

Case IPR2023-00970
U.S. Patent No. 7,552,482

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION
Petitioner

v.

DIGITAL DOORS, INC.
Patent Owner

IPR2023-00970
U.S. Patent No. 7,552,482
PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction.....	1
II. Grounds For Standing.....	3
III. Summary Of The '482 Patent.....	3
A. Overview	3
B. Prosecution History	4
C. Priority Date	5
IV. Level Of Ordinary Skill In The Art.....	5
V. Claim Construction.....	6
VI. Relief Requested And The Reasons For The Requested Relief.....	6
A. Challenged Claims And Statutory Grounds For Challenge.....	6
1. Merenda	7
2. Bossemeyer	10
B. Ground 1: Claims 1, 5, 25, 26, 30, And 50 Are Obvious Over Merenda.....	14
1. Independent Claims 1 and 26.....	14
2. Dependent Claims 5, 25, 30, and 50	34
C. Ground 2-3: Claims 1, 5, 25, 26, 30, And 50 Are Obvious Over Bossemeyer (Ground 2) Or Bossemeyer With Merenda (Ground 3)	36
1. Independent Claims 1 and 26.....	36
2. Dependent Claims 5, 25, 30, and 50	74

VII.	Discretionary Denial Would Be Inappropriate.....	77
A.	Discretionary Denial Under The <i>Fintiv</i> Factors Is Not Appropriate.....	77
1.	No evidence regarding a stay	78
2.	Parallel proceeding trial date	78
3.	Investment in the parallel proceeding	79
4.	Overlapping issues with the parallel proceeding	80
5.	Identity of parties	80
6.	Other circumstances	80
B.	Discretionary Denial Under 35 U.S.C. § 325(D) Is Not Appropriate.....	81
VIII.	Conclusion	81
IX.	Mandatory Notices.....	83
A.	Real Party-in-Interest	83
B.	Related Matters.....	83
C.	Lead and Back-up Counsel and Service Information	83

TABLE OF AUTHORITIES

	<u>Pages(s)</u>
<u>Cases</u>	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	77, 80
<i>Dish Network L.L.C. v. Broadband iTV, Inc.</i> , IPR2020-01359, Paper 15 (Feb. 12, 2021)	78
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	6
<i>PEAG LLC v. Varta Microbattery GmbH</i> , IPR2020-01214, Paper 8 (PTAB Jan. 6, 2021)	79
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	6
<i>Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC</i> , IPR2019-01393, Paper 24 (PTAB June 16, 2020)	78, 80
<u>Statutes</u>	
35 U.S.C. § 101	4
35 U.S.C. § 102(e)	7, 10
35 U.S.C. § 103	6
35 U.S.C. § 311	1
35 U.S.C. § 314(a)	1, 6
35 U.S.C. § 325(D)	81
<u>Rules</u>	
37 C.F.R. § 42.100	1
37 C.F.R. § 42.100(b)	6

Case IPR2023-00970
U.S. Patent No. 7,552,482

37 C.F.R. § 42.104(a).....	3
----------------------------	---

EXHIBIT LIST

Exhibit No.	DESCRIPTION
1001	U.S. Patent No. 7,552,482 to Redlich et al.
1002	Prosecution History of U.S. Patent No. 7,552,482
1003	Declaration of Dr. Erez Zadok
1004	<i>Curriculum Vitae</i> of Dr. Erez Zadok
1005	U.S. Patent No. 7,010,701 to Bossemeyer et al.
1006	U.S. Publication No. 2004/0148290 to Merenda et al.
1007	Amended Docket Control Order, <i>DigitalDoors, Inc. v. Int’l Bus. Machs. Corp.</i> , Civil Action No. 2:22-cv-00457-JRG-RSP (E.D. Tex. Apr. 5, 2023).
1008	Scheduling Order, <i>DigitalDoors, Inc. v. Int’l Bus. Machs. Corp.</i> , Civil Action No. 2:22-cv-00457-JRG-RSP (E.D. Tex. Feb. 7, 2023).
1009	Federal Case Management Statistics for the Eastern District of Texas, as of June 30, 2022
1010	Plaintiff DigitalDoors, Inc.’s Disclosure of Asserted Claims and Initial Infringement Contentions, <i>DigitalDoors, Inc. v. Int’l Bus. Machs. Corp.</i> , Civil Action No. 2:22-cv-00457-JRG-RSP (E.D. Tex. Feb. 28, 2023).
1011	U.S. Provisional Application No. 60/247,242
1012	U.S. Provisional Application No. 60/247,232
1013	Microsoft Computer Dictionary, Fourth Edition, Copyright 1999, Excerpts
1014	Beck et al., Linux Kernel Internals, 2nd Ed., Copyright 1998, pp. 148-187
1015	DOD Standard, Department of Defense Trusted Computer System Evaluation Criteria, December 26, 1985 (“Orange Book”)
1016	Director of Central Intelligence Directive No. 1/16, Security of Compartmented Computer Operations (“CIA”)
1017	Cheswick et al., Firewalls and Internet Security, Copyright 1994, p. 163
1018	Director’s June 21, 2022 Memorandum on Discretionary Denials
1019	U.S. Patent No. 7,356,533 to Schneider et al. (“Schneider”)

IBM citations to specific pages of exhibits follow the pagination added to those exhibits per 37 C.F.R. § 42.63(d)(2)(i).

All emphasis has been added unless noted otherwise.

All annotations in Figures have been added unless noted otherwise.

I. Introduction

Pursuant to 35 U.S.C. §§311, 314(a), and 37 C.F.R. §42.100, International Business Machines Corporation (“IBM” or “Petitioner”) respectfully requests that the Board cancel as unpatentable claims 1, 5, 25-26, 30, and 50 (the “Challenged Claims”) of U.S. Patent No. 7,552,482 (“’482 Patent,” EX1001).

The Challenged Claims cover methods for securing data by separating and securing sensitive portions of the data and then controlling access to the sensitive data based on a security clearance. Although the Examiner noted that the prior art taught separating data based on security levels and allowing full or partial reconstruction of data based on a respective security clearance, the Examiner ultimately concluded that the prior art did not disclose storing only security sensitive data for each security level at a security-controlled memory for each security level and storing remainder data at a separate memory location.

This Petition demonstrates that separating and securing sensitive data in a separate location was known. *See e.g.*, EX1006, (“Merenda”), ¶7 (“In an embodiment of the invention, data entered by a consumer into a Web form is separated into related records in a public and private data set.”); *and* EX1005, (“Bossemeyer”), 3:6-16 (“[T]he purchaser’s credit files are more likely to be stored in a database monitored by the credit reporting companies such as TransUnion or Equifax, as opposed to the central database server 10.... In the same way, insurance

information would ultimately reside with the insurer, medical records with the health provider, financial records with the bank or broker, and so on.”). EX1003, ¶¶51-62.

This Petition also demonstrates that controlling access to security-sensitive data based on a corresponding security level was known. EX1006, ¶29 (“[T]he 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.”); *and* EX1005, 2:40-47 (“The information contained within the central database server... can be classified as public information available to all the world; limited access information available to persons or selected groups with a user authentication code; or proprietary information accessible only by the owner of the information or a group with privileges to that directory information.”). EX1003, ¶¶63-78.

The Petition, supported by the declaration of Dr. Erez Zadok, demonstrates that the combination of the known elements of the Challenged Claims described in the prior art was nothing more than an obvious application of known technologies to address a known problem.

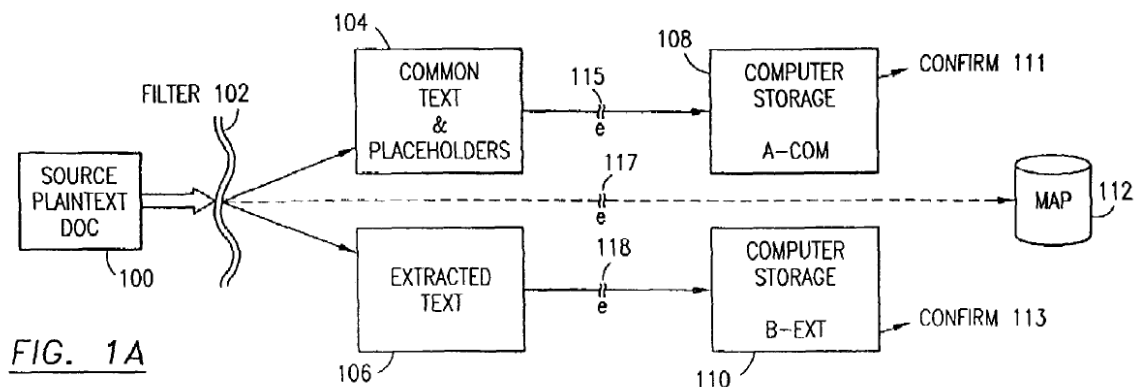
II. Grounds For Standing

Petitioner certifies that the '482 Patent is eligible for IPR and that Petitioner is not barred or estopped from requesting IPR. 37 C.F.R. § 42.104(a).

III. Summary Of The '482 Patent

A. Overview

The '482 Patent relates to “the extraction and controlled release of data, on a granular basis, utilizing security protocols” EX1001, 1:13-15. Figure 1A illustrates the disclosed data security system:



EX1001, Figure 1A. As shown, source document 100 which contains data is passed through filter 102. EX1001, 14:37-39. “Filter 102... separates out common text or remainder data 104 from uncommon text, words, characters or icons.” EX1001, 14:39-41. The common data objects are then placed into remainder document or common datafile 104, and the uncommon words (or security sensitive words) are placed into a separate extracted data file 106. EX1001, 14:48-54. The remainder

and extracted data are stored separately, with the remainder data stored in common storage memory 108, and the extracted data file 106 stored in a different memory computer storage 110. EX1001, 15:7-8, 15:14-15. EX1003, ¶¶79-84.

B. Prosecution History

The '482 Patent was filed on August 17, 2006. EX1001, 1. The Examiner rejected the claims on the grounds of nonstatutory obviousness-type double patenting and under 35 U.S.C. §101. EX1002, 121-127. The applicant filed terminal disclaimers to obviate the obviousness-type double patenting rejection and amended the claims to overcome the remaining objections. EX1002, 143-166. The Examiner issued a Notice of Allowance on March 10, 2009 (EX1002, 168-174) and stated: “The prior art teaches filtering data based on security levels and storing the data and allowing full or partial reconstruction of data based on a respective security clearance. The prior art also fails to teach storing only the extracted data for each security level at an extract store for each security level and storing the remainder data at a separate remainder store.” EX1002, 172. EX1003, ¶¶85-90.

But as this Petition illustrates, storing only the extracted data for each security level at an extract store for each security level and storing the remainder data at a separate remainder store was known in the art. For example, Bossemeyer—a prior art reference that was not considered by the Examiner—discloses only storing data in extract stores based on different security levels (e.g., public limited access,

restricted (EX1005, 2:17-27)), storing non-sensitive, remainder data in a separate remainder store (e.g., storing unrestricted data in stores 210, 212 (EX1005, Figure 3, 5:6-22). EX1003, ¶¶83.

C. Priority Date

The earliest claimed priority date is November 13, 2000, the filing date of two provisional applications which the '482 Patent claims priority to. EX1001, 1; EX1011; EX1012. Petitioner does not concede that the Challenged Claims are entitled to that priority date. However, because the references discussed here qualify as prior art under the November 13, 2000 date, Petitioner does not challenge the priority date of the Challenged Claims here but reserves the right to do so in other proceedings.¹ EX1003, ¶30.

IV. Level Of Ordinary Skill In The Art

A Person Of Ordinary Skill In The Art (“POSITA”) would have had 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 as of November 13, 2000. Less professional experience can be substituted by additional education, and vice versa. EX1003, ¶¶110-111.

¹ Petitioner reserves the right to raise §112 challenges in other proceedings.

V. Claim Construction

Claim terms in IPRs are construed according to their “ordinary and customary meaning” to those of skill in the art. 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*). Petitioner submits that, for the purposes of this proceeding and the grounds presented herein, no claim term requires express construction. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

VI. Relief Requested And The Reasons For The Requested Relief

A. Challenged Claims And Statutory Grounds For Challenge

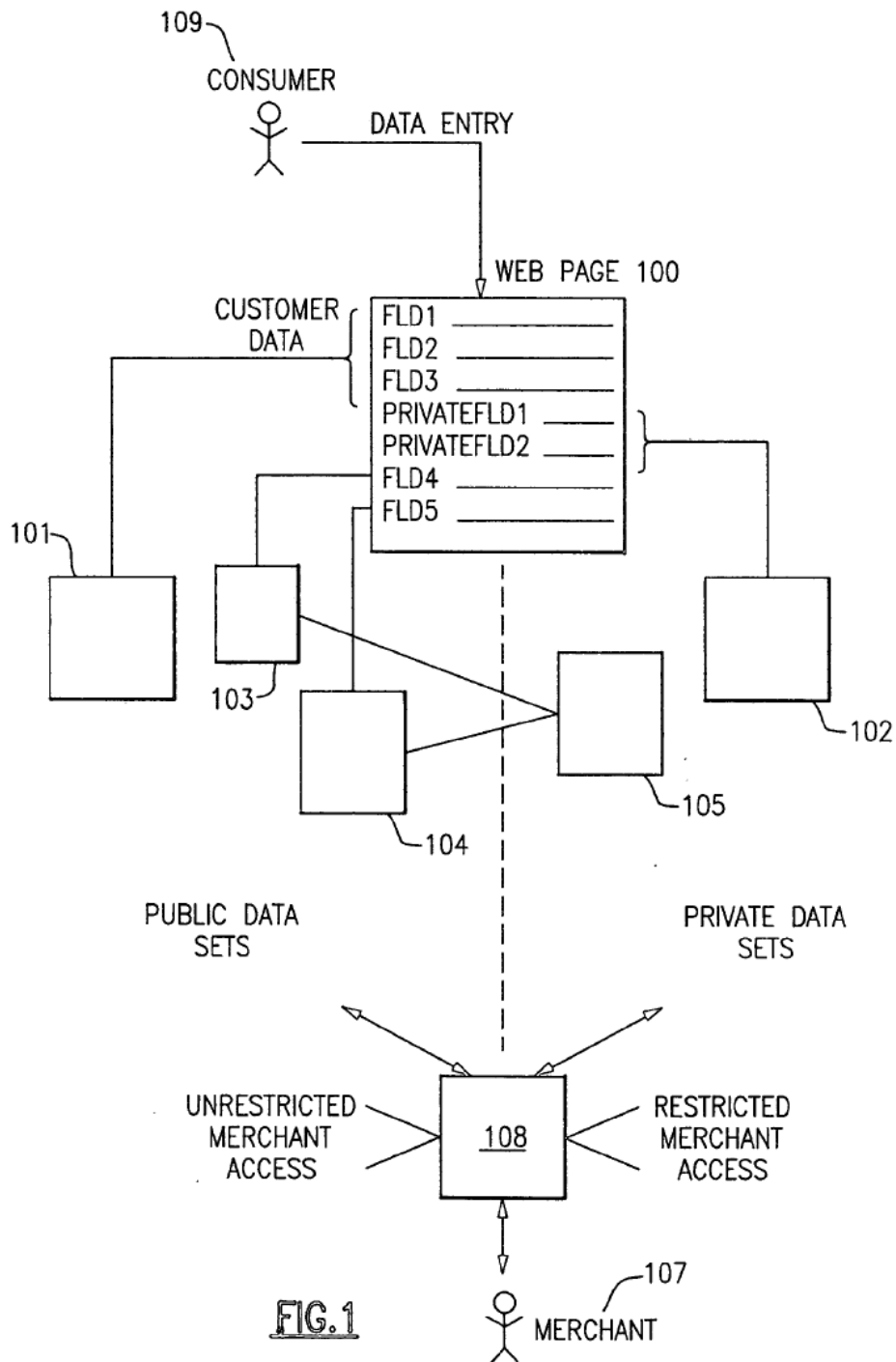
Petitioner requests the Board institute a trial for IPR and cancel the Challenged Claims under 35 U.S.C. §103. This Petition, supported by Dr. Erez Zadok’s Declaration (EX1003), demonstrates that there is a reasonable likelihood that Petitioner will prevail with respect to the Challenged Claims. 35 U.S.C. §314(a).

Grounds	Claims	Basis
#1	1, 5, 25-26, 30, and 50	(§103) Merenda
#2	1, 5, 25-26, 30, and 50	(§103) Bossemeyer
#3	1, 5, 25-26, 30, and 50	(§103) Bossemeyer And Merenda

1. Merenda

US Publication No. 2004/0148290 (EX1006, “Merenda”), filed on January, 14, 2004, is a divisional application of US Ser. No. 10/390,954, filed on Mar. 17, 2003, which is a divisional application of US Ser. No 09/563,639, filed on May 2, 2000. Merenda published on July 29, 2004, and is prior art under at least 35 U.S.C. §102(e). EX1003, ¶104.

