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 IPR2023-00970
U.S. Patent 7,552,482

PATENT OWNER DIGITALDOORS, INC.'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I. Introduction.....1

II. Background.....2

A. The DigitalDoors Technology.....2

B. The ’482 Patent.....5

C. Bossemeyer.....10

D. Merenda.....14

III. Governing Law.....16

IV. The Bossemeyer Reference Is Not Analogous Art to the ’482 Patent.....16

A. Bossemeyer and the ’482 Patent concern different fields of endeavor.....17

B. Bossemeyer is not pertinent to the problems faced by the inventors of the ’482 Patent.....20

C. Bossemeyer is not analogous to the ’482 Patent.....23

V. Bossemeyer and Merenda Both Fail to Teach Claimed *Extracting* and *Permitting Reconstruction* Method Steps, Warranting Denial on All of Petitioner’s Grounds for Challenging the Claims.....24

A. Bossemeyer does not disclose “extracting said security sensitive content.”.....25

B. Bossemeyer does not disclose “permitting full or partial reconstruction of said data.”.....33

C. Merenda does not disclose “extracting said security sensitive content” from input data.....39

D. Merenda does not disclose “permitting full or partial reconstruction of said data.”.....44

VI. Petitioner's Ground 3 Challenge also Fails Because the Combination of Bossemeyer and Merenda Was Not Obvious, Taught, or Suggested.....49

A. A POSITA would not have combined Bossemeyer and Merenda to reach the '482 claims.....50

B. None of Petitioner's five purported motivations to combine withstand scrutiny. 54

VII. The Board should deny institution on all grounds under *Fintiv*.....61

A. The district court is unlikely to grant a stay. 62

B. Trial is scheduled to finish five months before the Final Written Decision deadline. 63

C. Both parties have invested heavily in the district court proceedings..64

D. Petitioner has asserted the same two references in the district court proceedings.....65

E. The Petitioner and the Defendant in the district court proceeding are the same party.....66

F. The Petition does not present compelling evidence of unpatentability. 66

VIII. CONCLUSION.....68

TABLE OF AUTHORITIES

Cases

ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.,
694 F.3d 1312 (Fed. Cir. 2012) 58

Airbus S.A.S. v. Firepass Corp.,
941 F.3d 1374 (Fed. Cir. 2019) 19

Apple Inc. v. Fintiv, Inc.,
IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)..... passim

Belden Inc. v. Berk-Tek LLC,
805 F.3d 1064 (Fed. Cir. 2015) 56

Commscope Technologies LLC v. Dali Wireless, Inc.,
IPR2022-01242, Paper 23 (PTAB Feb. 27, 2023) 62

Continental Can Co. v. Monsanto Co.,
948 F.2d 1264 (Fed. Cir. 1991) 32

Dropworks, Inc. v. Bio-Rad Laboratories, Inc.,
IPR2021-00212, Paper 7 (PTAB. Jun. 1, 2021).....49

DSS Tech. Mgmt., Inc. v. Apple Inc.,
885 F.3d 1367 (Fed. Cir. 2018) 34

Harmonic Inc. v. Avid Tech., Inc.,
815 F.3d 1356 (Fed. Cir. 2016) 16

In re Bigio,
381 F.3d 1320 (Fed. Cir. 2004) 17, 57

In re Clay,
966 F.2d 656 (Fed. Cir. 1992) 18

In re Icon Health and Fitness, Inc.,
496 F.3d 1374 (Fed. Cir. 2007) 20

In re Oelrich,
666 F.2d 578 (C.C.P.A. 1981).....32

In re: Natural Alternatives, LLC,
659 Fed. Appx. 608 (2016).....52

Innovention Toys, LLC v. MGA Entm't, Inc.,
637 F.3d 1314 (Fed. Cir. 2011).....16

InTouch Techs., Inc. v. VGO Commc'ns, Inc.,
751 F.3d 1327 (Fed. Cir. 2014).....56

KSR Int'l Co. v. Teleflex Inc.,
550 U.S. 398 (2007) 16, 49, 52, 56

Laboratories, Inc. v. Toshiba Corp.,
993 F.2d 858 (Fed. Cir. 1993).....17

Neato LLC v. Rocky Mountain Traders,
138 F. Supp. 2d 245 (D. Ct. 2001) 18, 20

Netflix, Inc. v. DivX, LLC,
No. 2022-1138, F.4d (Fed. Cir. Sept. 11, 2023).....20

NHK Spring Co., Ltd. v. Intri-Plex Techs., Inc.,
IPR2018-00752, Paper 8 (PTAB Sept. 12, 2018) 64

PAR Pharm., Inc. v. TWI Pharms., Inc.,
773 F.3d 1186 (Fed. Cir. 2014).....33

Sanofi-Aventis Deutschland GmbH v. Myland Pharmaceuticals Inc.,
66 F.4th 1373 (Fed. Cir. 2023).....16

Sotera Wireless, Inc. v. Masimo Corp.,
IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020).....66

Tinnus Enterprises, LLC v. Telebrands Corp.,
846 F.3d 1190 (Fed. Cir. 2017).....20

Vill. Green Techs., LLC v. Samsung Elecs. Co.,
No. 2:22-CV-00099-JRG, 2023 WL 416419 (E.D. Tex. Jan. 25, 2023) 62

WBIP, LLC v. Kohler Co.,
829 F.3d 1317 (Fed. Cir. 2016).....52

Xerox Corp. v. Bytemark, Inc.,

IPR2022-00624, Paper 9 (August 24, 2022) 28

Xilinx, Inc. v. Analog Devices, Inc.,
No. IPR2020-01559, 2022 WL 945563 (PTAB Mar. 11, 2022).....57

Statutes

35 U.S.C. § 103 .....1, 16

35 U.S.C. § 312(a)(3)..... 16, 34

35 U.S.C. § 314(a). 1

37 C.F.R. § 42.104(b)(4).....16

Other Authorities

MPEP § 2141.01(a).....20

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, excerpted (Prentice Hall 1998, Third Edition)
2007	Order re Motion to Stay, *DigitalDoors, Inc. v. International Business Machines Corporation*, Case No. 2:22-cv-457, Eastern District of Texas
2008	Defendant's Invalidity Contentions Cover Pleading, April 25, 2023, *DigitalDoors, Inc. v. International Business Machines Corporation*, 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 707
2012	McClannan, Keith, *Implementing Smart Cards Into the Air Force Reserve*, Air Command and Staff College, April 2001
2013	Posey, Brien, *All about partitions: The right FAT can save your waste*, Daily Tech Insider, Sep. 2000
2014	Walker, Martin, *Splitting Your PC Data Across Multiple Drives & Partitions*, Sound on Sound, Aug. 2000

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

Exhibit Number	Document
2031	Ibarrera, *Merging data from multiple sources*, Data Ladder, Nov. 2021
2032	Audette, Lillian M. et. al., *Merging Multiple and/or Divergent Datasets using SPSS: A Method Review and Tutorial*, Graduate Student Journal of Psychology 2022, Vol. 19, 2022
2033	Al, Muhammad et. at., *Merge and Append Using Stata: How to Merge and Append Datasets*, Princeton University, May 2023
2034	Kadane, Joseph B., *Some Statistical Problems in Merging Data Files*, Journal of Official Statistics, Vol. 17, No. 3, 2001
2035	Groves, Robert M. et. al., *Federal Statistics, Multiple Data Sources, And Privacy Protection*, The National Academies Press, 2017
2036	*Department of Computer Science CSE Courses*, Stony Brook University
2037	*Lecture Notes for Chapter 3 System Security*, Stony Brook University
2038	Sekar, R., *CSE509 - Computer System Security*, Stony Brook University
2039	*A Brief History of NSF and the Internet*, National Science Foundation, Aug. 2003
2040	Lee, Tim Berners, *Early Chronology and Documents*, Stanford University, 2020

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. 7,552,482 ("the '482 Patent") filed by International Business Machines Corporation ("Petitioner" or "IBM").

