

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION
Petitioner,

v.

DIGITAL DOORS, INC.
Patent Owner.

Case IPR2023-00967
U.S. Patent 7,313,825

**PATENT OWNER DIGITALDOORS, INC.'S
PRELIMINARY RESPONSE**

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Background.....	2
	A. The DigitalDoors Technology.....	2
	B. The '825 Patent	5
	C. Bossemeyer	10
	D. Glick	14
	E. Carmichael.....	14
III.	Governing Law	15
IV.	The Bossemeyer Reference Is Not Analogous Art to the '825 Patent.	16
	A. Bossemeyer and the '825 Patent concern different fields of endeavor.	16
	B. Bossemeyer is not pertinent to the problems faced by the inventors of the '825 Patent.....	19
	C. Bossemeyer is not analogous to the '825 Patent.....	23
V.	Bossemeyer and Glick Each Fail to Teach Claimed <i>Extracted Data</i> and the <i>Reconstruction</i> Method Step, Warranting Denial on both of Petitioner's Grounds for Challenging the Claims.....	23
	A. Bossemeyer does not disclose “said security sensitive words, characters, data objects or icons extracted from said data to obtain extracted data.”	25
	B. Bossemeyer and Glick do not disclose “permitting full or partial reconstruction of said data via said extracted data.”	33
	i. Bossemeyer	33
	ii. Glick.....	40

VI.	Petitioner’s Grounds 1 and 2 Lack the Necessary Motivation to Combine Bossemeyer and Glick.	42
VII.	The Board should deny institution on both grounds under <i>Fintiv</i>	47
A.	The district court is unlikely to grant a stay.	48
B.	Trial is scheduled to finish over three months before the Final Written Decision deadline.	49
C.	Both parties have invested heavily in the district court proceedings..	50
D.	Petitioner has asserted the same three references in the district court proceedings.....	51
E.	The Petitioner and the Defendant in the district court proceeding are the same party.....	52
F.	The Petition does not present compelling evidence of unpatentability.	53
VIII.	CONCLUSION.....	54

TABLE OF AUTHORITIES

Cases

<i>Airbus S.A.S. v. Firepass Corp.</i> , 941 F.3d 1374 (Fed. Cir. 2019)	19
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020).....	passim
<i>Commscope Technologies LLC v. Dali Wireless, Inc.</i> , IPR2022-01242, Paper 23 (PTAB Feb. 27, 2023)	48
<i>Continental Can Co. v. Monsanto Co.</i> , 948 F.2d 1264 (Fed. Cir. 1991)	32
<i>Dropworks, Inc. v. Bio-Rad Laboratories, Inc.</i> , IPR2021-00212, Paper 7 (P.T.A.B. Jun. 1, 2021).....	42, 46
<i>DSS Tech. Mgmt., Inc. v. Apple Inc.</i> , 885 F.3d 1367 (Fed. Cir. 2018)	34
<i>Harmonic Inc. v. Avid Tech., Inc.</i> , 815 F.3d 1356 (Fed. Cir. 2016)	15
<i>In re Bigio</i> , 381 F.3d 1320 (Fed. Cir. 2004)	16
<i>In re Clay</i> , 966 F.2d 656 (Fed. Cir. 1992)	17, 19
<i>In re Icon Health and Fitness, Inc.</i> , 496 F.3d 1374 (Fed. Cir. 2007)	19
<i>In re Oelrich</i> , 666 F.2d 578 (C.C.P.A. 1981).....	32
<i>In re: Natural Alternatives, LLC</i> , 659 Fed. Appx. 608 (2016).....	42
<i>Innovention Toys, LLC v. MGA Entm't, Inc.</i> , 637 F.3d 1314 (Fed. Cir. 2011)	15

<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	15, 42, 45, 46
<i>Neato LLC v. Rocky Mountain Traders</i> , 138 F. Supp. 2d 245 (D. Ct. 2001)	17, 20, 44
<i>NHK Spring Co., Ltd. v. Intri-Plex Techs., Inc.</i> , IPR2018-00752, Paper 8 (PTAB Sept. 12, 2018)	50
<i>PAR Pharm., Inc. v. TWI Pharms., Inc.</i> , 773 F.3d 1186 (Fed. Cir. 2014)	32
<i>Sanofi-Aventis Deutschland GmbH v. Myland Pharmaceuticals Inc.</i> , 66 F.4th 1373 (Fed. Cir. 2023)	15
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> , IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020)	52
<i>Tinnus Enterprises, LLC v. Telebrands Corp.</i> , 846 F.3d 1190 (Fed. Cir. 2017)	19, 44
<i>Vill. Green Techs., LLC v. Samsung Elecs. Co.</i> , No. 2:22-CV-00099-JRG, 2023 WL 416419 (E.D. Tex. Jan. 25, 2023)	49
<i>Wang Laboratories, Inc. v. Toshiba Corp.</i> , , 993 F.2d 858 (Fed. Cir. 1993)	16, 44
<i>WBIP, LLC v. Kohler Co.</i> , 829 F.3d 1317 (Fed. Cir. 2016)	45, 46
<i>Xerox Corp. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 9 (August 24, 2022)	27

Statutes

35 U.S.C. § 103	15
35 U.S.C. § 312(a)(3)	15, 35
35 U.S.C. § 314(a)	1
37 C.F.R. § 42.104(b)(4)	15

37 C.F.R. § 42.107	1
--------------------------	---

Other Authorities

MPEP § 2141.01(a).....	19
------------------------	----

LIST OF EXHIBITS

Exhibit Number	Document
2001	Correspondence with William H. Webster
2002	Correspondence with Robert F. Behler
2003	The Most Cited US Patents in 2019 – Paper Digest
2004	Expert Declaration of Dr. William C. Easttom II
2005	Dr. William C. Easttom II CV
2006	Nader, Jonar, Prentice Hall’s Illustrated Dictionary of Computing: Internet Update (Prentice Hall 1998, Third Edition)
2007	Order re Motion to Stay, <i>DigitalDoors, Inc. v. International Business Machines Corporation</i> , Case No. 2:22-cv-457, Eastern District of Texas
2008	Defendant’s Invalidity Contentions Cover Pleading, April 25, 2023, <i>DigitalDoors, Inc. v. International Business Machines Corporation</i> , Case No. 2:22-cv-457, Eastern District of Texas
2009	USPTO Patent Classification Code Definitions – Class 726
2010	USPTO Patent Classification Code Definitions – Class 713
2011	USPTO Patent Classification Code Definitions – Class 380
2012	McClannan, Keith, <i>Implementing Smart Cards Into the Air Force Reserve</i> , Air Command and Staff College, April 2001
2013	Posey, Brien, <i>All about partitions: The right FAT can save your waste</i> , Daily Tech Insider, Sep. 2000
2014	Walker, Martin, <i>Splitting Your PC Data Across Multiple Drives & Partitions</i> , Sound on Sound, Aug. 2000

Exhibit Number	Document
2015	<i>BAI2</i> , Modern Treasury Corp
2016	<i>BAI2 Format Specification</i> , SEPA for Corporates, Jan. 2015
2017	Maheshwari, Ajay, <i>EBS – How to interpret a BAI2 file</i> , SAP, Oct. 2015
2018	<i>Standards MT</i> , Swift, 2023
2019	<i>ISO 20022 Message Definitions</i> , ISO, Sep. 2010
2020	<i>ACH Guide for Developers</i> , Nacha
2021	<i>Pass Design and Creation</i> , Wallet Developer Guide, Jan. 2018
2022	<i>About Pass Files</i> , Apple Inc., Nov. 2017
2023	Daswani, Neil et. al., <i>SWAPER00: A Simple Wallet Architecture for Payments, Exchanges, Refunds, and Other Operations</i> , USENIX Workshop, Aug. 1998
2024	Clark, Brent, <i>Electronic Wallets: Past, Present, and Future</i> , GPayments, 2001
2025	<i>NetPay Wallet</i> , Maithean
2026	Wayner, Peter, <i>Cyberchas’s Lesson in Web Survival</i> , The New York Times, Aug. 1998
2027	<i>HL7 Messages Examples – Complete Guide 2023</i> , folio3 Software Inc.
2028	<i>About SDA</i> , InterSystems, 2023
2029	<i>Guide to the 837 File Format</i> , Kasa Solutions
2030	Denecke, Kerstin, <i>Biomedical Standards and Open Health Data</i> , Science Direct, 2021

Exhibit Number	Document
2031	Ibarrera, <i>Merging data from multiple sources</i> , Data Ladder, Nov. 2021
2032	Audette, Lillian M. et. al., <i>Merging Multiple and/or Divergent Datasets using SPSS: A Method Review and Tutorial</i> , Graduate Student Journal of Psychology 2022, Vol. 19, 2022
2033	Al, Muhammad et. at., <i>Merge and Append Using Stata: How to Merge and Append Datasets</i> , Princeton University, May 2023
2034	Kadane, Joseph B., <i>Some Statistical Problems in Merging Data Files</i> , Journal of Official Statistics, Vol. 17, No. 3, 2001
2035	Groves, Robert M. et. al., <i>Federal Statistics, Multiple Data Sources, And Privacy Protection</i> , The National Academies Press, 2017
2036	<i>Department of Computer Science CSE Courses</i> , Stony Brook University
2037	<i>Lecture Notes for Chapter 3 System Security</i> , Stony Brook University
2038	Sekar, R., <i>CSE509 - Computer System Security</i> , Stony Brook University
2039	Dowing, Douglas, <i>Dictionary of Computer Terms</i> (Barron's Business Guide 1995, Fourth Edition)

I. Introduction

Pursuant to 37 C.F.R. § 42.107, Patent Owner DigitalDoors, Inc. submits this Preliminary Response to the above-captioned Petition for *Inter Partes* Review (“Pet.,” Paper 2) of United States Patent No. 7,313,825 (“the ’825 Patent”) filed by International Business Machines Corporation (“Petitioner” or “IBM”).

