryptographic element associated with a caller device.

Har, whether alone or in combination with Miller, does not teach or suggest receiving the claimed "cryptographic element," which a person of ordinary skill in the art would understand to require an element used in a cryptographic function.

Cryptography is generally understood as a method of protecting information by using a key and applying an algorithm to encrypt the information. For example, as explained by the '132 patent, when a caller device initiates a call to another device, the caller device can "securely convey[] information about the call to a verification service via a message encrypted with [a] symmetric key." Ex. 1001 ['132 Patent], at 12:59-67. The '132 patent provides several additional examples of cryptographic elements, including one or more public keys, one or more secret keys, certificates used to verify phone numbers, and one time pad codes, which are used in a cryptographic algorithm where text is combined with a random, secret key (the "pad") to produce a secure ciphertext. *Id.*, at 7:47-48, 14:63-65, 23:19-21 (claim 8).

Miller's disclosure is consistent with the '132 patent in this regard, stating that "[c]ryptography generally uses an algorithm...to combine cryptographic keys (which may be symmetric, public, or private, for example) with plain text to form a ciphertext." Ex. 1022 [Miller], at [0006]. According to Miller, "[t]he use of cryptography is common to authenticate identities, protect data, and digitally sign the summary (i.e. digest) of an action." *Id.*, at [0005].

The Petition relies on a different, overly broad understanding of the claimed "cryptographic element." According to the Petition "a POSA would understand that 'cryptographic element' encompasses techniques using certificates and public keys because they are examples of elements used for cryptographic purposes." Pet. at 37. This assertion is broader than the record will support. Patent Owner agrees that a cryptographic element is used for a cryptographic purpose, such as protecting the confidentiality of data. But for this purpose to be cryptographic, it must be achieved using cryptography, thus in a cryptographic function, as opposed to some other method such as delivering information to an intended recipient in a sealed envelope. A more accurate definition, and one that would be understood by a person of ordinary skill in the art as reflected by the consistent disclosures of the '132 patent and Miller, is that a cryptographic element is used in a cryptographic function.

Har, whether alone or combination with Miller, fails to teach or suggest receiving the claimed cryptographic element, which, according to the claim language

as it would be understood by the ordinary artisan, must be used in a cryptographic function, associated with a caller device, and received pursuant to a phone call initiated by the caller.

a) Har does not teach or suggest receiving a cryptographic element associated with a caller device.

The Petition's application of Har depends on an authentication server receiving information in an authentication request, which Har discloses can be sent using two different cryptographic functions. Pet. at 37-38. First, the message can be encrypted using the server's public key. Pet. at 38, Ex. 1004 [Har] at [0016]. Second, the message can be digitally signed using the private key of the user requesting authentication. Pet. at 38, Ex. 1004 [Har] at [0023]. Neither form of security involves receiving the claimed cryptographic element as information pertaining to a call.

The first form of security admittedly uses a type of cryptographic element, which is the server's public key. Ex. 1004 [Har] at [0016]. But the *server's* public key is not the claimed cryptographic element, because the claimed cryptographic element must be associated with *the caller device*. The Petition provides no explanation for why or how the server's public key is associated with the caller device.

In addition, the Petition does not establish that the server's public key is included in an authentication request received by the authentication server, which is

a necessary part of the Petition’s analysis of *receiving* a cryptographic element as *information pertaining to a call initiated by a caller device*. See, e.g., Pet. at 16 (describing a caller sending an authentication request as “Step 1” in the proposed combination of Har and Miller). Indeed, it would make little sense to include the server’s public key in Har’s authentication request, given that the authentication server presumably knows its own key, which, moreover, is public.

The server’s public key is also a static element not unique to any particular call. As such, it is not shown to be *information pertaining to a call* as required by the claims, but rather a piece of information pertaining to the server. For this additional reason, Har’s disclosure of using a server’s public key to encrypt an authentication request does not teach or suggest receiving the claimed cryptographic element as part of information pertaining to a call.

The second alleged cryptographic function identified by the Petition is verifying a digital signature of the user who is requesting authentication. *Id.*, at 38. While the digital signature, and the keys used to apply and verify it, may be cryptographic elements, they are not the claimed cryptographic elements because they are not associated with a caller device as the claims require. Rather, Har teaches that a digital signature and keys are associated with a user. See, e.g., Ex. 1004 [Har] at [0017] (authentication server can verify “that the message is *signed by the user*”), [0023] (authentication request “can be signed using *the caller’s* private key”), [0026]

(“digital signature can be verified using the public key *of the user* sending the message”) (emphases added).