Petitioner alleges that U.S. Publication No. 2004/0148290 ("Merenda") alone (Ground 1), U.S. Patent No. 7,010,701 ("Bossemeyer") alone (Ground 2), or the combination of Merenda and Bossemeyer (Ground 3) renders claims 1, 5, 25-26, 30, and 50 of the '482 Patent obvious.

The Petition does not present a reasonable likelihood that Petitioner will prevail with respect to any of the challenged claims under 35 U.S.C. § 314(a). Patent Owner, therefore, opposes institution of an IPR of DigitalDoors's '482 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 '482 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 '482 Patent is secure distribution and storage of files/documents/data objects across telecommunications networks. EX1005, Abstract; EX1001, 1:12-25. Bossemeyer is also not pertinent to the problems of data processing, distributing, and reconstructing to defeat hackers

that the ’482 Patent solves. This deficiency is sufficient to deny institution on Grounds 2-3.

2. Both Bossemeyer and Merenda lack the same two elements of the ’482 Patent’s challenged claims. Neither teaches “extracting said security sensitive content” from the original “data” nor “permitting full or partial reconstruction” of the original “data.” These two references, therefore, cannot invalidate any of those claims either individually or as a combination. This deficiency is sufficient to deny institution on all Grounds.

3. A person of ordinary skill would not have combined Bossemeyer or Merenda because of their very different technical fields and conflicting purposes. Petitioner’s purported motivations to combine misconstrue the law and face factual flaws. This deficiency is sufficient to deny institution on Ground 3.

4. The *Fintiv* factors dictate discretionary denial of institution on all 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, 8:18-20. 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. 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, 9:8-17.

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, 7:2-12.

Using different levels of security for access to different pieces allowed for control over reconstruction. EX1001, 18:59-61. 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, 7:2-12. These technologies, therefore, provided the desired digital security and survivability. *See e.g.,* EX1001, 9:8-17.

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 ’482 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 ’482 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 ’482 Patent

The ’482 Patent is titled “Data security system and method.” DigitalDoors filed for it in August 2006 based on utility and provisional applications going back to November 2000. The ’482 Patent issued on June 23, 2009.

Traditional methods of restricting data access before the ’482 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 inventions in the '482 Patent's challenged claims provide 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 for securing data on a personal computer having security sensitive content grouped into security levels, each with a clearance code, includes filtering and extracting sensitive content by security level and separately storing the security content in remote extract stores. Remainder data is stored locally or remotely. A map for selected extract stores may be generated. The filter and/or map may be destroyed or stored. The data input, extracted data and remainder data may be deleted from the originating computer. Encryption may be utilized to enhance security (including transfers of data, filter and map). Reconstruction of the data is permitted only in the presence of a

> predetermined security clearance. Full or partial reconstruction is possible, based upon the security clearances. A computer readable medium containing programming instructions and an information processing system is encompassed.

EX1001, Abstract. The claims detail 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.

Claim 1 of the ’482, with the elements critical to the Petition bolded, recites:

> 1. A method of securing data on a personal computer having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a distributed computer system with a plurality of other computers and a plurality of extract data stores for respective ones of said plurality of security levels, said personal computer, said other computers and said extract data stores operatively connected together over a communications network comprising:
>
> accepting data input which includes security sensitive content via said personal computer;

extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data;

storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in at least one of said personal computer and other computers; and,

permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

Every challenged claim of the '482 Patent includes these "extracting" and "reconstruction" steps.

The '482 Patent's specification illustrates various embodiments of these steps. Figure 1A, for example, is a basic system diagram showing filtering and storing extracted data and remainder data.

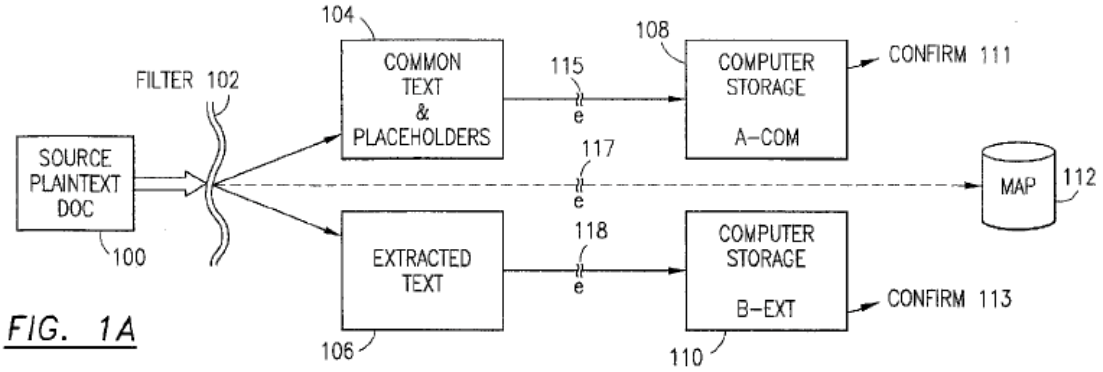

FIG. 1A

The system starts with a source document. EX1001, 14:35-39. Examples of such source documents include email, instant messages, Word documents, database

records, and XML documents. EX1001, 7:26-31. The system uses a filtering process to extract the security sensitive words, characters, or icons from original source document. EX1001, 14:41-43. 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, 15:49-53.

FIG. 1B illustrates the reconstruction step:

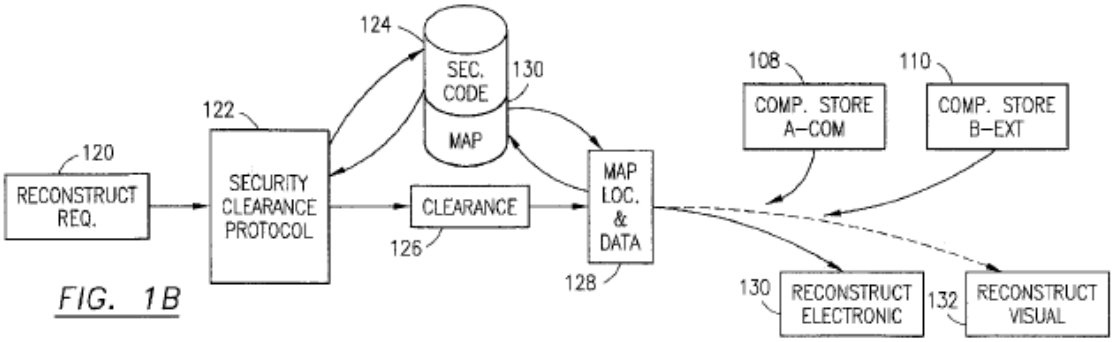

FIG. 1B

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, 16:4-8. The DigitalDoors claimed methods introduce multilevel security through extraction of security sensitive content from 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. *See e.g.,* EX1001, 11:11-20; 16:3-8. With the proper security clearance, a user can "download or recreate the entire original source, plaintext document." EX1001, 19:49-54. 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, 19:39-54.

Extraction and subsequent reconstruction are critical aspects of the invention: "[t]he present invention relates to a data security system and method and, more specifically, the extraction and controlled release of data, on a granular basis, utilizing security protocols." EX1001, 1:12-15.

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.