Merenda describes a system “allowing the viewer of a public data set to access related records in a private data set based upon a link which may be selectively provided to the viewer to authorize such access.” EX1006, ¶2. Merenda describes that “data entered by a consumer into a Web form is separated into related records in a public and private data set. The public records would be available without restriction for read access by a population of merchants. The private records would be available only per the indication of the consumer to the merchant in the population.” *Id.*, ¶7. This “separation of data elements may be accomplished using known techniques to any desired level of granularity, resulting potentially in multiple public and private data sets...” *Id.*, ¶24. EX1003, ¶¶105-106.



Merenda discloses that “[u]pon entering the data the consumer may be prompted to indicate whether they wish to provide merchants with access to their private data...The consumer may be offered and [sic] opportunity to choose among

the population of merchant the select merchant to whom they wish their private data to be provided.” EX1006, ¶8. “Once selected...the merchants may be provided with a pass code...[providing] the ability to view the particular consumers private data record in the private data set. *Id.*, ¶9. For example, a user of Merenda’s system requesting information, e.g., a merchant, can have access only to certain portions of the private information. That is, a merchant can access certain selected private data sets (e.g., private data sets having a first security level, such as *name, address, phone number, e-mail*), but cannot access other private data sets (e.g., private data sets having a second (higher) security level, such as *revenue, credit card*).

*[A]ccess 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. EX1003, ¶¶107-108.

Before the user data is separated into public and private data sets, it is entered into a “web form” by the user/consumer. EX1006, ¶7. The information is collected into tables and, when desired, assembled into an output web page that can be accessed by a merchant for whom access has been authorized. EX1006, ¶10. EX1003, ¶¶108-109.

2. Bossemeyer

US7,010,701 (EX1005, “Bossemeyer”), filed on October 19, 1999, and issued on March 7, 2006, is prior art under at least 35 U.S.C. §102(e). EX1003, ¶91.

Bossemeyer “describes a network arrangement which is readily accessible from different types of smart card terminals supporting various smart card applications.” EX1005, 1:44-49. Smart cards are devices that “can hold much more information [than data cards] and often include some ‘intelligence’ such as a microprocessor....” EX1005, 1:34-37, 3:28-31. EX1003, ¶¶92-93.

Bossemeyer’s network arrangement includes “a centralized server architecture [where] data...can be accessed by an individual smart card, predefined groups of...users, or the general public.” EX1005, 1:49-52. EX1003, ¶93.

Figure 1 shows an example:

The network arrangement makes use of a central database server 10 that supports many different smart card applications...A smart card 12, in combination with a smart card terminal 14, is used to access the central database server 10 through the network central office 16.... EX1005, 2:6-12.

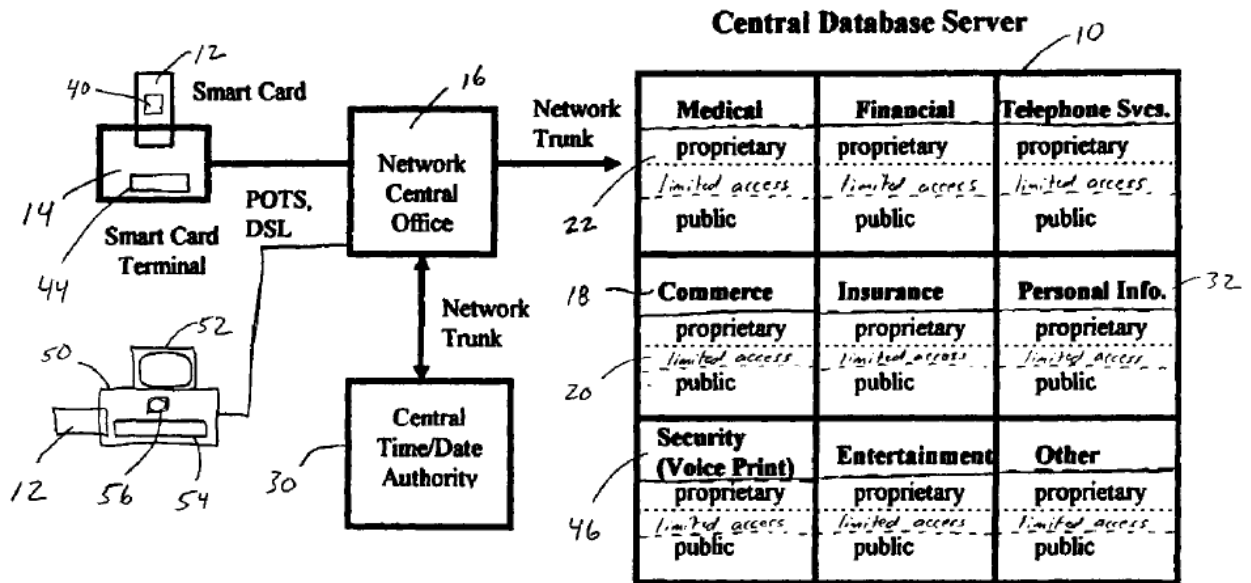


Figure 1

EX1005, Figure 1. EX1003, ¶¶94.

Bossemeyer discloses that multiple servers can make up the central database server. EX1005, 3:3-5 (“Although the central database server 10 is shown as a single server, *it is to be understood that multiple servers may comprise the central database server 10.*”). Bossemeyer describes storing different types of information (e.g., financial, insurance, medical information) in databases monitored by appropriate institutions such as credit report companies, insurers, health providers, and banks. EX1005, 3:5-16. EX1003, ¶¶95-96.

Bossemeyer’s system also includes “advance smart card terminals 50,” and “[a] smart card 12 coupled with such a terminal 50 having an established connection through the network central office 16 to the central database server 10 has the power of a typical networked computer.” EX1005, 4:9-15. EX1003, ¶¶97.

Bossemeyer further discloses controlling access to private or proprietary information. EX1005, 2:28-36 (“***Private or proprietary information*** is partitioned such that ***the owner of the information has control over how the information is transferred and used....***”). EX1003, ¶98.

Bossemeyer discloses accessing data from different partitions of the central database server using a user identification/authentication code or authorization/access code:

Once the user’s authorization has been verified, data pointers on the smart card 12 provide access to the relevant partitioned memory portions of the central database server 10. Routing circuitry...routes the data pointer to appropriate memory locations or database of the information keeper....Data from these various locations is supplied back to the smart card terminal 14....

EX1005, 3:63-4:6. See also EX1005, 4:50-65, Figure 2. EX1003, ¶92.

“The information is stored by category (medical, financial, etc.) as well as ***level of security (unrestricted, or public limited access, restricted)***.” EX1005, 2:13-27. EX1003, ¶¶99-100.

Figure 3 discloses examples of the type of information that is accessible using Bossemeyer’s networked system.

[I]nformation is stored in three levels of security: unrestricted, limited access, and restricted. In the pharmacy example,...the pharmacist may have access to the user’s digital wallet 210, medical alerts 212, and

insurance and prescription information 214. Without further authorization,...the pharmacy would not have access to the user's medical history 216.

EX1005, 5:8-15.

USER DATA ↙ 200

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

FIG. 3

EX1005, Figure 3. EX1003, ¶¶101-102.

Bossemeyer explains that different merchants may have access to information that has different levels of security. For example, “a grocer may have access to the

user's digital wallet 210 and medical alerts 212, ...but probably not be allowed to access any other user information.” EX1005, 5:16-19. “In contrast, a loan officer at a bank or automotive dealership would be allowed to access to the user's credit history 218 as well as the user's financial account balances 220.” EX1005, 5:20-22. EX1003, ¶103.

B. Ground 1: Claims 1, 5, 25, 26, 30, And 50 Are Obvious Over Merenda

1. Independent Claims 1 and 26

i. Claim 1 and 26 Preambles

To the extent the preamble is limiting, Merenda discloses and/or renders obvious the preambles of claims 1 and 26, as explained below. EX1003, ¶114.

a. [1pre-i] 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,

Merenda discloses and/or renders obvious this limitation. EX1003, ¶¶115, 123.

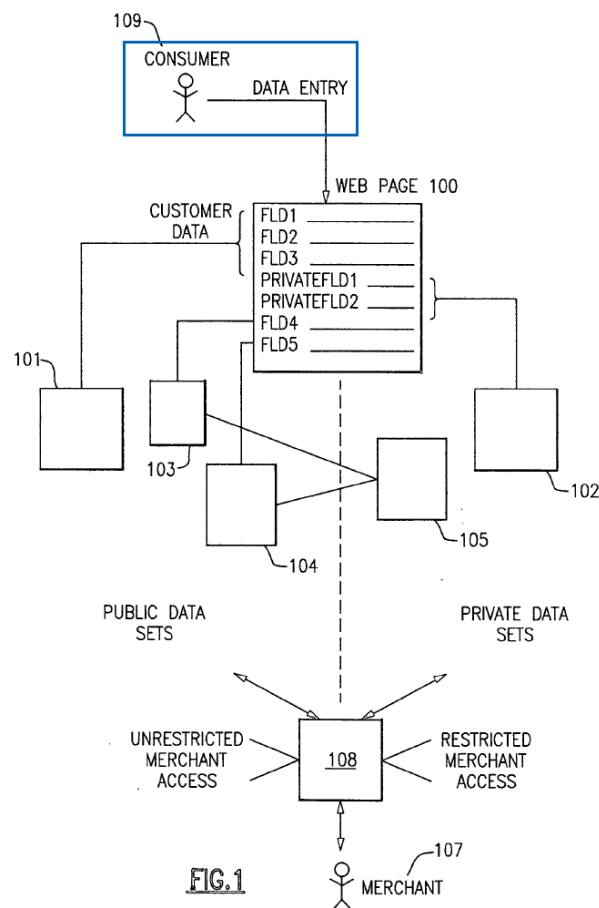
Merenda discloses a method of securing *data*. Specifically, Merenda discloses a customer entering *data* via a Web form and “separat[ing] [the data] into related records in a public and private data set” to control access to the data. EX1006, ¶7. Merenda discloses a method of securing *data* by restricting access to the *data*:

Upon *entering the data* the consumer may be prompted to indicate *whether they wish to provide merchants with access to their private data*.

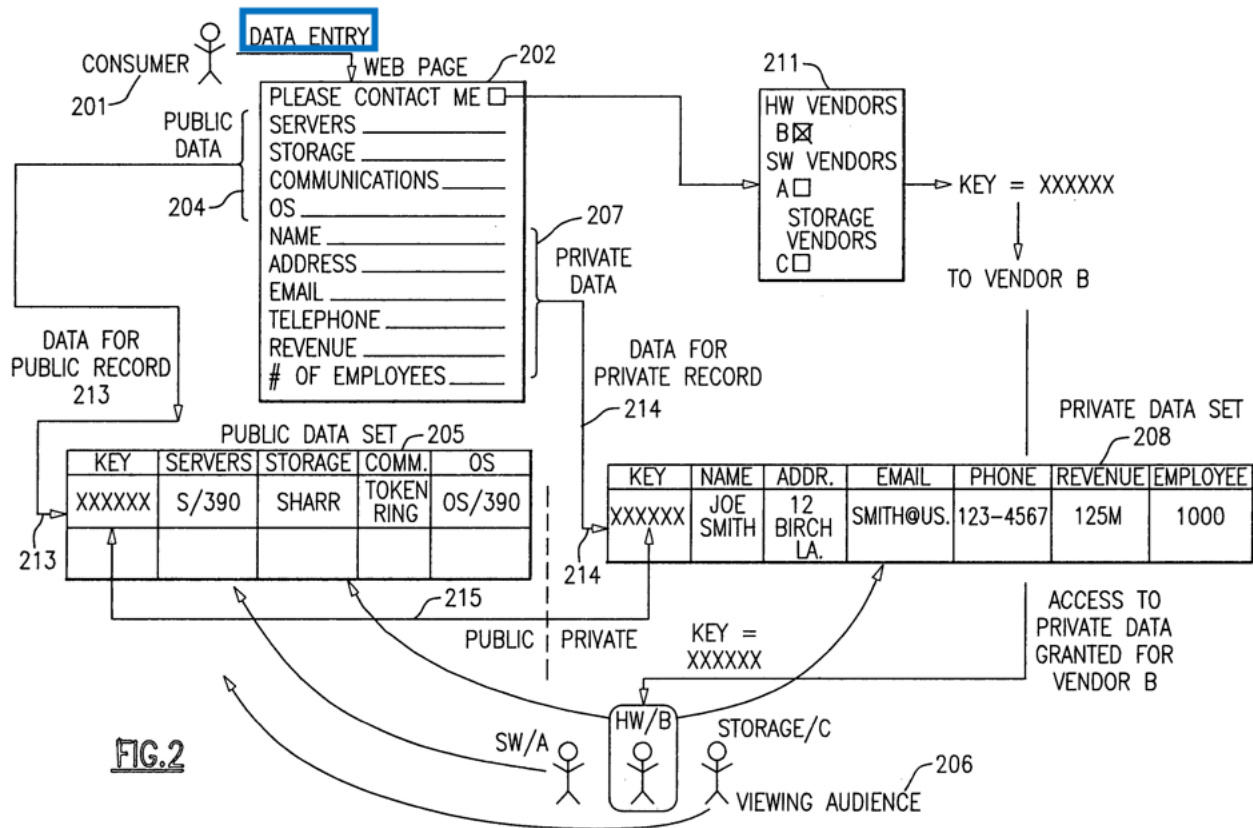
EX1006, ¶8.

As a result of the distribution of *data* elements among various public and private data sets, it is desirable to establish *a level of control over access to the public and private data* stored therein.

EX1006, ¶25. Figures 1 and 2 below show a consumer entering *data* that is separated into public and private data sets.



EX1006, Fig. 1.



EX1006, Fig. 2. EX1003, ¶¶116-118.

Merenda discloses the *data* entered into the Web form has security sensitive content, such as, security sensitive words, characters, images or data objects. EX1006, ¶23 (“Fundamental to the implementation of the present invention is the notion that 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..”), ¶24; Figures 1-2, 6. A POSITA would have understood that Merenda’s “private” data elements would include security sensitive

information because Merenda discloses restricting access to such information. A POSITA would have further recognized that such content could be presented in multiple forms, such as words for an address, a data element for a link to a bank account, or an image of a social security card. EX1003, ¶¶118-120.

A POSITA would have understood that the Web form or Web page for entering customer's personal or private data would be accessed by a consumer on a personal computer. For example, a POSITA would have found it obvious to use a personal computer, which would allow a web browser running on the personal computer to present the web page or web form to the user. A POSITA would have further understood that entering personal or private information via a personal computer would be more secure—compared, for example, with entering sensitive information to a public computer—and would reduce the risk of compromising the information, consistent with Merenda's interest in "protecting the privacy interests of individual user's [sic]." EX1006, ¶5. Furthermore, a POSITA would have understood that individuals store their personal information on their own personal computer, therefore it would be more readily accessed on a personal computer. EX1003, ¶¶121-122.

b. [26pre-i] A computer readable storage medium containing programming instructions for securing *data* on a personal computer having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein,

Merenda discloses and/or renders obvious this limitation. EX1003, ¶¶124, 127.

As discussed in Section VI.B.1.i.a, Merenda discloses and/or renders obvious a method for “securing *data* on a personal computer having security sensitive content represented by one or more security sensitive words, characters, images or data objects.” EX1003, ¶125.

Merenda also discloses “at least one *program storage device readable by a machine*, tangibly embodying at least one *program of instructions* executable by the machine to perform the capabilities of the present invention....” EX1006, ¶50. Merenda further discloses “computer readable program code means,” *i.e.*, programming instructions:

The present invention can be included in an article of manufacture (*e.g.*, one or more computer program products) having, for instance, *computer usable media*. The media has embodied therein, for instance, *computer readable program code means* for providing and facilitating the capabilities of the present invention.

EX1006, ¶49, *See also* EX1006, Claim 31. EX1003, ¶126.

Merenda specifically discloses using the computer readable code (*i.e.*, “the programming instructions”) to separate data into public and private sets (*i.e.*, “securing input data”). EX1006, Claim 31 (disclosing “computer readable program code for separating a data record into a public data record stored in a public data set and a private data record stored in a private data set.”). EX1003, ¶126.

c. [1/26pre-ii] said security sensitive content having a plurality of security levels, each security level having an associated security clearance,

Merenda discloses and/or renders obvious this limitation. EX1003, ¶¶128, 137.