Petitioner alleges that U.S. Patent No. 7,010,701 (“Bossemeyer,” EX1005) in combination with U.S. Patent No. 6,985,588 (“Glick,” EX1006) (Ground 1) or in combination with Glick and U.S. Patent No. 7,913,919 (“Carmichael,” EX1007) (Ground 2) renders Claim 81 of the ’825 Patent obvious.

The Petition does not present a reasonable likelihood that Petitioner will prevail with respect to the challenged Claim 81 under 35 U.S.C. § 314(a). Patent Owner, therefore, opposes institution of an IPR of the ’825 Patent.

The Petition is deficient for at least four reasons:

1. Bossemeyer is not analogous art and, therefore, cannot be considered in a 35 U.S.C. § 103 obviousness argument. Bossemeyer and the ’825 Patent are in far different fields of endeavor. Bossemeyer concerns “smart card applications using a smart card in combination with a smart card terminal” and the field of the ’825 Patent is secure distribution and storage of files/documents/data objects across telecommunications networks. EX1005, Abstract; EX1001, 1:35-43. Bossemeyer is also not pertinent to the problems of data processing, distributing, and reconstructing to defeat hackers that the ’825 Patent

solves. This deficiency is sufficient to deny institution on both Grounds 1 and 2.

2. All of the three references are missing the same two elements of the '825 Patent's challenged claim, "said security sensitive words, characters, data objects or icons extracted from said data" and "permitting full or partial reconstruction of" the original "data." These references, therefore, cannot invalidate Claim 81, either individually or as a combination. This deficiency is sufficient to deny institution on both Grounds 1 and 2.
3. A person of ordinary skill would not have combined Bossemeyer with Glick because Glick is non analogous art to Bossemeyer. This deficiency is sufficient to deny institution on Grounds 1 and 2.
4. The *Fintiv* factors dictate discretionary denial of institution on both grounds.

II. Background

A. The DigitalDoors Technology

Two decades ago, the private sector did not generate or keep the massive amounts of data it now does. Nor did it have the same concerns about data security or data recovery after a disaster. There was not much private-sector activity directed at addressing these issues.

The U.S. government was different. It, particularly the military and national security sectors, was starting to generate and use lots of data at that time. And it was

grappling with how to maintain the secrecy of all this stored data. External hackers were one threat. So were people authorized to access the data who might misuse it. Another concern was data recovery in the event of loss, such as destruction of a data center.

Ron Redlich and Martin Nemzow founded DigitalDoors in 2001 to develop data-security and survivability solutions for the U.S. Government, primarily the military and intelligence agencies. Core features of what DigitalDoors developed included extracting some content from files, documents, and data objects and then dispersing both the extracted and remainder data separately in pieces to different storage locations. *See e.g.*, EX1001, 11:63-66. This new and inventive method of data extraction and distributed storage increased security because hackers would have to hack multiple locations without knowing where or what they were, or how to fit pieces together. EX1001, 24:7-19. It also provided survivability, particularly when different copies of the same pieces were distributed in different locations, because a military strike would be unlikely to wipe out all the pieces of the data. EX1001, 12:57-67.

The DigitalDoors system enabled partial or complete reconstruction of the original files, documents, and data objects by pulling the distributed pieces back and putting them together into the whole in which they began. *See e.g.*, EX1001, 9:8-11.

Using different levels of security for access to different pieces allowed for control over reconstruction. EX1001, 28:10-13. Someone with a lower level of security clearance might only have authorization to recover less-significant pieces of data, resulting in partial reconstruction, while one with higher security clearance might be able to reconstruct the entire document. EX1001, 8:47-52. The DigitalDoors system also enables use of location information of portable devices for added control over the extraction and reconstruction processes. EX1001, 59:29-60:28. These technologies, therefore, provided the desired digital security and survivability. *See e.g.*, EX1001, 12:57-67.

DigitalDoors presented what it had developed as part of several military and government-agency processes seeking data-security solutions in the early 2000s. Its innovations were unique and well-received. William H. Webster, a former director of both the CIA and FBI, wrote, “we are impressed by your concepts for multilevel dissemination and collection of data stream information and believe it could have important uses for the security of our country.” EX2001. Ret. Major General Robert Behler, former Commander of the Air Force Command and Control, and Intelligence, Surveillance and Reconnaissance Center, Langley Air Force Base, then affiliated with the Johns Hopkins Applied Physics Laboratory, which was involved in evaluating proposed solutions, wrote, “[w]e are very encouraged about your

approach to this critical national challenge...I've heard many different approaches to [Information Assurance]...Yours seems to have t[he] most promise." EX2002.

DigitalDoors sought patents on these innovations, ultimately resulting in, among others, the '825 Patent. Unfortunately, as a small startup maneuvering the complex and bureaucratic government-contracting process, DigitalDoors was unable to secure a contract to complete development of and implement its solution.

In the ensuing years, the private sector began facing the same issues as those that prompted DigitalDoors's innovations: securing large amounts of data from external and internal security threats and disaster recovery. Efforts to develop solutions for the private sector followed.

Some of the resulting products adopted the same techniques that DigitalDoors had invented years earlier. The original DigitalDoors patents, consequently, have been cited thousands of times. In fact, four of this tiny company's patents (all family members of the '825 Patent) were among the top 100 most-cited U.S. Patents in 2019, based on the number of citations received that year. EX2003.

B. The '825 Patent

The '825 Patent is titled "Data security system and method for portable device." DigitalDoors filed for it in March 2003 based on CIPs and provisional applications going back to November 2000. The '825 Patent issued on December 25, 2007.

Traditional methods of restricting data access before the '825 Patent and its family members often followed a binary “all-or-nothing” approach: one could either access the entire document or none of it. When they did limit access to different pieces of data in a larger data set, they did so without first breaking up the data into pieces. These traditional data-control mechanisms also did not prevent the user from distributing the data to other parties. In addition, storing entire data files in a single location made them vulnerable to hacking because a hacker who breached one location gained access to the entire file. Finally, these security measures did nothing to enhance the survivability of the networks' data. Without redundant back-up storage locations, if one location was destroyed or crashed, the data stored there was lost.

The invention in the '825 Patent's challenged claim provides data security in a different fashion that avoids these technological limitations. Its abstract summarizes the patented approach, including extraction of content, distributed storage with multilevel security, and subsequent reconstruction:

The method, used with a portable computing device, secures security sensitive words, icons, etc. by determining device location within or without a predetermined region and then extracting the security data from the file, text, data object or whatever. The extracted data is separated from the remainder data and stored either on media in a local drive or remotely, typically via wireless network, to a remote store.

Encryption is used to further enhance security levels. Extraction may be automatic, when the portable device is beyond a predetermined territory, or triggered by an event, such a “save document” or a time-out routine. Reconstruction of the data is permitted only in the presence of a predetermined security clearance and within certain geographic territories. A computer readable medium containing programming instructions carrying out the methodology for securing data is also described herein. An information processing system for securing data is also described.

EX1001, Abstract. The challenged claim details extracting security sensitive content from an original data source, storing different pieces of data in separate stores, assigning different security clearance levels to users, and then permitting partial or full reconstruction of the filtered data only in the presence of corresponding security clearances and within a predetermined region.

Claim 81 of the '825, with the elements critical to the Petition bolded, recites:

A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective extract stores with security access controls thereat, **said security sensitive words, characters, data objects or icons extracted from said data** to obtain extracted data and remainder data which extracted data is stored in respective extract stores corresponding to a respective security level of

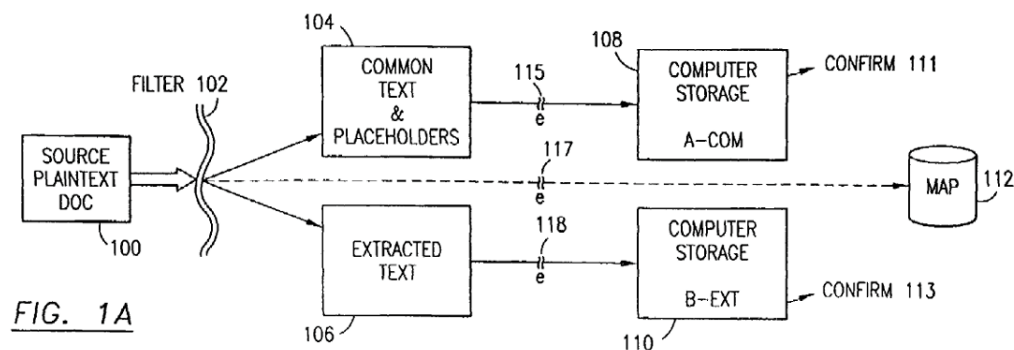
said extract stores, said computer system having at least one portable computing device locatable with current location data, comprising:

determining when said portable computing device is within a predetermined region based upon said current location data;

permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data only in the presence of a predetermined security clearance access control corresponding to said respective security level and only when said portable computing device is not beyond said predetermined region.

The challenged claim of the '825 Patent includes “extracted data” and a “reconstruction” step.

