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 IPR2025-00360
Patent 10,674,009 B1

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

TABLE OF CONTENTS

Page

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.) [5th-Amended-DCO]
2003	Michelle Umberger & Lissa Koop, *District court stays: a review of the past 12 months*, 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	*RightQuestion, LLC v. Verizon Communications Inc., et al*., No. 2:24-cv-00091-JRG, Dkt. Control Order (June 14, 2024) [June-14-2024-DCO]
2007	*USPTO rescinds memorandum addressing discretionary denial procedures*, 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 *RightQuestion, LLC v. Verizon Business Network Services LLC, et al*., No. 2:24-cv-00091-JRG [Amended-Invalidity-Contentions]
2009 [NEW]	L. Hall, "Relentless robocalls anger consumers," Consumer Action News (Spring 2019) [Relentless-Robocalls]

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 reference ("Miller") to challenge claims 1-23 under 35 U.S.C. §103. Miller, however, fails to teach or suggest at least two limitations of each independent claim.

First, Miller does not teach or suggest a "verification service provider" that obtains "information transmitted by a second ***device*** associated with a communications connection," between first and second devices. In the context of the claimed invention of the '009 patent, the ordinary meaning of the term "device" indicates a communication device used by a user (or a client device). The Petition, however, equates a "device" to a "service provider," which would have been understood to mean an entity that provides a service to a client device. Under their ordinary meanings, Miller's service provider is not a device as claimed, as confirmed by the disclosures of both Miller and the '009 patent.

In addition, the claimed verification service provider must receive, from the second device, "information … associated with a communications connection." In the context of the claimed invention, the '009 patent identifies this information as, for example, the caller ID presented to a user when receiving a communication such as a call or text. The called device then provides this number to the

verification service provider, along with a request for its verification, in order to start the verification process. In contrast, the Petition's application of Miller relies on "challenge-response" information transmitted by the calling device after the "challenge, response and validation" process has already begun. The Petition's assertion that Miller nevertheless suggests this claim limitation relies on flawed and unsubstantiated arguments.

Second, Miller does not teach a verification service provider that, "based at least in part on the security determination, selects an action comprising at least one of ***blocking*** a communication between the first and second devices, ***requesting*** additional authentication, and ***permitting*** the communication." Miller's DKCP, which the Petition equates to the claimed "verification service provider," does not select from these three actions. Instead, the Petition's analysis relies on Miller's service provider 14, which Petitioner equates to the claimed "second device," to select whether to block or permit a communication. The Petition thus fails to successfully map Miller to the claimed invention.

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 '009 Patent

U.S. Patent No. 10,674,009, entitled Validating Automatic Number Identification Data, was filed on November 5, 2018, and claims priority to provisional application No. 61/901,322 filed on November 7, 2013.

The invention of the '009 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] 1. 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 spoofers who frequently changed numbers or mimicked trusted sources.

As explained in the Background of the Invention of the '009 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 ['009 patent], at 1:20-30.

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 or responding to text messages. Consumers can better trust that the number they see on their screen is accurate, and telecom

providers can better filter out suspicious or fraudulent communications before they reach users.

B. Miller

The Petition relies solely 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 '009 patent.

Miller and the '009 patent solve different problems using different solutions. As explained in the previous section, the '009 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. 1021 [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 "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].

