

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

MICROSOFT CORPORATION,  
Petitioner,

v.

QOMPLX LLC,  
Patent Owner.

---

Case IPR2026-00184  
Patent 12,231,426

---

**PATENT OWNER'S PRELIMINARY RESPONSE**

**TABLE OF CONTENTS**

	<b>Page</b>
<b>I. INTRODUCTION .....</b>	<b>1</b>
<b>II. PETITIONER’S GROUNDS FAIL (ALL CLAIMS, ALL GROUNDS).....</b>	<b>3</b>
A. Petitioner Fails To Demonstrate That Its Grounds Disclose Or Render Obvious “Multidimensional Time-Series Database” (All Claims, All Grounds). .....	3
1. Petitioner Does Not Support Its Implicit Construction Of A “Multidimensional Time-Series Database.” .....	5
2. Petitioner’s Implicit Construction Is Inconsistent With The Intrinsic And Extrinsic Record. ....	9
3. There Is No Reason To Believe That Kirti’s Repository Is Optimized Or Especially Suited For Time-Series Data.....	13
B. Petitioner Fails To Demonstrate That Kirti Alone Or In Combination Discloses Or Renders Obvious “Determining Whether The Additional Verification Is Required To Grant Access” After “Receiv[ing] A Request To Authenticate A Client” (All Claims, All Grounds).....	14
1. The Claims Require That The “Determining” Step— Including Retrieving Historical Information From The MDTSDB—And Additional Verification Steps Occur After And In Response To “Receiv[ing] A Request To Authenticate A Client.” .....	15
2. Kirti’s System Determines Whether A Remediation Action Is Appropriate When It Retrieves Activity Data In Scheduled Batches, Not In Response To Receiving A Request To Authenticate A Client. ....	22

- 3. Kirti Does Not Determine Whether Additional Verification Is Required “To Grant Access” In Response To Receiving A Request To Authenticate.....25
  
- C. Petitioner Fails To Show That Kirti Alone Or In Combination With Coffin Discloses Or Renders Obvious “Select[ing] An Additional Verification Method From A Plurality Of Verification Methods” (All Claims, All Grounds).....28
  - 1. Kirti’s “Remedial Methods” Are Not “Verification Methods” (Ground 1).....30
  
  - 2. Petitioner Fails To Show That Its Kirti-Coffin Combination Teaches “Select[ing] An Additional Verification Method” (Ground 2).....36
  
- III. CONCLUSION .....44**

**TABLE OF AUTHORITIES**

**Page(s)**

**COURT DECISIONS**

*Ariosa Diagnostics v. Verinata Health, Inc.*,  
805 F.3d 1359 (Fed. Cir. 2015) .....43

*Function Media, LLC v. Google, Inc.*,  
708 F.3d 1310 (Fed. Cir. 2013) .....19

*Intelligent Bio-Systems, Inc. v. Illumina Cambridge, Ltd.*,  
821 F.3d 1359 (Fed. Cir. 2016) .....9

*In re Kahn*,  
441 F.3d 977 (Fed. Cir. 2006) .....32

*Kaneka Corp. v. Xiamen Kingdomway Grp. Co.*,  
790 F.3d 1298 (Fed. Cir. 2015) .....18

*KSR Int’l Co. v. Teleflex Inc.*,  
550 U.S. 398 (2007).....32

*In re Magnum Oil Tools Int’l, Ltd.*,  
829 F.3d 1364 (Fed. Cir. 2016) .....32

*Mformation Techs., Inc. v. Research in Motion Ltd.*,  
764 F.3d 1392 (Fed. Cir. 2014) .....18

*Virtek Vision Int’l ULC v. Assembly Guidance Sys., Inc.*,  
97 F.4th 882 (Fed. Cir. 2024); ..... 32, 43

**AGENCY DECISIONS**

*Edwards Lifesciences Corp. v. Aortic Innovations LLC*,  
IPR2023-01232, Paper 10 (Feb. 7, 2024).....44

*RPX Corp. v. Parity Networks, LLC*,  
IPR2018-00097, Paper 7 (Apr. 24, 2018).....43

*Xerox Corp. v. Bytemark, Inc.*,  
IPR2022-00624, Paper 9 (Aug. 24, 2022)  
(precedential) ..... 8, 9, 32

**REGULATIONS**

37 C.F.R. § 42.65(a).....32

<b>EXHIBIT LIST</b>	
2001	Declaration of Nathan Lowenstein in Support of Notice of Intent
2002	Declaration of Colette Woo in Support of Notice of Intent
2003	Amended Scheduling Order, <i>Qomplx LLC v. Microsoft Corp.</i> , No. 1:25-cv-01383, (W.D. Tex.) (Jan. 5, 2026) [Amended Scheduling Order]
2004	Defendant Microsoft Corporation’s Preliminary Invalidity Contentions, <i>Qomplx LLC v. Microsoft Corp.</i> , No. 1:25-cv-01383, (W.D. Tex.) (served Jan. 26, 2026) [Invalidity Contentions]
2005	Ex. A-10 to Defendant Microsoft Corporation’s Preliminary Invalidity Contentions, <i>Qomplx LLC v. Microsoft Corp.</i> , No. 1:25-cv-01383, (W.D. Tex.) (served Jan. 26, 2026) [Invalidity Contentions – Ex. A-10]
2006	Ex. A-11 to Defendant Microsoft Corporation’s Preliminary Invalidity Contentions, <i>Qomplx LLC v. Microsoft Corp.</i> , No. 1:25-cv-01383, (W.D. Tex.) (served Jan. 26, 2026) [Invalidity Contentions – Ex. A-11]
2007	Katie Roof, <i>Risk Analytics Firm Qomplx to Go Public Via Casper CEO SPAC</i> , BLOOMBERG (Mar. 1, 2021, 11:16 PM UTC), <a href="https://www.bloomberg.com/news/articles/2021-03-01/risk-analytics-firm-qomplx-to-go-public-through-casper-ceo-spac">https://www.bloomberg.com/news/articles/2021-03-01/risk-analytics-firm-qomplx-to-go-public-through-casper-ceo-spac</a> (archived at <a href="http://archive.ph/3bpk2">http://archive.ph/3bpk2</a> ) [Bloomberg]
2008	<i>On Point: EP. 3 Taking Qomplx Public via SPAC with Jason Crabtree '08</i> , <a href="https://www.oldgradclub.com/on-point/blog-post-title-two-ffmmh">https://www.oldgradclub.com/on-point/blog-post-title-two-ffmmh</a> [On Point Podcast]
2009	<i>West Point First Captains</i> , WEST POINT ASSOCIATION OF GRADUATES, <a href="https://www.westpointaog.org/about/history/west-point-first-captains/">https://www.westpointaog.org/about/history/west-point-first-captains/</a> [West Point]
2010	Compilation of Awards Given to Jason Crabtree [Crabtree Awards]

2011	<i>Jason Crabtree</i> , NEW AMERICA, <a href="https://www.newamerica.org/our-people/jason-crabtree/">https://www.newamerica.org/our-people/jason-crabtree/</a> [New America]
2012	<i>Meet the Team</i> , THE DAKOTA FOUNDATION, <a href="https://www.dakotafoundation.org/team">https://www.dakotafoundation.org/team</a> [Dakota Foundation]
2013	Joe Panettieri, <i>SPAC Cybersecurity Merger: Tailwind, QOMPLX Tackle Microsoft Active Directory Security</i> , MSSPALERT (Mar. 2, 2021), <a href="https://www.msspalert.com/news/spac-cybersecurity-merger-tailwind-qomplx-tackle-microsoft-active-directory-security">https://www.msspalert.com/news/spac-cybersecurity-merger-tailwind-qomplx-tackle-microsoft-active-directory-security</a> [MSSPALert]
2014	<i>Architect's Corner: Qomplx leverages automation to run stateful services in containers for the financial and cybersecurity industries</i> , PORTWORX (Sept. 20, 2018), <a href="https://portworx.com/blog/devops-realized-qomplx-leverages-automation-run-stateful-services-containers-massive-scale/">https://portworx.com/blog/devops-realized-qomplx-leverages-automation-run-stateful-services-containers-massive-scale/</a> [Portworx]
2015	QOMPLX, Inc., <i>QOMPLX CEO Jason Crabtree Wins Ernst &amp; Young Entrepreneur Of The Year® 2020 Mid-Atlantic Award</i> (Aug. 10, 2021), <a href="https://finance.yahoo.com/news/qomplx-ceo-jason-crabtree-wins-135600025.html">https://finance.yahoo.com/news/qomplx-ceo-jason-crabtree-wins-135600025.html</a> [Yahoo! Finance]
2016	Sydney Lake, <i>Tyson's analytics firm Qomplx plans to go public</i> , VIRGINIA BUSINESS (Mar. 2, 2021), <a href="https://virginiabusiness.com/tysons-analytics-firm-qomplx-plans-to-go-public/">https://virginiabusiness.com/tysons-analytics-firm-qomplx-plans-to-go-public/</a> [Virginia Business]
2017	Tailwind Acquisition Corp., <i>QOMPLX, Inc., Frequently Asked Questions about Tailwind Transaction</i> , <a href="https://www.sec.gov/Archives/edgar/data/1814215/000110465921033365/tm219025d2_425.htm">https://www.sec.gov/Archives/edgar/data/1814215/000110465921033365/tm219025d2_425.htm</a> [SEC FAQ]
2018	<i>QOMPLX and Tailwind Acquisition Corp. Mutually Agree To End Business Combination Due to Market Conditions</i> , BUSINESSWIRE (Aug. 17, 2021, 8:21 AM EDT), <a href="https://www.businesswire.com/news/home/20210817005565/en/QOMPLX-and-Tailwind-Acquisition-Corp.-Mutually-Agree-To-End-Business-Combination-Due-to-Market-Conditions">https://www.businesswire.com/news/home/20210817005565/en/QOMPLX-and-Tailwind-Acquisition-Corp.-Mutually-Agree-To-End-Business-Combination-Due-to-Market-Conditions</a> [BusinessWire]