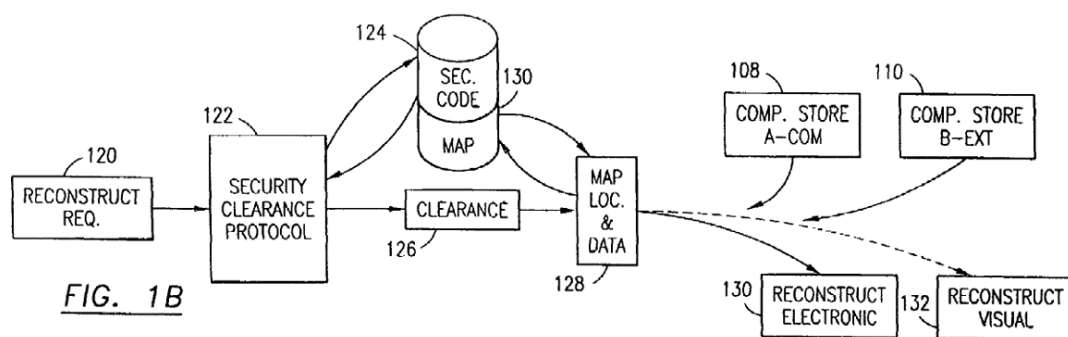
The '825 Patent's specification illustrates various embodiments of these elements. Figure 1A, for example, is a basic system diagram showing filtering and storing extracted data and remainder data.



The system starts with a source document, also sometimes referred to as a “data object.” EX1001, 22:28-31. Examples of such source documents include email,

instant messages, Word documents, database records, and XML documents. EX1001, 10:64-67. The system uses a filtering process to extract the security sensitive words, characters, or icons from original source document. EX1001, 19:48-50. The result is two sets of data, extracted text and remainder, or “common” text. The system then stores the extracted data in memory separate from the storage of the remainder data. EX1001, 21:67-22:4.

FIG. 1B illustrates the reconstruction step:



After the user initiates the reconstruction process, the system determines the level of security clearance and whether full or partial reconstruction will take place. EX1001, 24:55-60. The claimed method “introduces multilevel security through sanitization of critical content of a source or plaintext document (or data object) with the unique ability to reconstruct all or part of the original document in conformance to the classification level of the user.” EX1001, 39:54-59. With the proper security clearance a user can “download or recreate the entire original source, plaintext

document.” EX1001, 29:14-18. As one example, certain security sensitive words removed from a plaintext document are re-inserted into their original locations, “recreat[ing]” the “original source, plaintext document.” EX1001, 29:3-18. The system can also determine the location of a portable computing device from which the secure data is accessed and permit reconstruction of the data only within certain geographic boundaries. EX1001, Abstract; EX1001, 61:7-16.

Extraction and subsequent reconstruction are critical aspects of the invention:

The system and method creates a high level of security by automatic selection and removal of critical and prioritized contents from a data objects stream, whether it be a digital document, digital file, database, sound bite, video clip, other structured, or streaming data formats. The system and method enables a controlled release of the extracted data objects, enabling instant display of the instantaneous returned contents, contingent on verification of user identity, access rights, time of operation, location of source and or user, destination of source and or user, and determine threat modes.

EX1001, 22:46-56.

C. Bossemeyer

Bossemeyer is titled, “Network arrangement for smart card applications.” Not surprisingly, its abstract focuses on smart card applications and terminals:

A network for *smart card applications* using a *smart card* in combination with a *smart card terminal*. The network arrangement

includes a communications network connected to at least one *smart card terminal*, and a central database server in operative communication with the network central office. The network central office is part of the public switched telephone network and transmits *smart card data* between the *smart card terminal* and central database server. The central database server includes many partitioned memory locations each containing information associated with a *smart card application*. The information contained in the partitioned memory locations is accessible by data pointers stored on the individual *smart cards*. In this manner, the amount of data stored on the *smart cards* using the system is reduced and all of the information relating to a *smart card user* is centralized in one location. The central database server includes means for distinguishing between public information and proprietary information stored in the partitioned memory locations.

EX1005, Abstract (emphasis added). The specification describes Bossemeyer's technical field as "smart card applications and, more particularly, to a network arrangement to provide access to an architecture that supports a variety of advanced smart card applications." EX1005, 1:7-11.

"Smart cards" are "substitute, replacement, or consolidation cards" for credit/debit/ATM cards as well as car rental, hotel, and airline membership cards. EX1005, 1:17-20, 27-31. They hold "much more information" than conventional magnetic stripe cards and "often include some 'intelligence' such as a microprocessor." EX1005, 1:34-38.

Figure 1 shows one embodiment of Bossemeyer's network arrangement for smart cards. EX1005, 1:61-62.

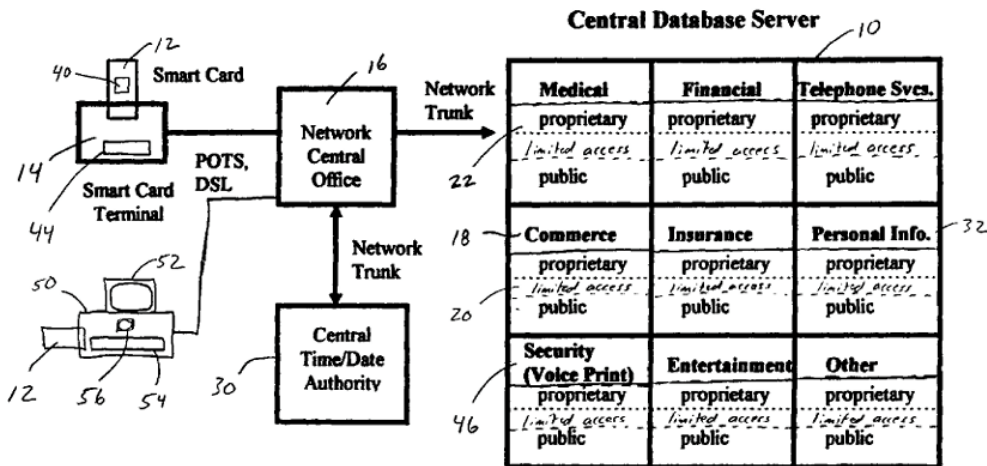


Figure 1

The smart card and smart card terminal connect through the telephone system central office to a central database server. The smart card stores “pointers” to different areas of the central server’s memory. EX1005, 2:58-60.

That central database server’s memory is partitioned, with different types of information in separate areas. EX1005, Fig. 1, 2:13-36. Some of the information, such as personal medical information, is considered private or proprietary. EX1005, 2:27-36.

When a user goes to a store or office in person, he or she inserts the smart card into the merchant’s smart card terminal. EX1005, 3:52-53. After user verification, the data pointer points to the partitioned area of memory with the desired piece of

information. EX1005, 3:63-66. Data from that location is then supplied back to the smart card and smart card terminal. EX1005, 4:3-6.

Bossemeyer's Figure 3 provides another example of partitioned memory and the types of information stored within each area:

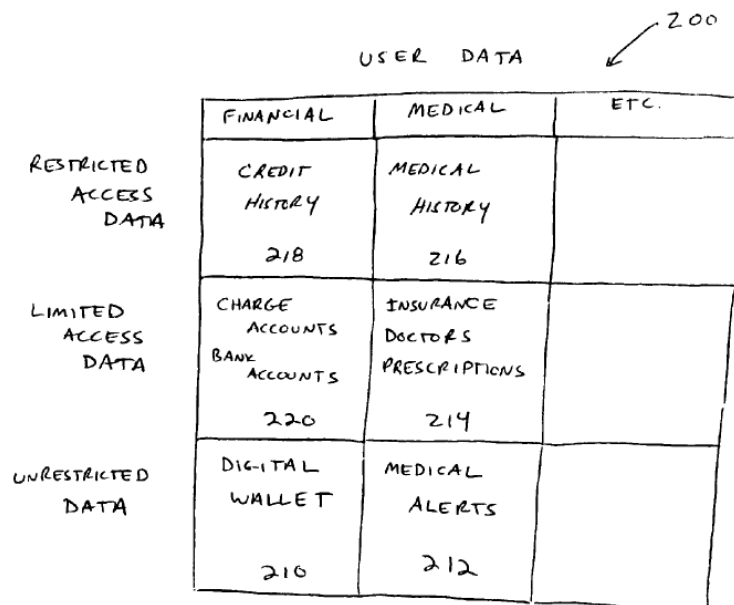


FIG. 3

In this example, a pharmacist might “have access to the user’s digital wallet 210, medical alerts 212, and insurance and prescription information 214,” but not “to the user’s medical history 216.” EX1005, 5:9-15.

Bossemeyer says nothing about how pieces of information originally get to the central database server or how they get stored within the different partitioned areas. Bossemeyer merely mentions when this process occurs: “the user data

becomes populated when the user subscribes as part of the smart card activation process. Additional data is created as the user and the merchants interact with the system.” EX1005, 5:28-31.

D. Glick

Glick’s focus isn’t smart cards; it is protecting copyright-protected media from unauthorized copying and distribution. Glick’s title is “System and Method for Using Location Identity to Control Access to Digital Information.” EX1006. It focuses on using location information to prevent unauthorized access to and copying of copyright-protected content, such as text, data, software, music, video, graphics. EX1006, 3:22-23, 5:21-24. For each piece of copyrighted content, Glick defines a specific geographic location within which that copyrighted content may be viewed/listened to. EX1006, 3:27-30. Glick works by identifying the location of an appliance/device seeking access to the content, and allowing that access when the appliance is on the list of approved locations. EX1006, 3:43-60.

E. Carmichael

Carmichael is titled “Multi Application Smartcard with Currency Exchange, Location, Tracking and Personal Identification Capabilities.” Carmichael is another smart card reference, this one adding various functionalities to the card such as currency conversion and geolocation. EX1007, 4:1-64. The geolocation feature is

provided to help find the card if lost or stolen, and to generate travel logs for the card holder. EX1007, 4:6-12.

III. Governing Law

Petitioner has the burden of proof. *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016). In petitions seeking obviousness-type invalidation under 35 U.S.C. § 103, that burden begins with establishing that the reference is analogous to the challenged patent. *Sanofi-Aventis Deutschland GmbH v. Myland Pharmaceuticals Inc.*, 66 F.4th 1373, 1380 (Fed. Cir. 2023). Claims cannot be invalidated under 35 U.S.C. § 103 based on non-analogous art. *See e.g., Innovention Toys, LLC v. MGA Entm't, Inc.*, 637 F.3d 1314, 1321 (Fed. Cir. 2011).