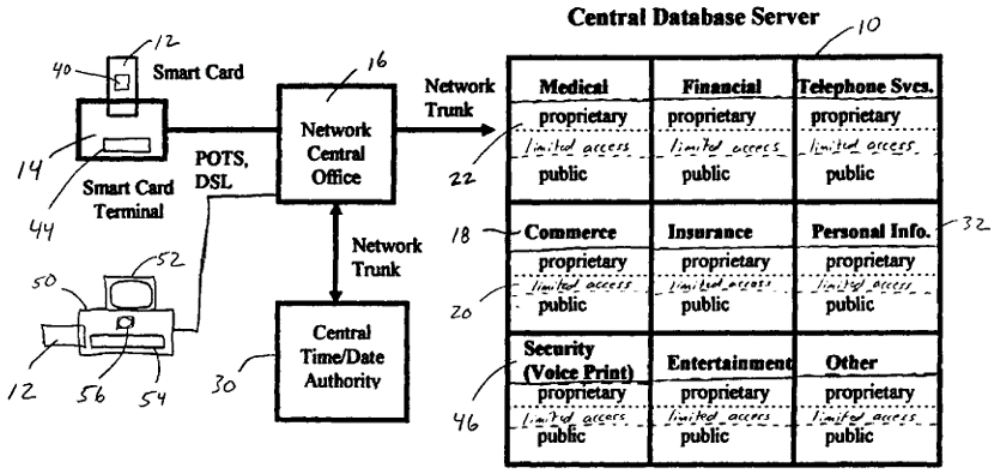

Figure 1

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:

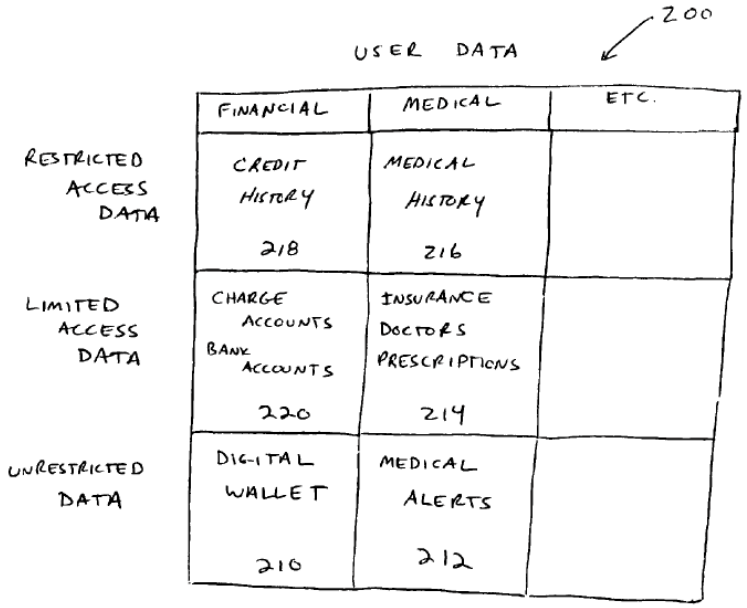

FIG. 3

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. Merenda

Merenda's focus isn't smart cards; it is eCommerce targeted marketing. EX1006, ¶4. Merenda describes its purpose in the following way: "As the Internet evolves … merchants seeking to leverage data about Internet user's [sic] to better focus their marketing efforts must do so in a manner that respects the privacy interests of their intended customer." EX1006, ¶4. It seeks to provide "solutions which provide a means for merchants to make use of customer data [for directed marketing] while still protecting the privacy interests of individual user[s]." EX1006, ¶5. It never mentions in-person transactions or smart cards.

Merenda begins with a user entering pieces of information in input fields on a web page. EX1006, ¶23. Those pieces of information are stored in separate data sets, some "public," some "private." EX1006, ¶24. Users then select which merchants may see their private data to use in marketing to them. EX1006, ¶5.

Merenda discloses two main embodiments that the Petition focuses on. In the first, illustrated in Figure 2, Merenda stores some pieces of information entered by the consumer on a web form as a single record in a "public data set" and other pieces of information as a single record in the "private data set." EX1006, ¶26, Fig. 2. It keeps those public and private sets separate. EX1006, ¶25, Fig. 2. A randomly generated key links a particular consumer's public and private records.

EX1006, ¶27. Merenda does not limit access to the public data sets but does for the private data sets. EX1006, ¶25.

In this embodiment, when customers select merchants that may contact them, those merchants receive the randomly generated key specific to a particular customer, allowing the merchants to look up that customer's private information to use in marketing. EX1006, ¶¶28, 29, 33, 35.

In Merenda's second embodiment, which is shown in Figure 3, the user also enters information on a web form. EX1006, ¶31. Its first difference from the other embodiment is that it includes multiple public and private data sets for a single consumer rather than just one of each for a single consumer. EX1006, ¶31, Fig. 3. As with the first embodiment, a customer-specific key value links the different records. EX1006, ¶31.

The second difference with this embodiment is how the merchant accesses a consumer's private data. Merenda aggregates the various tables of a customer's public and private data into a "query result web page having a URL" with an identifier for that customer's key value. EX1006, ¶36. It then emails a hyperlink with that key-coded URL to the merchant, which the merchant uses to access the consumer's data to engage in direct marketing to that consumer. EX1006, ¶¶32, 36.

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 '482 Patent.

Two of Petitioner's grounds for challenging the '482 Patent's claims depend on Bossemeyer as the primary reference. Ground 2 depends on Bossemeyer (with modifications) alone. Ground 3 depends on Bossemeyer in view of Merenda.

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 ’482 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 ’482 Patent or reasonably pertinent to the problems the ’482 Patent addresses, both Grounds 2 and 3 fail.

A. Bossemeyer and the ’482 Patent concern different fields of endeavor.

Petitioner briefly seeks to establish Bossemeyer as analogous by characterizing the field of endeavor as “securing security-sensitive information,” and then quoting two Bossemeyer snippets. Pet., 72. 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." 993 F.2d at 858. 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, ¶89. 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 quotes on page 72 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 '482 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, the extraction and controlled release of data, on a granular basis, utilizing security protocols." EX1001, 1:12-15.

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" versus filter[ing], extract[ing], dispers[ing], … permit[ting] reconstruction … [of] data."). EX2004, ¶¶88-90. 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 ’482 Patent.

Not surprisingly, based on the discussion above, Bossemeyer has no pertinence to the problems the inventors of the ’482 Patent faced. To be “reasonably pertinent,” a reference must “logically commend 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). 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. And in *Netflix, Inc. v. DivX, LLC*, the court found the prior art not reasonably pertinent as substantial evidence in the specification, claims and patent file history supported the Board’s determination that the problems addressed by the patent at issue did not appear in the prior art. No. 2022-1138, F.4d, at *16 (Fed. Cir. Sept. 11, 2023).

That Bossemeyer and the ’482 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; EX2004, ¶¶ 27, 90. The ’482 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, 6:39-56.

They also use their equipment for entirely different purposes to solve entirely different problems, as the Petition unintentionally demonstrates. On pages 72-73, the Petition presents and misinterprets the following from the ’482 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, 6:8-11. Although Petitioner tries to suggest otherwise, the problem the ’482 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 inventors of the ’482 Patent were seeking to solve

[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

the problem of creating such a secure system in the face of attacks. EX1001, 8:18-26, 12:5-23. Bossemeyer never envisions hacking attacks, and any hacker that accessed Bossemeyer's central database server would have access to everything in it. EX2004, ¶90.

The Petitioner's other quote[2] in this section, purportedly from the Abstract of the '482 Patent, does not exist in the '482 Patent and should be disregarded. Pet., 73.

Bossemeyer 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. EX2004 ¶29. It is simply concerns getting access to information stored in partitioned memory. *See supra* II.C.; EX2004 ¶90.

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 ¶298. Bossemeyer merely sends

---

security system and method and, more specifically, the extraction and controlled release of data, on a granular basis, utilizing security protocols." EX1001, 1:12-15.

[2] The Petition at page 73 again cites the Zadok declaration, EX1003, ¶387, but that cited portion is merely an exact replica of the Petition.