2019	<i>Entrepreneurship Essentials for the Military Community</i> , USPTO, <a href="https://www.uspto.gov/about-us/events/entrepreneurship-essentials-military-community">https://www.uspto.gov/about-us/events/entrepreneurship-essentials-military-community</a> [Entrepreneurship Essentials for the Military Community]
2020	<i>2024 Veterans Innovation and Entrepreneurship Program</i> , USPTO, <a href="https://www.uspto.gov/about-us/events/2024-veterans-innovation-and-entrepreneurship-program">https://www.uspto.gov/about-us/events/2024-veterans-innovation-and-entrepreneurship-program</a> [Veterans Innovation and Entrepreneurship Program]
2021	<i>Ready, set, compete! How we’re helping veterans and military family members innovate and start new businesses</i> , USPTO (May 25, 2023) <a href="https://www.uspto.gov/blog/ready-set-compete-how-we">https://www.uspto.gov/blog/ready-set-compete-how-we</a> [Ready, Set, Compete]
2022	Time to Trial Statistics for J. Alan Albright (generated via DocketNavigator) [Albright Time To Trial]
2023	Declaration of Sam Malek, Ph.D.
2024	<i>Time series database explained</i> , INFLUXDATA, <a href="https://www.influxdata.com/time-series-database/">https://www.influxdata.com/time-series-database/</a> (accessed Mar. 5, 2026) [InfluxData]
2025	Marie Fayard, <i>Time Series Database (TSDB): A Guide With Examples</i> , DATACAMP (updated Feb. 21, 2025), <a href="https://www.datacamp.com/blog/time-series-database">https://www.datacamp.com/blog/time-series-database</a> [Datacamp]
2026	Piotr Grzesik & Dariusz Mrozek, <i>Comparative Analysis of Time Series Databases in the Context of Edge Computing for Low Power Sensor Networks</i> , COMPUTATIONAL SCIENCE – ICCS 2020, 371. [Grzesik]
2027	Niels de Waal, <i>Literature Study: Timeseries Databases</i> (Dec. 16, 2022) [Literature Study: Timeseries Databases]

2028	Keith D. Foote, <i>A Guide to Time Series Databases</i> , DATAVERSITY (Sept. 15, 2022), <a href="https://www.dataversity.net/articles/a-guide-to-time-series-databases/">https://www.dataversity.net/articles/a-guide-to-time-series-databases/</a> [A Guide to Time Series Databases]
2029	<i>The ultimate guide to time series databases</i> , KX, <a href="https://kx.com/time-series-database/">https://kx.com/time-series-database/</a> (accessed Apr. 7, 2026) [The ultimate guide to time series databases]
2030	Alex Vondrak, <i>How Time Series Databases Work-and Where They Don't</i> , HONEYCOMB (Jan. 6, 2026), <a href="https://www.honeycomb.io/blog/time-series-database">https://www.honeycomb.io/blog/time-series-database</a> [Honeycomb]
2031	<i>What Is a Time Series Database? How It Works + Use Cases</i> , Timeplus (Feb. 2, 2024), <a href="https://www.timeplus.com/post/time-series-database">https://www.timeplus.com/post/time-series-database</a> [What is a Time Series Database?]
2032	U.S. Pat. No. 10,204,147 ['147]
2033	Alexandre Gaillard, <i>Top 5 User Identity Verification Methods for 2025</i> , INVESTGLASS (updated July 3, 2025), <a href="https://www.investglass.com/top-5-user-identity-verification-methods-for-2025/">https://www.investglass.com/top-5-user-identity-verification-methods-for-2025/</a> [InvestGlass]
2034	DOUGLAS DOWNING ET AL., <i>DICTIONARY OF COMPUTER AND INTERNET TERMS</i> (BARRON'S BUSINESS GUIDES), 530 (12 <sup>th</sup> ed. 2017) [Barron's Dictionary of Computer and Internet Terms]

## I. INTRODUCTION

The Petition should be denied because Petitioner fails to demonstrate a reasonable likelihood of prevailing as to any challenged claim. Petitioner's grounds fail for at least three independent reasons.

First, Petitioner fails to demonstrate that its grounds disclose or render obvious a "multidimensional time-series database" ("MDTSDB"). *See* Section II.A. Petitioner's argument relies on an unstated and expansive construction of that term under which virtually any database storing multiple attributes over time would qualify. But Petitioner provides no basis to adopt that understanding, and that alone is sufficient reason to reject the Petition. *See* Section II.A.1. Nor is there any reason to assume that Petitioner's expansive view is correct; rather, it is inconsistent with the intrinsic and extrinsic record, which shows that a time-series database is a specialized database optimized or especially suited at least for interacting with time-series data. *See* Section II.A.2. Far from identifying a time-series database, Kirti makes clear that its system does not require any particular kind of database (let alone a specialized one) because it can use "*any* database." *See* Section II.A.3.

Second, Petitioner fails to demonstrate that Kirti satisfies the claim requirement that, upon "receiv[ing] a request to authenticate a client," the system "determin[es] whether additional verification is required to grant access," which

“comprises” “retrieving ... historical information about previous access requests.”

Ex. 1001 [’426] cls. 1, 9. The claim language requires that this determination, including the claimed retrieval, be performed in response to the authentication request itself. *See* Section II.B.1. Petitioner does not show that Kirti performs any such request-driven determination. Petitioner relies on Kirti’s batch collection and analysis of activity data across multiple users to build profiles and identify threats. Such collections and analyses, however, are divorced from and not in response to any particular authentication request. *See* Section II.B.2. Nor does Petitioner show that Kirti performs the claimed determination “to grant access” to the authentication request being evaluated. The additional authentication measures Petitioner relies upon arise from a cloud-to-cloud warning system, in which, when a first application detects a security threat, it warns a second cloud application, which may then impose additional security measures. Here too, those measures are not part of determining whether “to grant access” to the authentication request being evaluated. *See* Section II.B.3.

Third, Petitioner fails to demonstrate that Kirti alone or in combination with Coffin discloses or renders obvious “select[ing] an additional verification method from a plurality of verification methods.” *See* Section II.C. Petitioner’s Kirti theory conflates a plurality of remediation measures (which relate to eliminating a threat) with a plurality of verification methods (which relate to verifying a user),

even though Kirti identifies at most a single remedial action—“adding additional steps to authentication”—that could qualify as a verification method. *See* Section II.C.1. Petitioner’s Coffin theory fares no better. Coffin is a textbook that provides a general discussion of authentication techniques. Coffin does not disclose a *system* that *selects* an “additional verification method from a plurality of verification methods.” When pressed to identify a “selection,” Petitioner instead shifts to an altogether different portion of Coffin that discusses sending a passcode via pager, cell phone, or email. But as the ’426 patent makes clear, use of a passcode—regardless of whether it is delivered by pager, phone, email, or otherwise—is a single verification method, not selecting among different verification methods. Petitioner’s fallback reliance on generalized “knowledge in the art” cannot supply the missing limitation. *See* Section II.C.2.

Because Petitioner fails to demonstrate a reasonable likelihood of prevailing, the Director should deny institution.

## **II. PETITIONER’S GROUNDS FAIL (ALL CLAIMS, ALL GROUNDS).**

### **A. Petitioner Fails To Demonstrate That Its Grounds Disclose Or Render Obvious “Multidimensional Time-Series Database” (All Claims, All Grounds).**

Each of the claims requires and largely centers on the use of a “multidimensional time-series database” to authenticate a client. Claim 1, for instance, involves a computer system configured to receive a request to

authenticate a client, storing information about the request in a multidimensional time series database, and retrieving from that database historical information about prior access requests to determine whether additional verification is required to grant access.