The Petition must identify with particularity all evidence and arguments supporting the challenge to each claim. 35 U.S.C. § 312(a)(3). The Petition “must specify where each element of the claim is found” in the references relied upon. 37 C.F.R. § 42.104(b)(4). To show obviousness, merely showing that the prior art includes references covering each separate limitation in a challenged claim is not enough; the Petitioner must articulate a reason why a person of ordinary skill in the art would have combined or modified the references. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398 (2007).

IV. The Bossemeyer Reference Is Not Analogous Art to the '825 Patent.

Both of Petitioner's grounds for challenging the '825 Patent's Claim 81 depend on Bossemeyer as the primary reference. Ground 1 depends on Bossemeyer (with modifications) alone. Ground 2 depends on Bossemeyer in view of Glick.

To prove Bossemeyer is analogous, Petitioner bears the burden of establishing that it either is from the same field of endeavor, or reasonably pertinent to the particular problem faced by the inventors of the '825 Patent. *In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004).

Because the Petition fails to establish that Bossemeyer is from the same field of endeavor as the '825 Patent or reasonably pertinent to the problems the '825 Patent addresses, both Grounds fail.

A. Bossemeyer and the '825 Patent concern different fields of endeavor.

Petitioner briefly seeks to establish Bossemeyer is analogous by characterizing the field of endeavor as “securing security-sensitive information,” and then citing two Bossemeyer snippets. Pet., 72-73. There are at least two problems with its approach.

First is its characterization of the field—which is so broad as to encompass almost anything—when the law demands a much narrower definition. In *Wang Laboratories, Inc. v. Toshiba Corp.*, the challenged patent and prior art related to

different kinds of computer memory. 993 F.2d 858, 864 (Fed. Cir. 1993). The Federal Circuit panel deemed even that relatively narrow characterization of the field as “computer memory” too broad because of differences between the patent’s “compact modular memories” and the alleged prior art’s “memory circuits in which modules of varying sizes may be added or replaced.” *Id.* Likewise, the “petroleum industry” was too broad a formulation in *In re Clay*, 966 F.2d 656, 659 (Fed. Cir. 1992). And in *Neato LLC v. Rocky Mountain Traders*, the court warned against defining the field of endeavor broadly where both the patent in question and the prior art related to labeling audio recording products. 138 F. Supp. 2d 245, 253 (D. Ct. 2001). The court held that they were from different fields because the patent concerned a manually-operated single-compact-disc labeler, whereas the prior art concerned an automated labeling system for the audio tapes. *Id.*

Petitioner’s “securing security-sensitive information” field of endeavor would be almost limitless, encompassing, for example, encryption, dual-factor authentication, malware tools, firewall systems, tokenization (tap to pay) of financial information, blockchain, face ID, captcha, fingerprint scanners on computers, computer database technologies, cloud technologies, anti-surveillance technologies, etc. EX2004, ¶72. A characterization that broad does not qualify as an acceptable field of endeavor under the law.

The second issue is that the two Bossemeyer snippets Petitioner cites on page 73 do not suggest that it even falls within that expansive field:

This invention relates to smart card applications and, more particularly, to a network arrangement to provide access to an architecture that supports a variety of advanced smart card applications. EX1005, 1:8-11.

[T]he present invention describes a network arrangement which is readily accessible from different types of smart card terminals supporting various smart card applications. EX1005, 1:44-47.

These two snippets are all Petitioner presents on field of endeavor, and neither even supports its legally improper definition of that field.

How the two patents describe their fields from the beginning reveals how far afield from each other they are:

Start of Bossemeyer	Start of '825 Patent
“Technical Field This invention relates to smart card applications and, more particularly, to a network arrangement to provide access to an architecture that supports a variety of advanced smart card applications.” EX1005, 1:6-11.	“The present invention relates to a data security system and method and, more specifically, to a process, program and system which operates to secure files and data objects in portable computing devices. The invention extracts, disperses, via a controlled release of data segments to storage locations, and permits reconstruction utilizing security protocols to provide a security system for data..” EX1001, 1:23-29

The applications these patents support have nothing in common (smart card transactions versus email and browsing), and their technical focuses have nothing in common (providing “access to an architecture” for smart cards versus filter[ing], extract[ing], dispers[ing], ... permit[ting] reconstruction ... [of] data.”). EX2004, ¶¶15, 69-72. It is common sense that their fields of endeavor are different. *See Airbus S.A.S. v. Firepass Corp.*, 941 F.3d 1374, 1381 (Fed. Cir. 2019) (common sense and reality precluded a finding that the alleged art was from the same field of endeavor as the challenged patent).

B. Bossemeyer is not pertinent to the problems faced by the inventors of the '825 Patent.

Not surprisingly, based on the discussion above, Bossemeyer has no pertinence to the problems the inventors of the '825 Patent faced. To be “reasonably pertinent,” a reference must “logically would have commended itself” to an inventor’s attention in considering his problem. *In re Icon Health and Fitness, Inc.*, 496 F.3d 1374, 1379- 80 (Fed. Cir. 2007) (*citing In re Clay*, 966 F.2d at 658-59). *See also* MPEP § 2141.01(a). In *Tinnus Enterprises, LLC v. Telebrands Corp.*, technology for filling an endoscopic balloon was “far removed” from the problem of how to rapidly fill multiple balloons with fluid. 846 F.3d 1190, 1207 (Fed. Cir. 2017). And in *Neato LLC*, the court pointed to the different equipment used in the prior art compared to that used in the patent at issue, and the different purposes for

the use of that equipment, as indicating the former was not reasonably pertinent. 138 F.Supp.2d at 254-55.

That Bossemeyer and the '825 Patent employ different equipment is clear. Bossemeyer employs smart cards with stored data pointers, smart card readers, and a single central database server. EX1005, Figs.1-3, 2:9-27. The '825 Patent employs hardware for processing, filtering, and distributing data, often across multiple computers/locations, with a mapping functionality to later find the data pieces. EX1001, Figs. 1A, 1B, 2, 6, 8:10-28.

They also use their equipment for entirely different purposes to solve entirely different problems, as the Petition unintentionally demonstrates. On page 73, the Petition cites and misinterprets the following from the '825 Patent: “It is an object of the present invention to provide a data security system, an information processing system and a method for securely storing data and rebuilding that data in the presence of an adequate security clearance.” EX1001, 6:55-58. Although Petitioner tries to suggest otherwise, the problem the '825 sought to solve was providing a very specific type of data security system: one that implements a specific “information

processing system and a method” that involves “securely storing data” and “rebuilding that data.”¹

The Petitioner’s other cite² from the ’825 Patent in this section reinforces the specific nature of the problem the inventors were trying to solve: “It is a further object of the present invention to secure files and data objects in portable computing devices.” EX1001, 7:64-65. The inventors were seeking to solve the problem of creating such a system in the face of hacking attacks. EX1001, 11:9-17, 24:7-19. Bossemeyer never envisions hacking attacks, and any hacker that accessed

¹ The interpretation of this quote is consistent with the nearly identical language that appears elsewhere in the specification, “The present invention relates to a data security system and method and, more specifically, to a process, program and system which ... extracts, disperses, via a controlled release of data segments to storage locations, and permits reconstruction utilizing security protocols to provide a security system for data.” EX1001, 1:23-29.

² The Petition at page 73 again cites the Zadok declaration, EX1003, ¶¶269, 300, but that portion again contains the same citations as the Petition itself with no additional explanation.

Bossemeyer’s central database server would have access to everything in it. EX2004, ¶70.

Bossemeyer, on the other hand, doesn’t seek to provide “an information processing system,” let alone one that “parses” and “distributes” data. As noted already, Bossemeyer never discusses the original receipt, processing, and storage of data. It is simply concerns getting access to information stored in partitioned memory. *See supra* II.C.; EX2004, ¶28.

Nor does Bossemeyer address “rebuilding” or “reconstructing” data. In fact, Dr. Zadok’s declaration concedes that Bossemeyer does not disclose reconstruction: “Although Bossemeyer does not explicitly state that the information, once reaching the terminal, is merged/reconstructed...” EX1003, ¶216. Bossemeyer merely sends data stored in different partitioned areas of memory to an authorized merchant for use. EX1005, 4:59-65. We address this issue in more detail in the discussion below of Bossemeyer’s failure to satisfy the “reconstruction” claim element.

The only evidence from Bossemeyer that Petitioner cites to establish pertinence is a single snippet: “The central database server 10 is a centralized partitioned database server which partitions information both in terms of the smart card application as well as the accessibility of the information. The information is stored by category ... as well as level of security.” EX1005, 2:17-22. But this quote

does not demonstrate or even suggest trying to address problems of “processing,” “parsing,” “dispersing,” or “reconstructing” as the ’825 Patent does.

Bossemeyer, therefore, does not provide any solutions, let alone solutions that would “logically commend themselves,” to the ’825 Patent’s inventors working on these specific problems.

C. Bossemeyer is not analogous to the ’825 Patent.

The Petition failed to carry its burden of proving either that Bossemeyer is in the same field of endeavor as, or reasonably pertinent to the problems of, the ’825 Patent. Facing the mountain of evidence that it is not, the fact that the Petition marshalled, in total, just three short snippets from Bossemeyer highlights the weakness of Petitioner’s case. Because Bossemeyer is not analogous, it cannot support Petitioner’s obviousness challenges to Claim 81 of the ’825 Patent, and those challenges by necessity must fail.

V. Bossemeyer and Glick Each Fail to Teach Claimed *Extracted Data* and the *Reconstruction* Method Step, Warranting Denial on both of Petitioner’s Grounds for Challenging the Claims.