This user association makes sense, and is consistent with the disclosures in the patent and the art, because the purpose of using a digital signature is to verify that the user authorized or is the source of the signed information. The user can accomplish this objective regardless of which device is used to apply the signature, whether it is the user’s mobile phone, laptop, or desktop, or even a device belonging to someone else. Docusign provides a ubiquitous example of this capability, allowing a user to apply an electronic signature as “a legally binding way to sign documents online from any device.” *See* Ex. 2010 [docusign-eSignature].

The Petition offers several further arguments for why receiving the claimed cryptographic element is suggested by Har, but each argument is flawed.

First, the Petition argues that a user’s digital signature is “data *related to* ... a cryptographic element associated with the caller device,” because the digital signature is associated with one or more keys, which are themselves cryptographic elements that must be used in order to verify the digital signature. Pet. at 38. This argument fails for essentially the same reason explained above: there is no teaching in Har that any of the keys associated with a digital signature is associated with a caller device. Rather, Har teaches that the keys upon which the Petition relies are

either associated with a user (the user's private and public keys) or with the authentication server (the server's public and private keys). *See, id.*, at 38.

Second, the Petition argues that a digital certificate, as well as the caller's private key, are related to and associated with whatever user device creates a digital signature. *See, id.*, at 39 (digital certificate is signed by a user's key, and created and transmitted by a device that stores the key in its memory), and 38 (caller's private key is stored on the user's mobile device and used by the mobile device to apply a digital signature). The Petition cites no disclosure in Har to support these assertions. Rather, the Petition's only support for this argument is the testimony of its declarant, Dr. McDaniel, repeating the argument in the Petition. *Id.*, at 39 (citing Ex. 1003 [McDaniel Decl.], ¶112). This *ipse dixit* of Petitioner's declarant is entitled to no weight in satisfying Petitioner's burden of proof, since neither the Petition nor the declaration substantiates it with any other evidence. *See* 37 C.F.R. § 42.65 (a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.").

Third, the Petition argues that the Board should reject any argument that Har's teaching is limited to a user's keys, because according to the Petition's declarant, "[a] POSA would know cryptographic keys cannot be meaningfully associated with a user, but rather with a device." *Id.*, at 39 (citing Ex. 1003 [McDaniel Decl.], ¶113). The declaration identifies no evidence to support Dr. McDaniel's assertion; nor does

it identify any disclosure in either the '132 patent or in Har that support his purported explanation for how keys operate. This unsupported opinion is thus entitled to little if any weight. And, even if Dr. McDaniel is assumed to be correct, neither the declaration nor the Petition asserts or substantiates that a user's key is included in the authentication request, which is necessary for the Petition's theory of how an authentication server receives information pertaining to a call.

Fourth, the Petition argues that Har teaches the general concept that keys can be associated with devices, because Har references a server's public and private keys and a server is (allegedly) a device. Pet. at 39-40. But as already explained in the prior section, the Petition is incorrect that a person of ordinary skill in the art would understand that Har's server is the "device" recited in the claimed invention.

b) The addition of Miller does not fill the gaps in Har's disclosure.

The Petition next asserts that a response generated by computer 18, as part of Miller's challenge-response process, is a "cryptographic element" as claimed because Miller calls the response a "key." Pet. at 40 ("Miller unequivocally discloses a cryptographic element (a 'key')" based on minutia specific to a device). This argument, however, relies on a flawed application of different meanings for the term "key."

Miller uses the term "key" to mean *a unique identifier* for computer 18, which is created during Miller's challenge-response process. As shown in and described

in connection with Miller's Figure 2, Miller's DKCP builds a challenge by selecting a collection of possible computer minutia types and then sending that collection to computer 18. Ex. 1022 [Miller], at Fig. 2B, steps 116 and 2020, [0063]. Miller's computer 18 then collects the values of the minutia identified in the challenge and aggregates those values to form a response. *Id.*, at Fig. 2B, step 2040, [0065].

Miller calls this response a key. *Id.*, at [0065] (computer 18 fetches values of minutia to "build a key"). And this key, as described by Miller, is used to identify the computer. *See, e.g., id.*, at [0055] ("The computer 18 may have specific values for the [listed minutia], from which it may be possible to accurately and uniquely identify the specific computer 18."), [0056] ("each single computer 18 can be uniquely identified by matching its unique computer minutia").