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," "extracting," "dispersing," or "reconstructing" as the '482 Patent does.

Bossemeyer, therefore, does not provide any solutions, let alone solutions that would "logically commend themselves," to the '482 Patent's inventors working on these specific problems.

C. Bossemeyer is not analogous to the '482 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 '482 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 the claims of the '482 Patent, and those challenges by necessity must fail.

V. Bossemeyer and Merenda Both Fail to Teach Claimed *Extracting* and *Permitting Reconstruction* Method Steps, Warranting Denial on All of Petitioner's Grounds for Challenging the Claims.

Every challenged claim of the '482 requires both "*extracting said security sensitive content*" from input data and "*permitting full or partial reconstruction of said data*." Claim 1 provides an example of the steps these claims generally cover, with the relevant language bolded:

> 1. A method of securing data on a personal computer having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a distributed computer system with a plurality of other computers and a plurality of extract data stores for respective ones of said plurality of security levels, said personal computer, said other computers and said extract data stores operatively connected together over a communications network comprising:
>
> accepting data input which includes security sensitive content via said personal computer;
>
> **extracting said security sensitive content** to obtain extracted data for each corresponding security level and remainder data;

> storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in at least one of said personal computer and other computers; and,
>
> **permitting full or partial reconstruction of said data** with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

The other challenged independent claim (Claim 26) discloses identical "extracting" and "reconstruction" steps.

Neither of the references in the Petition's Ground 1 (Merenda alone), Ground 2 (Bossemeyer alone), or Ground 3 (Bossemeyer combined with Merenda) include either step.

A. Bossemeyer does not disclose "extracting said security sensitive content."

The '482 Patent describes the extraction process as occurring at an initial processing step that "separates," or "filters out" security-sensitive data from other data prior to distributed storage. *See e.g.,* EX1001, 6:39-44, 14:41-43, 15:3-6, 23:56-59.

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:

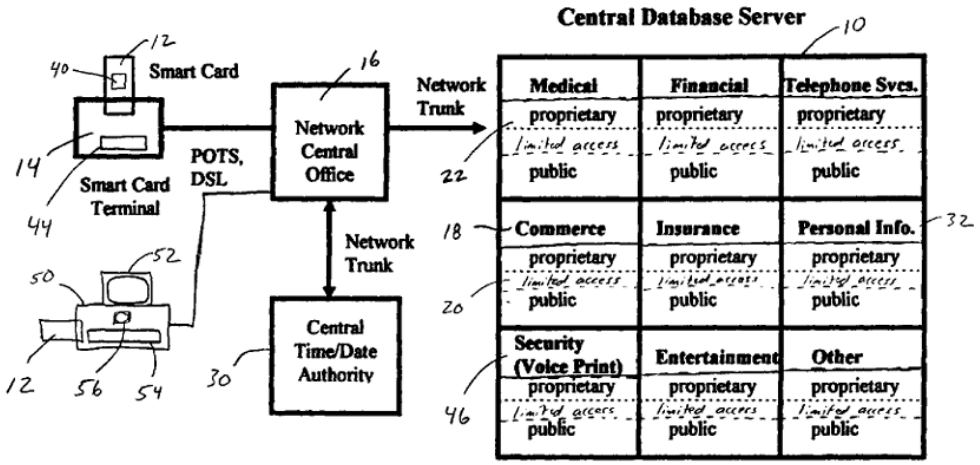

Figure 1

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, 2:27-36. Bossemeyer's Figure 3 shows varied levels of privacy related to different types of data:

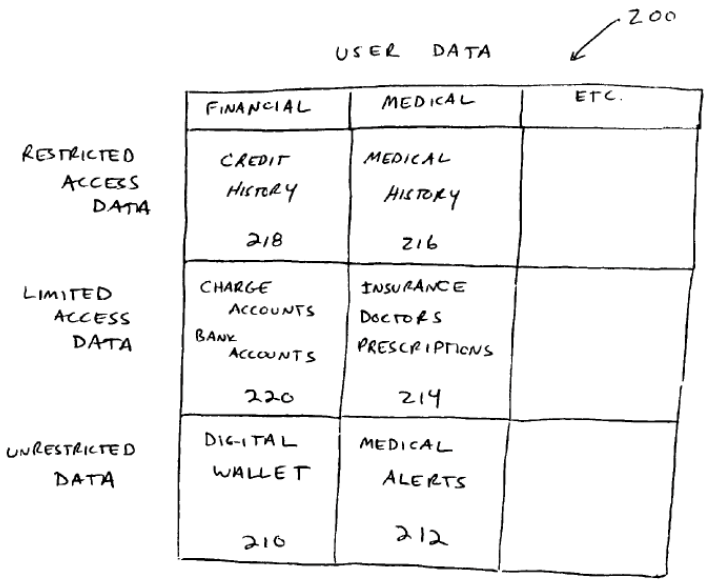

FIG. 3

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, ¶29. 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 in Bossemeyer on page 55 with a conclusory statement supported by four paragraphs from its expert's declaration. But each of those four paragraphs is merely a short, conclusory, completely unsupported statement that the element exists in the prior art. *See* EX1003, ¶¶266, 277, 347, 350. 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 word-for-word copies of Petitioner's brief. *Compare, for example,* EX1003, ¶¶267-270 *with* Pet., 55-58. 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, 2:17-27. 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, ¶¶30-36.

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, ¶30. 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, ¶275; EX2004, ¶30. That latter definition is "[a] logically distinct portion of memory or a storage device that functions as though it were a physically separate unit." EX1013, 18. 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…." EX1013, 6; EX2004, ¶30. 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, 3; EX2004, ¶32. Dr. Easttom's declaration cites additional contemporary sources saying the same thing. EX2004 ¶30.

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, ¶¶30-33. 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, ¶35.

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 56 merely refers to what kinds of information the central database stores. EX1005, 2:40-47; EX2004, ¶¶28-29. Petitioner then presents Bossemeyer's Figure 1, but it merely illustrates what kinds of information the central database stores graphically. EX2004, ¶28. 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, ¶35. Petitioner then presents Bossemeyer's Figure 3, again merely illustrating what kinds of information the central database stores graphically. EX2004, ¶28. Petitioner concludes by quoting Bossemeyer's description of what kinds of information are stored in the different partitioned areas in Figure 3. EX1005, 5:9-22. None of these pieces of evidence discloses, teaches, or suggests extraction of security sensitive data from a larger whole. EX2004, ¶¶28-33.

The Petition effectively concedes its lack of evidence when it states "[t]o the extent that … Bossemeyer does not explicitly disclose 'extracting data,'" and argues

that "a POSITA would have understood that Bossemeyer's method parses received information into private and non-private elements." Pet., 59. Confusingly, Petitioner cites Merenda, not Bossemeyer (because Bossemeyer never uses "parse"), and two paragraphs of Dr. Zadok's declaration that are nearly word-for-word copies of the paragraph in the Petition. *Compare* Pet., 59 *with* EX1003, ¶¶274-275. None of this constitutes evidence. What follows at the bottom of page 59 is a paragraph—without supporting citations— making assertions about a theoretical "medical data file" that Bossemeyer never mentions. EX2004, ¶42. 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 "partitioned disk" above shows, hard disks always must be partitioned before use. EX1013, 6; EX2004, ¶32. 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, ¶41. Data is "often loaded into partitioned memory without a prior extraction step." EX2004, ¶41.

Because Petitioner's Ground 2 relies exclusively on Bossemeyer, that challenge fails due to Bossemeyer's lack of extraction.

B. Bossemeyer does not disclose "permitting full or partial reconstruction of said data."

Petitioner's Ground 2 fails for a separate and independent reason: Bossemeyer's lack of "reconstruction." Petitioner's own expert, Dr. Zadok, effectively 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, ¶298.