Petitioner alleges that Kirti’s “analytics and threat intelligence repository database” is the claimed “multidimensional time-series database.” Pet., 30-31. Petitioner, however, reaches this conclusion only through an expansive, implicit, and unsubstantiated construction of “multidimensional time-series database.” Kirti never refers to its repository database or anything else as a “multidimensional time-series database.” At best, Petitioner implicitly contends that a “multidimensional time-series database” only requires “multiple parameters/attributes” and “the same activity data (i.e., values for the same parameters/attributes) for multiple time points.” *Id.*, 31. But under this reading, any online checking account or email inbox would become a “multidimensional time-series database,” regardless of how that system was actually designed. Petitioner does not provide any explanation or evidence in support of this construction. *See id.*; Section II.A.1.

Nor does Petitioner attempt to square its implicit construction with the intrinsic or extrinsic record. As discussed in Section II.A.2, both the art and the intrinsic record are inconsistent with Petitioner’s position and instead consistently

describe time-series databases as specialized data stores optimized or especially suited at least for time-series data. Because Petitioner neither proves its construction nor shows that Kirti meets the limitation under a construction grounded in the intrinsic or extrinsic record, it fails to demonstrate that its grounds disclose or render obvious a “multidimensional time-series database.” This alone warrants denial of institution. *See* Section II.A.2. Petitioner also fails to demonstrate that Kirti’s repository is optimized or especially suited for anything, let alone for time-series data. Rather, Kirti teaches that its repository may be “any database.” *See* Section II.A.3.

1. Petitioner Does Not Support Its Implicit Construction Of A “Multidimensional Time-Series Database.”

Petitioner asserts that no terms require construction and further purports to apply “the plain and ordinary meaning of each claim term.” Pet., 15. In fact, Petitioner provides an implicit and expansive construction of “multidimensional time-series database.” Petitioner, however, provides no cognizable evidence in support of its construction.<sup>1</sup>

---

<sup>1</sup> Notably, although Petitioner relies upon Coffin which relates to “programming secure Oracle database applications” (Ex. 1005 [Coffin] Cover), Coffin does not even mention a time-series database. *See generally id.*

Petitioner argues that “Kirti’s analytics and threat intelligence repository database *is* a multidimensional time-series database.” Pet., 31. Petitioner’s argument in support of this position is set forth below:

It is multidimensional because each time point includes activity data for multiple parameters/attributes (e.g., IP address, login attempt result (success or failure), identifier (e.g., username), resources accessed, etc.). EX1004, 4:46-5:3, 10:25-50, 10:60-11:4, 12:1-18, 12:35-13:29, 13:44-59, 14:48-54, 16:28-40, 16:55-67, 17:9-55, 18:9-23, 18:38-41). And it is a time-series database at least because it includes the same activity data (i.e., values for the same parameters/attributes) for multiple time points. *E.g.*, EX1004, 13:27-30 (“[D]ata collected over time is used to build models of normal behavior (e.g., patterns of events and activity) and flag behavior that deviates from normal as abnormal behavior.”).

Pet., 31-32.

As can be seen above, Petitioner argues the database is (i) multidimensional “because each time point includes activity data for multiple parameters/attributes” and is (ii) a time-series database “because it includes the same activity for multiple time points.” Taken together, Petitioner’s analysis implicitly assumes that a “multidimensional time-series database” is any database storing multiple attributes across multiple points in time, regardless of how those points are stored or accessed.

But under that understanding, virtually any ordinary database would qualify. For example, an individual's online checking-account includes multiple attributes (*e.g.*, account identifier, transaction amount, merchant) for transactions occurring at different times. Likewise, an email inbox stores multiple attributes (*e.g.*, sender, recipient, subject) for messages received over time. Yet these stores could be implemented in any number of ways, and no one would describe them all as "multidimensional time-series databases." Petitioner provides no evidence that a POSITA would adopt such an expansive understanding.

Indeed, Petitioner does not provide *any* evidence for why a POSITA would have this understanding of either "multidimensional" or "time-series database." As can be seen above, Petitioner does not cite any intrinsic or extrinsic evidence in support of its positions, nor does Petitioner demonstrate that its understanding is known in the art. Petitioner's only support for its position is Dr. Black's testimony, but he merely parrots the Petition's conclusory statement. Ex. 1003 [Black-Decl.] ¶ 84. He too provides no reasoning or evidence in support of this understanding.

It is well-settled that conclusory expert testimony such as this is entitled to little or no weight:

We have reviewed this excerpt from Dr. Jones' declaration and note that it merely repeats, *verbatim*, the conclusory assertion for which it is

offered to support. ... Dr. Jones does not cite to any additional supporting evidence or provide any technical reasoning to support his statement. Thus, the cited declaration testimony is conclusory and unsupported, adds little to the conclusory assertion for which it is offered to support, and is entitled to little weight.

*Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9, 15 (Aug. 24, 2022) (precedential) (emphasis in original, citations omitted). *Xerox* similarly found expert testimony unconvincing where, as here, it was conclusory and failed to construe the limitation-in-question:

Again, however, Dr. Jones offers only a *verbatim* restatement of the assertion being supported, without any supporting evidence or technical reasoning. Neither Petitioner nor [the expert] offers a construction for the terms “data value” or “data record,” for example.

This is particularly problematic in cases where, like here, expert testimony is offered ... to supply a limitation missing from the prior art.

*Id.*, 16 (emphasis in original, citations omitted).

Similar to *Xerox*, Petitioner and Dr. Black argue “Kirti’s analytics and threat intelligence repository database *is* a multidimensional time-series database” but do not explain the basis for the expansive implicit construction that conclusion is founded upon. Neither provides a formal construction of “multidimensional time-series database” nor do they defend their implicit construction. Under *Xerox*, Petitioner may not show a missing limitation in this fashion. Nor can the reply

cure this deficiency. *Xerox* denied institution (*id.*, 18) and the Federal Circuit has long made clear that a petitioner must prove its case in the petition. *Intelligent Bio-Systems, Inc. v. Illumina Cambridge, Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016) (“the expedited nature of IPRs bring with it an obligation for petitioners to ***make their case in their petition*** to institute.”).

Because Petitioner’s position rests upon an unsubstantiated implicit construction, it should be rejected.

2. Petitioner’s Implicit Construction Is Inconsistent With The Intrinsic And Extrinsic Record.

As just discussed, Petitioner’s implicit construction—wherein a multidimensional time series database is any database storing multiple attributes across multiple points in time—is wholly unsupported. That is sufficient reason to reject its position. Nor is there any basis to simply assume that Petitioner’s expansive understanding is correct. If more is needed, Petitioner’s implicit construction is also not supported by the intrinsic and extrinsic record.

As an initial matter, Petitioner analyzes the term “multidimensional time-series database” by looking at the terms “multidimensional,” “time-series,” and “database” in isolation. *See* Pet., 31-32. But this approach does not establish the meaning of the phrase as a whole. A “hot dog,” for example, does not refer to a heated canine. Similarly, a “relational database,” if analyzed word-by-word might

appear to be a database that can store relationships. But a “relational database” has a specific meaning that bears on its structure and the kinds of queries that can be performed. *See* Ex. 1045 [Buyya NPL] 32 (relational databases “offer fast and reliable structured data storage and transaction processing, but may lack scalability”); *id.*, 110 (contrasting “relational” databases with “key-type” and “NoSQL”). Petitioner does not explain why parsing the individual words yields the meaning of the claimed term, and simply assumes that it does.

Contrary to Petitioner’s position, the literature consistently describes a “time-series database” as a database especially suited or optimized for time series data. The ’426 patent and its incorporated-by-reference applications are consistent with that usage and describe specialized databases designed to efficiently store time-series data.

As Dr. Malek explains, the literature describes a “time-series database” as a specialized database optimized or especially suited for time-series data:

The term “time-series database” is used in numerous sources and primers to refer to specialized databases optimized for time-series data. For example, InfluxData explains that a “time series database (TSDB) is a database optimized for time-stamped or time series data” and is “built specifically for handling metrics and events ... that are time-stamped.” Ex. 2024 [InfluxData]. Similarly, DataCamp explains that time-series databases are “specialized databases designed to manage

data that is organized and indexed by time,” and distinguishes them from “traditional databases ... optimized for general-purpose data storage.” Ex. 2025 [DataCamp].