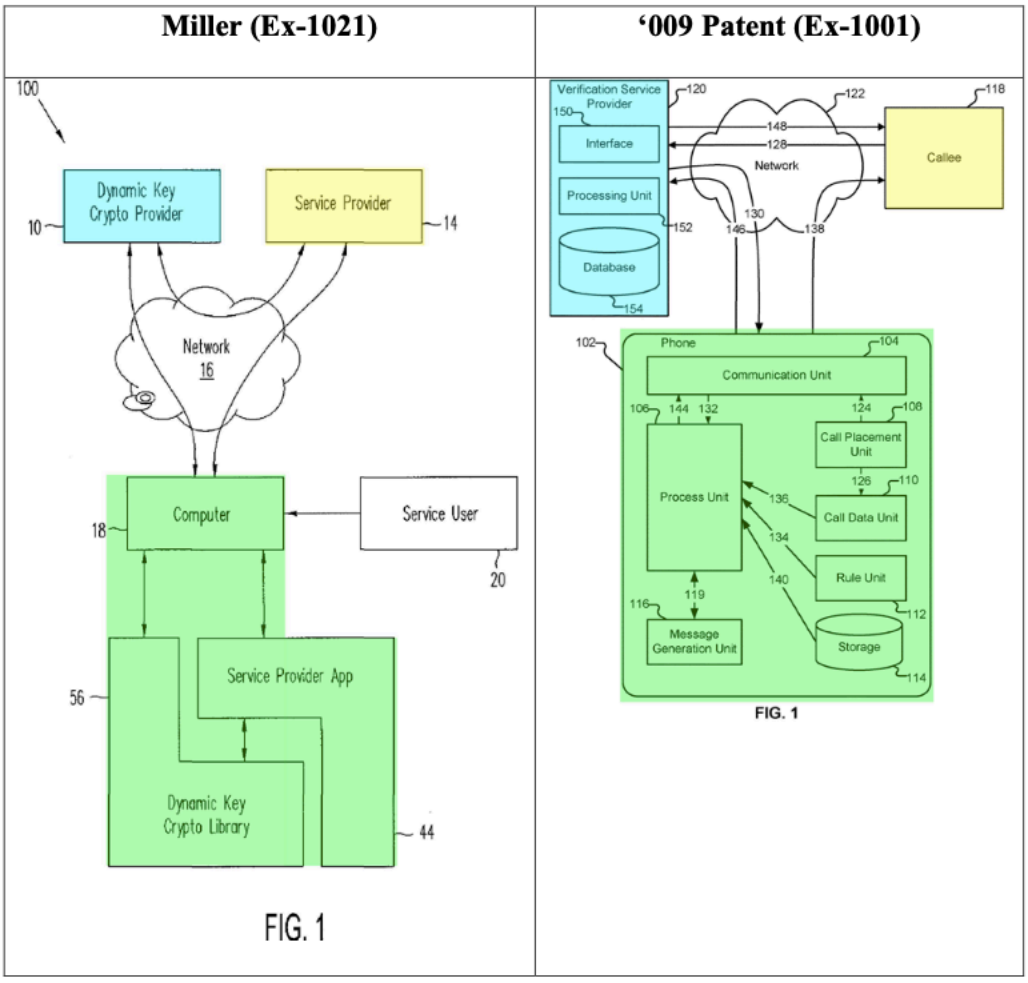
The DKCP can also calculate a "score" for the response received from the service user's computer. *Id.*, at Fig. 6 and [0104]. Miller's compute score process 144 shown in its Figure 6A computes a heuristic and probabilistic scoring based on the returned minutiae and then compares the resulting score 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's sole ground depends on the following purported correlation between the system of Miller and the system shown in Figure 1 of the '009 patent:



Pet. at 11. According to the Petition, Computer 18 is the claimed first device; Service Provider 14 is the claimed second device; and DKCP 10 is the claimed verification service provider. *Id*.

The Petition relies on a flawed analysis and should be denied because it fails to demonstrate a reasonable likelihood that Miller teaches or suggests at least two limitations included in each of the independent claims.[1] ***First***, Miller does not teach or suggest a verification service provider that obtains information transmitted by a second device associated with a communications connection. ***Second***, Miller does not teach or suggest a verification service provider that, based on a security determination, selects an action comprising at least one of blocking a communication between first and second devices, requesting additional authentication, and permitting the communication.

A. Miller is not shown to teach or suggest a verification service provider configured to obtain "information transmitted by a second device associated with a communications connection."

Claim 1 requires a verification service provider that is configured to "enroll a first device" and "obtain, at the verification service provider, information transmitted by a second device associated with a communications connection." Ex. 1001 ['009 Patent], at 22:50 and 22:58-60.

[1] Independent claims 1, 10, and 17 use nearly identical language to describe a verification service provider. The following analysis, while specific to claim 1, is applicable to all three independent claims.

Miller, as applied by Petitioner, is not shown to teach or suggest the claimed second device. Nor is Miller shown to teach a verification service provider configured to obtain information transmitted by a second device associated with a communications connection between the first and second device, as required by the claims.