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 the extent that Petitioner is relying on inherency, its arguments 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 2 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 4:50-65. Pet., 63-64. 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, ¶¶45-46.

Petitioner then turns to 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., 65-66. 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, ¶54.

Petitioner finishes with a citation to multiple paragraphs of its expert declaration in which Dr. Zadok extrapolates that some kind of data merger would (inherently or obviously?) occur, even though Bossemeyer says nothing about such a step. Pet., at 66 (citing EX1003, ¶¶292-300). Petitioner's expert assumes that for a "merchant or bank to be able to process a financial transaction" the data from different partitioned areas of memory would be merged because if it wasn't, "the transaction would fail." EX1003, ¶¶297-298. Dr. Zadok's declaration provides no support for this assumption or his hypothetical merging of data.

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., 5, 81.

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, ¶297. 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, ¶48. 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, ¶¶48, 52. Data operations often use pieces of information from different sources without merging or combining them. EX2004, ¶52.

Dr. Easttom also explains that there are reasons not to merge the information. EX2004, ¶¶49-50. For example, Bossemeyer's Figure 3 financial data includes restricted data such as credit history (218) and charge accounts (220). EX2004, ¶49. 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, ¶49. 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, ¶49. Thus, merging them would reduce the security of that data. *Id*. 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, ¶¶50-51.

Fourth, even if Petitioner could establish some kind of merging of data, it would not establish claimed "reconstruction of said data." The language of every challenged claim requires that the "said data" being reconstructed is the same as the "data" that was processed in an extraction process, as claim 1, for example, shows:

> 1. A method of securing data… having security sensitive content… comprising:
>
> accepting data input which includes security sensitive content…;
>
> ***extracting said security sensitive content*** to obtain extracted data … and remainder data;
>
> storing said extracted data … and storing said remainder data…; and,
>
> ***permitting full or partial reconstruction of said data***….

See also EX1001, Abstract, 19:49-54. To establish "reconstruction of some or all of 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, ¶43.

There is no evidence that the different pieces of information stored in the partitioned areas of Bossemeyer's 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, ¶¶29, 53. As a result, not only does Petitioner make no effort to establish that its expert's proposed merged data would be the same as the data in its original form, but it would be impossible to do so. EX2004, ¶53. 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, ¶53.

Petitioner's Ground 2, therefore, separately fails due to Bossemeyer's lack of reconstruction.

C. Merenda does not disclose "extracting said security sensitive content" from input data.

Petitioner's Grounds 1 and 3 rely on Merenda to supply the "extracting" and "reconstruction" steps. But Merenda lacks those same two elements.

The aspects of Merenda relevant to potential extraction are as follows. In both Merenda's general example (Figure 1) and its first two embodiments (Figures 2 and 3), a customer enters certain pieces of information in fields on a web form. EX1006, Figs. 1-3, ¶¶23, 26, 31. Before that process begins, each of those fields has been designated as calling for either "public" or "private" information. EX1006, ¶23.

Once entered in a field on the web form, that piece of information immediately goes to either a public or private data set, depending on how that field was initially categorized, where it is stored as a "data record." EX1006, ¶¶24, 26, 31. In the Figure 2 embodiment, there are a single public and a single private data set, whereas the Figure 3 embodiment involves multiple public and private data sets. EX1006, Figs. 2-3, ¶¶26, 31.

Because the pieces information entered in the different fields on the web form are never stored as a coherent whole, and instead immediately route to a data set, there is no extraction. Pieces of data aren't removed from a larger data set. Dr. Easttom characterizes the process like the security line at the airport. EX2004, ¶64. As people (like individual items of information) arrive, they are immediately routed to either the pre-check security line (like the private data set) or the standard security line (like the public data set), depending on whether they were pre-verified as pre-check or not. EX2004, ¶64.

Petitioner begins its attempt to find "extraction" in Merenda on page 27 of the Petition with a conclusory statement supported by two paragraphs from its expert's declaration. But each of those two paragraphs is merely a short, conclusory, completely unsupported statement that the element exists in the prior art. *See* EX1003, ¶¶164, 172. Such *ipse dixit* statements are not evidence.

Petitioner then moves to three string-cited quotes and a citation to Figures 1-3 from Merenda. Petitioner's first quote from Merenda's ¶23 states that "a set of data may be parsed…" As with "partition" in Bossemeyer, Petitioner appears to misconstrue the term "parse" to mean "extraction." EX1006, ¶23.

A close reading of that very paragraph reveals, however, that Merenda's "parsing" has nothing to do with removing pieces of data from a larger whole:

> [A] set of data may be ***parsed*** into private and non-private elements. At the most simplistic level ***this might entail***, for example, ***identifying input fields on a Web page as requiring sensitive data input*** such as an address, credit card or social security number, ***versus non-sensitive information*** such as the name of the item being purchased, the date, time etc.

EX1006, ¶23 (emphasis added). This complete statement reveals that Merenda does not "parse" a set of data; instead, its "parsing" entails conceptually designating fields as either public or private long before any data is entered, while the fields are empty. EX2004, ¶¶69-70.

Returning to the airport security-line analogy, an official is instructed in advance that everyone with a green "pre-check" on his/her boarding pass gets in a special line, while those without go elsewhere; the "parsing" is of categories of boarding passes, *ex ante*, before anyone with a boarding pass arrives at the airport.

EX2004, ¶64. The rest of the paragraph from which the Petition quotes at the start of its "extraction" discussion reinforces this interpretation:

> At a more sophisticated level ***this notion [parsing] might entail the combination of otherwise non-sensitive data elements into a combined sensitive data construct***. For example, information such as the state and town in which a person resides may be itself be deemed not sensitive but when combined with the person's occupation and alma mater, it may become a simple task to narrow the field down to a single person, and as such the combination of that data may be deemed sensitive.

EX1006, ¶23 (emphasis added). This more sophisticated version of "parsing" doesn't remove anything, it ***combines*** data fields. EX2004, ¶70. So, Petitioner's reliance on "parsing" in its first quote is misplaced.

The petition's second quote is from Merenda's ¶24, but because that quote refers back to the end of ¶23 that the Petition leaves out, we'll start there. Pet., 27-28. Paragraph 23 ends by stating that "the mechanics by which the various data elements ***are parsed*** into sensitive and public data sets is not critical, however the notion that ***such separation***, at various levels of sophistication and granularity can, and does occur, is essential…." In other words, Merenda equates the previously-described "parsing" with "separation." When the portion of ¶24 that the Petition quotes on page 27-28 then refers to "such separation," that conceptual "parsing" of

data-entry fields is again what it's referring to. EX1006, ¶24; EX2004, ¶72. Petitioner's second quote, therefore, is equally unavailing.

Petitioner appears to have included the third quote, from Merenda ¶31, simply because it includes "remaining," which bears superficial similarity to the claimed "remainder data." But that quote uses "remaining" to mean those data sets it didn't previously describe as "private"; it has nothing to do with removing data from a larger set and leaving some behind: "Any of these data sets may be designated as including private data, and the remaining data sets include public data." EX1006, ¶31; EX2004, ¶73.

Petitioner next reproduces Figures 1 and 2 from Merenda with its added color-coding but provides no additional explanation. Those figures merely reiterate that Merenda does not "parse" a set of data but, instead, designates fields on web pages as either public or private before any data is entered, while the fields are empty. EX2004, ¶¶69-70.

Petitioner also cites paragraphs 165-168 of its expert declaration. Pet., 29. But those paragraphs cite to the same portions of Merenda and face the same issues described above.

Petitioner closes this section by describing how merchants access the data in Merenda. Pet., 29-30. But that process has nothing to do with the initial "parsing"

step and is instead what Petitioner relies on for the "reconstruction" step, as described below.