Other technical and academic sources confirm the same understanding. *See, e.g.*, Ex. 2026 [Grzesik] 373 (“Time series database (TSDB) is a database type designed and optimized to handle timestamped or time-series data”); Ex. 2027 [Literature Study: Timeseries Databases] 1 (describing time-series databases as “specialized” systems “optimize[d]” for time-indexed data); Ex. 2028 [A Guide to Time Series Databases] (time-series databases “have been optimized for processing time series data”); Ex. 2029 [The ultimate guide to time series databases] (time-series databases are “optimized to store, retrieve, and manage timestamped data points”); Ex. 2030 [Honeycomb] (time series database is “a specialized database that efficiently stores and retrieves time-stamped data”); Ex. 2031 [What is a Time Series Database?] 1 (explaining that time-series databases are “specialized” systems “specifically designed” to handle time-stamped data).

These sources consistently describe time-series databases as databases specialized for time-indexed data, not general-purpose databases that merely happen to store data over time. Neither Petitioner nor Dr. Black address this well-known usage in the art. *See generally* Pet.; Ex. 1003 [Black-Decl.].

Ex. 2023 [Malek-Decl.] ¶¶ 38-40.

The intrinsic record is consistent with that usage. As Dr. Malek explains, the '147 patent (incorporated by reference in the '426 patent<sup>2</sup>) describes a database specifically structured to accommodate time-series data:

The '147 patent (incorporated by reference in the '426 patent) teaches that “the sensor data is passed without transformation to the data management engine 120, where it is aggregated and organized for storage *in a specific type of data store 125 designed to handle the multidimensional time series data* resultant from sensor data.” Ex. 2032 ['147] 6:34-39; *see id.*, 7:20-25. It further explains that, due to the volume and continuous nature of such time series data, it cannot be stored arbitrarily, but instead must be organized using timestamps and defined sampling intervals—*e.g.*, storing data “every 10 seconds, using the timestamp as the key.” *Id.*, 6:51-56.

The “specific type of data store,” thus, is “designed to handle the multidimensional time series data” and utilizes, for example, timestamp keys, to efficiently process time-series workloads. Accordingly, the intrinsic record describes a specialized database designed to process

---

<sup>2</sup> “U.S. patent application Ser. No. 15/091,563, titled ‘System For Capture, Analysis And Storage Of Time Series Data From Sensors With Heterogeneous Report Interval Profiles’, filed on Apr. 5, 2016, now issued as U.S. Pat. No. 10,204,147.” Ex. 1001 ['426] 1:61-65.

time-series data, rather than a general-purpose database that merely stores data over time.

Ex. 2023 [Malek-Decl.] ¶¶ 41-42.

Thus, both the technical literature and the intrinsic record describe a “time-series database” as a specialized database optimized or especially suited for time-series data, not a generic database. Petitioner’s contrary view—under which any database containing multiple attributes across multiple time points regardless of implementation would qualify—is far afield of that record and at minimum required Petitioner to support its view of “multi-dimensional time-series database.”

3. There Is No Reason To Believe That Kirti’s Repository Is Optimized Or Especially Suited For Time-Series Data.

Petitioner does not demonstrate that Kirti’s repository is a specialized database optimized or especially suited for time-series data. Kirti makes clear that its repository may be “*any* database.” Ex. 1004 [Kirti] 10:61-63. As Dr. Malek explains:

There is no evidence that Kirti’s repository is a specialized database optimized or especially suited for time-series data. Rather, Kirti states that “[t]he analytics and threat intelligence repository database 211 may be *any database* or data repository with query capability.” Ex. 1004 [Kirti] 10:61-63. A system that may be implemented using *any* database does not require a specialized database optimized or especially suited for time-series data. Rather, it

is a generic repository capable of storing activity logs or other information.

Ex. 2023 [Malek-Decl.] ¶ 44.

Nothing in Kirti suggests that its repository is a specialized database or optimized or especially suited for time-series data. Instead, Kirti describes a general-purpose repository that may be implemented using any database.

Petitioner therefore fails to demonstrate that Kirti discloses or renders obvious a multidimensional time-series database.

**B. Petitioner Fails To Demonstrate That Kirti Alone Or In Combination Discloses Or Renders Obvious “Determining Whether The Additional Verification Is Required To Grant Access” After “Receiv[ing] A Request To Authenticate A Client” (All Claims, All Grounds).**

The claims require that when the computer system “receive[s] a request to authenticate a client,” the system then “determine[s] whether additional verification is required to grant access,” which comprises “retrieving, from the multidimensional time-series database, historical information about previous access requests.” Ex. 1001 [’426] cl. 1, 9 (similar). Petitioner fails to demonstrate that Kirti performs this required determination. The claim language requires that this determination, including the claimed retrieval, be performed in response to the authentication request itself and as part of deciding whether to grant access to that request. Petitioner shows neither.

As explained in Section II.B.1, the claim requires a request-driven determination in which the system evaluates the authentication request by retrieving historical information about prior access requests. But the disclosures on which Petitioner relies describe periodic, batch analysis of activity data across multiple users, not a determination performed in response to an authentication request. *See* Section II.B.2. And the additional authentication measures Petitioner identifies arise from a cloud-to-cloud warning system, in which a second application may impose heightened authentication after a threat is detected by a first application, not as part of deciding whether to grant access to the authentication request being evaluated. *See* Section II.B.3. Petitioner therefore fails to demonstrate that Kirti discloses or renders obvious the claimed determination.

1. The Claims Require That The “Determining” Step—Including Retrieving Historical Information From The MDTSDb—And Additional Verification Steps Occur After And In Response To “Receiv[ing] A Request To Authenticate A Client.”

In the claims, the computer system must first “receive a request to authenticate a client” and, in response, “retriev[e], from the multidimensional time-series database, historical information about previous access requests associated with the user account.” Claim 1, in relevant part, reads as follows:

1. A computer system configured to execute software instructions stored on nontransitory machine-readable storage media, wherein the software instructions comprise instructions that:

[1.2] *receive a request to authenticate a client*, wherein the request comprises a first identifier and a password,

[1.3] store, in a multidimensional time-series database, information about the request,

[1.4] determine whether the password corresponds to a first user account identified by the first identifier,

[1.5] *determine whether an additional verification is required to grant access*, wherein determining whether the additional verification is required to grant access comprises:

[1.6] *retrieving, from the multidimensional time-series database, historical information about previous access requests* associated with the first user account, and

...

[1.8] based on the additional verification being required to grant access:

[1.9] select an additional verification method from a plurality of verification methods,

[1.10] cause the client to be prompted to complete the additional verification method, and

Ex. 1001 [’426] cl. 1 (utilizing Petitioner’s claim limitation identifications).

Method claim 9, the other independent claim, includes substantially identical limitations.

The claims, thus, do not recite a collection of independent capabilities. Rather, they recite a series of operations performed in response to an authentication request. The claim begins with limitation [1.2], which requires the system to “receive a request to authenticate a client, wherein the request comprises a first identifier and a password.” The subsequent limitations are performed in response to that request. For example, limitation [1.3] stores information about “the request,” and limitation [1.4] evaluates “the password” and “the first identifier” provided in that request. Limitations [1.5]-[1.7] then determine whether “an additional verification is required to grant access,” including by “retrieving ... historical information about previous access requests associated with the first user account.” Finally, limitations [1.8]-[1.11] implement the additional verification should one be required.

Thus, as a matter of logic and grammar, the later-recited steps follow and are in response to the “request” received in limitation 1.2. The system determines whether the identifier and password are sufficient or whether “an additional verification is required,” a determination made by “retrieving ... historical information” from the multidimensional time series database about the user’s

previous access requests. The system then implements the additional verification in order to complete limitation 1.2's request.

The Federal Circuit has made clear that such ordering is required where the claim language itself reflects this dependency—*i.e.*, where later operations rely on the results of earlier ones. *See Mformation Techs., Inc. v. Research in Motion Ltd.*, 764 F.3d 1392, 1398-99 (Fed. Cir. 2014) (“a claim ‘requires an ordering of steps when the claim language, as a matter of logic or grammar, requires that the steps be performed in the order written, or the specification directly or implicitly requires’ order of steps.”); *Kaneka Corp. v. Xiamen Kingdomway Grp. Co.*, 790 F.3d 1298, 1306 (Fed. Cir. 2015) (“A method claim can also be construed to require that steps be performed in order where the claim implicitly requires order, for example, if the language of a claimed step refers to the completed results of the prior step.”). That is the case here: the system cannot “store ... information about the request,” evaluate “the password” and “the identifier,” or determine whether additional verification is required—including retrieving historical information—unless it has first received the authentication request.

The claimed “retrieving” of “historical information,” thus, is part of the determination performed for the authentication request itself, and therefore must occur in response to receiving that request. As the Federal Circuit has explained, operations such as “processing” necessarily presuppose the prior existence of what

is being processed. *Function Media, LLC v. Google, Inc.*, 708 F.3d 1310, 1320 (Fed. Cir. 2013) (claim that recites “processing” an “electronic advertisement” necessarily indicates that “the creation of the ad must happen before the processing begins”). Likewise here, the claimed determination—and the retrieval that forms part of it—necessarily occurs after, and in response to, the received authentication request.