Merenda discloses a *plurality of security levels* for the private data sets and allowing access to that data based *associated security clearances*. EX1006, ¶25 (“As a result of the distribution of data elements among various public and private data sets, it is desirable to *establish a level of control over access to the public and private data* stored therein.”). Public data may be available without restriction, while private or sensitive data would only be available based on the associated security level(s) indicated, for example, by the consumer (e.g., the individual who provides the data) or the level of control indicated for the data set:

[A] public data set is available, without restriction, to the entire population of Internet users, or,..., to a select subset of merchants 107
....The present invention is directed toward providing the level of control 108 required in keeping the public and private data separate,

and *allowing access to the private data either at the explicit direction of the consumer 109 (the individual that is the subject of the public and private data) or in such a manner as to protect the privacy concerns of the consumer.*

EX1006, ¶25.

The public data set does not impose any access restrictions to its viewing audience 206. Other items of information, such as the name, location, phone, e-mail, revenue, number of employees, may for our purposes, be designated as a single record 214 of private data elements 207 and as such will be stored separately in *a private data set 208 which imposes certain restrictions on access by the viewing audience 206.*

EX1006, ¶26; *id.*, ¶¶10-13, 23, 34-35. EX1003, ¶¶129-134.

Merenda discloses, and/or renders obvious, a plurality of security levels for the private data sets. For example, someone requesting information, e.g., a merchant, can have access only to certain portions of the private information. That is, a merchant can access certain selected private data sets (e.g., private data sets having a *first security level*, such as *name, address, phone number, e-mail*), but cannot access other private data sets (e.g., private data sets having a *second (higher) security level*, such as *revenue, credit card*).

[A]ccess 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.*

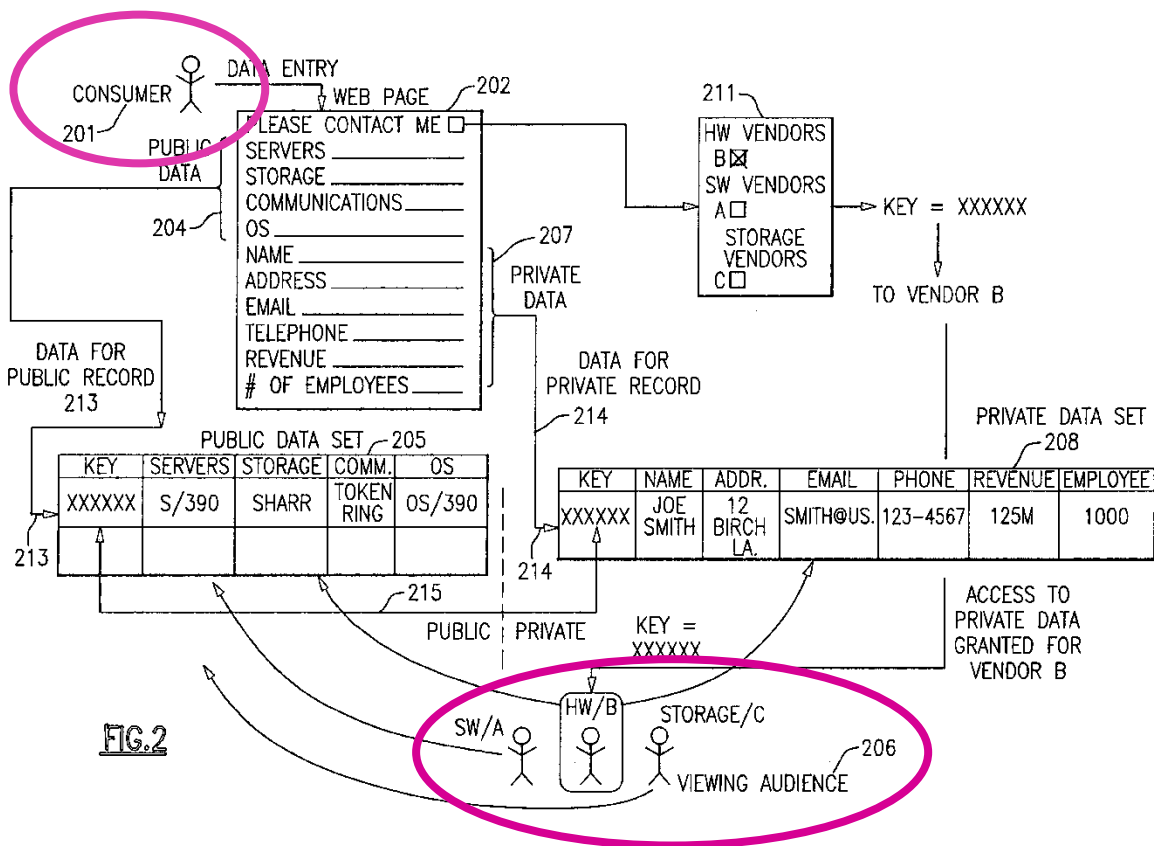
EX1006, ¶29. EX1003, ¶135.

Further, Merenda discloses separating data at any level of granularity potentially resulting in multiple private data sets and providing access to reconstructed data based any desired level of granularity. *Id.*, ¶24 (“As previously noted, such separation of data elements may be accomplished using known techniques to *any desired level of granularity, resulting potentially in multiple public and private data sets...*”), ¶29 (“[A]ccess to the data elements in the private data set may be made on an element-by-element basis...”), ¶¶8-10, 23-26, 29-30, 34-36. EX1003, ¶136.

d. [1/26pre-iii] 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**,

Merenda discloses and/or renders obvious this limitation. EX1003, ¶¶138, 154.

First, Merenda discloses that *multiple individuals* can provide and access information, as illustrated in Figure 2:



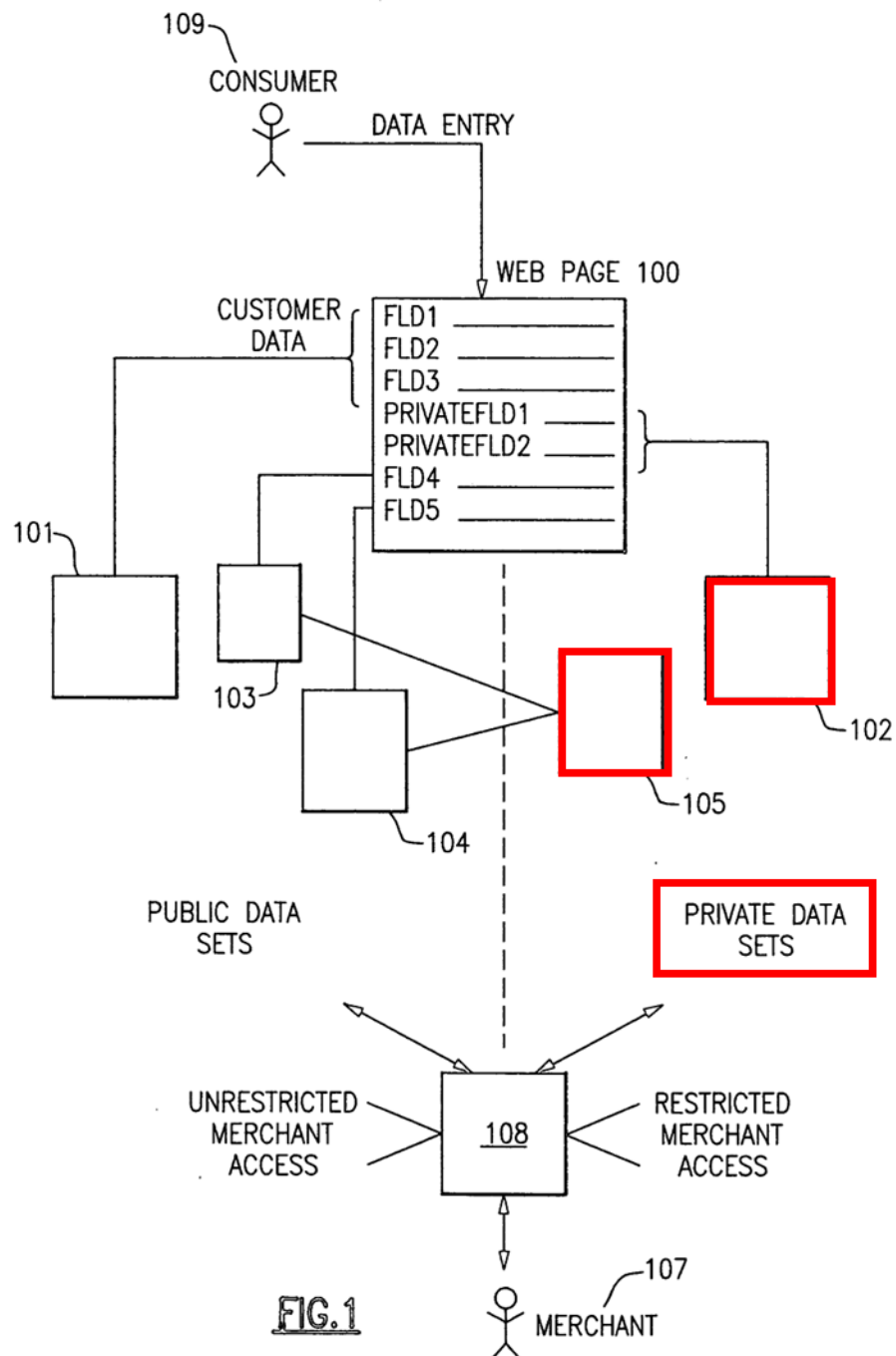
EX1006, Figure 2. EX1003, ¶139.

For example, as discussed in Sections VI.B.1.i.a and VI.B.1.i.b, a POSITA would have found it obvious to use Merenda’s method of entering user data through a web page/web form via a personal computer. A POSITA would have understood that Merenda’s system would have accommodated multiple customers entering data into web forms via their personal computers (e.g., a plurality of other computers). EX1003, ¶140.

Additionally, Merenda describes a “viewing audience 206,” such as merchants, that access the information stored in Merenda’s system. EX1006, ¶26

(“The public data set does not impose any access restrictions to its *viewing audience 206*. Other items of information...will be stored separately in a private data set 208 which imposes certain restrictions on access by the *viewing audience 206*.”). A POSITA would have recognized that an “audience” typically consists of more than one person. A POSITA would have further recognized that multiple merchants would not have used the same computer to implement Merenda’s system, and in fact would have used multiple computers (*e.g.*, a plurality of other computers). Additionally, this system of computers would include databases and a POSITA would have understood these databases to have been implemented on one or more computers (*e.g.*, *other computers*). See EX1006, ¶24 (“The public 101 and private 102 data sets are, in a preferred embodiment, relational databases...”); EX1019, 2:58-59 (“System 10 comprises a database computer 12 storing a central database 14”), 3:10-12 (“[T]he database containing the information is stored in central database 14 in database computer 12”). EX1003, ¶¶141-144.

Second, Merenda teaches private data sets and that the “private data sets are...*relational databases* [plural]” (EX1006, ¶24), *i.e.*, a *plurality of extract stores*, for respective ones of said *plurality of security levels*. These private data sets, which are relational databases, are illustrated in Figure 1:



EX1006, Fig. 1.

[S]eparation of data elements may be accomplished using known techniques to any desired level of granularity, resulting *potentially in*

multiple public and *private data sets*....The public 101 and *private 102 data sets* are, in a preferred embodiment, relational databases....
EX1006, ¶24. EX1003, ¶¶145-146.

Further, Merenda discloses and/or renders obvious that private data sets can be assigned different *security levels*. Merenda teaches that a merchant may be granted limited access to certain selected private data (e.g., *private data sets* having *first security level*, such as *name, address, phone number, e-mail*), but cannot access other private data sets (e.g., *private data sets* having a *second (higher) security level*, such as *revenue, credit card*):

*[A]ccess 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. EX1003, ¶147.

As discussed above, Merenda suggests private data sets are stored in *databases* (plural), meaning there is more than one database for the private data sets (e.g., *a plurality of extract stores*). EX1006, ¶24 (“The public 101 and private 102 data sets are, in a preferred embodiment, relational databases...”). A POSITA would have found it obvious to store private datasets with different *security levels* in separate databases for better control of the secure data. This would enable the

database(s) holding private data sets with *first security level* data (such as *name, address, phone number, email*) to have different security measures than the database(s) holding private data sets with *second security level data* (such as *revenue, credit card*). A POSITA would have recognized that if a merchant has access to limited pieces of the stored information, it would be obvious to store these pieces in separate databases or locations from one another. EX1003, ¶¶148-153.

e. [1/26pre-iv] said personal computer, said other computers and said extract data stores operatively connected together over a communications network [, the programming instructions] comprising:

Merenda discloses and/or renders obvious this limitation. EX1003, ¶¶155, 157.

As discussed in Section VI.B.1.i.d, Merenda discloses and/or renders obvious a method of securing data deployed in a distributed computer system. EX1003, ¶138.

Additionally, Merenda discloses its distributed computer system being connected over a communications network, e.g., the internet. EX1006, ¶25 (“[A] public data set is available, without restriction, to the entire population of **Internet users...**”), ¶5 (“[T]he solution should...allow an Internet user to proactively indicate their desire to selectively provide their private data to selected merchants while their public data...”), ¶3. EX1003, ¶156.

ii. [1/26a] accepting data input which includes security sensitive content via said personal computer;

Merenda discloses and/or renders obvious this limitation. EX1003, ¶¶158, 163.

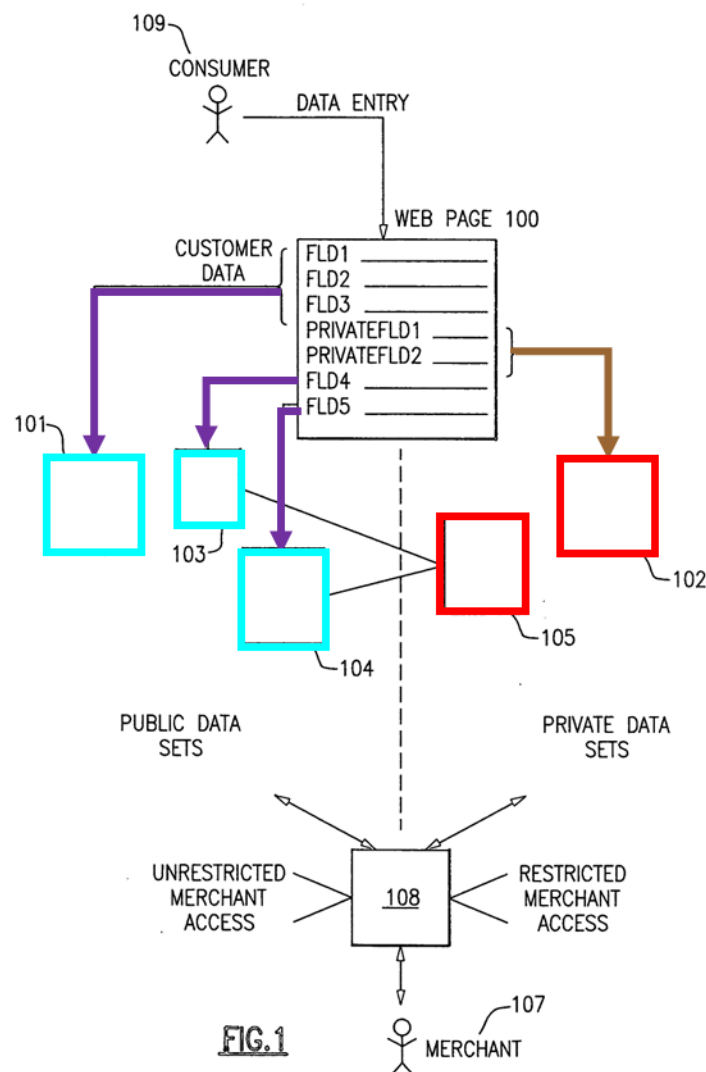
As discussed in Section VI.B.1.i.a, Merenda discloses a web page or web form accepting data input by a customer or user, which a POSITA would have found obvious to occur at a personal computer, wherein said data input includes security sensitive content. EX1003, ¶¶159-162.

iii. [1/26b] extracting said security sensitive content to obtain **extracted data for each corresponding **security level** and **remainder data**;**