Because Petitioner's Grounds 1 and 3 challenges depend on Merenda for the "extracting" element, they fail for this independent reason.

D. Merenda does not disclose "permitting full or partial reconstruction of said data."

Petitioner's Grounds 1 and 3 challenges separately fail for relying on Merenda for "permitting full or partial reconstruction of said data," which it also lacks.

As already explained with respect to Bossemeyer, the language of every challenged claim requiring that "said data" be reconstructed refers back to the "data having security sensitive content" prior to the extraction step. The Petitioner appears to argue that the filled-in customer web form constitutes the "data" from which pieces are extracted. As shown above, however, that isn't the case. *See supra* V.C. Those individual pieces of information are never stored as a unified whole from which they are later "extracted." *Id.*; EX2004, ¶¶58-65. And because there is no extraction from a whole data set having security sensitive content, there can be no "reconstruction." EX2004, ¶75.

Regardless, the individual items of data entered into the web form, or even portions of it, are never reconstructed. Here is what those web forms look like:

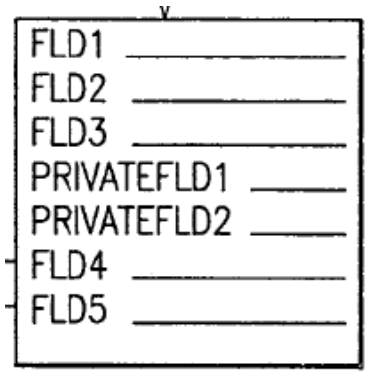

Fig. 1

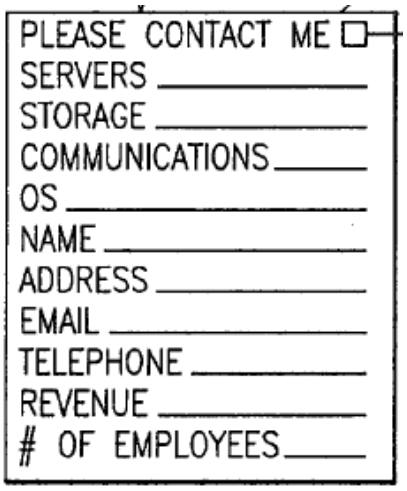

Fig. 2

In the Merenda's first embodiment, some of the information pieces are then stored as a record in a public data set, and others are stored as a record in a private data set. EX1006, FIG. 2, ¶26.

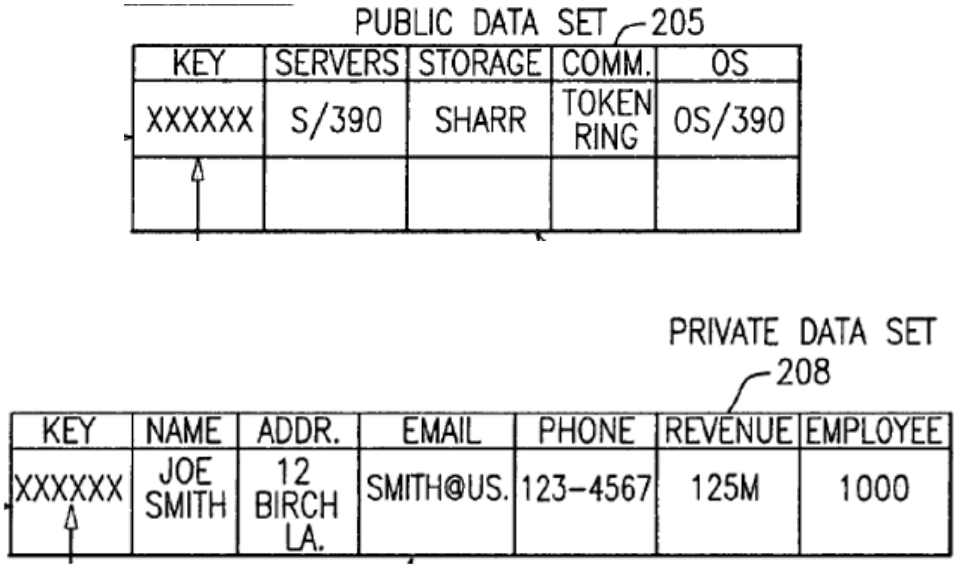

Fig. 2

Merenda describes those public and private datasets as DB2 databases, an IBM product. EX1006, ¶¶24, 31. These DB2 databases, however, don't exist until information is routed away from the web form and a "record is created" in the DB2 database, which is a separate, subsequent step to the customer's entry of data in the web form. EX1006, ¶¶24, 26, 31. This distinction between the data entered on the web form and the subsequently created public and private data sets, taking the form of DB2 databases, prevents Merenda from teaching reconstruction of said data based on anything having to do with the public and private datasets in the DB2 database. These datasets do not exist at the time when what Petitioner points to as "the data" is originally created. They are something new and different from that web form. Indeed, they have an entirely different data structure—that of a DB2 database. EX2004, ¶¶76, 85.

Petitioner points to Merenda's first embodiment for "reconstruction of said data," but authorized merchants are merely allowed to access and view information about customers in these datasets/DB2 databases using the customers' unique key numbers. EX1006, ¶¶28-29, 35. Getting viewing access to things that aren't reconstructions isn't reconstruction. EX2004, ¶76. The DB2 database records those merchants view did not exist at the time of web form entry (Petitioner's original "data") and bear no relation to the original web forms. *Compare* Web Page 100 in Fig. 1 and Web Page 202 in Fig. 2 *with* Public Data Set 205 and Private Data Set

208 in Fig. 2; EX2004, ¶¶76-77. The act of viewing information in these databases does not reconstruct the original web form in whole or in part. EX2004, ¶76.

In the Figure 3 embodiment, the merchant receives an email with a URL to a web page with key-coded information from the public and private data sets the merchant is authorized to see. EX1006, ¶30. But Petitioner presents no evidence that what this URL provides access to takes the form of the original customer web entry form in whole or in part. EX2004, ¶¶78-80. Merenda suggests otherwise, mentioning that IBM's Net.Data software product can be used to generate what the merchant views. EX1006, ¶32. That Net.Data product is designed for working with DB2 databases. EX2004, ¶65. Thus, what the merchant views is one more step removed from the customer data-entry webpage, generated based on things (the public and private DB2 datasets) that came into separate existence only after that form was filled out.

Petitioner's Merenda argument about this element begins on page 32 of the Petition. Petitioner again opens with citations to two unsupported, conclusory statements in its expert's declaration that do not constituted evidence. Pet., 32 (citing ¶¶181, 190).

Petitioner provides little explanation about the purported "reconstruction" but appears to assert that merely "providing access" is enough to qualify as reconstruction. It quotes Merenda's ¶7 and ¶25 about providing access to data, ¶10

and ¶30 about providing access via the second embodiment's URL mechanism, and then ¶29 about providing access to the data sets for viewing in the first embodiment. Pet., 32-33. That last quote actually undermines Petitioner, suggesting that access is merely to pieces individually, element by element, rather than as something combined/constructed (let alone reconstructed):

> It is useful to note that the present invention contemplates that provision of access to the data elements in the private data set may be made ***on an element-by-element basis***, that is to say, that the merchant may be provided with access to certain select pieces of private data within the single data record 214, such as the contact information (name, address, phone number, e-mail) but not to other sensitive data such as revenue, credit card etc.

EX1006, ¶29.