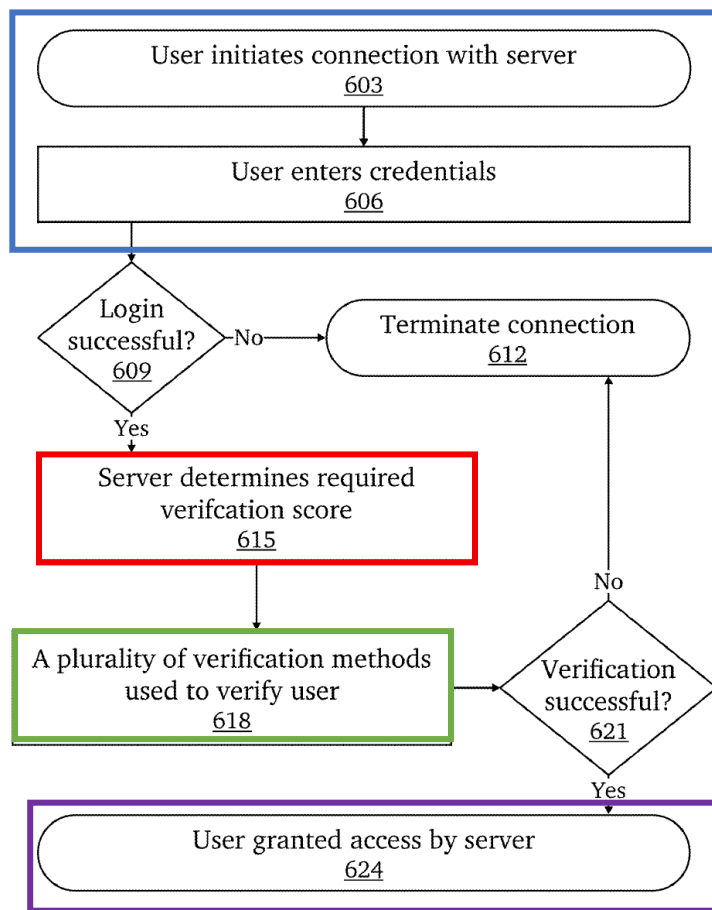
This reading is confirmed by the claim language itself. As Dr. Malek explains:

The logic of the claim language requires the steps be performed in order. Each of the recited operations depends on the authentication request received in limitation [1.2]. Limitation [1.3] stores information about “the request” and limitation [1.4] evaluates the “password” and “first identifier” provided in that request. Limitations [1.5] and [1.6] recite “determin[ing] whether an additional verification is required to grant access” which “comprises” “retrieving, from *the* multidimensional time-series database, historical information about *previous* access requests associated with *the* first user account.” Limitations [1.8]-[1.11] then implement the required additional verification. Because these later operations act on the request and data introduced in limitation [1.2], they necessarily occur as part of processing that request.

Ex. 2023 [Malek Decl.] ¶ 47.

The specification confirms this request-driven sequence. As Dr. Malek explains, the '426 patent is clear that the request to authenticate happens before determining whether additional verification is needed:

The '426 patent's Figure 6 depicts a process in which a **user first requests access** (steps 603 and 606) before **the server determines the required verification score** (step 615) and **verifies the user** (step 618):



600

**Fig. 6**

Ex. 1001 ['426] Fig. 6 (annotated). If the verification is successful, **the user is granted access by the server** (step 624).

The '426 patent's corresponding written description also confirms this order. The '426 patent teaches that “[a]t an initial step 603, a user requests access from a server.” *Id.*, 11:63-64. Then, “[a]t step 606, the server requests login credentials from the user.” *Id.*, 11:65-66. “*If the login is successful at step 609, the server dynamically determines a required verification score required* before the user can access the server at step 615.” *Id.*, 12:2-4. Then, “[a]t step 618, a plurality of verification methods may be used to verify the user.” *Id.*, 12:9-10. “If the verification is successful at step 621, the user is granted access at step 624.” *Id.*, 12:18-19.

The determination step thus presupposes a prior authentication request. This corresponds directly to limitations [1.5]-[1.6], which require determining whether additional verification is required—including retrieving historical information—as part of evaluating that request and the determination of whether to grant access. Thus, both the claim language and the specification describe a system that performs the claimed determination—and the associated retrieval—only after, and in response to, the authentication request.

Ex. 2023 [Malek Decl.] ¶¶ 49-51.

Accordingly, the claims require a request-initiated operation in which historical information is retrieved as part of evaluating a particular authentication request and determining whether to grant access. Systems that instead retrieve or analyze such information independently of any specific authentication request—

such as through periodic, batch, or precomputed processes—do not satisfy this requirement.

2. Kirti’s System Determines Whether A Remediation Action Is Appropriate When It Retrieves Activity Data In Scheduled Batches, Not In Response To Receiving A Request To Authenticate A Client.

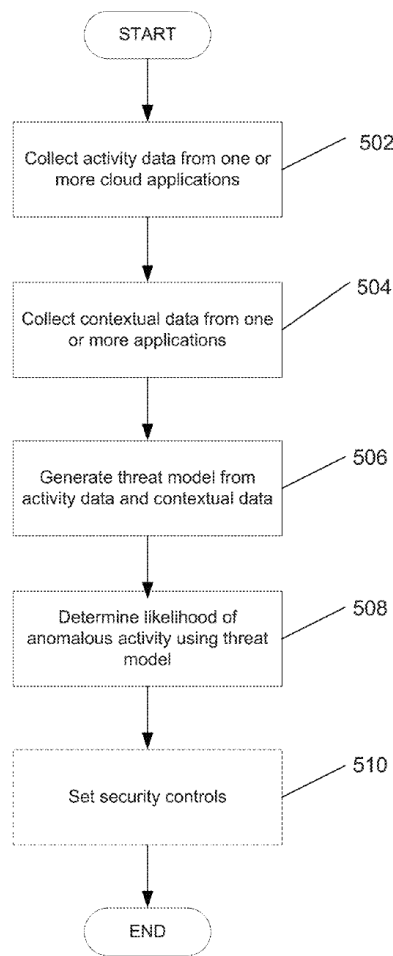
Petitioner does not and cannot demonstrate that Kirti performs any aspect of the claimed determination (including retrieving historical information from the multidimensional time-series database) as part of evaluating a request to authenticate a client. Instead, the cited portions of Kirti show that its system analyzes activity for threats and possible remediation actions whenever its system collects data from the cloud applications in periodic batches, independent of any particular authentication request.

Petitioner argues that Kirti “teaches” the “determine whether an additional verification is required to grant access” limitation because “Kirti[’s] system analyzes a user’s historic login activity to identify potential threats and determine whether to apply ‘remedial measures, such as adding additional steps to authentication.’” Pet., 34. But Petitioner does not show that Kirti performs any of this analysis when evaluating an authentication request. Instead, Kirti builds user profiles and threat models when activity data is collected from cloud applications

and applies remediation measures when a threat is identified—not as part of evaluating a particular authentication request.

As Dr. Malek explains, Kirti builds user profiles, determines threat models, and implements remediation actions whenever activity data is gathered from Kirti’s cloud applications:

Petitioner relies heavily upon Kirti’s Figure 5B as allegedly “show[ing] an exemplary process in which activity data is retrieved and used to generate threat models (step 506) that ‘include baseline user profiles over various periods of time.’” Pet., 42. But Figure 5B is not initiated in response to any authentication request. Indeed, no such request appears in the figure or Kirti’s corresponding description:



**FIG. 5B**

Ex. 1004 [Kirti] Fig. 5B.

Rather, Kirti's system generates a threat model and sets appropriate security controls in steps 506-510 whenever data is collected from the cloud applications in steps 502-504. And, as Petitioner acknowledges (Pet., 39), Kirti describes that it collects activity data from cloud applications "periodically," "e.g., every 4 hours or every 6 hours." Ex. 1004 [Kirti] 10:9-17. Thus, Kirti determines whether additional verification is required on a periodic basis, not when a request to authenticate a client is received.

Ex. 2023 [Malek-Decl.] ¶¶ 53-54.

Petitioner also relies upon Kirti’s collection of activity data in batches. Pet., 39 (“the activity data stored in Kirti’s analytics and threat intelligence repository database (a multidimensional, time-series database) is historical at least because the database ... receives new data in *batches (e.g., from the most recent 24-hour period).*”). In other words, rather than determining whether additional verification is required in response to a particular authentication request, that determination is made when large volumes of data for multiple users are gathered in periodic batches.