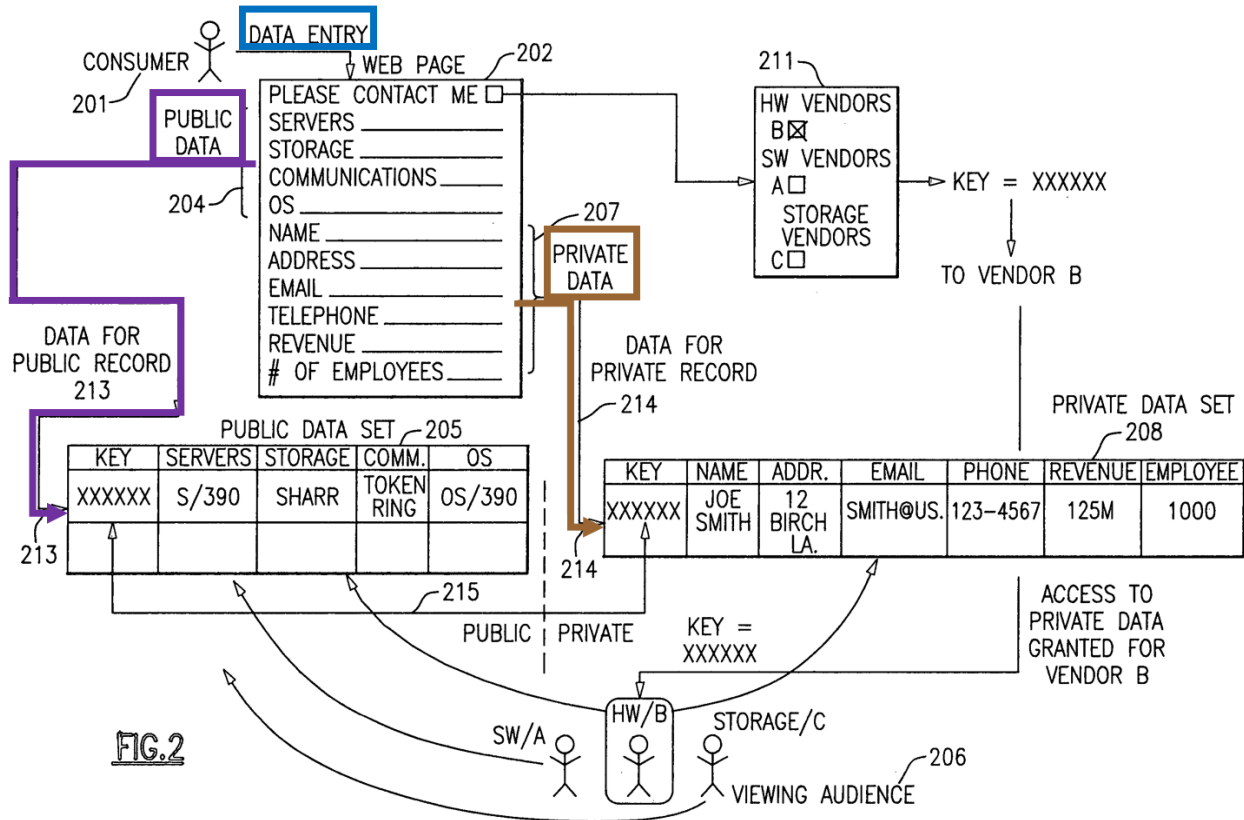
Merenda discloses and/or renders obvious this limitation. EX1003, ¶¶164, 172.

Merenda discloses extracting, e.g., parsing, security sensitive content, e.g., *private elements*, from *user data* to obtain subsets of *extracted data*, e.g., *address*, *credit card* or *social security number* and *remainder data*, e.g., *non-private elements*. EX1006, ¶23 (“[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.”), ¶24 (“[S]eparation of data

elements may be accomplished using known techniques to any desired level of granularity, resulting potentially in multiple public and private data sets”), ¶31 (“[A] web form may generate a number of data sets 301a-d....Any of these data sets may be designated as including private data, and the *remaining data sets* include public data.”), Figures 1-3.



EX1006, Figure 1.



EX1006, Figure 2. EX1003, ¶¶165-168.

Further, Merenda discloses that private data (e.g., extracted data) has a plurality of *security levels*, and the system extracts private data for each *corresponding security level*. For example, someone requesting information, e.g., a merchant, can have access *only to certain portions of the private information*. That is, the merchant can access certain selected private data sets (e.g., private data sets having a *first security level*, such as *name, address, phone number, e-mail*), but cannot access and extract other private data sets (e.g., private data sets having a *second (higher) security level*, such as *revenue, credit card*).

[A]ccess 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. EX1003, ¶¶169-171.

- iv. [1/26c] 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,

Merenda discloses and/or renders obvious this limitation. EX1003, ¶¶173, 180.

As discussed in Sections VI.B.1.i.d and VI.B.1.iii, Merenda discloses and/or renders obvious parsing data into *public data sets* (e.g., *remainder data*) and *private data sets* (e.g., *extracted data*) and storing the *extracted data*, for each corresponding *security level*, as respective *private data sets* (e.g., in *databases (extract stores)*). EX1003, ¶¶174-176.

As explained above, Merenda discloses separating the data elements at any desired level of granularity resulting in multiple *private data sets*. See, EX1006, ¶24. Additionally, Merenda discloses providing differing levels of access, including determining access level on an element-by-element basis. *Id.*, ¶29 (“[A]ccess 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.”). Merenda discloses a merchant accessing selected private data sets of a certain security level (e.g., a private data set having a *first security level*, such as *name, address, phone number, e-mail*) but not allowing the merchant to access other private data sets (e.g., private data sets having *second (higher) security level*, such as *revenue, credit card*). EX1003, ¶¶176-177.

Merenda suggests private data sets are stored in *databases* (e.g., *extract stores*). EX1006, ¶24 (“The public 101 and *private 102 data sets* are, in a preferred embodiment, relational databases...”). As discussed in Section VI.B.1.i.d, it would be obvious to store private datasets with different *security levels* in separate databases for better control of the secure data. EX1003, ¶178.

Additionally, Merenda discloses *public data sets* (e.g., *remainder data*). In Merenda, *public data sets* can be databases and a POSITA would have understood these databases to have been implemented on a computer(s) (e.g., *other computers*). See EX1006, ¶24 (“The *public 101* and private 102 data sets are...relational databases...”); EX1019, 2:58-59 (“[A] database computer 12 storing a central database 14”), 3:10-12 (“[T]he database [] is stored in central database 14 in database computer 12”). EX1003, ¶179.

- v. [1/26d] 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**.

Merenda discloses and/or renders obvious this limitation. EX1003, ¶¶181, 190.

As discussed in Sections VI.B.1.i.d and VI.B.1.iii, Merenda discloses and/or renders obvious parsing data into **private data sets** (e.g., **extracted data**) and **public data sets** (e.g., **remainder data**) and storing the **private data sets** in **extract stores** and the **public data sets** in database computers. EX1003, ¶188.

Merenda discloses permitting full or partial reconstruction of data by combining the public and part or all of the private data, when the requester has the **associated security clearance**. *Id.*, ¶7 (“The private records would be **available only per the indication of the consumer** to the merchant in the population.”), ¶10 (“**[U]pon designation by the consumer, the various logically linked records in public and private tables for that consumer may be collected and assembled into an output Web page....**”The merchant for whom access has been indicated is provided either via e-mail or otherwise, **with a hyperlink to the coded URL** thereby enabling the selected merchant to access both the public and private data.”), ¶25 (“The present invention is directed toward providing the level of control 108 required in keeping the public and private data separate, and **allowing access to the**

private data either at the explicit direction of the consumer 109 (the individual that is the subject of the public and private data) or in such a manner as to protect the privacy concerns of the consumer.”), ¶30 (“[T]he combined information including the contact information from the private data set and the technical data from the public data set may be provided to the merchant by way of a customized Web page....”). EX1003, ¶¶182-185.

Further, Merenda discloses permitting full or partial reconstruction of data based on any desired level of granularity. *Id.*, ¶29 (“[A]ccess 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.”), ¶¶8-10, 23-26, 29-30, 34-36. EX1003, ¶¶182-188.

A POSITA would have understood that to reconstruct (e.g., assemble) data, which includes private data sets, Merenda’s method would access the respective *extract stores* for the corresponding *security levels* (e.g., highest level for full reconstruction of data), which would suggest using the *associated security clearance* to access the corresponding extract store. EX1003, ¶189.

2. Dependent Claims 5, 25, 30, and 50

i. [5/25pre] A method as claimed in claim 1.

Merenda discloses and/or renders obvious claim 1. *See* Section VI.B.1.
EX1003, ¶191.

ii. [30/50pre] A computer readable storage medium containing programming instructions as claimed in claim 26.

Merenda discloses and/or renders obvious claim 26. *See* Section VI.B.1.
EX1003, ¶192.

iii. [5/30a] permitting full or partial reconstruction of said data occurs at one of said personal computer and said other computers.

Merenda discloses and/or renders obvious alone this limitation for the reasons discussed in Section VI.B.1.v. As discussed above, Merenda discloses providing partial access to data and/or providing full access to the data. Merenda discloses permitting reconstruction of the data into an output Web page provided to a user. EX1006, ¶¶8-10, 23-26, 29-30, 34-36. A POSITA would have understood that the output Web page would be presented at the merchant computer (e.g., *said other computer*), when a merchant has requested access to the stored data. Additionally, a POSITA would have understood that the consumer entering the data on their *personal computer* would have also been able to access the data (e.g., *reconstruct*

the data) on their *personal computer* after entering it, for example, in case the consumer wanted to update the data. EX1003, ¶¶193-202.

iv. [25/50a] wherein extracting occurs either automatically or manually with operator input.

As an initial matter, the claimed extraction occurring “automatically or manually with operator input” does not impose a narrowing limitation. That is, the “extracting” will either happen automatically (without operator input) or manually (with operator input). In any case, Merenda discloses and/or renders obvious this limitation. EX1003, ¶¶203-206, 208.

As discussed in Section VI.B.1.iii, Merenda discloses and/or renders obvious extracting security sensitive content. Merenda discloses the administrator of a web page setting the parameters of the data (private and non-private), and the system *automatically extracting* the data. EX1006, ¶23 (“[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.”), ¶24, ¶31 (“[A] web form may generate a number of data sets 301a-d including demographics 301a, server data 301b, user data 301c, and cost data 301d. Any of

these data sets may be designated as including private data, and the remaining data sets include public data.”), Figures 1-3. EX1003, ¶207.

C. Ground 2-3: Claims 1, 5, 25, 26, 30, And 50 Are Obvious Over Bossemeyer (Ground 2) Or Bossemeyer With Merenda (Ground 3)

1. Independent Claims 1 and 26

i. Claim 1 and 26 Preambles

To the extent the preamble is limiting, Bossemeyer alone or in combination with Merenda renders obvious the preambles of claims 1 and 26, as explained below. EX1003, ¶¶209, 319.

a. [1pre-i] 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,

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation. EX1003, ¶¶210, 222, 320, 325.

Bossemeyer discloses a method of securing *data*. Specifically, Bossemeyer discloses partitioning sensitive data to control how the data is transferred and used. EX1005, 2:28-30 (“Private or proprietary information is partitioned such that *the owner of the information has control over how the information is transferred and used.*”). Bossemeyer further discloses restricting access to sensitive data:

The information contained within the central database server is associated with the user identification codes on the smart cards 12 such that it can be classified as public information available to all the

world; **limited access information** available to persons or selected groups with a user authentication code; or **proprietary information** accessible only by the owner of the information or a group with privileges to that directory information. Besides **restricting others access to a smart card holder's information/data**, the information or data within the server 10 can limit options available to cardholders.

EX1005, 2:40-50; Figures 1, 3 (reproduced below).

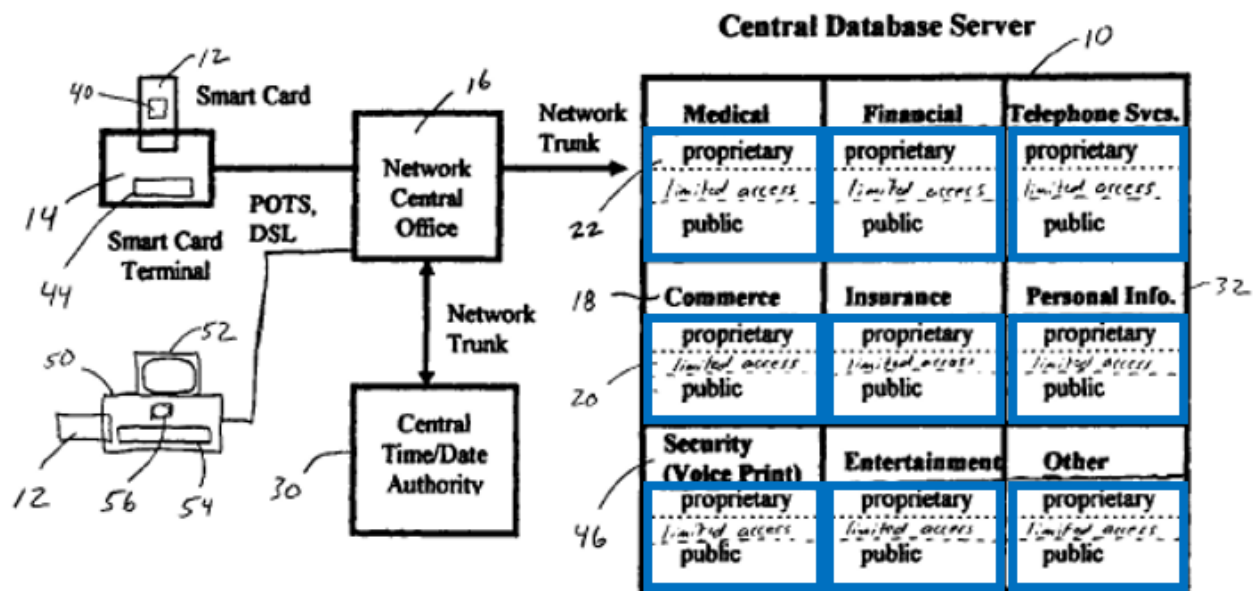


Figure 1

EX1005, Figure 1.

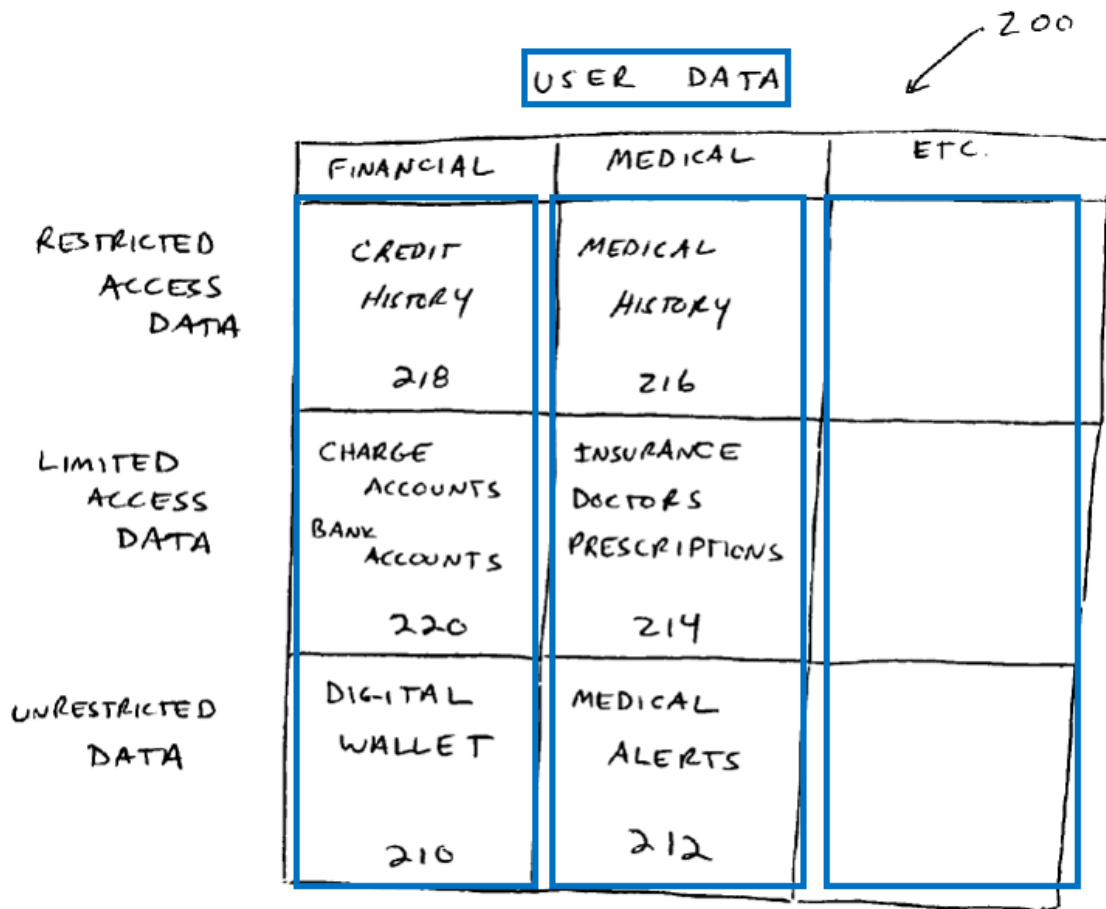


FIG. 3

EX1005, Figure 3. EX1003, ¶¶211-215.