Petitioner concludes with a string cite to various Merenda paragraphs discussing both embodiments (¶¶8-10, 23-26, 29-30, 34-36), and then to ¶¶182-189 of Dr. Zadok's declaration. Pet., 33. Those paragraphs of Dr. Zadok's declaration are either *ipse dixit* statements lacking any citation or support (¶¶182, 189) or cite to the same portions of Merenda and face the same shortcomings described above. Dr. Zadok's ¶187 quotes Merenda's ¶¶8-9 about the first embodiment: a user granting access to a merchant, who then uses the key code to view information in the data sets. Dr. Zadok's ¶¶183-184 quote Merenda's ¶7 and ¶25 about allowing access to

data at the direction of the consumer to protect the privacy of the consumer. Dr. Zadok's ¶188 quotes Merenda's ¶29 about providing access to the data sets for viewing in the first embodiment. And Dr. Zadok's ¶¶183, 185-186 quote Merenda's ¶¶10, 30, 36, and Fig. 4, concerning the second embodiment's providing access to view the datasets via the URL. As explained above, neither embodiment teaches "reconstruction of said data."

That is the sum of the petition's citations and reasoning concerning whether Merenda includes "permitting full or partial reconstruction of said data." Because nothing supports that conclusion, Petitioner's Grounds 1 and 3 separately fail for lacking that element.

VI. Petitioner's Ground 3 Challenge also Fails Because the Combination of Bossemeyer and Merenda Was Not Obvious, Taught, or Suggested.

Petitioner's Ground 3 fails for a different and independent reason: a POSITA would never have combined Merenda with Bossemeyer. Petitioner needed to establish both that a POSITA would have had the skill to combine two different references and "*what would have prompted* the ordinarily skilled artisan to make the proffered combination to yield the claimed method." *KSR*, 550 U.S. at 417; *Dropworks, Inc. v. Bio-Rad Laboratories, Inc.*, IPR2021-00212, Paper 7 (PTAB Jun. 1, 2021). Petitioner did neither of these, when a failure on either would warrant denial of its Ground 3 challenge.

A. A POSITA would not have combined Bossemeyer and Merenda to reach the '482 claims.

Bossemeyer and Merenda are from dramatically different fields. Bossemeyer concerns smart card technology. Smart cards exist to facilitate in-person transactions at stores and offices. EX1005, 2:22-26; EX2004, ¶27. A customer walks in, picks up the product, and goes to the checkout, where he or she presents the smart card. EX2004, ¶27. A special reader at that location reads information on the card to facilitate the transaction. EX2004, ¶27. In Bossemeyer's case, that process involves communicating with a remote server. EX1005, 2:22-26; EX2004, ¶27. The customer then leaves the store with the product. EX2004, ¶27.

Merenda has nothing whatsoever to do with smart cards and is antithetical to that technology. EX2004, ¶¶16, 57. Instead of in-person transactions, Merenda is focused on the World Wide Web, eCommerce, and directed marketing. EX1006, ¶¶2-4; EX2004, ¶¶57, 91. It concerns web forms, URLs, and email. EX1006, ¶¶7, 10; EX2004, ¶57. Merenda never wants you to walk into a store to present a smart card to make a purchase. EX2004, ¶57.

The only technical commonality between these two references is that both store data in computer memory on a server. EX2004, ¶92. But all the technology surrounding those servers is different. Bossemeyer uses smart cards storing digital pointers, special smart card readers, the "plain old telephone service" to carry data,

and an undefined server with undefined software. One has to understand these technologies to implement Bossemeyer. Merenda, on the other hand, uses a form generated on the World Wide Web to obtain information, special software for automatically generating both web pages with information and corresponding URLs for accessing those web pages, and software for automatically sending emails with these URLs. EX1006, ¶¶2, 7, 10; EX2004, ¶85.

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] Merenda is in an entirely different class, 707, "Data Processing: Database and File Management or Data Structures," subclass 10, "distributed or remote access."[4]

The two references are also pertinent to very different problems. As already explained, *supra* IV.B., Bossemeyer is trying to improve operation of smart cards

---

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

[4]https://web.archive.org/web/20041108063552/http://www.uspto.gov/web/patents/classification/uspc707/defs707.htm, EX2011.

used for in-person transactions through "integration of [the cards with] a centralized server architecture or a network arrangement for multiple smart card applications." EX1005, 1:39-43. Merenda supports electronic directed marketing while preserving customer control over private information. EX1006, ¶¶3-5.

Bossemeyer and Merenda are not analogous art to each other and would not have been combined. *See In re: Natural Alternatives, LLC*, 659 Fed. Appx. 608, 610 (2016) (denying motivation to combine references in different fields pertinent to different problems). 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). Moreover, it is unlikely that the POSITA would have had the skill to combine these two references because of their technical differences. *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., 5. 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, ¶¶24, 93-94. The Petition makes no effort to establish that its POSITA would have had

training or experience with them. EX2004, ¶¶93-94. 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. *Id*. 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, ¶94. Even the single graduate-level course that Dr. Easttom was able to find only addresses smart cards in passing, not in detail. *Id*.

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 Ground 2 based on the combination.

A person of ordinary skill in the art would also understand that adding Merenda to Bossemeyer would conflict with Bossemeyer's purpose. Bossemeyer seeks to "facilitate" in-person transactions by providing necessary data. EX1005, 2:37-40; 3:3-14. Examples of these transactions are those at gas stations, grocery stores, department stores, and hotels. EX1005, 1:17-21, 5:16. In those situations, where the customer is physically present seeking to make the transaction, speed and ease are paramount. EX2004, ¶27. Bossemeyer makes these transactions seamless, because when the customer inserts the card and enters a PIN, the server's partitioned

memory automatically and immediately returns the requested information. EX1005, 3:52-4:6.

Adding Merenda would add an extra step to this process, slowing it and complicating it, which the merchants and customer would hate. Merenda isn't about facilitating transactions. EX1006, ¶¶2-4. In both Merenda embodiments, a unique key code is appended to the customer's information. In embodiment one, the server sends the merchant the customer's key code, and then the merchant looks up the customer's information in the database using that key code. EX1006, ¶¶29, 35. In embodiment two, the merchant receives a "key-coded URL" that the merchant uses to access the customer's information in the database. EX1006, ¶¶32, 36. Combining Merenda with Bossemeyer in the manner Petitioner suggests to satisfy "reconstruction" would require an extra, time-consuming step to every transaction.

Not only would there be no reason to combine Merenda with Bossemeyer, but there is also a strong reason not to do so, which is an independent ground for denying Petitioner's Ground 3 challenge.

B. None of Petitioner's five purported motivations to combine withstand scrutiny.

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, in this petition, and Carmichael, IPR2023-00967, IPR2023-00968, IPR2023-00969, IPR2023-00971, IPR2023-00972)
- Copyright protection and DRM (Glick, IPR2023-00967)
- Direct email marketing (Merenda, in this petition and IPR2023-00968, IPR2023-00969, 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.

Before addressing the first four of Petitioner's five purported motivations to combine, it's important to note that they only can support adding Merenda's "parsing" to Bossemeyer to try to satisfy "extraction." Pet., 67-70. None of the four has anything to do with combining Merenda with Bossemeyer to satisfy "reconstruction." As already noted, however, Petitioner's own expert conceded that Bossemeyer lacks "reconstruction." EX1003, ¶298. So, no matter what happens

with the first four, Petitioner's Ground 3 challenge fails if the Board disagrees with Petitioner on its fifth motivation to combine.

Petitioner's first purported motivation—that the "combination [of Merenda's "parsing"] … represents the use of known techniques according to known methods in the same way to yield predictable results"—isn't anything of the sort and contravenes the law.[5] Pet., 67. The question is not whether references could be combined; it is what would have prompted ordinarily skilled artisans to combine them to arrive at the claimed invention. *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (*citing InTouch Techs., Inc. v. VGO Commc'ns, Inc.*, 751 F.3d 1327, 1352 (Fed. Cir. 2014)); *Dropworks*, IPR2021-00212, Paper 7 at 12.