Even the Petition recognizes, however, that the purpose of this "key" is to be "a unique device identifier" to identify computer 18. *See* Pet. at 33 ("Miller creates a unique device identifier using sets of 'computer minutia'"). As an identifier for computer 18, this "key" in Miller is not shown to serve any cryptographic function and is therefore not the claimed cryptographic element. Nor does this unique identifier become a cryptographic element merely because it can be encrypted by applying a function *Fn.* *See*, Pet. at 41 (quoting Ex. 1022 [Miller] at [0065]). An encrypted message and a cryptographic element are not the same thing; nor, unsurprisingly, does Petitioner attempt to show otherwise.

Notably, Miller separately discloses a “cryptographic key,” which can be “used to encrypt an actual response to [a] challenge.” Ex. 1022 [Miller] at [0013]. But the Petition does not rely on this cryptographic key as corresponding to the claimed cryptographic element. And, Miller states that this “cryptographic key is never transmitted from the device across any communication channel.” *Id.*, at [0013]. As such, Miller explicitly teaches that its cryptographic key is *not* information received by the DKCP. Miller’s DKCP therefore cannot perform the claimed step of receiving this information.

Alternatively, and similarly, the Petition argues that Miller’s response key is *data related to* a cryptographic element because the computer can apply a cryptographic function F_n to it. Pet. at 41. This argument is flawed because, as explained above, information does not become a cryptographic element, or related to a cryptographic element, merely because it has been encrypted.

The Petition also argues that Miller’s key is relevant because the ’132 patent purportedly discloses a “‘cryptographic element’ that is similar to Miller’s cryptographic function.” Pet. at 41-42. It is true that the ’132 patent discloses a caller device sending a cryptographic element to a verification service provider, as demonstrated by the excerpt cited by the Petition. Pet. at 41-42 (citing 132 Patent, 15:66-16:7). But the Petition provides no explanation for how that correlates to “Miller’s cryptographic function,” whatever that may mean. The Petition therefore

again fails to show that which is to be proved: that Miller meets the claimed “cryptographic element” limitation.

Finally, neither the Petition nor its expert’s supporting declaration provides an explanation for how Miller’s key supposedly should be combined with Har’s authentication message in order to form the claimed cryptographic element, or why it would be desirable to do so. *See* Pet. at 40-42. Regardless of whether the Petition’s arguments about Miller are correct, the Petition therefore fails to establish that combining Miller with Har teaches or suggests receiving the claimed cryptographic element.

B. Har in Combination With Miller Does Not Disclose Performing A Security Determination Based On The Claimed Cryptographic Element.

As explained in the previous section, Har alone or in combination with Miller does not teach or suggest “receiving information pertaining to a call initiated by a caller device, wherein the information pertaining to the call comprises data related to a cryptographic element associated with the caller device.” *See* Ex. 1001 [’132 Patent], at 22:55-60 (claim 1).

Without first receiving the claimed cryptographic element, the combination of Har and Miller cannot teach or suggest performing the claimed security determination. In addition to this flaw, the Petition’s combination of Har with Miller fails for additional reasons.

According to the Petition, the purported Har/Miller authentication server performs the claimed security determination in two ways, *see* Pet. at 42, which the Petition characterizes as a certificate-based determination and an information verification. Pet. at 44. Neither alleged security determination is shown to use a cryptographic element associated with a caller device, as the claims require.

For the “certificate”-based determination, the Petition relies on Har’s authentication server being able to decrypt an encrypted authentication request using the server’s public key and verify the digital signature of the user using the user’s public key. Pet. at 44. As explained in the previous section, neither a server’s public key, a user’s public key, or the user’s digital signature, is a *cryptographic element associated with a caller device*. As such, the Petition’s alleged certificate-based determination is not shown to be the claimed security determination performed based on a cryptographic element, as claimed.

For the information verification determination, the Petition first relies on Har’s authentication server to perform this verification. In the alternative, it relies on a combination of functionalities from Har’s authentication server and Miller’s DKCP. *See* Pet. at 18, 44-45. Neither approach teaches or suggests the claimed step of performing a security determination based on a cryptographic element.

First, the Petition notes that Har’s “authentication server 102 can verify that information included in the transmission sent by the sender agrees with information

for the sender stored in a data store associated with the authentication server.” Pet. at 44 (quoting Ex. 1022 [Miller] at [0026]). The Petition does not, however, identify anything in Har that teaches or suggests how a cryptographic element associated with a caller device is part of this information verification process. Instead, the Petition asserts without explanation that the information verified by Har’s authentication server can include Miller’s cryptographic key. Pet. at 44. The Petition’s only support for this statement is the testimony of its declarant, Dr. McDaniel, which repeats the Petition verbatim. Pet. at 44 (citing Ex. 1003 [McDaniel Decl.], ¶ 126). This *ipse dixit* is entitled to no weight, since neither the Petition nor the declaration substantiate it with any other facts or evidence. *See* 37 C.F.R. § 42.65 (a) (“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.”).