Thus, rather than demonstrating that Kirti teaches performing the process of retrieving activity data and generating a threat model whenever a request to authenticate a client is received, Petitioner at most shows that Kirti periodically batch collects activity data for multiple users (*e.g., every 4, 6, or 24 hours*). Any such retrieval is therefore not performed in response to an authentication request.

3. Kirti Does Not Determine Whether Additional Verification Is Required “To Grant Access” In Response To Receiving A Request To Authenticate.

Petitioner’s theory also fails because it does not show that Kirti performs the claimed determination “to grant access” to a received authentication request. The claims do not merely require determining whether additional verification is required in the abstract. Rather, they require determining whether additional

verification is required to grant access to the authentication request being evaluated, *i.e.*, as part of deciding whether that request will be allowed or denied. Ex. 1001 [’426] cls. 1, 9; *see also* Section II.B.1, *infra*. The claimed determination is thus tied to the specific authentication request itself.

Petitioner relies upon Kirti’s teaching of selecting a remediation method which includes “additional steps to authentication” as allegedly teaching “selecting an additional verification method from a plurality of verification methods.” Pet., 49-50. Petitioner then argues that it would have been “[i]n the cases where the remedial action involved ‘additional steps to authentication,’ such as a one-time password, performing that authentication would necessarily involve prompting the client to complete the additional authentication and then determining whether it was corrected completely.” *Id.*, 50.<sup>3</sup>

---

<sup>3</sup> Petitioner’s combination “combines Kirti’s threat detection and remediation system with Coffin’s implementation details on how to select and perform an additional verification process.” Pet., 20. Because Petitioner relies upon Kirti’s overall process of determining whether additional verification is required and only relies upon Coffin’s alleged teachings of “the specific types of measures,” Petitioner’s argument fails for both Kirti alone (Ground 1) and Kirti in combination with Coffin (Ground 2).

But that theory fails. Assuming, counterfactually, that Kirti does determine whether additional verification is required in response to a request to authenticate, Kirti's "additional steps to authentication" are not applied in deciding whether to grant access to the authentication request being evaluated. Instead, they are applied in a different context altogether; after a threat is detected and in connection with other cloud applications.

As Dr. Malek explains, Kirti discusses adding additional steps to authentication in a cloud-to-cloud warning system:

As Petitioner acknowledges, Kirti discusses additional verification twice throughout its disclosure. Pet., 22 (citing Ex. 1004 [Kirti] 28:33 and 5:34). But these disclosures are in the context of a first cloud application detecting a threat and alerting a second cloud application which may then impose additional authentication requirements. As Kirti explains:

One cloud application can *proactively warn another cloud application of a potential threat*. ... When a threat is identified in a first cloud (e.g., a query from a blocked IP address), a cloud security monitoring and control system in accordance with embodiments of the invention can automatically *notify a second cloud* that is part of the business process. The notification can include a request or recommendation for a higher level of security controls,

such as elevated authentication or OTP validation, in the business process.

Ex. 1004 [Kirti] 28:24-34.

Thus, Kirti’s additional verification is not used to determine whether to grant access to the authentication request that triggered the analysis. Rather, it is applied proactively by a different cloud application and in connection with a different authentication to that second cloud if one is attempted, not in deciding whether to grant access to the request being evaluated.

Ex. 2023 [Malek Decl.] ¶¶ 57-58.

Petitioner therefore fails to identify any disclosure in Kirti where, upon receiving an authentication request, the system determines whether additional verification is required to grant access to that request—much less does so by retrieving historical information and prompting the client to complete the additional verification, as required by the claims.

**C. Petitioner Fails To Show That Kirti Alone Or In Combination With Coffin Discloses Or Renders Obvious “Select[ing] An Additional Verification Method From A Plurality Of Verification Methods” (All Claims, All Grounds).**

The claims require a computer system configured to “select an additional verification method from a plurality of verification methods.” Ex. 1001 [’426] cls. 1, 9 (claiming “[a] method implemented on a computer system” performing the limitation). Thus, an “additional verification method” must be selected and it must

be selected “from a plurality of verification methods.” Petitioner presents two alternative theories, both of which fail.

First, Petitioner contends that Kirti alone teaches this limitation because Kirti’s system “determine[s] whether to apply ‘*remedial*’ measures, such as adding additional steps to authentication.” Pet., 34. But that argument conflates two different things. At most, Petitioner demonstrates that Kirti selects among a plurality of “remediation measures.” But only one of those remediation measures is alleged to be a “verification method.” And there is no reason to believe that “remediation measures” are the same as “verification methods.” Thus, Kirti is not shown to select an additional verification method “from a *plurality* of verification methods.” See Section II.C.1.

Second, tacitly recognizing Kirti’s deficiency, Petitioner turns to Coffin because Kirti allegedly “provides little implementation detail for these steps.” Pet., 51; see also *id.*, 20-21. Petitioner argues that Coffin supplies “implementation details on how to select and perform an additional verification process, such as 2-factor authentication.” *Id.*, 20. But Coffin does not disclose a computer system selecting an “additional verification method” from a plurality of such methods. At most Petitioner shows that Coffin discusses different delivery mechanisms for a passcode-based verification technique. Selecting among delivery mechanisms for

one verification technique (a passcode) is not selecting an additional verification method from a plurality of verification methods. *See* Section II.C.2.

Thus, neither Kirti alone nor Kirti in combination with Coffin teaches the claimed limitation.

1. Kirti’s “Remedial Methods” Are Not “Verification Methods” (Ground 1)

Petitioner first argues that Kirti alone “teaches” “select[ing] an additional *verification* method from a plurality of verification methods” through its disclosure of “recommending and performing a *remedial action* when a threat is detected.”

Pet., 49-50. Specifically, Petitioner argues that:

Kirti teaches recommending and performing a *remedial action* when a threat is detected and mentions that *one such remedial action* is “adding additional steps to authentication,” i.e., requiring completion of an additional verification step (e.g., enter a one-time password). *E.g.*, EX1004, 5:27-37, 28:24-36. EX1003, ¶107.

Kirti discloses manually or automatically selecting which one of a plurality of *remedial actions* to use. *E.g.*, EX1004, 5:27-37, 5:55-57 (“embodiments of the invention may include remediation functions that provide manual and/or automated processes in response to threats.”), 6:10-14, 14:64-67, 25:15-20, 25:45-52, 27:10-12. EX1003, ¶108.

*Id.*

That argument does not satisfy the claim language. The claim requires selecting an additional verification method “from a *plurality of verification methods*.” Petitioner instead points to Kirti’s alleged selection from a plurality of remedial actions. Petitioner never identifies in Kirti a plurality of verification methods, much less a computer system selecting from such a plurality.

Nor does Petitioner explain why Kirti’s plurality of remedial actions should be treated as a plurality of verification methods. Although Petitioner does not say so expressly, its argument depends on that unstated equivalence. *See* Pet., 49-50. But Petitioner offers no reasoning and no evidence to bridge that gap. A plurality of remedial actions is not, without more, a plurality of verification methods.

That failure is especially glaring because Petitioner itself acknowledges that only “one such remedial action is ‘adding additional steps to authentication.’” *Id.* Thus, even accepting Petitioner’s premise that “adding additional steps to authentication” could qualify as a verification method, Petitioner still identifies only one such method. The claim, however, requires selecting “from a plurality of verification methods,” *i.e.*, more than one verification method. Petitioner never shows that Kirti discloses more than one verification method from which the system selects.

Petitioner’s contrary assertion is unsupported and conclusory. It is well-settled that “rejections on obviousness grounds cannot be sustained by mere

conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Likewise, “[t]o satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

Petitioner relies on Dr. Black’s declaration, but Dr. Black merely repeats the same unsupported premise. Unsupported expert testimony, such as this, is entitled to “little or no weight.” 37 C.F.R. § 42.65(a). And the Federal Circuit recently reaffirmed that “the conclusory assertions in Dr. Mohazzab’s declaration do not provide substantial evidence for finding a motivation to combine.” *Virtek Vision Int’l ULC v. Assembly Guidance Sys., Inc.*, 97 F.4th 882, 887 n.2 (Fed. Cir. 2024); *see also Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9, 15 (Aug. 24, 2022) (precedential) (“conclusory and unsupported” expert testimony “adds little to the conclusory assertion for which it is offered to support...”); *see also* Section II.A.1.

Quite simply, Petitioner identifies a plurality of remedial actions, then simply assumes that this teaches a plurality of verification methods. Dr. Black

provides no technical reasoning and no supporting evidence for that leap. Under *Xerox*, that is not enough.