1. Miller is not shown to teach or suggest the claimed second device.

The ’009 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 [’009 Patent], at 2:41-48 (“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 ’009 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 2:61-63. 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. 1021 [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]. Even the Petition recognizes that Miller and the '009 patent use the term consistently, stating that "Miller and the '009 patent describe the same types of 'devices' in the communication," presenting a table to this effect:

Miller devices	**'009 Patent devices**
"e.g., a mobile phone, computer system, smart phones, laptops, tablets, … or any other communication capable electronic computer." Ex-1021, [0048].	"a smartphone, tablet, PC, phablet, or wearable computer." Ex-1001, 12:26-31.

Pet. at 12. Miller and the '009 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 "second device" as claimed. *Id.*, at 11 (equating service provider 14 to "a second device (yellow)"). 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." *Id.*, 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 '009 patent. Here again, Miller and the '009 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." *Id.* The '009 patent identifies a service provider as a bank or other entity, Ex. 1001 ['009 Patent], at 4:41, and includes an extensive description of a verification service provider as an entity that provides identification services. *See, e.g.*, *id.*, at Figs. 1, 2A and 2B and accompanying descriptions. Even the Petition uses the term service provider in this manner, stating that "Miller's service provider…provides services to computer 18 via a network." Pet. at 29.

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. 1021 [Miller] [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 '009 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 '009 patent claims or as understood by a person of ordinary skill in the art. Miller therefore fails to disclose or render obvious the claimed verification service provider that is configured to obtain information transmitted by a second device.

2. Miller is not shown to teach or suggest a verification service provider that is configured to obtain the claimed information transmitted by a second device.

Claim 1 requires a verification service provider configured to "obtain, at the verification service provider, ***information*** transmitted by a second device ***associated with a communications connection***." Ex. 1001 ['009 Patent], at 22:58-60. The Petition fails to show that Miller discloses or suggests this limitation.

Instead, its arguments are directed to information transmitted by a purported "***first*** device," and fail to show what is claimed.

The '009 patent discloses that information associated with a communications connection can be the caller ID or ANI data of the calling device. For example, Figure 2B illustrates a process "for verification of caller identification information." *Id.*, at Fig. 2B, 16:53-55. The process begins at step 222, when a request is received "to verify a first ***communication connection … associated with an observed caller ID***." *Id.*, at Fig. 2B, 16:53-60. Upon receiving this request, the verification service provider begins the process of verifying the phone number of the calling device.

Miller does not teach a verification service provider that receives, from a called device, the phone number or caller ID of the calling device that initiated the call. Nor does the Petition attempt to argue that Miller provides such a teaching. Instead, the Petition tries to correlate the claimed information transmitted by a second device to ***a challenge-response*** transmitted by Miller's purported ***first*** device, computer 18, which initiated a communication with service provider 14. Pet. at 11.

According to the Petition, with respect to the claimed "information transmitted by a second device associated with a communications connection," "Miller teaches this element when computer 18 sends a 'response' containing

'computer minutia' to the DKCP 'indirectly via the service provider 18 [sic].'" Pet. at 28. But this is not the "information transmitted by a ***second device associated with a communications connection***" required by the claim and as described by the '009 specification. Rather it is different information transmitted by the ***first*** device as identified by the Petition.

In addition, this argument fails for yet another independently sufficient reason. As established in the prior section, Miller's service provider 14 is not the claimed second device. It follows that whatever information the service provider 14 may provide to the DKCP is not information transmitted by a second device, as required by the claim.

Petitioner also asserts, in the alternative, that "it would be an obvious variation for Miller's computer 18 to transmit information to/from the DKCP through the service provider." Pet. at 34. This assertion relies on three flawed arguments.

First, the Petition states that "[s]uch transmissions allow the computer 18 to communicate ***only*** with the service provider to ***simplify*** its communications." *Id.* (emphases added). But the opposite would be true under the Petition's indirect transmission theory. An indirect transmission process to the DKCP is more complicated on its face, because it requires an additional step of transmitting information from the service provider to the DKCP. The Petition fails to show that

an ordinary artisan would have had any reason to understand, let alone would have found obvious, that departing in this regard from what Miller actually discloses would "simplify its communications."

The statement also appears to have an unspoken premise that computer 18 does not communicate with the DKCP because it only communicates with the service provider 14. But if computer 18 does not communicate with the DKCP, it undermines the Petition's entire invalidity analysis, which correlates the computer 18 to the claimed first device and the DKCP 10 to the claimed verification service provider. *See, e.g.,* Pet. at 11. As discussed above, in embodiments of the claimed invention the "enrolling a first device with a verification service provider" as claimed entails a user connecting the device to be enrolled with the verification service. Ex. 1001 ['009 patent], at 19:5-24; *see supra* Section II.A.