The only challenged claim of the ’825 Patent is Claim 81, which requires extracted data and a reconstruction step:

81. A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective extract stores

with security access controls thereat, *said security sensitive words, characters, data objects or icons extracted from said data to obtain extracted data* and remainder data which extracted data is stored in respective extract stores corresponding to a respective security level of said extract stores, said computer system having at least one portable computing device locatable with current location data, comprising:

determining when said portable computing device is within a predetermined region based upon said current location data;

permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data only in the presence of a predetermined security clearance access control corresponding to said respective security level and only when said portable computing device is not beyond said predetermined region.

The Petition relies only on Bossemeyer for the “extracted” element in both Grounds 1 and 2. Because Bossemeyer lacks that element, both grounds fail for that reason. For both Grounds 1 and 2, the Petition relies on Bossemeyer and Glick for the “reconstruction” element. Both references lack that element, which constitutes a separate reason for denying institution based on either ground.

A. Bossemeyer does not disclose “said security sensitive words, characters, data objects or icons extracted from said data to obtain extracted data.”

The '825 Patent describes the extraction process as occurring at an initial processing step that removed or filters out security-sensitive data from other data prior to distributed storage. *See e.g.*, EX1001, 22:46-48, 7:52-54, 21:54-66, 23:9-11.

To understand why Bossemeyer lacks this element, it’s important to begin with a review of how Bossemeyer works. In Bossemeyer, a smart card reader/terminal connects through a network central office of a standard public-switched telephone network to a central database server accessible to different merchants. EX1005, 2:4-12. Figure 1 shows this setup:

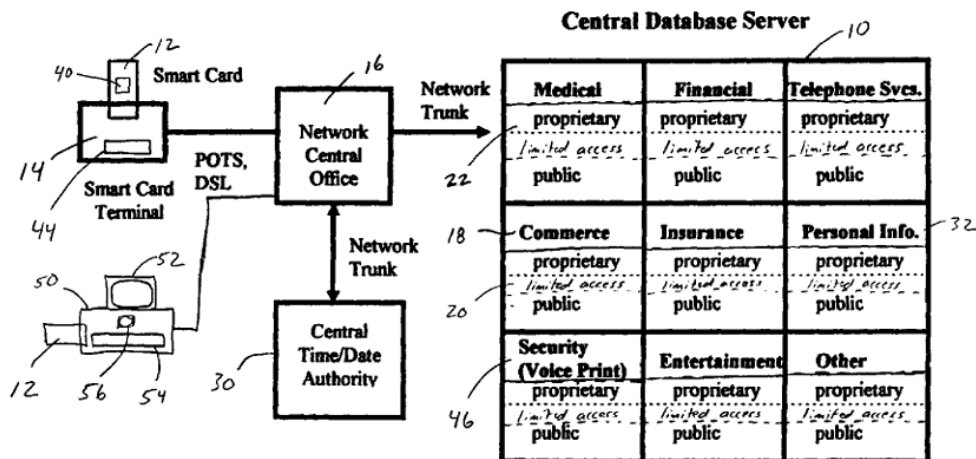


Figure 1

That central database server’s memory is “partitioned,” with different types of information stored in separate areas. EX1005, Fig. 1, 2:13-36. For each category (Medical, Financial, etc.), there are areas for storing information of varying levels

of sensitivity: “proprietary” (highest), “limited access” (some sensitivity), and “public” (no sensitivity). EX1005, 2:22-36. Bossemeyer’s Figure 3 shows varied levels of privacy related to different types of data:

200
↙

USER DATA

	FINANCIAL	MEDICAL	ETC.
RESTRICTED ACCESS DATA	CREDIT HISTORY 218	MEDICAL HISTORY 216	
LIMITED ACCESS DATA	CHARGE ACCOUNTS BANK ACCOUNTS 220	INSURANCE DOCTORS PRESCRIPTIONS 214	
UNRESTRICTED DATA	DIGITAL WALLET 210	MEDICAL ALERTS 212	

FIG. 3

Bossemeyer never addresses how these different types of information end up in different partitioned areas of memory in the first place, and Petitioner never tries to argue that it does. EX2004, ¶28. Bossemeyer simply starts with pieces of data already stored in those different locations separated from each other. That’s a fundamental problem for Petitioner’s argument about “extraction.”

Merchants access those partitioned areas of memory when the user inserts a smart card in the merchant’s card reader, enters a PIN, and selects the desired application/transaction type (medical, financial, etc.). EX1005, 3:52-53. After

verifying authorization, the reader reads the pointers stored on the card. EX1005, 3:63-65. Those pointers point to different areas of the partitioned memory, providing access to the pieces of information stored in them. EX1005, 3:63-66. The central server then sends the requested piece of information back to the merchant's smart-card reader/terminal. EX1005, 4:3-6.

Petitioner begins its effort to establish extraction of data on page 35 with a conclusory statement supported by three paragraphs from its expert's declaration. But each of those three paragraphs is merely a short, conclusory, completely unsupported statement that the element exists in the prior art. *See* EX1003, ¶¶159, 171, 274. Such *ipse dixit* statements are not evidence.

Only then does Petitioner start citing to evidence from Bossemeyer, usually accompanied with an additional citation to its expert report. But most of these statements in the expert report are nearly word-for-word copies of Petitioner's brief. *Compare, for example*, EX1003, ¶¶160-170 *with* Pet., 35-39. As such, they are entitled to very little weight. *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 (August 24, 2022) (expert declarations that are exact restatements of the petition's arguments are disregarded). Our response will focus on the evidence in the references themselves unless the expert declaration departs from this approach and warrants special mention.

Petitioner's argument for extraction is based on it misconstruing Bossemeyer's use of the word "partition," equating it first to "separating" and then to "extracting." The Petition starts with a quote from Bossemeyer about how the "central database server 10 is a centralized partitioned database server which partitions information both in terms of the smart card application as well as the accessibility of the information. The information is stored by category (medical, financial, etc.) as well as level of security (unrestricted, or public limited access, restricted)." EX1005, 2:17-23. Petitioner seeks to extrapolate from this statement that "partition" refers to a data processing step of removing different pieces of data from a larger whole prior to storage. But that is not what "partitioning" refers to, either in the art or in Bossemeyer itself. EX2004, ¶¶29-33.

In the art, a "partition" is just a logical separation of different areas of *memory*, and the act of partitioning refers to separating *memory* into logically separate areas, not extracting pieces of security sensitive data from a larger whole. EX2004, ¶29. Petitioner's own evidence supports this reading. Petitioner's expert, Dr. Zadok, cited a Microsoft technical dictionary for its definition of "parse," a term that does not appear in Bossemeyer, while ignoring its definition of "partition" which does appear on the very same page. EX1003, ¶168; EX2004, ¶29. That latter definition is a "logically distinct portion of memory or a storage device that functions as though it

were a physically separate unit.” EX1023, 25. That same dictionary defines “disk partition” in a similar manner, as “[a] logical compartment on a physical disk drive. A single disk might have two or more logical disk partitions....” EX1023, 6; EX2004, ¶29. And when used as a verb, partition means dividing memory into sections prior to use, not extracting pieces of data from a larger whole: “Partition: Before a hard disk can be used for the first time, it must be partitioned and then formatted. Partitioning is a software function that involves dividing the storage space into usable sections, with each section assigned a letter as though it were a separate drive.” EX2006; EX2004, ¶31. Dr. Easttom’s declaration cites additional contemporary sources saying the same thing. EX2004, ¶29.

Bossemeyer uses “partition” the same way, as separated areas of memory, not extracting some data from a larger set. *See, e.g.*, EX1005, 2:40 (“partitions in the database”); 2:59-60 (“partitions of the central database server”); 3:58-60 (“The desired application is then selected which relates to a memory partition of the central database server”); 3:65-66 (“access to the relevant partitioned memory portions of the central database server”); 4:17-18 (“pointers to relevant data within the partitioned central database server”); 4:43-44 (“FIG. 3 shows a schematic diagram of the partitioned server database”). *See also* EX2004, ¶¶30-32. Even in instances referring to partitioning of information, Bossemeyer is clear that it merely means

storing in these partitioned areas, which the partitions keep separate, not some processing step done on input data:

- “[A] merchant may require access to a user’s credit information to determine whether to accept the user’s credit for a particular dollar amount. This information *may be partitioned in the limited access region* 20 of commercial transaction applications 18.” EX1005, 2:23-27 (emphasis added).
- “Private or proprietary information *is partitioned such that the owner of the information has control over how the information is transferred and used [by limiting access to those partitioned areas].*” EX1005, 2:28-30 (emphasis added).

See also EX2004, ¶34.

So “partitioning” does not carry the meaning Petitioner wants, and Petitioner’s other evidence from Bossemeyer is equally unhelpful. Its second Bossemeyer quote on page 39 merely refers to what kinds of information the central database stores. EX1005, 2:40-47; EX2004, ¶27. Petitioner then presents Bossemeyer’s Figure 1, but it merely illustrates what kinds of information the central database stores graphically. EX2004, ¶27. Petitioner’s quotation of EX1005, 2:28-33 is next, replicated in the second bullet above, and it supports Respondent’s read of “partitioning.” EX2004, ¶34. Petitioner then presents Bossemeyer’s Figure 3, again merely illustrating what kinds of information the central database stores graphically. EX2004, ¶27. Petitioner

concludes by quoting Bossemeyer’s description of what kinds of information are stored in the different partitioned areas in Figure 3. EX1005, 5:9-15. None of these pieces of evidence discloses, teaches, or suggests extraction of security sensitive data from a larger whole. EX2004, ¶¶27-35.