Moreover, the record confirms that Kirti’s remedial actions are not the claimed verification methods. As Dr. Malek explains, Kirti discloses several remediation measures, but only one is even arguably tied to further authentication:

Kirti teaches that when a threat is detected, its system can “secure other services on which a user maintains data by apply remedial measures [*sic*], such as adding additional steps to authentication, changing passwords, blocking a particular IP address or addresses, blocking email messages or senders, or locking accounts.” Ex. 1004 [Kirti] 5:27-37; 25:45-49 (“any of a variety of security measures may be taken to address an identified threat such as, but not limited to, deactivating an account, resetting a password, or setting stronger security controls.”).

As Petitioner and Dr. Black tacitly admit, only one of these options (“adding additional steps to authentication”) is possibly a verification method. *See* Pet., 49-50 (Kirti “mentions that ***one such remedial action*** is ‘adding additional steps to authentication,’ i.e., requiring completion of an additional verification step (e.g., enter a one-time password).”). But, even if that were a verification method, Kirti is not shown to disclose a “plurality of verification methods”—*i.e.*, more than one verification method—that is selected from.

Ex. 2023 [Malek-Decl.] ¶¶ 64-65.

Dr. Malek also explains why Kirti's other remedial measures are not "verification methods" as that term is used in the art and in the '426 patent:

To the extent that Petitioner meant to argue that Kirti's other "remedial" measures are "verification methods," there is simply no reason to believe this is so. Verification is intended to confirm that a user is who he or she claims to be. *See* Ex. 2033 [InvestGlass] ("The process of identity verification serves as an essential safeguard, crucial in establishing that individuals are genuinely who they claim to be."); Ex. 2034 [Barron's Dictionary of Computer and Internet Terms] 530 ("verified user on Twitter, an account belonging to a public figure that has been authenticated. *The person posting is who they claim to be and has submitted documentation to prove it.*"); Ex. 1005 [Coffin] 177 ("we are looking for further constraints on identity that can *assure us that the person sitting at the keyboard is who they claim to be.*").

Consistent with the usage in the art, the '426 patent describes several verification methods, meant to confirm that a user is who he or she claims to be. The '426 patent provides many examples of "verification methods" such as "biometrics scans, such as fingerprint scan, iris scan, facial recognition, and the like; voice recognition; and employee badge scanning using some near-field technology such as radio-frequency identification (RFID), or near field communication (NFC)." Ex. 1001 ['426] 10:34-40; *see also id.*, 10:43-52 ("a user's co-worker or security personnel" may provide additional verification); 10:53-65 (a "rewards program" "disguised so that it may appear as a simple activity ... without overtly making it a means of verifying the

user”); 10:66-11:3 (using “videos or pictures”); 11:4-20 (“Device ID” and “Network monitoring 415e may be passive verification by the server based on information regarding the connection requesting access”); 11:21-27 (“One-time use codes 415g may be uniquely generated codes that are sent to the user through a text message or email, or generated on-demand on the user’s mobile device.”). Each of these methods is used to confirm that a user is who he or she claims to be.

Ex. 2023 [Malek-Decl.] ¶¶ 66-67.

That distinction matters. Verification methods are methods for confirming identity. Kirti’s remedial actions, by contrast, are broader security responses to an identified threat. As Dr. Malek explains:

In contrast to confirming that a user is who he or she claims to be, Kirti’s remedial actions are intended to more broadly secure its system and address the threat. In accord, Kirti only teaches that one possible remediation action is “adding additional steps to verification” (Ex. 1004 [Kirti] 5:27-37) because that is only one method of remediating possible threats. Kirti also considers selecting from additional remedial methods of “deactivating an account,” “changing the password, blocking a particular IP address or addresses, blocking email messages or senders, or locking accounts” (*id.*; *id.*, 25:45-49) which “remediate” possible threats by eliminating vulnerabilities or vectors for attack. These methods do not have anything to do with verifying whether a user is who he or she claims to be.

Ex. 2023 [Malek-Decl.] ¶ 68.

In short, Kirti teaches a plurality of remediation measures, not a plurality of verification methods. Because Petitioner never shows that Kirti discloses “select[ing] an additional verification method from a plurality of verification methods,” Petitioner fails to demonstrate that Kirti alone teaches the limitation.

2. Petitioner Fails To Show That Its Kirti-Coffin Combination Teaches “Select[ing] An Additional Verification Method” (Ground 2)

Tacitly recognizing Kirti’s deficiencies, Petitioner next turns to Coffin. Petitioner acknowledges that Kirti “provides little implementation detail for” the steps of “selecting and performing additional verification.” Pet., 51. Petitioner therefore argues that Coffin “expressly teaches details for selecting one of a plurality of verification methods.” *Id.* But Petitioner’s Coffin theory fails for a basic reason: Petitioner never identifies a computer system that selects an additional verification method from a plurality of verification methods as the claims require.

Petitioner first points to Coffin’s list of authentication techniques, including, *e.g.*, a “‘second password or PIN,’ ‘a CAPTCHA,’ an ‘answer [to] personal questions,’ a ‘biometric scan[], like fingerprint, retina, or facial recognition,’ and ‘pass codes sent to [] e-mail, pager, or cell phone[.]’” *Id.*, 51-52 (quoting Ex. 1005 [Coffin] 177). But Petitioner does not actually contend that the alleged Kirti-

Coffin combination selects from that list. Nor could it. Coffin's generic discussion of authentication techniques in the art does not disclose a particular system selecting among those techniques as required by the claims.

As Dr. Malek explains:

Coffin is a textbook that lays out concepts for securing Oracle applications. Ex. 1005 [Coffin] 1 (“We will not be building any specific application, but will focus on the security aspects in building an application.”). While Coffin lays out a list of the “many things that are being done in computer security to attempt to achieve” authentication, that list is disembodied and not tethered to any particular system. *Id.*, 177. In other words, Coffin's list of authentication methods is not a “plurality of verification methods” from which a particular system will select an additional verification method as required by the claims. Rather, it is a list of methods being attempted in computer security. Unsurprisingly, Coffin never mentions or teaches how a system would “select an additional verification method” from Coffin's general, list of authentication methods.

Coffin's disclosure in this regard is analogous to a textbook on automobiles stating that various engines used in the automobile industry include gasoline, diesel, hybrid, or electric engines. This is merely a disclosure that a car may have any one of those engines, not a disclosure that the car has access to a plurality of engines that it may select an additional engine from.

Ex. 2023 [Malek-Decl.] ¶¶ 71-72. A generic list of techniques that exist in the field is not the same as a computer system selecting one of those techniques. The claim requires the latter. Petitioner identifies only the former.

Indeed, when Petitioner turns from identifying a supposed “plurality of verification methods” to identifying the required “selection,” Petitioner abandons Coffin’s generic list of authentication techniques and shifts to a different disclosure altogether: Coffin’s discussion of what device a two-factor passcode is sent.

Petitioner argues that:

Coffin also teaches a heuristic for selecting an additional verification method from the plurality of passcode verification methods: select the user’s pager and/or cell phone if these devices are available, otherwise select email. *E.g.*, EX1005, 183, 185, 200 (“By preference, [the system] will send the two-factor code to the user’s pager and cell phone. If neither of those is available, [the system] will send the code to the user’s e-mail.”), 201. It also was well known in the art to select an additional verification method from a plurality of verification method, for example, to ensure successful delivery of the additional verification based on the availability of the verification methods, cost, user preferences, etc. *Supra* Section IV.B.2. EX1003, ¶112.

Pet., 52.

That is not a disclosure of selecting an additional verification method from a plurality of verification methods. At most, it is a disclosure of selecting a delivery

channel for one verification method—a passcode. Receiving a code by pager, cell phone, and email are not different verification methods. They are merely different ways of delivering the same passcode-based verification technique. As Dr. Malek explains:

Petitioner and Dr. Black do not identify any teaching in Coffin of selecting from the list Petitioner identifies as the “plurality of verification methods.” *See* Pet., 51-52; Ex. 1003 [Black-Decl.] ¶¶ 111-112. Petitioner instead turns to Coffin’s description of the “process of requesting and receiving the two-factor *pass code*.” Pet., 52; Ex. 1005 [Coffin] 183. Per Petitioner, Coffin teaches “selecting an additional verification method from the plurality of passcode verification methods: select the user’s pager and/or cell phone if these devices are available, otherwise select email.” Pet., 52. But these alleged “verification methods” are not the same as the earlier-identified list of verification methods. *Compare* Ex. 1005 [Coffin] 177 *with id.*, 183. Rather, this is a list of methods for obtaining a pass code, *e.g.*, via pager, cell phone, or email.

But, sending a pass code to different devices (a pager, cell phone, or computer) is merely selecting from a plurality of delivery methods. Only a single verification method—obtaining a passcode—is disclosed. Thus, at best, Petitioner demonstrates that Coffin teaches selecting a delivery method from the options of pager, cell phone, or email from a particular verification method (passcode). This is not the same as

“select[ing] an additional verification method from a plurality of verification methods.”