A POSITA would have understood that Bossemeyer’s “limited access information” and/or “proprietary information” would have included security sensitive information, such as, words, characters, images or data objects, because Bossemeyer discloses restricting access to such information. Bossemeyer discloses different types of security sensitive information, as shown, for example in Figure 3, including a user’s medical history 216, prescription information 214, credit history

218, and bank accounts 220. A POSITA would have understood that medical history is highly sensitive information and can include images of medical charts, insurance information can include images of the user's insurance card, prescription information can include the names of the drugs prescribed to the user, etc. *See, e.g.*, EX1005, 3:25-27 (“[P]ersonal information 32 such as digitized photograph...can be included as part of a photo identification such as a driver's license.”). EX1003, ¶¶216-217.

A POSITA would have also found it obvious that Bossemeyer's method secures other types of security sensitive words, characters, images, or data objects. For example, Figure 3 of Bossemeyer includes additional columns for storing user data with a restricted- or limited-access security level (e.g., financial data). Similarly, Figure 1 shows different types of data that include security sensitive information, e.g., stored as proprietary or limited access data. EX1003, ¶218.

Bossemeyer's system utilizes “advance smart card terminals 50,” that have the power of a typical network computer. EX1005, 4:9-11 (“*[A]dvance smart card terminals 50* which include a *display unit 52, a keyboard 54, and a pointing device such as a track ball 56 or mouse.*”), 4:9-15 (“[a] smart card 12 coupled with such a terminal 50 having an established connection through the network central office 16 to the central database server 10 has the power of a typical networked computer.”). A POSITA would have understood that the data displayed on advance smart card

terminals 50 are secure data as part of Bossemeyer's system. Bossemeyer also discloses that "the user data becomes populated when the user subscribes as part of the smart card activation process." EX1005, 5:28-30. A POSITA would have found it obvious to use a personal computer to enter user data, which would be conveniently stored on the personal computer, into Bossemeyer's system. EX1003, ¶¶219-221.

For Ground 3, to the extent Digital Doors Inc. ("Patent Owner") argues Bossemeyer does not disclose and/or render obvious this limitation, Merenda does for the reasons discussed in Section VI.B.1.i.a. EX1003, ¶321.

For example, Merenda discloses securing data by, for example, separating the *data* into public and private or sensitive data sets and allowing access to that data like Bossemeyer. EX1006, ¶¶23-25 ("As a result of the distribution of data elements among various public and private data sets, it is desirable to establish a level of control over access to the public and private data stored therein."). Additionally, a POSITA would have found it obvious to use Merenda's method of entering user data through a web page or web form via a personal computer in the combined Bossemeyer/Merenda system, for example, when a user subscribes to Bossemeyer's smart card services. EX1005 (Bossemeyer), 5:28-30 ("the user data becomes populated when the user subscribes as part of the smart card activation process"). A POSITA would have understood that a user would have used a personal computer,

which would allow a web browser running on the personal computer to present the web page or web form to the user. EX1003, ¶¶322-323.

As discussed in Section VI.C.1.vi, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in the combination. EX1003, ¶324.

b. [26pre-i] A computer readable storage medium containing programming instructions for securing data on a personal computer having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein,

Bossemeyer renders obvious alone (or with Merenda for Ground 3) this limitation. EX1003, ¶¶223, 228, 326, 329.

As discussed in Section VI.C.1.i.a, Bossemeyer discloses and/or renders obvious a method for “securing data having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein.” A POSITA would have understood that Bossemeyer’s method would have been implemented using programming instructions and that these programming instructions would be stored in a computer readable storage medium. EX1003, ¶224.

For example, Bossemeyer’s method is performed in a computer system: Bossemeyer’s network arrangement for securing data is implemented over an interconnected network of computers, i.e., a computer system having a plurality of computers. EX1005, 1:44-52, 4:11-15, 4:19-22. Bossemeyer’s computer system

would execute programming instructions, which would require storage in a storage medium. To implement its computerized method, Bossemeyer's computer system would read the programming instructions from the storage medium and execute them, for example, in an execution unit. EX1003, ¶¶225-227.

For Ground 3, to the extent Patent Owner argues Bossemeyer does not render obvious this limitation, Merenda does for the reasons discussed in Section VI.B.1.i.b. EX1003, ¶327.

As discussed in Section VI.C.1.vi, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in the combination. EX1003, ¶328.

c. [1/26pre-ii] said security sensitive content having a plurality of security levels, each security level having an associated security clearance,

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation. EX1003, ¶¶229, 237, 330, 333.

Bossemeyer discloses securing sensitive content by restricting access to the sensitive content with a plurality of security levels, e.g., limited access data or restricted access data, each having an associated security clearance:

The information contained within the central database server...can be classified as public information available to all the world; *limited access information* available to persons or selected groups with a user authentication code; or *proprietary information* accessible only by the

owner of the information or a group with privileges to that directory information. Besides *restricting others access to a smart card holder's information/data*, the information or data within the server 10 can limit options available to cardholders.

EX1005, 2:40-50.

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)*... [A] merchant may require access to a user's credit....This information may be partitioned *in the limited access region 20* of commercial transaction applications 18.

EX1005, 2:17-27; Figures 1, 3 (reproduced below).

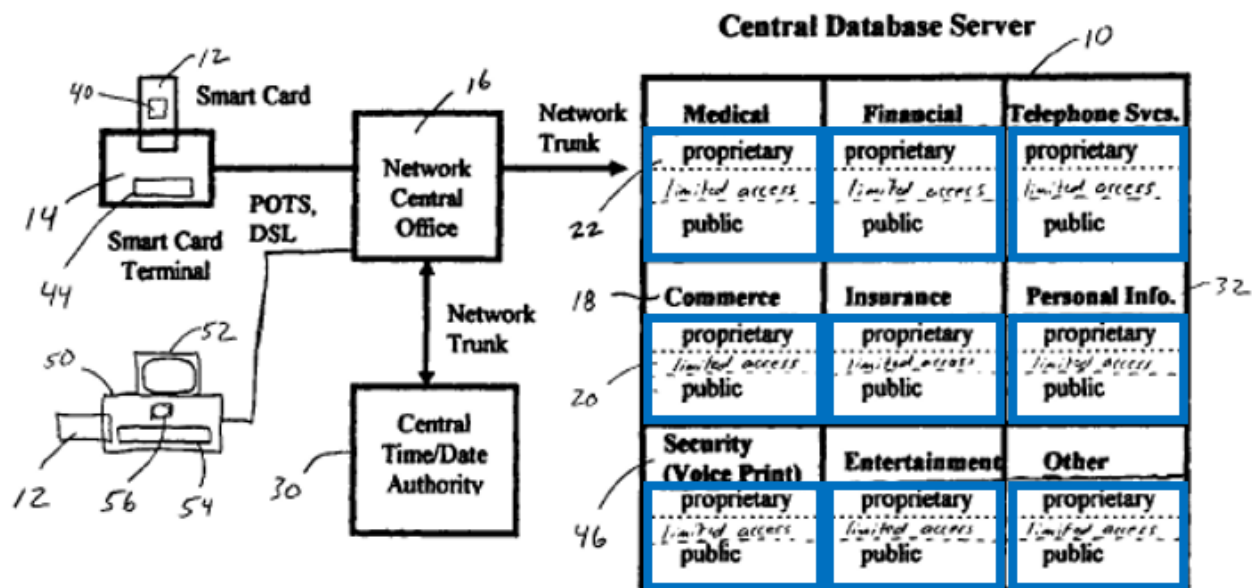


Figure 1

EX1005, Figure 1.

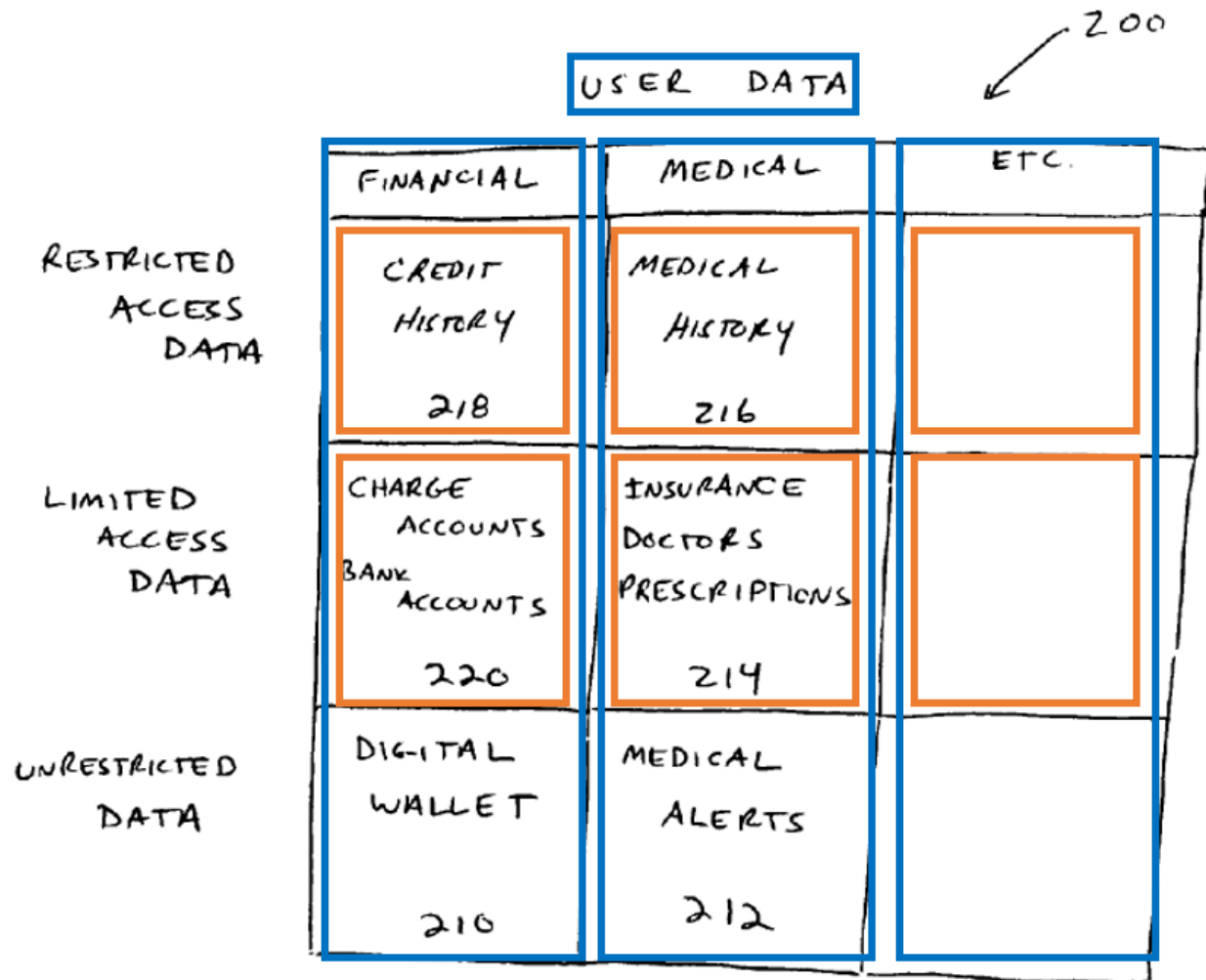


FIG. 3

EX1005, Figure 3. EX1003, ¶¶230-232

Moreover, Bossemeyer discloses controlling how the security sensitive content is transferred and used. EX1005, 2:28-30 (“Private or proprietary information is partitioned such that *the owner of the information has control over how the information is transferred and used.*”). Specifically, in Bossemeyer, each *security level* has an *associated security clearance* e.g., *user*

identification/authentication code or *authorization/access code* associated with a particular *security level*. Specifically, Bossemeyer teaches that “[d]ifferent *user identification codes*, or data pointers, provided by smart cards 12 *allow access to partitions in the database.*” EX1005, 2:38-40; 3:63-4:6. Bossemeyer teaches that data with a *limited access security level* is “available to *persons or selected groups with a user authentication code*” (EX1005, 2:44-45), while data with a *proprietary information security level* is “accessible only by the *owner of the information or a group with privileges* to that directory information.” *Id.*, 2:45-47; 4:50-58. For example, a merchant with a corresponding merchant code can access information available to the particular merchant:

The network server 10, 110 validates the user identification by decrypting the *authorization code*. This information is then cross-referenced with the *merchant code* to identify *the information available to the merchant*. The merchant can then view the information stored within the server 10, 110, upload/download information, and perform transactions....

EX1005, 4:59-65; Figure 2. EX1003, ¶¶233-235.

In another example, Bossemeyer explains that a pharmacist will have clearance to access data with *limited access security level*, e.g., a user’s *insurance and prescription information 214*, but will not have clearance to access data with *proprietary information security level*, e.g., a user’s *medical history 216*.

[I]nformation is stored in three levels of security: unrestricted, *limited access, and restricted*. In the pharmacy example, once the user's authentication code and merchant code have been verified by the system, the pharmacist may have access to the user's digital wallet 210, medical alerts 212, and *insurance and prescription information 214*. Without further authorization, however, the pharmacy would not have access to the user's *medical history 216*.

EX1005, 5:8-15.

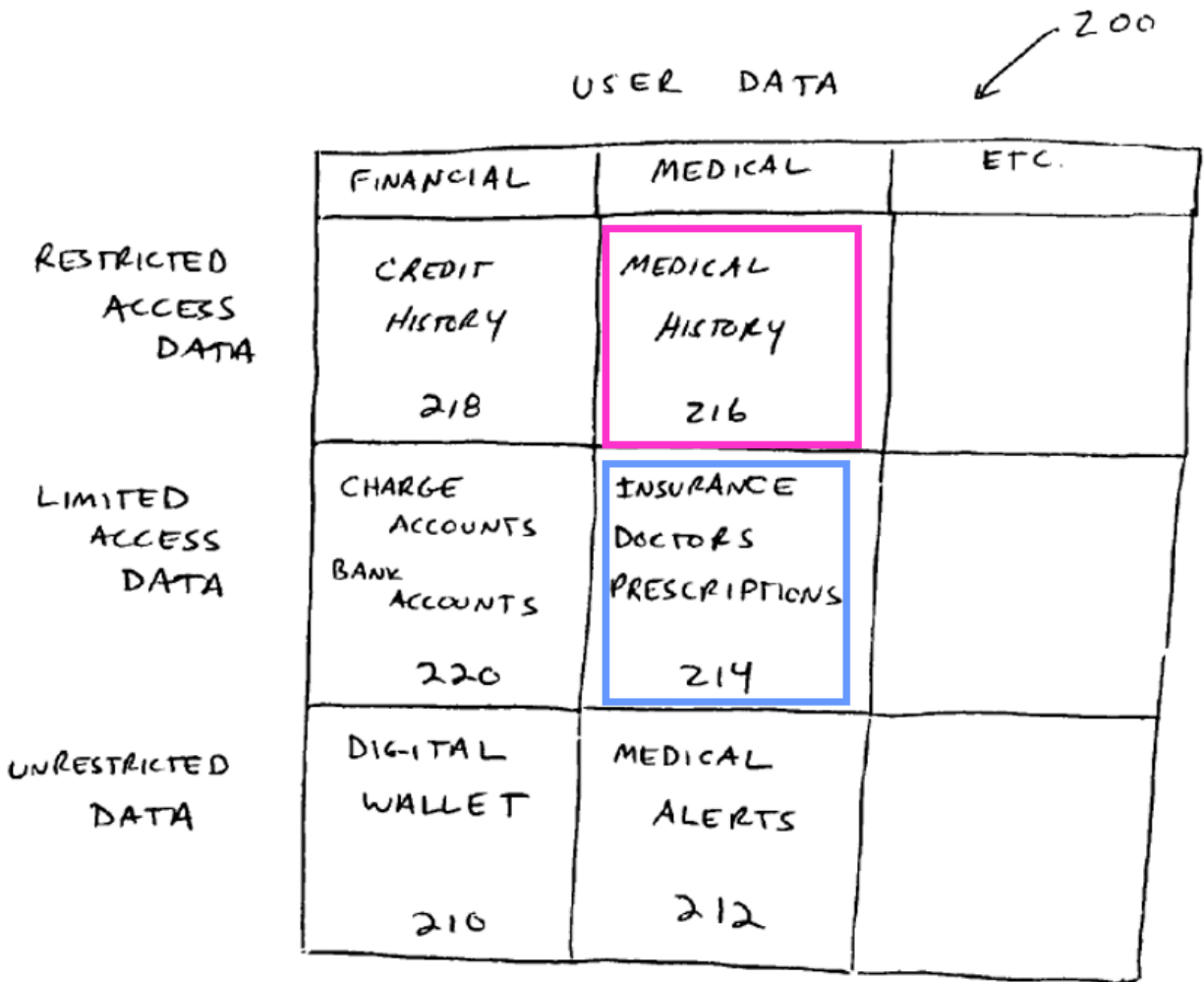


FIG. 3

EX1005, Figure 3. EX1003, ¶236.