It then argues that, “[t]o the extent that ... Bossemeyer does not explicitly disclose ‘extracted data,’ ... a POSITA would have understood that Bossemeyer’s method can parse the received information into private and non-private elements.” Pet., 38. But its evidence for that statement doesn’t come from Bossemeyer. Instead, the Petitioner cites to a reference that isn’t involved with either Ground 1 or Ground 2 or this petition in any way, U.S. Publication No. 2004/0148290 (“Merenda,” EX1008). Petitioner has cited to Merenda in other petitions. *See* IPR2023-00968, IPR2023-00969, IPR2023-00970, IPR2023-00971, and IPR2023-00972. In those petitions as well, it erroneously cites to Merenda to support the same statement about Bossemeyer. But here, the error stands out because Merenda isn’t involved in this petition. And the petition’s discussion about the meaning of “parse” in unrelated art is particularly irrelevant, because Bossemeyer never uses “parse.”

Petitioner also cites Dr. Zadok’s declaration that is nearly a word-for-word copy of the paragraph in the Petition. *Compare* Pet., 38 *with* EX1003, ¶168. None of this constitutes evidence. What follows at the bottom of page 38 is a paragraph

making assertions about a theoretical “medical data file” that Bossemeyer never mentions. EX2004, ¶41. Therefore, Petitioner lacks any evidence whatsoever for its argument.

Petitioner appears to be arguing inherency, in that extraction is inherent in getting data into a partitioned memory. But this absence of evidence cannot begin to satisfy inherency’s rigid legal standard. To establish inherency, the extrinsic evidence “must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill.” *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1268 (Fed. Cir. 1991). Inherency cannot be “established by probabilities or possibilities. The mere fact that a certain thing *may* result from a given set of circumstances is not sufficient.” *Id.* at 1269 (quoting *In re Oelrich*, 666 F.2d 578, 581 (C.C.P.A. 1981)). A party must “meet a high standard in order to rely on inherency to establish the existence of a claim limitation in the prior art in an obviousness analysis—the limitation at issue necessarily must be present, or the natural result of the combination of elements explicitly disclosed by the prior art.” *PAR Pharm., Inc. v. TWI Pharms., Inc.*, 773 F.3d 1186, 1195–96 (Fed. Cir. 2014).

An extraction step is unnecessary for storing data in a partitioned memory. As the definition of “partition” above shows, hard disks always must be partitioned

before use. EX1023, 6; EX2004, ¶31. If Petitioner were right, then extraction would always have to occur before storing data on a hard drive, which is obviously not the case. EX2004, ¶40. Data is often loaded into partitioned memory without a prior extraction step. EX2004, ¶40.

Because Petitioner’s Grounds 1 and 2 rely exclusively on Bossemeyer for the “extracted data” limitation in the challenged claim, both Grounds fails due to Bossemeyer’s lack of extraction.

B. Bossemeyer and Glick do not disclose “permitting full or partial reconstruction of said data via said extracted data.”

Petitioner’s Grounds 1 and 2 rely on the same two references, Bossemeyer and Glick, to establish the claimed “reconstruction.” Its argument focuses on Bossemeyer but does add once sentence about Glick. The absence of any teaching of “reconstruction” in these references, however, serves as an independent reason for denying both grounds of Petitioner’s challenge.

i. Bossemeyer

Petitioner’s own expert, Dr. Zadok, concedes that Bossemeyer does not “reconstruct ... said data,” admitting that “[a]lthough Bossemeyer does not explicitly state that the information, once reaching the terminal, is merged/reconstructed...” EX1003, ¶216.

This admission puts Petitioner in a bind. It must either show that reconstruction is inherent or would have been obvious to add to a person of skill in the art. But Petitioner never reveals which route it's attempting. To some degree, Petitioner again appears to be arguing for inherency: "As Dr. Zadok explains, when a merchant or bank initiates a financial transaction, partial or full reconstruction of user information enables the processing of the financial transaction, otherwise the transaction would fail.... [A] POSITA would understand that said data is merged/reconstructed in that terminal...." Pet., 54. This reads like inherency but lacks anything approaching what the law would require: its necessary presence, not a mere possibility or probability.

Petitioner also faces hurdles if relying on common-sense obviousness to add the missing reconstruction step. The Federal Circuit restricts the circumstances in which this approach may be used: to fill in a *missing* limitation only when the limitation in question is unusually simple or does not play a major role in the subject matter claimed, when the technology is particularly straightforward, and never as a wholesale substitute for reasoned analysis and evidentiary support. *DSS Tech. Mgmt., Inc. v. Apple Inc.*, 885 F.3d 1367, 1374 (Fed. Cir. 2018). But Petitioner presents no evidence or even argument that data reconstruction applied to Bossemeyer would be unusually simple, that reconstruction does not play a major

role in the claim, or that the technology is unusually straightforward. *See DSS Tech. Mgmt.*, 885 F.3d at 1375.

There are strict requirements on the specificity and clarity demanded in IPR petitions. 35 U.S.C. § 312(a)(3). Petitioner’s silence on whether it is relying on inherency or obviousness, and its complete failure to present evidence or argument meeting either standard should, by itself, warrant denial of the Ground 1 challenge.

There, of course, remain serious flaws with the argument Petitioner does make. Petitioner’s brief begins with three quotes from Bossemeyer, EX1005, 2:38-47, 3:63-4:6, and 4:59-65. Pet., 53-54. Those quotes merely describe the merchant getting “access” to, “viewing,” or being “supplied” information stored on the central database server. None are the same as reconstruction. EX2004, ¶¶43-45.

At this point, the Petitioner extrapolates that some kind of data merger would (inherently or obviously?) occur, even though Bossemeyer says nothing about such a step. Petitioner hypothesizes about a “merchant or bank initiat[ing] a financial transaction” and assumes that the data from different partitioned areas of memory would be merged because if it wasn’t, “the transaction would fail.” Pet., 54. Its only support is ¶¶215-217 of Dr. Zadok’s declaration.

There are numerous problems with this extrapolation, in addition to the fact that no effort is made to comply with the legal requirements of inherency or

obviousness. One is the complete absence of evidence of Dr. Zadok's qualification to state such an opinion. Petitioner presents him simply as an expert in "the relevant art" of "computer science, computer engineering, electrical engineering, or equivalent" and "data storage systems and data security," and nothing in his background or publications suggests experience, much less expertise, in smart cards or electronic financial transactions. Pet., 11, 78.

A second problem is the obvious inaccuracies in what Dr. Zadok wrote on this subject. He opines, without support, that the merchant would receive from the server "public information such as a customer's name" and "proprietary or limited access information such as ... account PIN/numbers." EX1003, ¶215. But neither of these pieces of information is on the server. The customer's name would either be embossed on the card or stored on the card itself. EX1005, 3:31-35 ("The face of the smart card 12 may have information printed or embossed on it such as a photograph, in addition to the name of the card holder. The same information can alternatively or additionally be provided in the memory contained within the card 12."). And the customer, not the central database server, provides the PIN: "the smart card 12 is inserted into the smart card terminal 14 and a personal identification number (PIN) is optionally entered using an input device." EX1005, 3:52-54. It would not be

necessary, therefore, to pull these pieces of information from the server and merge them together to execute a transaction as Dr. Zadok opines. EX2004, ¶¶47-51.

A third problem is that Dr. Zadok's conclusion about need for merging to execute a transaction is simply wrong. In contrast to Dr. Zadok, Dr. Easttom, is qualified to opine on electronic financial transactions. He worked as a senior software engineer developing financial applications for banks in the late 1990s, very close to Bossemeyer's filing date. EX2004, ¶47. His declaration notes that each piece of data could be returned and used separately for a separate part of the transaction process without them ever being merged. EX2004, ¶¶47, 51. Data operations often use pieces of information from different sources without merging or combining them. EX2004, ¶51.

Dr. Easttom also explains that there are reasons not to merge the information. EX2004, ¶48. For example, Bossemeyer's Figure 3 financial data includes restricted data such as credit history (218) and charge accounts (220). EX2004, ¶48. Processing a payment only requires a sufficient amount available; the customer's credit history is not relevant and including it could prove problematic for numerous reasons. EX2004, ¶48. Merging the data shown in Figure 3 would mean merging data that Bossemeyer identifies as *restricted*, *limited*, or *unrestricted* (such as bank account numbers, credit history, and a digital wallet) into the same dataset. EX2004,

¶48. Thus, merging them would reduce the security of that data. EX2004, ¶48. Technical reasons also would have prevented merging these pieces of information, due to the likely differing file structure of these different pieces of information, as Dr. Easttom details in his declaration. EX2004, ¶¶49-51.

Fourth, even if Petitioner could establish some kind of merging of data, it would not establish claimed “reconstruction of said data.” The language of the challenged claim requires that the “said data” being reconstructed is the same as the “data” that was processed in an extraction process, as Claim 81, for example, shows:

81. A method of securing *data* having one or more security sensitive words, characters, data objects or icons ... said security sensitive words, characters, data objects or icons *extracted from said data to obtain extracted data* and remainder data...

...

permitting full or partial reconstruction of *said data via said extracted data* from said extract stores...

See also EX1001, 29:14-18, 32:45-49. To establish “reconstruction said data,” therefore, Petitioner would need to prove that its hypothetical merged data is in the same form as what originally existed before any extraction step and before storage in the partitioned memory. And because, as already shown, Bossemeyer lacks

“extraction,” it cannot have “reconstruction” based on the surrounding claim language. EX2004, ¶42.

There is no evidence that the different pieces of information stored in the partitioned areas of the central database server’s memory were ever part of a single whole. Bossemeyer says nothing about where the pieces of information come from or their form before storage in the different areas of memory. EX2004, ¶¶28, 52. As a result, not only does Petitioner make no effort to establish that its proposed merged data would be the same as the data in its original form, but it would be impossible to do so. EX2004, ¶52. Such a merger would more likely be the initial construction of a novel dataset with multiple pieces of information, not a “reconstruction” as the claim requires. EX2004, ¶52.