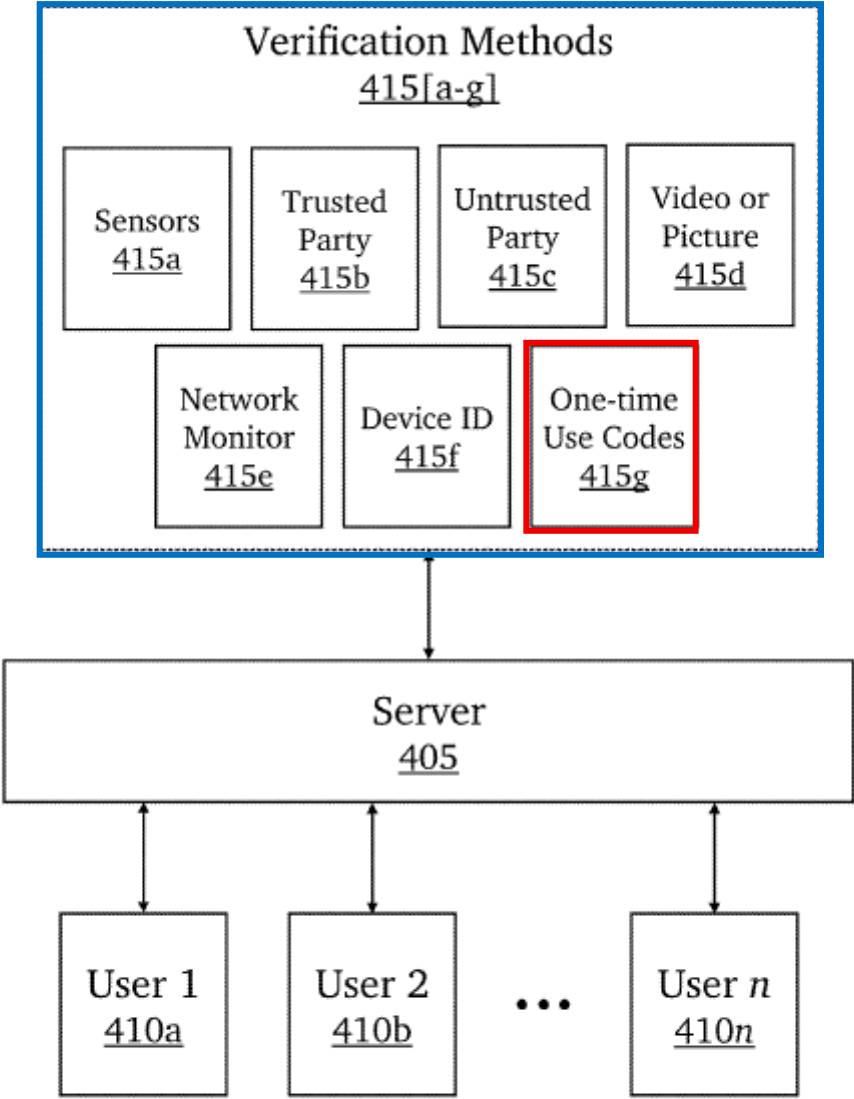
Ex. 2023 [Malek-Decl.] ¶¶ 73-74.

Thus, Petitioner’s Coffin theory equivocates between two different “pluralities.” First, Petitioner points to Coffin’s generic list of authentication techniques at page 177. But Petitioner never identifies any teaching that a system selects from that list. Then, when attempting to identify the required “selection,” Petitioner pivots to Coffin’s separate disclosure about sending a passcode by pager, cell phone, or email. But that second disclosure concerns delivery mechanisms for a passcode, not selection among different verification methods. The claim requires selection among verification methods, not selection among channels for delivering one method.

The ’426 patent itself confirms that distinction. As Dr. Malek explains, the patent treats “one-time-use codes” as a single verification method, while recognizing that those codes may be delivered through different channels:

The ’426 patent discloses that its system 400 uses “one or more verification methods 415[a-g], which may include, without limitation, sensors 415a, trusted parties 415b, untrusted parties 415c, video or picture 415d, network monitoring 415e, device ID 415f, and *one-time-use codes 415g*.” Ex. 1001 [’426] 10:28-33. As can be seen in Figure

4 below, these are each separate and independent **verification methods**, with the **one-time-use code** as a single verification method:



400

**Fig. 4**

*Id.*, Fig. 4 (annotated). Within the description of the one-time-code verification method, the '426 patent describes that the codes “may be uniquely generated codes that are sent to the user through a text message or email, or generated on-demand on the user’s mobile device.” *Id.*, 11:21-23.

Thus, the '426 patent makes clear that the use of a “one-time code” is itself the verification method and that delivery of the one-time code through text message or through email are not separate verification methods.

Ex. 2023 [Malek-Decl.] ¶¶ 76-77.

Finally, left without Kirti or Coffin for an adequate teaching of this limitation, Petitioner asserts that it was:

*well known* in the art to select an additional verification method from a plurality of verification methods, for example, to ensure successful delivery of the additional verification based on the availability of the verification methods, cost, user preferences, etc. *Supra* Section IV.B.2. EX1003, ¶112.

Pet., 52.

This argument also fails. As an initial matter, Petitioner’s own explanation of this supposed background knowledge again focuses on “*successful delivery* of the additional verification based on the availability of the verification methods, cost, user preferences, etc.” *Id.* So even this fallback theory continues to collapse

verification methods into delivery considerations.

More fundamentally, Petitioner cites only a generalized background discussion and Dr. Black's declaration. *Id.*, 52, 7-9. Dr. Black, in turn, cites several systems that purportedly "offer several multi-factor verification options." Ex. 1003 [Black-Decl.] ¶ 42. But Petitioner does not analyze those systems in its obviousness grounds, does not propose combining them with Kirti or Coffin, and does not explain how they may properly supply the missing limitation.

That is not enough. Although references beyond a Petitioner's grounds may "document the knowledge that skilled artisans would bring to bear in reading the prior art identified as producing obviousness," *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1365 (Fed. Cir. 2015), Petitioner cannot use generalized "knowledge in the art" to fill a missing claim limitation that its asserted Kirti-Coffin combination does not teach.

Nor may Petitioner invoke unasserted systems as a substitute for an actual analysis of the proposed combination. *Virtek Vision Int'l ULC v. Assembly Guidance Sys., Inc.*, 97 F.4th 882, 886-7 (Fed. Cir. 2024) ("It does not suffice to meet the motivation to combine requirement to recognize that two alternative arrangements ... were both known in the art."); *RPX Corp. v. Parity Networks, LLC*, IPR2018-00097, Paper 7, 14 (Apr. 24, 2018) ("Petitioner also cites to several other references . . . but does not assert these references are part of the

combination. Relying on knowledge in the art does not . . . show a motivation to combine existing components in the manner claimed free of hindsight motivation.”); *Edwards Lifesciences Corp. v. Aortic Innovations LLC*, IPR2023-01232, Paper 10, 36 (Feb. 7, 2024) (“Petitioner’s rationale to modify Spenser II based on inchoate and unasserted combinations is also unpersuasive.”).

In short, Petitioner’s Coffin theory fails at every step. Coffin’s generic list of authentication techniques does not disclose a computer system selecting among those techniques. Petitioner’s actual “selection” theory concerns only delivery channels for a passcode, not selection among verification methods. And Petitioner’s generalized appeal to background knowledge cannot supply the missing limitation. Petitioner therefore fails to demonstrate that Kirti in combination with Coffin teaches “select[ing] an additional verification method from a plurality of verification methods.”

### **III. CONCLUSION**

Thus, Petitioner fails to demonstrate a reasonable likelihood of success as to any of the challenged claims, and the Petition should be denied.

Respectfully submitted,

/Kenneth J. Weatherwax/

Kenneth J. Weatherwax (Reg. No. 54,528)  
Nathan Lowenstein, *pro hac vice* pending  
Colette Woo, *pro hac vice* pending  
LOWENSTEIN & WEATHERWAX LLP

Date: April 8, 2026

**CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITS**

This Patent Owner Preliminary Response (the “POPR”) consists of 8,764 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/

Abbie Neufeld

Date: April 8, 2026

**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 PRELIMINARY RESPONSE**

**EXHIBITS 2023-2034**

The names and addresses of the parties being served are as follows:

Andrew M. Mason	andrew.mason@klarquist.com
Frank Morton-Park	frank.morton-park@klarquist.com
Todd M. Siegel	todd.siegel@klarquist.com
Samuel B. Thacker	samuel.thacker@klarquist.com
	Msft-Qomplx@klarquist.com

Respectfully submitted,

/Abbie Neufeld/  
Abbie Neufeld

Date: April 8, 2026