Petitioner's "known technique" language comes from *KSR*. 550 U.S. at 418. However, *KSR* still requires "an apparent reason *to* combine the known elements in the fashion claimed by the patent at issue." *Id*. (emphasis added). The PTAB recently rejected Petitioner's "known technique" approach because of the "lack of an articulated reason and supporting evidentiary underpinnings" for the combination.

[5] Petitioner makes no effort to establish that Merenda's purported "reconstruction" was a known-technique and limits its analysis to Merenda's purported "extraction," parsing. That is why the first purported motivation only applies to "extraction."

Xilinx, Inc. v. Analog Devices, Inc., No. IPR2020-01559, 2022 WL 945563, at *23 (PTAB Mar. 11, 2022).

Here, Petitioner argues that Merenda's "parsing" was a known technique. Leaving aside the meaning of "parsing" in Merenda, even if that were true, it would not provide an articulated reason for combining Merenda's "parsing" with Bossemeyer as the law requires.

Petitioner also argues that the references are from "the same field" and "address the same problem," but that is merely a restatement of the analogous-art test. *See Bigio,* 381 F.3d at 1325 and *supra*, section VI. If that were the proper test, then a motivation would exist for all analogous art references.

These are the only explanations Petitioner offers for its lead motivation to combine, and they are inconsistent with the legal standard for establishing such a motivation.

Petitioner's second purported motivation is that "Merenda identifies a known problem (e.g., controlling access to private information) and provides a solution to address the problem (e.g., parsing user data to extract the private elements and store private elements and non-private elements in separate memory stores)." Pet., 68. Petitioner again gets the law wrong, because knowledge of a problem and motivation to solve it are entirely different from motivation to combine particular references. *ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.,* 694 F.3d 1312, 1327 (Fed.

Cir. 2012). Petitioner offers no specific motivation with respect to these particular references.

Even were that not the case, Petitioner's "known" or "universal" problem doesn't match up with its purported solution. Its purported solution is "parsing" and separate storage. In Petitioner's view, "parsing," means removing data from a larger whole, which is wrong for the reasons stated above. *See supra* V.C.; EX2004, ¶¶68-74. But, regardless, "parsing" is merely a precursor to the steps that Merenda takes to control access to private information. EX2004, ¶103. Control over access is found elsewhere in Merenda, not with "parsing" or storage. *Id.*

Merenda's access control is limiting which and how merchants can view private data, an entirely separate step from the initial storage of different pieces of information. Merenda controls access by either providing approved merchants with a key code to use for looking up the private data in the database (embodiment one) or providing a key coded URL for viewing that data (embodiment two). EX1006, ¶¶28-29, 33, 34-35. Those are the aspects of Merenda that control access to the data, but they are not the same as "parsing," which is what Petitioner presents as the solution. Thus, Petitioner's proposed solution does not match its purported "known problem."

Petitioner's third purported motivation contends that adding Merenda's "parsing" would allow "'separation [to occur] ***at various levels of sophistication***

and granularity.'" Pet., 69 (*quoting* EX1006, ¶23) (emphasis in petition).[6] The problem for Petitioner is its misunderstanding of Merenda's "at various levels of sophistication and granularity," and how it is inapplicable to Bossemeyer. Petitioner didn't explain what these "various levels" would be, and whether/how they would work with Bossemeyer. As already discussed, *supra* V.C., the "various levels" refers to two levels of parsing earlier in that same ¶23, "identifying input fields on a Web page as requiring sensitive data input" and "the combination of otherwise non-sensitive data elements into a combined sensitive data construct." Because Petitioner emphasized the "various" levels, presumably it means at least both of these levels.

The problem is that the level that entails "the combination of otherwise non-sensitive data elements into a combined sensitive data construct" is inapplicable to Bossemeyer. EX2004, ¶106. In Bossemeyer, there would be no way to limit access to combinations of "otherwise non-sensitive data elements." EX2004, ¶¶107-108. In Bossemeyer, the "pointers" stored on the smart card point directly to areas of the partitioned memory. EX1005, 3:63-66. There would be no way for these pointers to be prevented from accessing those areas because data from another area of the partitioned memory was being sought simultaneously, the combination scenario

[6] By expressly limiting itself to "parsing," this motivation is also limited to "extraction."

Merenda is describing. EX2004, ¶108. Yet this feature is what Petitioner contends would have motivated one to combine Merenda with Bossemeyer. Since that purported improvement wouldn't work, however, it cannot serve as a motivation to combine.

Petitioner's fourth purported motivation to combine is one sentence and largely redundant of the first and second motivation with the added assumption that Bossemeyer was "ready for improvement." Pet., 70. This statement is not actually a motivation to combine; it is a conclusory opinion that Bossemeyer and Merenda could be combined. Again, it is based on a misunderstanding of Merenda's "parsing." EX2004, ¶111. The same problems with motivations one and two, above, apply to this purported motivation.

Petitioner's fifth and final proposed motivation to combine is the only one relevant to "reconstruction": with the growth of direct marketing in eCommerce and the World Wide Web, the need for controlling access to private information will increase. Pet., 70. That is a strange reason for combining Merenda with Bossemeyer. Bossemeyer is unconcerned with eCommerce, targeted marketing, or the World Wide Web. EX2004, ¶¶112-114. Also, Bossemeyer is antithetical to those issues. EX2004, ¶113. Bossemeyer's focus is facilitating in-person transactions using smart cards. EX2004, ¶¶27, 113.

Moreover, Bossemeyer cannot support Merenda's direct email marketing that Petition is relying on for this motivation to combine. In Bossemeyer, there is no way to reach the customer with marketing. EX2004, ¶115. The customer has a smart card and is using a smart card terminal; the customer is not using a computer to access the Web, nor do they receive emails or digital pop-up ads on the screen. EX2004, ¶115.

What Bossemeyer is clear about is the need to restrict information from getting to merchants unless it is necessary for a transaction. EX2004, ¶116; EX1005, 5:6-15. In this sense, Bossemeyer is in open conflict with Merenda. Bossemeyer's smart card system would prevent merchants from gaining access to user information for marketing purposes. Merenda gives it to them for that purpose. EX2004, ¶116. This fifth purported motivation is even less of a fit than the first four.

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

On November 28, 2022, DigitalDoors, the Respondent, sued IBM, the Petitioner, for infringement of five patents, including the '482 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) (EX1018, "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 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 five months before the Final Written Decision deadline.

Trial in the pending district court case is scheduled to end about five 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 January 2025, not December 2024 at Petitioner asserts, well after trial. Pet., 78. 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. EX1018, 8 ("Parties may present evidence regarding ***the most recent statistics*** on median time-to-trial") (emphasis added); Pet., 79 (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. EX1009. 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 over 4,150 documents, and IBM produced, and DigitalDoors

reviewed over 25,780 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 two references in the district court proceedings.

Because the Petitioner asserts the Bossemeyer and Merenda 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 '482 Patent claims, the Petitioner lists its grounds for invalidity as: "**Merenda**, Kohane, Singhal, Thuraisingham I, **Bossemeyer**, Thuraisingham II, Kou, Chiganti, Fujitsu SafeFile, Honeywell LDV, MITRE Inference Controller, Unisys SDDM, GPFS, Legato Networker) ***with each other and/or with one or more additional references***." 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***." EX1018, 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 two of its obviousness grounds, Bossemeyer, is analogous art to the '482 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 "extracting" or "reconstruction" elements found in every 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 Merenda teaches the "extracting" or "reconstruction" elements found in every claim, where Merenda 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 Merenda 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 both references, legally and factually insufficient motivations to combine, and *Fintiv* prudential concerns.

Respectfully submitted,

Dated: October 20, 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 13,945 which is less than the 14,000 words allowed under 37 CFR § 42.24(b)(1).

Dated: October 20, 2023

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

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on October 20, 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