For Ground 3, to the extent Patent Owner argues Bossemeyer does not disclose and/or render obvious this limitation, Merenda does for the reasons discussed in Section VI.B.1.i.c. As discussed in Section VI.C.1.vi, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in the combination. EX1003, ¶¶331-332.

d. [1/26pre-iii] 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**,

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation. EX1003, ¶¶238, 256, 334, 337.

First, Bossemeyer discloses an interconnected network of computers, *i.e.*, a distributed computer system having a plurality of computers, including smart card terminals that have the power of a typical networked computer and Bossemeyer's interconnected network of computers. EX1005, 1:44-49 (“[The] invention describes a network arrangement which is readily accessible from different types of smart card terminals....***The network connections are facilitated by the present telephone network or an interconnected network of computers such as the Internet.***”), 4:11-15 (“A smart card 12 coupled with such a terminal 50 having an established connection through the network central office 16 to the central database server 10 has the power of ***a typical networked computer.***”), 4:19-22 (“It is contemplated that such smart card ‘docking stations’ could transform hotel room entertainment centers or airplane seat video screens into ***networked computers*** with the insertion of a user's smart card.”), 4:25-28 (“[T]he network arrangement of FIG. 2 is implemented over ***an interconnected network of computers*** such as the Internet 100 as well as or alternatively to the traditional telephone network 102.”). EX1003, ¶¶239-244.

Additionally, Bossemeyer's system includes a central database server, which can include multiple servers (e.g., *plurality of other computers*). EX1005, Abstract ("The network arrangement includes a communications network connected to at least one smart card terminal, and a *central database server*), 1:44-52, 2:6-12, 2:13-16 ("The *central database server 10* includes partitioned memory...as well as a microprocessor for processing data received from and transmitted to the smart card terminal 14."); 3:3-5 ("[M]ultiple servers may comprise the central database server 10."). EX1003, ¶¶245-247.

Second, Bossemeyer discloses that the central database server includes a plurality of memories (e.g., *plurality of extract stores*) for respective ones of said *plurality of security levels* operatively coupled over a communications network. Specifically, Bossemeyer's computer system includes a central database server with a memory that is broken into different partitions that can be located in different servers/databases, *i.e.*, *a plurality of extract stores*. EX1005, 2:13-16 ("The *central database server 10* includes *partitioned memory*...as well as a microprocessor for processing data received from and transmitted to the smart card terminal 14."); 3:3-9 ("Although the central database server 10 is shown as a single server, it is to be understood that multiple servers may comprise the central database server 10. For example, in the merchant transaction discussed above, the purchaser's credit files are more likely to be stored in a database monitored by the credit reporting

companies such as TransUnion or Equifax, as opposed to the central database server 10.”). EX1003, ¶¶248-250.

Bossemeyer’s *memory partitions* are security-controlled because they store data having respective *levels of security/accessibility*:

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)*.

Thus, for example, in a retail purchase application 18, 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, 2:17-27. EX1003, ¶251.

Therefore, Bossemeyer teaches controlling the access of sensitive information, e.g., by allowing unrestricted or *limited access* or *restricting access* to the sensitive information. Accordingly, Bossemeyer’s memory partitions have security access controls. Figures 1 and 3 illustrate the *memory partitions (plurality of extract stores)* with limited-access and restricted information.

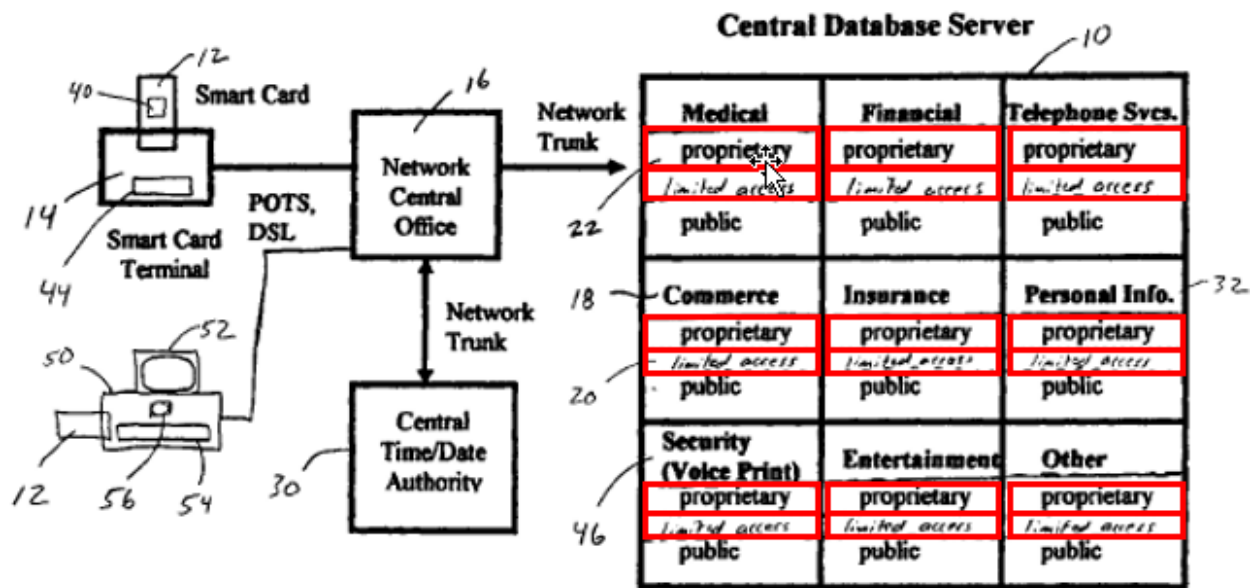


Figure 1

EX1005, Figure 1.

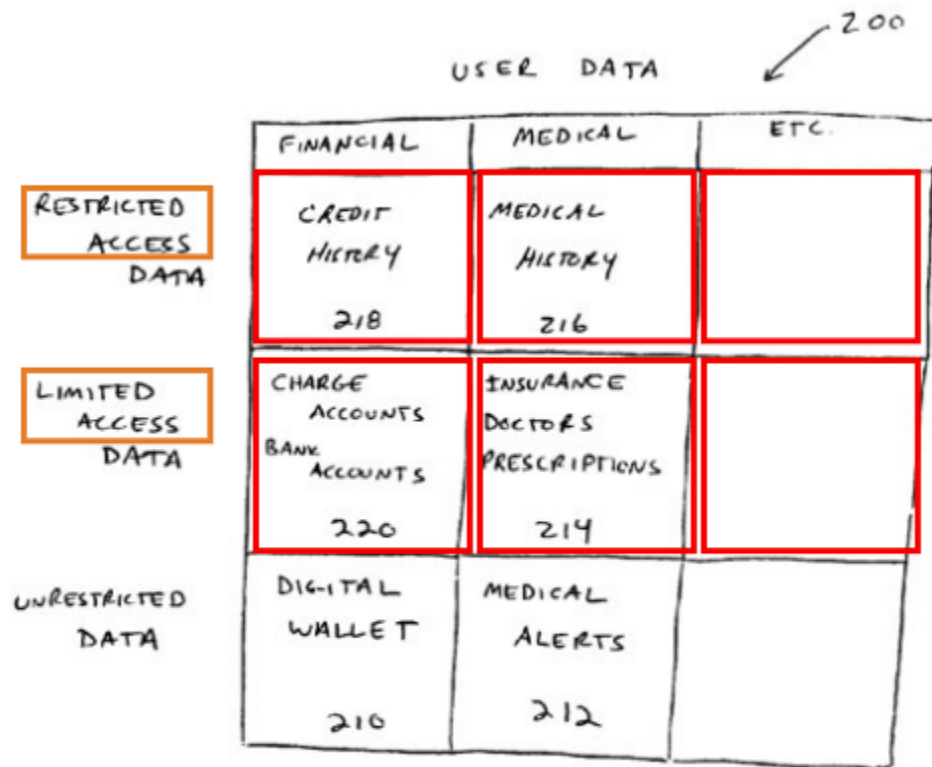


FIG. 3

EX1005, Figure 3. Accordingly, Bossemeyer's central database server, implemented by multiple servers, satisfies both the "plurality of other computers" and the "*plurality of extract data stores*" (e.g., the servers/databases that store the security sensitive content). EX1003, ¶¶252-255.

For Ground 3, to the extent Patent Owner argues that Bossemeyer does not disclose and/or render obvious this limitation, Merenda does for the reasons discussed in Section VI.B.1.i.d. As discussed in Section VI.C.1.vi, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in the combination. EX1003, ¶¶335-336.

e. [1/26pre-iv] said personal computer, said other computers and said extract data stores operatively connected together over a communications network [, the programming instructions]comprising:

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation. EX1003, ¶¶257, 259, 338, 341.

Bossemeyer discloses a computer system where the plurality of computers and the plurality of memories (e.g., central database server and/or memories at various locations) are coupled over a communications network. EX1005, 1:44-49 (“[The] invention describes a network arrangement...*The network connections are facilitated by the present telephone network or an interconnected network of computers such as the Internet.*”), 4:11-15 (“A smart card 12 coupled with such a terminal 50 having *an established connection through the network central office 16 to the central database server 10* has the power of a typical networked computer.”), 4:25-28 (“[T]he network arrangement of FIG. 2 is implemented over *an interconnected network of computers* such as the Internet 100 as well as or alternatively to the traditional telephone network 102.”). A POSITA would have also understood that when the user uses the personal computer to enter user data, the personal computer would also have been connected over the communications network, for example, to allow the transmission of the entered user data to Bossemeyer’s database server for storage. EX1003, ¶258.

For Ground 3, to the extent Patent Owner argues Bossemeyer does not disclose and/or render obvious this limitation, Merenda does for the reasons discussed in Section VI.B.1.i.e. As discussed in Section VI.C.1.vi, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in the combination. EX1003, ¶¶339-340.

ii. [1/26a] accepting data input which includes security sensitive content via said personal computer;

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation. EX1003, ¶¶260, 265, 342, 346.

Bossemeyer discloses that “the *user data* becomes populated when the user subscribes as part of the smart card activation process.” EX1005, 5:28-30. As discussed in Section VI.B.1.i.a, a POSITA would have found it obvious to use a personal computer to complete an action involving personal information, such as subscribing to smart card services. EX1003, ¶¶261-264.

For Ground 3, to the extent Patent Owner argues that Bossemeyer does not disclose and/or render obvious this limitation, Merenda does for the reasons discussed in Section VI.B.1.ii. For example, Merenda discloses that a user enters data through a website on the user’s computer device. EX1006, ¶7. Like Bossemeyer, Merenda discloses that the user data provided by the user is “separated” into parts. *Id.*, ¶7 (“[D]ata entered by a consumer into a Web form is *separated* into

related records in a public and *private data* set.”), ¶¶23-24, 34, Figures 1, 4. EX1003, ¶¶343-344.

A POSITA would have found obvious to use Merenda’s method of entering user data through a website, when a user subscribes to Bossemeyer’s smart card services, because using a website and the Internet was a ubiquitous way of signing up to different services from different providers. EX1003, ¶344.

As discussed in Section VI.C.1.vi, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in the combination. EX1003, ¶345.

iii. [1/26b] extracting said security sensitive content to obtain **extracted data** for each corresponding **security level** and **remainder data**;

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation. EX1003, ¶¶266, 277, 347, 350.

Bossemeyer discloses partitioning or separating (*e.g.*, extracting), *data* in terms of the *data’s level of security/accessibility*:

The central database server 10...*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)*. Thus, for example, in a retail purchase application 18, 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.*"

EX1006, 2:17-27. EX1003, ¶267.

Specifically, Bossemeyer partitions or separates (e.g., extracts), *user data* into subsets of *extracted data* e.g., *limited access information* and/or *proprietary information*, and *remainder data* e.g., *public information*:

The *information* contained within the central database server... can be classified as *public information* available to all the world; *limited access information* available to persons or selected groups with a user authentication code; or *proprietary information* accessible only by the owner of the information or a group with privileges to that directory information.

EX1006, 2:40-47. As discussed in Section VI.C.1.i.a, *limited access information* and/or *proprietary information* includes security sensitive content, such as, words, characters, data objects or icons. For example, Figure 1 of Bossemeyer shows *medical information* 22 stored in central database 10 as proprietary information.

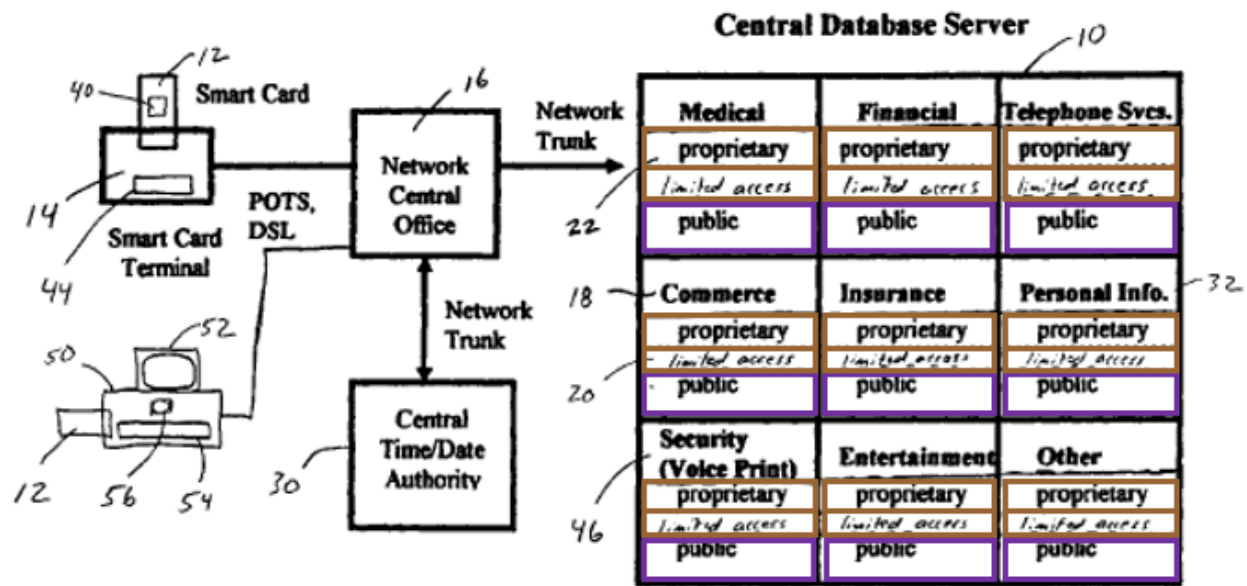


Figure 1

EX1005, Figure 1, 2:28-33 (“Private or proprietary information is partitioned such that the owner of the information has control over how the information is transferred and used. Thus, for example, *medical information* 22 provided to a health professional may be considered private and only available by way of special authorization from the owner of the information.”). EX1003, ¶¶268-269.

Figure 3 of Bossemeyer provides another example of partitioning *user data* into *extracted data* and *remainder data*.