Petitioner finishes with Bossemeyer’s Figure 3 again, showing storage of different kinds of medical information in different partitioned areas, some of which a pharmacist can access. Pet., 55-56. A merchant accessing information in different partitioned areas, however, says nothing about what the merchant does with those different pieces of information, whether they are combined, or what form they would take if combined. EX2004, ¶53.

Petitioner then turns to Glick.

ii. Glick

Petitioner’s argument for “reconstruction” in Glick is a single sentence: “Glick also discloses an appliance that reconstructs requested information.” Pet., 56.

Petitioner’s first problem is the claim language. Claim 81 requires “reconstruction of said data via said extracted data,” meaning that the original data is reconstructed from what was previously extracted from it. EX1001, Cl. 81; EX2004, ¶59. But the Petitioner never argues that Glick includes an “extraction” step. EX2004, ¶59; *See* Pet., 35-39. Without such a step that extracts data, Glick cannot disclose a “reconstruction” step “via said extracted data.” EX2004, ¶59.

Petitioner’s second problem is that its only evidence from Glick describes decryption, which is not “reconstruction.” EX1006, 4:4-8; EX2004, ¶¶60-63. Glick decrypts encrypted text, software, music, video, graphics files. EX1006, 5:22-24. Petitioner points to nothing in Glick suggesting that this process involves combining data previously “extracted” from these items, and nothing in Glick does so. EX2004, ¶60.

Moreover, nothing about the meaning of “decryption” in the art suggests it either. “Decryption” entails “decoding - that is, translating information from an unreadable or secret format into a form in which it can be used.” EX2041, Barron’s Dictionary of Computer Terms; *see also* EX2006, Prentice Hall’s Dictionary of

Computing (defining “decryption” as “[t]he process of decoding information so that it can be read and manipulated”); EX2004, ¶¶61-62. And the ’825 Patent itself makes clear that “decryption” is separate and apart from reconstruction:

- Of course, every use of encryption requires decryption of the data prior to reconstruction. EX1001, 32:25-27.
- Optionally, the decryption could occur at the recipient’s e-mail device somewhat prior to the reconstitution of the e-mail plaintext document 100 during step 634. EX1001, 55:47-49.

EX2004, ¶63.

The only other thing Petitioner cites to support its single sentence of argument is ¶220 of Dr. Zadok’s declaration: “Glick discloses an appliance that reconstructs requested information in an analogous manner to Bossemeyer.” This statement lacks any support from Glick other than Dr. Zadok’s cite to the same statement about decryption discussed above. EX1003, ¶220 (citing EX1006, 4:4-8). And the statement is odd, given Dr. Zadok concession in his Bossemeyer discussion that “Bossemeyer does not explicitly state that the information, once reaching the terminal, is merged/reconstructed...” EX1003, ¶216. Regardless, none of it establishes that Glick’s decryption satisfies the claimed “reconstruction.”

Because neither Glick nor Bossemeyer disclose reconstruction, both its Ground 1 and 2 challenges fail for this independent reason.

VI. Petitioner's Grounds 1 and 2 Lack the Necessary Motivation to Combine Bossemeyer and Glick.

Both Petitioner's Grounds 1 and 2 depend on combining Glick with Bossemeyer to meet Claim 81's "portable computing device locatable with current location data" and "computing device is within a predetermined region" elements. Pet., 45-47, 51-52. To do so, Petitioner needed to establish first that a POSITA working with Bossemeyer would have looked to Glick, which requires that the latter be analogous art to former. *In re: Natural Alternatives, LLC*, 659 Fed. Appx. 608, 610 (2016) (denying motivation to combine references in different fields pertinent to different problems). Petitioner also needed to establish that the POSITA would have had the skill to combine the two references. *KSR*, 550 U.S. at 417; *Dropworks, Inc. v. Bio-Rad Laboratories, Inc.*, IPR2021-00212, Paper 7 (P.T.A.B. Jun. 1, 2021).

Glick is not analogous art to Bossemeyer. The two are from dramatically different fields of endeavor. EX2004, ¶¶69-71. Bossemeyer concerns smart card technology facilitating in-person transactions at stores and offices. EX1005, 2:22-26; EX2004, ¶¶15, 70. The technologies involved relate to specialized storage on a card, specialized card readers, and methods for communicating with remote repositories. EX2004, ¶¶15, 70. In Bossemeyer's case, that process involves communicating with a remote, dedicated server storing different types of information in different partitioned areas. EX1005, Fig. 1, 2:4-12, 3:53-58. The

amount of information transferred between the two, however, is extremely limited, nothing like the communication of media files. EX1005, 4:50-54; 2:58-63; EX2004, ¶15.

Glick has nothing whatsoever to do with smart cards. It focuses on media sharing over the Internet, preventing unauthorized copying of copyright-protected content. EX1006, 3:21-23; EX2004, ¶17, 71. There are no cards or readers. Instead, Glick involves “Digital Rights Management” (DRM) systems accessing and transferring media files. EX2004, ¶17, 71; EX1006, 1:54-2:4, 2:33-53. These media files are much larger than the information being transferred in Bossemeyer. Glick controls distribution of and access to media using location information and location-based restrictions. EX1006, 1:7-12; 3:27-32; EX2004, ¶17, 71.

The PTO considered these references to be dramatically different, which their divergent classification codes demonstrate. Bossemeyer’s primary PTO classification code is class 713, “Electrical Computers and Digital Processing Systems: Support,” subclass 201, “for computer network security in general or in combination with nominal cryptography.”³ Glick is in an entirely different class, 380,

³<https://web.archive.org/web/20050422055224/http://www.uspto.gov/web/patents/classification/uspc713/defs713.htm>, EX2010

“Cryptography,” subclass 258 for “position dependent or authenticating,” which the USPTO describes as “subject matter wherein cryptographic protection is based upon or validates the spatial location of a transmitter or receiver.”⁴

Nor is Glick reasonably pertinent to the problems of Bossemeyer, particularly in comparison to guidance the courts provide. *See Tinnus*, 846 F.3d at 1207 (filling endoscopic balloon “far removed” from filling multiple balloons); *Wang Labs*, 993 F.2d at 864 (different types of computer memory not pertinent to each other); *Neato LLC*, 138 F.Supp.2d at 254-55 (different equipment, different purposes for that equipment not reasonably pertinent). They employ different equipment for different purposes: smart cards, readers, communication protocols for communicating limited data to facilitate in person transactions, centralized storage on a server (EX2004, ¶¶ 15, 70, 72) versus appliances for viewing/listening to the media file, DRM systems, communication of media files across the Internet, encryption and geolocation technology all for preventing copyright infringement. EX2004, ¶¶ 17, 71, 72. Specifically, Bossemeyer seeks to improve smart card operation during in-person transactions through “integration of [the cards with] a centralized server architecture

⁴<https://web.archive.org/web/20050205203531/http://www.uspto.gov/web/patents/classification/uspc380/defs380.htm>, EX2011.

or a network arrangement for multiple smart card applications.” EX1005, 1:39-43. Glick uses location information and encryption to prevent “widespread copyright piracy” and the illicit use of online file sharing systems like Napster. EX1006, 1:8-12, 2:11-32; EX2004, ¶17, 71.

It is hard to imagine, let alone “reasonably likely,” that one working in the field of one of these references would have looked to the other field for solutions, picking the other reference “out of the sea of prior art” for combination. *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1337 (Fed. Cir. 2016).

It also is unlikely that the POSITA would have had the skill to combine these two references. *See KSR*, 550 U.S. at 417 (combinations cannot be obvious if beyond a POSITA’s technical skill). Petitioner’s person of ordinary skill in the art has “a bachelor’s degree in computer science, computer engineering, electrical engineering, or equivalent, and approximately two years of experience working in the field of data storage systems and data security.” Pet., 11. But smart cards are a specialized field (specialized storage on the card, specialized readers, etc.) that, at the time, was not widely used or adopted. EX2004, ¶¶23, 75. The Petition makes no effort to establish that its POSITA would have had training or experience with smart cards. EX2004, ¶¶75-76. Dr. Easttom, on the other hand, explains in his declaration that even those meeting Petitioner’s POSITA definition would not likely have had

any knowledge of or experience with smart cards. EX2004, ¶¶75-76. One graduating from Dr. Zadok's own university with a bachelor's degree in computer science, computer engineering, or electrical engineering would likely have no exposure to smart-card technology. EX2004, ¶76. Even the single graduate-level course that Dr. Easttom was able to find only addresses smart cards in passing, not in detail. EX2004, ¶76.

Petitioner had the burden of demonstrating a POSITA's ability to combine these two references and failed to do so. In fact, the only available evidence suggests that would not have been the case. That fact by itself warrants denial of Petitioner's proposed Grounds based on the combination.

Petitioner does offer five purported reasons to combine Glick with Bossemeyer in an effort to show what would have prompted a POSITA to make this combination of these two specific references in the "sea of prior art," as the law requires. *Pet.*, 63-68; *KSR*, 550 U.S. at 417; *Dropworks, Inc. v. Bio-Rad Laboratories, Inc.*, IPR2021-00212, Paper 7 (P.T.A.B. Jun. 1, 2021); *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1337 (Fed. Cir. 2016).