Second, the Petition asserts that a "POSA would recognize that ***any path*** that provides communication of the verification information can be utilized, and that the specification of such path does not provide any patentable improvement in light of known network techniques…." Pet. at 34 (emphasis added). Even if this is assumed to be true, the Petition fails to identify or substantiate a motivation for why a person of ordinary skill would select what the Petition calls the indirect path between the second device and verification service provider.

In addition, the Petition's only support for this argument is the testimony of its declarant, Dr. McDaniel. Pet. at 34 (citing Ex. 1003 [McDaniel Decl.], ¶ 86). But Dr. McDaniel provides no evidence to support the assertions that the Petition then repeats, verbatim. This *ipse dixit* of Petitioner's declarant is entitled to no weight, since neither the Petition nor the declaration substantiates it. *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 erroneously concludes that Fig. 9 of the '009 patent supports the obviousness of the claimed invention because, the Petition argues, it discloses an "indirect" communication "from the 'first device' to the 'verification service provider'…via the second device." Pet. at 34-36. But Figure 9 discloses the same communication path as Figure 1: (1) "communication unit 906 is one or more of a communication unit such as communication unit 104 of FIG. 1 and an app, such as app 806 of FIG. 8, that are installed on smartphone device 904 and used to make a phone call (916) to relying party 910 (also referred to herein as the 'callee'), (2) "relying party 910 passes, at 918, the user's phone number (the phone number indicated via caller id or ANI data that is observed by the relying party) to verification service 912," and (3) "The verification service sends, at 920, an SMS message or other communication with a unique identifier to smartphone device 904." Ex. 1001 ['009 Patent], at 20:40-51.

Moreover, Figure 9 uses a different kind of verification process, which does not involve enrolling a user device. It starts when the verification service provider 912 generates a unique identifier and then passes it to smartphone 904, using the phone number provided by relying party 910. *Id.*, at 20:49-51. If the smartphone is not being spoofed, it will receive the unique identifier and then pass it on to relying party 910, using the connection already established when smartphone 904 called relying party 910. *Id.*, at 20:62-64. Relying party 910 then passes the unique identifier back to verification service provider 912. *Id.*, at 20:67-21:2. If the verification service provider receives back the same unique identifier that it started with, it can conclude with reasonable certainty that smartphone 904 is not being spoofed. *Id.*, at 21:1-3. Whatever communication paths may or may not be involved, this full-circle verification process differs from the claimed invention of the '009 Patent, which is directed to the aspect of the invention which, *inter alia*, uses a device fingerprint generated during a device enrollment process. The claims of the '009 patent are expressly directed to, *inter alia*, an "enrolled first device." *Id.*, 22:67; *see also id.*, 23:56 (claim 10) (same), 24:41 (claim 17) (same).

Relying on these three flawed arguments, the Petition fails to establish that Miller teaches or renders obvious the claimed verification service provider that is configured to obtain information transmitted by a second device associated with a communications connection between the first and second devices.

B. Miller is not shown to teach or suggest a verification service provider that is configured to select an action comprising at least one of blocking, requesting or permitting.

The last-recited limitation of claim 1 requires a verification service provider that is configured to "based at least in part on the security determination, select an action comprising at least one of ***blocking*** the communication, ***requesting*** additional authentication, and ***permitting*** the communication." Ex. 1001 ['009 Patent], at 23:1-4 (emphasis added).

Miller, as applied by Petitioner, does not teach or suggest a verification service provider that selects from these three actions. Instead, the Petition concedes that "[f]or the 'blocking' and 'permitting' selected actions above, Miller's teaching is primarily that the 'service provider' (and not the DKCP) performs the actual denial (block) or allow (permit)." Pet. at 49. In fact, that is Miller's only teaching in this regard. The Petition consequently proceeds to present an obviousness analysis for this claim limitation, which is flawed and should be rejected.