The Petition then alternatively switches to combining the functionalities of Har’s authentication server and Miller’s DKCP. *See* Pet. at 45-48. For this proposed combination/modification, the Petition relies on Miller’s DKCP making an alleged security determination “through its ‘*matching*’ and through its ‘*scoring*’ system.” Pet. at 48 (emphases added). Neither of these processes as described by Miller is shown to use the claimed cryptographic element to make a security determination.

As described by the Petition, Miller’s purported “matching” function corresponds to step 2050 of Fig. 2B. *Id.*, at 46. Miller’s DKCP performs this

function by “attempting to match any one or more of the Hx/Fy/Sz triplet as subject to Miller’s ‘cryptographic function’” against “information stored by the DKCP during the registration process prior to a security determination.” *See, id.*, at 46-47 (referring to steps 2007 of Fig. 2A and 2050 of Fig. 2B). The Petition identifies two reasons why matching an encrypted Hx/Fy/Sz triplet in this manner is a security determination based on a cryptographic element associated with a caller device. *Id.*, at 47. Both alleged reasons are flawed.

First, the Petition argues that the triplet used in the match is a cryptographic element because it “is subject to a cryptographic function.” *Id.*, at 46-47. Presumably, the Petition is referring to Miller’s disclosure that computer 18 can apply a mathematical or cryptographic function F_n to the computer minutiae it has collected for a response. Ex. 1022 [Miller] at [0065]. But, as previously noted above, information does not become a cryptographic element merely because it has been encrypted.

Second, the Petition suggests that a match is based on a cryptographic element “because Miller’s DKCP can store the registered information (for performing the match) in its ‘pre-processed’ form by calculating all the available encrypted responses that can be received.” Pet. at 47. To the extent that this assertion is understood, the Petition seems to be arguing that information gathered and stored

during a registration process, when encrypted, somehow equates to the claimed cryptographic element used to make a security determination.

This argument is flawed for at least the reason that the Petition's analysis for claim element 1.ii does not identify stored registered information as "data related to...a cryptographic element associated with the caller device." *See, id.*, at 40-42. The Petition's argument also fails because any information stored as part of a registration process presumably was received by Miller's DKCP prior to the initiation of a call for which a user seeks verification. Miller's DKCP therefore is not shown to perform the step of *receiving* this stored registered information as *information pertaining to a call initiated by a caller device*, as required by the claims. It follows that this stored registered information is not shown to form the basis for performing the claimed security determination, which must be based on a cryptographic element received as information pertaining to a call.

The Petition next argues that Miller's "scoring" function teaches or renders obvious the claimed security determination because, allegedly, "[t]o calculate the score, Miller compares (matches) the received minutia to verify the device." Pet. at 48 (emphasis added); *see also* Ex. 1022 [Miller] at [0105] (compute score process 144 computes a scoring of the minutia and minutia values used in a validated response).

This argument fails for at least the reason that it relies on individual computer minutia to make the security determination. Neither the Petition nor its supporting declaration argues or attempts to demonstrate that individual computer minutiae can be the claimed cryptographic element associated with a caller device. Rather, the Petition equates Miller's "key" to the claimed cryptographic element. *See*, Pet. at 40-42. The Petition never shows that individual computer minutia are the cryptographic element associated with a caller device.

Moreover, Miller explains that its scoring function is based on changes to individual minutiae, the values of which "can (and are expected to) change and evolve over time." Ex. 1022 [Miller] at [0030]. Miller's scoring function "isolates and evaluates the minutiae that have changed and uses confidence weightings against the predictability of such changes." *Id.* Nothing in the Petition or its supporting declaration suggests that changes in minutiae values could be equivalent to the claimed cryptographic element. As such, calculating a score from computer minutia, or from changes in computer minutia, is not performing the claimed security determination based on a cryptographic element, as claimed.

The Petition also appears to rely again on information previously stored during a registration process. Pet. at 48 (scoring process "matches at least a portion of Miller's store [sic] computer information which may be in encrypted form"). But as already explained, previously stored registration information is not the claimed

cryptographic element, which must be received as *information pertaining to a call initiated by a caller device*.