Notably, Petitioner offers the same five reasons for combining references in all six of the IPR petitions it has filed using Bossemeyer, regardless of the patent claim in question or the references involved. These purported reasons' plasticity is

evident from the way Petitioner seamlessly applies them whether the reference in question concerns:

- Smart cards (Bossemeyer and Carmichael in this petition, as well as IPR2023-00968, IPR2023-00969, IPR2023-00970, IPR2023-00971, IPR2023-00972)
- Copyright protection and DRM (Glick, this petition)
- Direct email marketing (Merenda, in petitions IPR2023-00968, IPR2023-00969, IPR2023-00970, IPR2023-00971, IPR2023-00972)

If these same five motivations are flexible enough to be used regardless of the prior art and elements being combined, they cannot satisfy the legal requirement for a motivation specific to the references in question in a particular case.

A POSITA would not have combined Glick with Bossemeyer, which is an independent reason to Petitioner's Grounds 1 and 2 challenges.

VII. The Board should deny institution on both grounds under *Fintiv*

On November 28, 2022, DigitalDoors, the Respondent, sued IBM, the Petitioner, for infringement of five patents, including the '825 Patent, in the Eastern District of Texas. *Apple Inc. v. Fintiv, Inc.*, established six factors for determining whether to deny a petition based on a pending district court case. IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential). The process begins with the first five

factors, and when they collectively weigh in favor of denial, the Board considers whether the merits are strong enough to overcome those factors and compel institution. *Commscope Technologies LLC v. Dali Wireless, Inc.*, IPR2022-01242, Paper 23 (PTAB Feb. 27, 2023) (precedential). That compelling-merits question requires a higher standard of proof, “highly likely to prevail,” than the statutory standard for institution, “reasonably likely to prevail.” USPTO Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (June 21, 2022) (EX1030, “Memorandum”); *Commscope*, IPR2022-01242, Paper 23.

All five initial factors here favor denial, and the petitioner is unlikely, not highly likely as required, to succeed on the merits. Denial is warranted based on *Fintiv* as well.

A. The district court is unlikely to grant a stay.

The Petitioner already filed one motion to stay the pending district court case, which that court denied. EX2007. That district court looks at specific criteria when deciding whether to grant stays for IPR proceedings, including whether review of all claims-in-suit has been instituted by the PTAB and whether the IPR petition and institution decision are timely – “where timely means a final written decision is expected in the ordinary course before the trial in this case would otherwise take

place.” *Vill. Green Techs., LLC v. Samsung Elecs. Co.*, No. 2:22-CV-00099-JRG, 2023 WL 416419, at *3 (E.D. Tex. Jan. 25, 2023).

There are 54 claims and seven patents in the district court proceeding. That court has made clear that it will not grant a stay unless the PTAB institutes IPR proceedings for every asserted claim. EX2007, 5.

If instituted, a final written decision would be expected in the ordinary course 3.5 months after the trial is scheduled to take place, which also makes a stay less likely under the timeliness factor considered by the district court.

Because a stay is unlikely, initiating an IPR here would result in two parallel proceedings, which would be inefficient and burdensome. This factor, therefore, strongly favors denial.

B. Trial is scheduled to finish over three months before the Final Written Decision deadline.

Trial in the pending district court case is scheduled to end about three and a half months before the deadline for a final written decision, so this factor also strongly favors denial. The Eastern District of Texas court scheduled trial to begin August 19, 2024, and patent trials in that venue typically take a week or less. Despite that fact, were the Board to institute an IPR based on this Petition, the Final Written Decision would not be due until December 2024, well after trial. Accordingly, instituting a trial would be an inefficient use of Board resources. *See Fintiv*,

IPR2020-00019, Paper 15 at 12-13 (denying institution where district court trial was scheduled two months before the final decision deadline); *NHK Spring Co., Ltd. v. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper 8 at 20 (PTAB Sept. 12, 2018) (precedential) (institution of IPR when the district court trial would resolve validity “would not be consistent with ‘an objective of the AIA...to provide an effective and efficient alternative to district court litigation’”).

The Petitioner ignores this scheduled trial date and instead cites out-of-date statistics to suggest trial would not take place before the Final Written Decision deadline. EX1030, 8 (“Parties may present evidence regarding *the most recent statistics* on median time-to-trial”) (emphasis added); Pet., 75 (relying on March 2022 statistics instead of March 2023 statistics). But even ignoring the actual scheduled trial date, the appropriate time-to-trial statistics still favor denial. The most recent of those statistics show an Eastern District of Texas median time-to-trial of just 19 months, which would be June 2024, even earlier than the actual trial date. EX1011. Petitioner’s purported reliance on older statistics is inappropriate.

C. Both parties have invested heavily in the district court proceedings.

The parties have expended substantial resources on the pending district court case in the eight months since this suit was filed. The Plaintiff/Respondent, DigitalDoors, prepared and served 1,067 pages of infringement contentions. IBM,

the Defendant/Petitioner, drafted and served 10,171 pages of invalidity contentions. DigitalDoors produced 4,152 documents, and IBM produced, and DigitalDoors reviewed 25,785 documents. There have already been multiple fact witness depositions and multiple rounds of discovery requests and responses. Despite the court's not having yet issued a *Markman* ruling, it still denied Petitioner's motion to stay the parallel proceeding because "much discovery had occurred." EX2007.

Much of this activity occurred in the six months between the filing of this case and the IPR petition. While not egregious, this delay does suggest that IBM did not file its Petition "promptly after becoming aware of the claims being asserted." *Fintiv*, Paper 11 at 11.

For these reasons, this factor is either neutral or slightly favors denial.

D. Petitioner has asserted the same three references in the district court proceedings.

Because the Petitioner asserts the Bossemeyer and Glick references separately and in combination both here and in its invalidity contentions in district court, institution of an IPR risks duplication of resources and conflicting outcomes. In its district-court invalidity contentions for the '825 Patent, the Petitioner lists its grounds for invalidity as: "a skilled artisan would have been motivated to combine one or more file storage references listed above (e.g., Merenda, Kohane, Singhal,

Thuraisingham I, **Bossemeyer** ... with each other and/or with one or more additional references (e.g., Shimada, Carpenter, **Glick, Carmichael**...).” EX2008.

Petitioner’s stipulation that, if the IPR is instituted, it will not pursue the same grounds in the district court litigation is insufficient to overcome these concerns of duplicative efforts and conflicting outcomes based on the Board’s own current guidance on the *Fintiv* factors. That guidance requires petitioners to stipulate that they will not “pursue in a parallel proceeding the same grounds *or any grounds that could have reasonably been raised before the PTAB*.” EX1030, 3. (emphasis added). It is this second part that Petitioner notably left out of its purported stipulation, and this factor, therefore, still favors denial. Petitioner did not stipulate that it would not pursue any ground raised or that could have been reasonably raised in an IPR. *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020).

E. The Petitioner and the Defendant in the district court proceeding are the same party.

Because IBM is both the petitioner and the defendant in the pending district court case, this factor weighs in favor of denial of institution. *Fintiv*, Paper 11 at 13–14.

F. The Petition does not present compelling evidence of unpatentability.

Consideration of the merits is appropriate because four of the five factors above favor or strongly favor denial, and the fifth is either neutral or slightly favors denial. The merits evaluation requires a “high likelihood” of the Petitioner prevailing for institution to take place under these circumstances.

The merits of the Petition are discussed above and prevent the Petition from establishing such a “high likelihood of prevailing” on all of the following:

- There is no high likelihood of Petitioner proving that the basis for its two obviousness grounds, Bossemeyer, is analogous art to the ’825 Patent, where the former is focused on smart-card technology rather than parsing, extraction, and reconstruction of data.
- There is no high likelihood of Petitioner proving that Bossemeyer discloses the “extracted data” or “reconstruction” elements found in the challenged claim, where Petitioner relies on a misunderstanding of Bossemeyer’s “partitions” for “extracting,” and Petitioner’s expert concedes that Bossemeyer lacks “reconstruction.”
- There is no high likelihood of Petitioner proving that Glick teaches the “reconstruction” element found in the challenged claim, where Glick does not teach a collection of data from which subsets are extracted and no data is ever recompiled into its original form.

- There is no high likelihood of Petitioner proving that a person of ordinary skill in the art would have combined Glick with Bossemeyer where they are from completely different fields and there is no evidence of a reason to combine them.

Each of these points, and particularly their combination, weigh in favor of discretionary denial of institution.

VIII. CONCLUSION

There are multiple reasons to deny the Petition: its lack of analogous art, the absence of two claim elements in all three references, lack of a motivation to combine, and *Fintiv* prudential concerns.

Respectfully submitted,

Dated: September 7, 2023

/Ragnar Olson/
Ragnar Olson
Reg. No. 58,684

Global IP Law Group, LLC
55 W. Monroe Street, Suite 3400
Chicago, IL 60603
Ph.: (312) 241-1503
Lead Counsel for Patent Owner

CERTIFICATE UNDER 37 CFR § 42.24(d)

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Patent Owner's Preliminary Response totals 10,821 which is less than the 14,000 words allowed under 37 CFR § 42.24(b)(1).

Dated: September 7, 2023

/Ragnar Olson/
Ragnar Olson
Reg. No. 58,684

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on September 7, 2023, a complete and correct copy of the foregoing PATENT OWNER'S PRELIMINARY RESPONSE and EXHIBITS was served via electronic mail on the following counsel of record for

Petitioner:

Theodoros Konstantakopoulos
(Reg. No. 74,155)
tkonstantakopoulos@desmaraisllp.com
DESMARAIS LLP
230 Park Ave
New York, NY 10169

Brian D. Matty
Desmarais LLP
230 Park Ave
New York, NY 10023
bmatty@desmaraisllp.com
USPTO Reg. No. 70,358

Emily Weber
Desmarais LLP
101 California Street
San Francisco, CA 94111
eweber@desmaraisllp.com
USPTO Reg. No. 79,973

/Ragnar Olson/
Ragnar Olson, Reg. No. 58,684
rolson@giplg.com
Global IP Law Group, LLC
55 W. Monroe Street
Suite 3400
Chicago, IL 60603