First, the Petition asserts that, because Miller's validation failure can result in a denied service request, it does not matter which entity performs the claimed function of "selecting an action…blocking the communication." *Id*., at 47. But it does matter: the plain language of the claim requires the verification service provider to perform this selection, and the Petition fails to provide any motivation

for another entity to do so instead. Furthermore, the Petition also ignores Miller's disclosure that a validation failure does not necessarily result in denying a service request. Rather, when Miller's service provider 14 receives a validation failure notice it could decide ***not*** to deny the service request and instead conduct "an out-of-band identity proofing of the service user." Ex. 1003 [Miller], at [0118].

Continuing with its argument improperly based on results achieved, the Petition states that, "given that Miller expressly teaches a logic path in which the result is 'denying the service request,' it would be obvious that such denial would be effectuated by selecting an action blocking the communication because such blocking is one known way of such denial." Pet. at 47-48. Neither the Petition nor the supporting expert declaration states or substantiates a motivation for implementing Miller's alternative logic path. They also fail to point to any evidence demonstrating that "blocking is one known way of such denial." Pet. at 48 (citing only Ex-1003 [McDaniel Decl.], ¶106). The declarant's *ipse dixit* is entitled to no weight. *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.").

Second, the Petition argues that "Miller's DKCP teaches, or renders obvious, this element ***when the DKCP selects the action***, and informs Miller's 'service provider' of the selected action." Pet. at 49 (emphasis added). This

statement contradicts the very argument Petitioner just spent several paragraphs developing: that the DKCP does ***not*** select the blocking or permitting actions, but the claim is nonetheless obvious based on the results achieved when the service provider performs the selection. *Id.*, at 47-49. In addition, the Petition cites no evidence to support this assertion. Again, its declarant's mere *ipse dixit* cannot carry the day.

Third, the Petition supports its obviousness theory by stating that "Miller operates exactly how the '009 patent operates." *Id*., at 49. They do not, in fact, operate in the same way, for at least the reasons identified in the prior section. As explained, Miller's DKCP is not a verification service provider configured to "obtain information transmitted by a second device associated with a communications connection." *See supra* Section III.A.2.

Finally, the Petition argues that "in the '009 embodiments [that] correspond to the claim (e.g., Figs. 8 and 9 and their disclosure), the 'verification service' does not sit in the communication path between the first and second devices. The verification service does not have any practical operation to block/allow the call …." Pet. at 50. Even assuming for the sake of argument that the Petition is correct that the '009 verification service does not have any practical operation to block/allow the call, the Petition's argument is beside the point. The claim does not require the verification service provider to perform the operation of blocking or

allowing the call; it must only ***select*** which action should be performed. The Petition says as much just a few paragraphs earlier ("the claim does not recite that the verification service provider must perform the selected action"). *Id*., at 49.

In addition, the Petition's characterization of the patent's disclosures is factually incorrect. The Petition asserts that "the 'verification service' does not sit in the communication path between the first and second devices," as noted above. *Id*., at 50. But the '009 patent's Fig. 8 shows the Verification Service 812 having direct communication paths 822 and 826 with the calling user's device 804, as well as direct communication paths 818 and 824 with the replying party 810. Ex.1001 ['009 Patent], at Fig. 8. The figure plainly shows the verification service provider sitting directly in a communication path between first and second user devices.

Petitioner also contradicts itself by making this argument. Earlier in the Petition, when trying to correlate Miller to the claimed requirement that the verification service provider receives information transmitted by the claimed second device, Petitioner points to Figure 8 as showing a "direct" communication from the first device to the verification service. Pet. at 34-36. This earlier argument is directly contrary to the Petition's present argument, that the verification service provider does not even "sit in the communication path between the first and second devices."

For at least these reasons, the Petition fails to establish that Miller teaches or suggests a verification service provider that is configured to "based at least in part on the security determination, select an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication." Ex. 1001 ['009 Patent], at 23:1-4.

C. Miller does not teach or suggest any of the remaining claims 2-23.

Independent claims 1, 10, and 17 use nearly identical language to describe a verification service provider. Claim 1 claims "a system, comprising a verification service provider." Claims 10 claims a corresponding method, and claim 17 claims a corresponding computer program claim. The analysis presented above with respect to claim 1 applies equally to independent claims 10 and 17. As well, because Miller does not teach or suggest each and every element of any independent claim, it does not teach or suggest each and every element of any of dependent claims 2-9, 11-16, and 18-23.

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 4902 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
EXHIBIT 2009

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