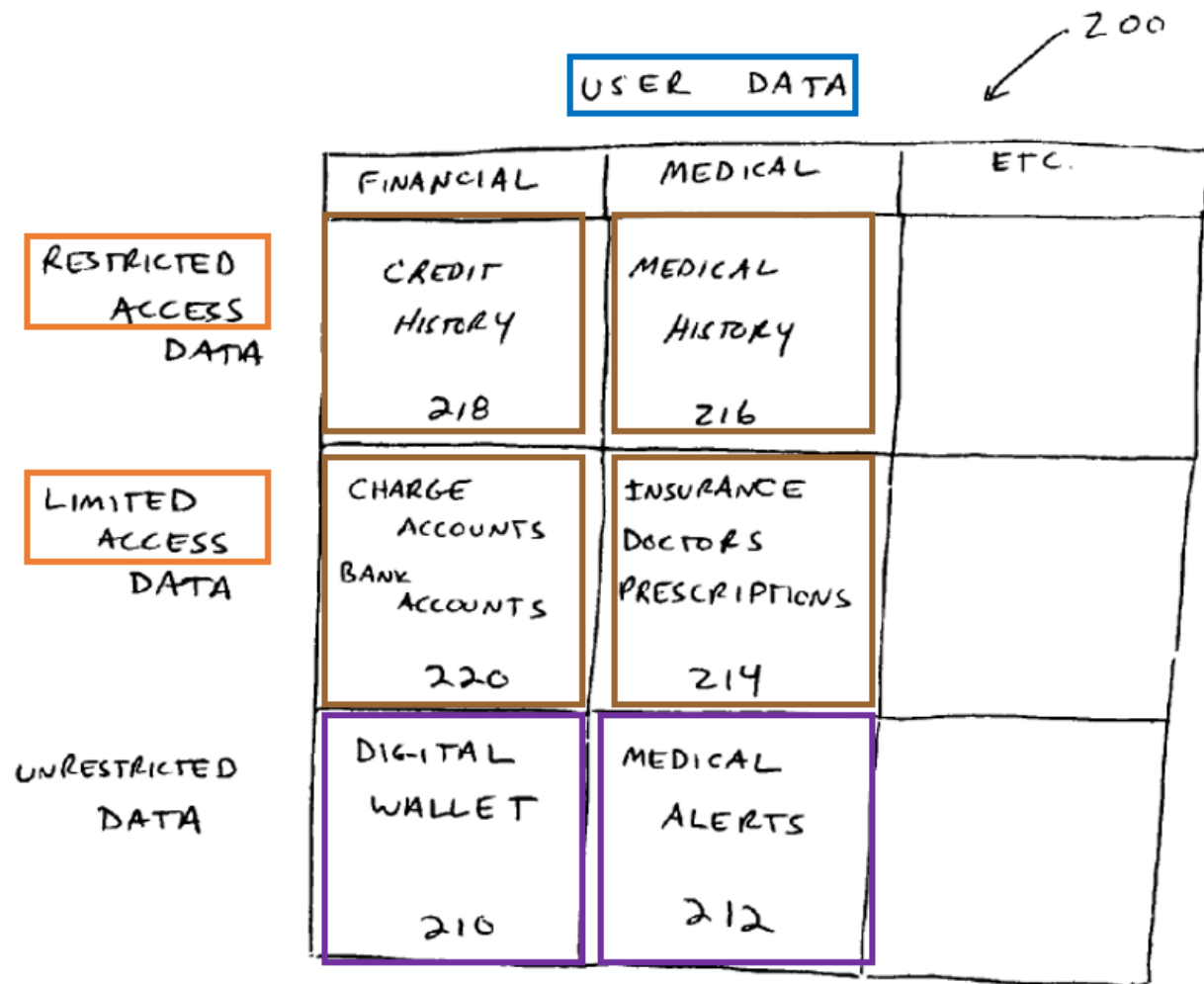


FIG. 3

EX1005, Figure 3, 5:9-22 (“In the pharmacy example,...the pharmacist may have access to the *user’s digital wallet 210*, *medical alerts 212*, and *insurance and prescription information 214*. Without further authorization, however, the pharmacy would not have access to the user’s *medical history 216*.”). EX1003, ¶¶270-273.

To the extent that Patent Owner argues that Bossemeyer does not explicitly disclose “extracting data,” a POSITA would have understood that when Bossemeyer’s “central database server partitions [user] information... in terms of... the accessibility of the information” (EX1005, 2:17-20), Bossemeyer’s method would filter and extract the secure sensitive information, (*e.g.*, restricted- and/or limited-data), from the received user data, (*e.g.*, from a user data file), to store the restricted- and/or limited-data in the appropriate security-level store, while storing the remaining information in the user data file as unrestricted data, (*e.g.*, public data). For example, a POSITA would have understood that Bossemeyer’s method parses received information into private and non-private elements. *See e.g.*, EX1006, ¶7 (“[A] set of data may be parsed into private and non-private elements.”). EX1003, ¶¶274-275.

When Bossemeyer’s central database server receives a *user’s medical data file*, as shown in Bossemeyer’s Figure 3 below, Bossemeyer’s method extracts the *user’s medical history information 216*, and *insurance, doctors, prescriptions information 214*, and stores them into respective extract stores corresponding to the appropriate *corresponding security level*. For example, a POSITA would have understood that medical history information can include images of medical charts, insurance information can include icons of the user’s insurance card, prescription information can include the names of the drugs prescribed to the user, etc.

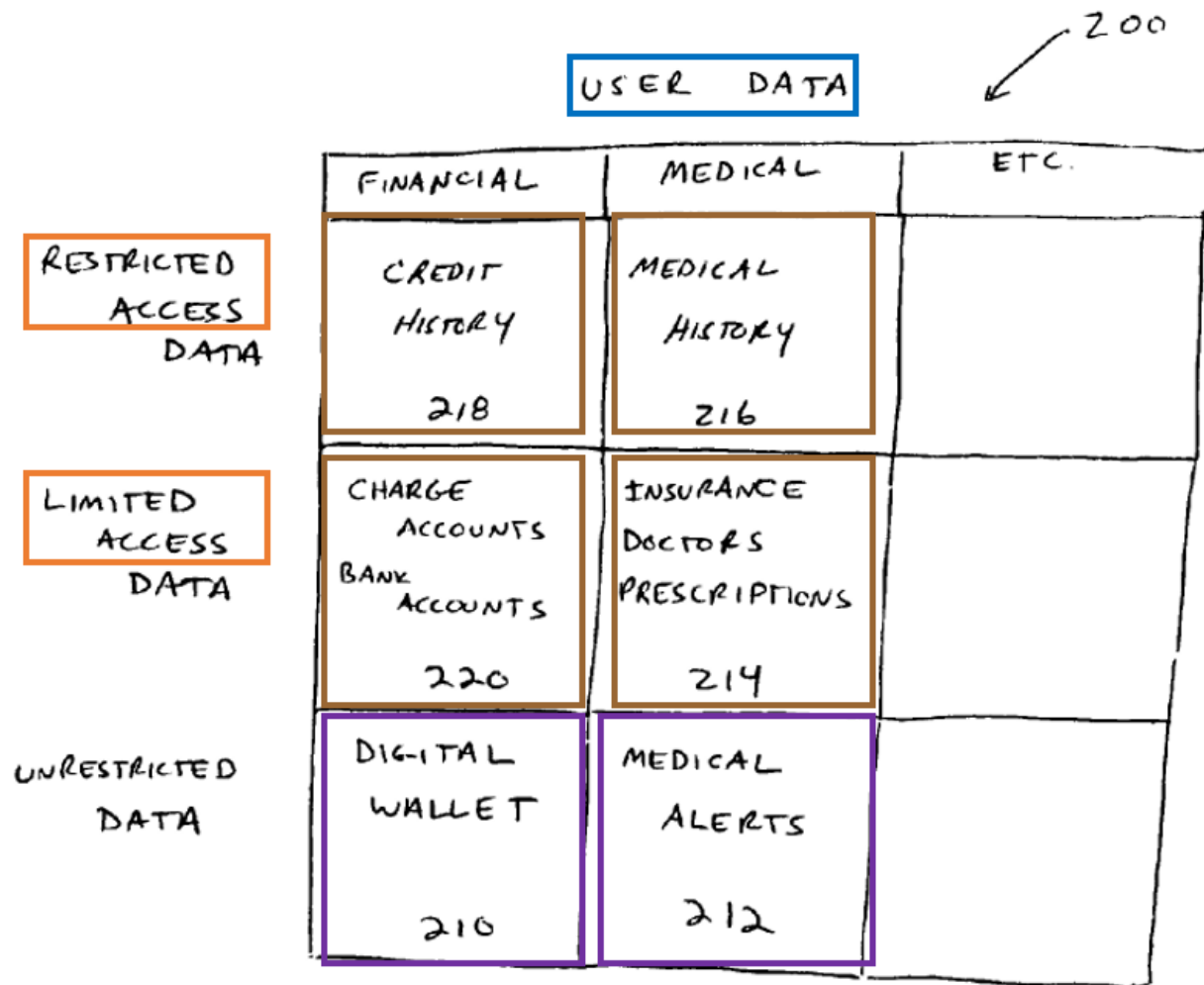


FIG. 3

EX1005, Figure 3. EX1003, ¶276.

For Ground 3, to the extent Patent Owner argues Bossemeyer does not disclose and/or render obvious this limitation, Merenda discloses extracting, e.g., parsing, security sensitive content, e.g., *private elements*, from *user data* to obtain subsets of *extracted data*, e.g., *address*, *credit card* or *social security number* and *remainder data*, e.g., *non-private elements*. See Section VI.B.1.iii. EX1003, ¶348.

As discussed in Section VI.C.1.vi, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in the combination. EX1003, ¶349.

- iv. [1/26c] 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,

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation. EX1003, ¶¶278, 283, 351, 355.

As discussed in Section VI.C.1.i.d, Bossemeyer's central database server includes servers that form the "plurality of other computers" and servers that form the "**plurality of extract data stores**" (e.g., the servers/databases that store the **extracted data**). Bossemeyer discloses extracting security sensitive content from user data to obtain **restricted access** data (**credit history 218** and **medical history 216**) and **limited access** data (**charge/bank accounts 220** and **insurance, doctors, prescriptions 214**) and **remainder data**. As also discussed in Section VI.C.1.i.d, Bossemeyer also discloses storing **extracted data**, e.g., **restricted access data** and **limited access data** in respective **extract stores** and the **remainder data** in the **partition/server**, which stores public information. This is illustrated in Figure 3 below.

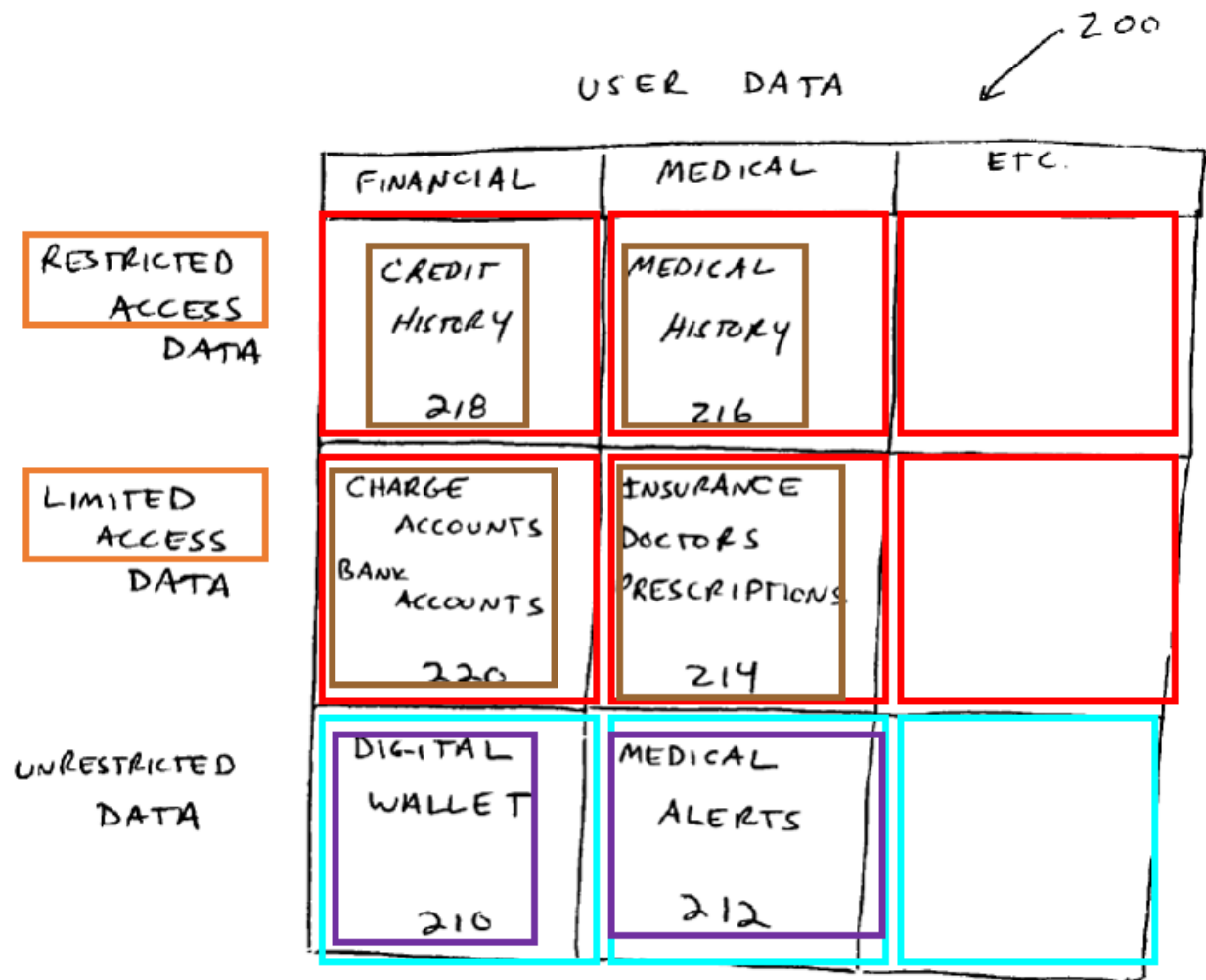


FIG. 3

EX1005, Figure 3; Figure 1. EX1003, ¶¶279-282.

For Ground 3, to the extent Patent Owner argues that Bossemeyer does not disclose and/or render obvious this limitation, Merenda does for the reasons discussed in Section VI.B.1.iv. As discussed in Section VI.C.1.vi, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in the combination. EX1003, ¶¶352-354.

- v. [1/26d] 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**.

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation. EX1003, ¶¶284, 301, 356, 359.

Bossemeyer discloses permitting the reconstruction of the partitioned data, e.g., allowing access to the partitioned data, only in the presence of an **associated security clearance**, e.g., **user identification/authentication code** or **authorization/access code** associated with a particular security level:

*Different **user identification codes**, or data pointers, provided by smart cards 12 **allow access to partitions in the database**. The information contained within the central database server is associated with the **user identification codes** on the smart cards 12 such that it can be classified as public information available to all the world; **limited access** information available to **persons or selected groups with a user authentication code**; or **proprietary information** accessible only by the **owner of the information or a group with privileges to that directory information**.*

EX1005, 2:38-47. EX1003, ¶¶285-289.

Specifically, Bossemeyer discloses that partitioned data is retrieved from the **extract stores** of the central database server 10, and is presented, e.g., at a terminal, based on a particular **user's authorization**:

Once the *user's authorization* has been verified, data pointers on the smart card 12 provide access to the relevant partitioned memory portions of the central database server 10. Routing circuitry...routes the data pointer to appropriate memory locations or database of the information keeper relating to the application at issue such as medical, financial, etc. *Data from these various locations is supplied back to the smart card terminal 14, and if appropriate, the data stored on the smart card 12 is updated.*

EX1005, 3:63-4:6.

Preferably, the smart card provides a one-time encrypted *user authentication code based on the user's digital signature or certificate*. This code, in turn, is transmitted over the communication network 100, 102 along with the merchant identification code to the server 10, 110. Thus, the digital signature of the card does not change, but an *authorization code* generated by an encryption scheme known to the server provides a unique *access code* each time the card is involved in a transaction with the network.

The network server 10, 110 *validates the user identification* by decrypting the *authorization code*. This information is then cross-referenced with the merchant code *to identify the information available to the merchant. The merchant can then view the information* stored within the server 10, 110, upload/download information, and perform transactions which are recorded at the server 10, 110.

EX1005, 4:50-65. EX1003, ¶¶290-291.

Bossemeyer's *user identification codes* correspond to respective *security levels*, which as discussed in Sections VI.B.1.i.c, VI.B.1.i.d, VI.B.1.iii, and VI.B.1.iv, correspond to respective *extract stores*. For example, Bossemeyer discloses accessing a user's medical data by permitting partial reconstruction (e.g., reconstruction of some) or full reconstruction (e.g., reconstruction of all) of the user's medical data based on the *security level* of the *user identification codes*. Specifically, Bossemeyer discloses using the *user authentication code* to allow permit partial reconstruction of a user's medical data with “*unrestricted*” and “*limited access*” security level (e.g., the user's *medical alerts 212* and *insurance and prescription information 214*) but requiring *further authorization* to permit full reconstruction to the user's medical data with “restricted access” security level (e.g., the user's *medical history 216*):

FIG. 3 provides one example of the type of information accessible within or through the server 200....[I]nformation is stored in three levels of security: unrestricted, limited access, and restricted. In the pharmacy example, once the *user's authentication code* and merchant code have been verified by the system, the pharmacist may have access to the user's digital wallet 210, *medical alerts 212*, and *insurance and prescription information 214*. Without *further authorization*, however, the pharmacy would not have access to the user's *medical history 216*.

EX1005, 5:6-15.