Finally, the Petition provides no explanation for why the act of calculating a score is the same as *performing a security determination*, as required by the claims. According to Miller, the DKCP calculates a score and then compares it against a threshold defined by the service provider. Ex. 1022 [Miller], [0105], [0111]. If the score meets the threshold, the DKCP sends the score to the service provider. *Id.*, at [0111]. The service provider then decides whether to grant the user access to the service. *Id.*, at [0119]. If the score is below the threshold, then the DKCP performs an additional authentication process, called a “step-up request.” *Id.*, at [0112]. Miller’s score by itself, without comparing a security threshold as a reference point, falls short of being a security determination.

C. The Petition fails to establish that a person of ordinary skill in the art would have been motivated to combine Miller with Har.

The Petition’s proposed combination of Har and Miller purportedly “augments” Har’s user authentication by adding Miller’s device authentication. Pet. at 15. According to the Petition, there are two reasons why a person of ordinary skill in the art would be motivated to make this combination. First, the references themselves suggest making the combination in order to achieve enhanced security. Second, the combined system would be more efficient. *Id.*, at 21-24.

Neither argument establishes that a person of ordinary skill in the art would have been motivated to make the proposed combination. Rather, a person of ordinary skill would, if anything, have recognized that the proposed combined system would add complexity to Har without any corresponding benefit to what can be achieved by Har alone.

The Petition's motivation to combine first relies on Miller's disclosure of its scoring process to fill alleged deficiencies in Har's disclosure of its matching process. *See, id.*, at 21-22. According to the Petition, Miller's disclosure provides additional details missing from Har, which can provide "significantly 'increased security' and authentication." *Id.*, at 21. But the Petition's analysis does nothing more than identify portions of Miller's process that purportedly *could* be added to Har. *See, id.*, at 22. The Petition does not identify specific portions of either reference that provide an express reason *why* to do so.

If anything, Har suggests that there would *not* be an enhanced security benefit achieved by adding Miller's device authentication to Har's user's authentication. Har teaches that its user identification system is meant to ensure that a caller is who he says he is, before providing or receiving sensitive personal information or account information. *See, e.g.*, Ex. 1003 [Har], at [0011]. Once a caller has been identified using information unique to that caller, Har's goal is fully satisfied. There is no further benefit achieved from adding the complexity described in Miller, in which a

score is derived from a broad array of device minutiae through an iterative challenge-response process. Nor is there any further benefit to Har shown from implementing the varying degrees of user authenticity contemplated by Miller through its subjective scoring process. In Har's system, a user is either identified or not, and there is no indication that variable levels of user validity would provide any improvement.

Har also provides an express teaching away from relying on device authentication. One of the problems that Har seeks to remedy is that "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." Ex. 1004 [Har], at [0011]. As explained by Har, "a service provider may call an account holder's mobile telephone number but without some degree of questioning, does not know if the user who answered the call is the account holder or someone else." *Id.* Adding Miller's device authentication process does nothing to address this problem and could, in fact, lead to a bad result if the caller relies on device information instead of user information.

For all of these reasons, the Petition fails to establish its first purported motivation to combine from the references themselves: "to improve security and better vouch for the calls and interactions with service providers as described in Har." Pet. at 22.

The Petition next argues that a person of ordinary skill in the art would be motivated to create a combined system because it would be more efficient. *See* Pet. at 23. Specifically, the Petition proposes that a combined system could use Har’s authentication of a digital signature as an initial, quick check. *Id.* If the check fails, then the process stops and “time and effort can be saved by not performing Miller’s detailed additional authentication (Har’s Step 2A above).” *Id.*

This argument apparently concedes that adding Miller’s device authentication process to Har adds a level of complexity, time, and effort that is so undesirable that it should only be performed when necessary (upon successfully authenticating a digital signature). Moreover, if the Petition’s earlier arguments are accepted, *arguendo*, that a digital signature is associated with a device, not a user, then this proposed process could lead to diminished system performance by rejecting a call from a legitimate user based on a device authentication failure. The Petition’s proposed combination therefore creates a more complicated system without any shown corresponding benefit over the results that can be achieved by Har alone.

D. Har in combination with Miller does not teach or suggest any of the remaining claims 2-19.

Claims 2-19 depend on claim 1. Because the combination of Har with Miller does not teach or suggest each and every element of independent claim 1, it does not teach or suggest each and every element of any of dependent claims 2-19.

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 9,218 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,

/ Abbie Neufeld /

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