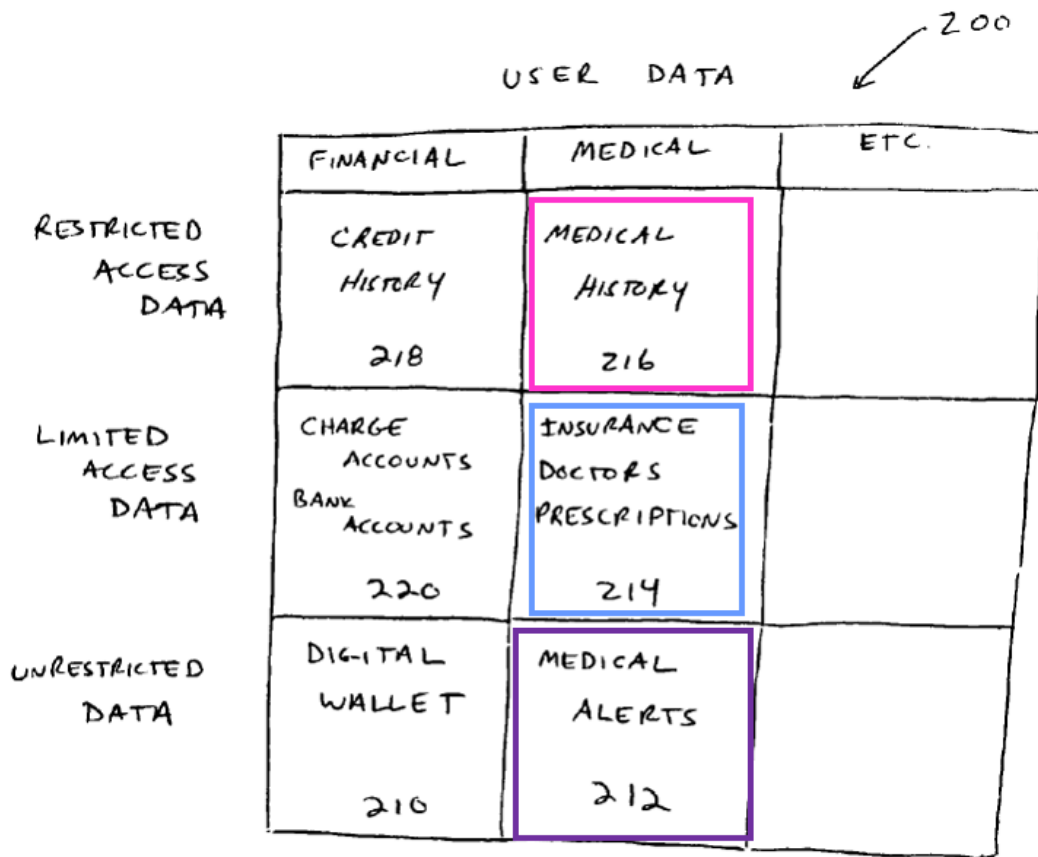


FIG. 3

EX1005, Figure 3. EX1003, ¶¶292-300.

A POSITA would have understood that “*further authorization*” would be in the form of a different *user authorization code* that allows access to the “restricted access” data. EX1005, 2:38-40 (“Different *user identification codes*, or data pointers, provided by smart cards 12 *allow access to partitions in the database.*”). EX1003, ¶¶294-298.

For Ground 3, to the extent Patent Owner argues Bossemeyer does not disclose and/or render obvious this limitation, Merenda does for the reasons

discussed in Section VI.B.1.v. As discussed in Section VI.C.1.vi, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in the combination. EX1003, ¶¶357-358.

vi. Reasons To Combine Bossemeyer With Merenda

A POSITA would have been motivated to combine Bossemeyer and Merenda to parse user data that includes private and non-private elements, as taught by Merenda, in Bossemeyer's system to extract the private elements and subsequently store them separately from the non-private elements, for several reasons. EX1003, ¶360.

First, the combination of Bossemeyer and Merenda represents the use of known techniques according to known methods in the same way to yield predictable results. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). Bossemeyer and Merenda relate to the same field of providing different users access to information and address the same problem of controlling access to information. The combination would merely involve using Merenda's data parsing technique in Bossemeyer's system according to the methods for separating private and non-private elements within user data. EX1005, 2:17-20 ("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."), 1:49-52 ("With a centralized server architecture, data related to an individual can be accessed by an

individual smart card, predefined groups of smart card users, or the general public.”), 2:28-30 (“Private or proprietary information is partitioned such that the owner of the information has control over how the information is transferred and used.”), 2:38-40; EX1006, ¶25 (“As a result of the distribution of data elements among various public and private data sets, it is desirable to establish a level of control over access to the public and private data stored therein...The present invention is directed toward providing the level of control...required in keeping the public and private data separate, and allowing access to the private data either at the explicit direction of the consumer...or in such a manner as to protect the privacy concerns of the consumer.”), ¶26; *see also*, EX1005, 2:40-55, 4:50-65, 5:6-31; EX1006, ¶¶10-13, 23, 29, 34-35. EX1003, ¶¶361-367.

Second, a POSITA would have been motivated to combine Bossemeyer with Merenda, because 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). “Nothing more is required to show a motivation to combine under *KSR*....” *See Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1381 (Fed. Cir. 2023) (holding that it was “enough for [Petitioner] to show that there was a known problem” in the art and that the referenced prior art helped address that issue). Merenda’s use of parsing data to extract private elements

and store the private elements separately from non-private elements, thereby controlling access to sensitive/proprietary information is a “universal motivation” known in the field of providing users with access to information and improves the technology, by ensuring that access to the sensitive/proprietary information is only limited to specific users (e.g., merchants that have been granted access to the information). “‘Universal’ motivations known in a particular field to improve technology provide ‘a motivation to combine prior art references even absent any hint of suggestion in the references themselves.’” *Intel Corp.*, 61 F.4th at 1380. EX1003, ¶¶368-371.

Third, a POSITA would have been motivated to use Merenda’s parsing technique to identify private elements within user data, because it would improve Bossemeyer’s system for controlling access to sensitive/proprietary information. Bossemeyer’s system would improve by using Merenda’s technique because it would enable separation of private elements and non-private elements where “separation [can occur] at *various levels of sophistication and granularity...*” EX1006, ¶23. That is, the combination would merely be a use of a known technique (e.g., parsing user data) to improve similar methods (e.g., controlling access to information) in the same way (e.g., by allowing access to information at the appropriate granularity level). *KSR*, 550 U.S. at 417. As discussed in Section VI.B.1.ii, Bossemeyer discloses and/or renders obvious extracting security sensitive

content in terms of the data's level of security or accessibility. Adding Merenda's teachings of parsing user data to identify various private elements would be an improvement to the security and access control afforded to users of Bossemeyer's system, because it would allow the separation of the private elements "at various levels of sophistication and granularity..." (EX1006, ¶23) and therefore could allow a greater number of security levels to correspond to the different private elements. For example, implementing Merenda's technique in Bossemeyer's system could allow access to groups of users (e.g., merchants) that, otherwise, would not have access to portions of the user data. EX1003, ¶¶372-376.

Fourth, a POSITA would have been motivated to combine Bossemeyer with Merenda, because the combination would involve applying a known technique (e.g., using Merenda's parsing of user information) to a known device (e.g., Bossemeyer's network arrangement with a central database server storing user information), which was ready for improvement to yield predictable results. *KSR*, 550 U.S. at 401. EX1003, ¶¶377-379.

Fifth, Merenda provides express motivations that would have led a POSITA to combine Merenda's and Bossemeyer's teachings. Indeed, Merenda acknowledges that "[t]he incredible growth of the Internet has provided ready access to a wealth of information. The World Wide Web is an ever-expanding repository of information spanning any and all conceivable topics limited only by the

imagination of the information content provider.” EX1006, ¶3. However, Merenda recognizes that “[t]he overwhelming benefits attendant to this ubiquity, however, are counterbalanced...by the inevitable loss of privacy associated with accessing a global computer network.” *Id.* Merenda also discloses that “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.” *Id.*, ¶4. EX1003, ¶¶380-381.

Merenda provides examples of the benefits of its methods for respecting the privacy interests of the public. For example, Merenda teaches that user private information will be available to merchants only if the user indicates that a particular merchant can access their private information:

The public records would be available without restriction for read access by a population of merchants. ***The private records would be available only per the indication of the consumer to the merchant in the population.***

EX1006, ¶7; ¶8. In fact, Merenda’s method allows consumers to allow access to private data only to selected merchants among the available merchants. EX1006, ¶8 (“The consumer may...select merchant to whom they wish their private data to be provided.”) Merenda’s disclosed method also allows merchants to data mine or statistically process the customer’s private information. *Id.*, ¶¶5, 12. EX1003, ¶¶382-385.

A POSITA would have found that Bossemeyer and Merenda were analogous to the '482 Patent. All three pertain to the same field of endeavor, *i.e.*, securing security-sensitive information. *Compare* EX1001, Abstract (“The data security method, system and associated data mining enables multiple users, each having a respective security clearance level to access security sensitive words, data objects, characters or icons.”) *with* EX1005, 1:8-11 (“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.”), 1:44-47 (“[T]he present invention describes a network arrangement which is readily accessible from different types of smart card terminals supporting various smart card applications.”) *and* EX1006, ¶2 (“The present invention in relates in general to the field of data processing, and in particular to a method, system and program product for allowing the viewer of a public data set to access related records in a private data set based upon a link which may be selectively provided to the viewer to authorize such access.”). EX1003, ¶386.

To the extent that Patent Owner argues that the references are not in the same field of endeavor as the '482 Patent, Bossemeyer and Merenda are still reasonably pertinent to the particular problem with which the '482 Patent's invention is involved, *i.e.*, securing information. *Compare* EX1001, 6:9-12 (“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.”), Abstract (“The data security method, system and associated data mining enables multiple users, each having a respective security clearance level to access security sensitive words, data objects, characters or icons.”) *with* EX1005, 2:17-22 (“The central database server 10 is a centralized partitioned database server which partitions information... in terms of 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).”) *and* EX1006, ¶23 (“Fundamental to the implementation of the present invention is the notion that a set of data may be parsed into private and non-private elements.”), ¶37 (“The separation of data into public and private data sets creates a volume of public data which is generally usable by the viewing public 206. This data has value by itself for marketing purposes, as it can be used for data mining to spot trends, in IT purchasing etc.”). EX1003, ¶387.

A POSITA would also have had a reasonable expectation of success in combining Bossemeyer with Merenda. Combining Bossemeyer with Merenda would merely involve including parsing user data in Bossemeyer’s system and storing private elements within the user data according to their respective security level in Bossemeyer’s various extract stores. In fact, Merenda provides different ways for doing so, all of which are within the reach of a POSITA:

Fundamental to the implementation of the present invention is the notion that *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.. At a more sophisticated level this notion 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. For purposes of the present invention 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 to the practice of the invention.

EX1006, ¶23. EX1003, ¶¶388-390.

2. Dependent Claims 5, 25, 30, and 50

i. [5/25pre] A method as claimed in claim 1.

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) claim 1. *See* Sections VI.C.1, VI.B.2.i. EX1003, ¶¶302, 391-393.

- ii. **[30/50pre] A computer readable storage medium containing programming instructions as claimed in claim 26.**

Bossemeyer renders obvious alone (or with Merenda for Ground 3) claim 26.

See Sections VI.C.1, VI.B.2.ii. EX1003, ¶¶303, 394-396.

- iii. **[5/30a] permitting full or partial reconstruction of said data occurs at one of said personal computer and said other computers.**

As discussed in Section VI.C.1.v, Bossemeyer discloses and/or renders obvious permitting full or partial reconstruction of said data. EX1003, ¶¶304, 312, 397, 401.

Bossemeyer also discloses permitting full or partial reconstruction at one of the other computers (e.g., *central database server 10*) and presenting the reconstructed data to the user at the smart card terminal (which a POSITA would have found obvious to implement as a personal computer). Specifically, Bossemeyer discloses that the central database server 10 routes the data pointers to the appropriate memory for the information, which is supplied back to the smart card terminal:

Once the user's authorization has been verified, data pointers on the smart card 12 provide access to the relevant partitioned memory portions of the central database server 10. Routing circuitry controlled by the microprocessor within the *central database server 10 routes the data pointer to appropriate memory locations or database* of the

information keeper relating to the application at issue such as medical, financial, etc. ***Data from these various locations is supplied back to the smart card terminal 14***, and if appropriate, the data stored on the smart card 12 is updated.

EX1005, 3:63-4:6.

The ***network server 10***, 110 ***validates the user identification*** by decrypting the ***authorization code***. This information is then cross-referenced with the merchant code ***to identify the information available to the merchant [at a client/merchant computer]***. ***The merchant can then view the information*** stored within the ***server 10***, 110, upload/download information....

EX1005, 4:59-65, 3:16-18. EX1003, ¶¶305-311.

For Ground 3, to the extent Patent Owner argues Bossemeyer does not disclose this limitation, Merenda does for the reasons discussed in Section VI.B.2.iii. As discussed in Section VI.C.1.vi, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success with the combination. EX1003, ¶¶398-400.

iv. [25/50a] wherein extracting occurs either automatically or manually with operator input.

As discussed in VI.B.2.iv, the claimed extraction occurring “automatically or manually with operator input” does not impose a narrowing limitation. That is, the “extracting” will either happen automatically (without operator input) or manually

(with operator input). In any case, Bossemeyer alone (or with Merenda) renders obvious this limitation. EX1003, ¶¶313-316, 318, 402, 405.

As discussed in Section VI.C.1.iii, Bossemeyer discloses extracting data. Bossemeyer discloses that extracting data occurs automatically at the central database server, which partitions information automatically in terms of application/category and accessibility/level of security. EX1005, 2:17-20 (“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.”). EX1003, ¶317.

For Ground 3, to the extent Patent Owner argues Bossemeyer does not disclose this limitation, Merenda does for the reasons discussed in Section VI.B.2.iv. As discussed in Section VI.C.1.vi, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success with the combination. EX1003, ¶¶403-404.

VII. Discretionary Denial Would Be Inappropriate

A. Discretionary Denial Under The *Fintiv* Factors Is Not Appropriate

The six factors considered for §314 denial strongly favor institution. *See Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential).

1. No evidence regarding a stay

No motion to stay has been filed, so this factor is neutral. *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB June 16, 2020) (informative); *see also Dish Network L.L.C. v. Broadband iTV, Inc.*, IPR2020-01359, Paper 15 (Feb. 12, 2021) (“It would be improper to speculate, at this stage, what the Texas court might do regarding a motion to stay...”).

2. Parallel proceeding trial date

This factor is neutral. The Board’s Final Written Decision is expected in December 2024.² While trial is currently scheduled for August 19, 2024 (EX1008), the Board recognizes “that scheduled trial dates are unreliable and often change.” *See* Director’s June 21, 2022 Memorandum on Discretionary Denials (“EX1018”), 8. Accordingly, the Board now uses median time-to-trial statistics in the relevant venue to determine a projected trial date for *Fintiv* purposes: “The PTAB will weigh this factor [factor 2] against exercising discretion to deny institution under *Fintiv* if the median time-to-trial is around the same time or after the projected statutory deadline for the PTAB’s final written decision.” EX1018, 9.

² December 2024 is 18 months after June 2023, when Petitioner expects a notice of accorded filing date for this petition.

The co-pending district court case was filed in the Eastern District of Texas on November 28, 2022. The statistics for the two most recent periods show a median time-to-trial in the Eastern District of Texas between 19 months (March 2023) and 24.2 months (March 2022). EX1009, 1. Accordingly, the projected trial date for purposes of *Fintiv* is between June 2024 (which is unlikely since June 2024 is before the scheduled trial date of August 2024) and December 2024—approximately 24.2 months after November 28, 2022—and around the Board’s Final Written Decision, which is expected in December 2024. Because the projected trial date based on the two most recent statistics is either before or “around the same time or after” the Board’s expected final written decision, and because the median-time-to-trial statistics can fluctuate by months for consecutive periods, this factor is neutral.

3. Investment in the parallel proceeding

The co-pending litigation is in its very early stages, and the investment in it has been minimal. *See* EX1007, EX1010. The parties have not exchanged preliminary positions on claim construction, and expert discovery has not begun. *See PEAG LLC v. Varta Microbattery GmbH*, IPR2020-01214, Paper 8, 17 (Jan. 6, 2021) Further, the Markman hearing is not scheduled until March of 2024. EX1007, 4.

Moreover, Patent Owner served their infringement contentions on Petitioner and confirmed which claims were being asserted only on February 28, 2023.

EX1010. Under *Fintiv*, Petitioner’s prompt filing “weigh[s] against exercising the authority to deny institution.” *Fintiv*, Paper 11 at 11 (“If the evidence shows that the petitioner filed the petition expeditiously, such as promptly after becoming aware of the claims being asserted, this fact has weighed against exercising the authority to deny institution under NHK”). This factor favors institution.

4. Overlapping issues with the parallel proceeding

Petitioner stipulates that if the IPR is instituted, Petitioner will not pursue the same grounds in the district court litigation. *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24, 7 (PTAB June 16, 2020) (informative).

5. Identity of parties

Petitioner is a defendant in the litigation. That is true of most Petitioners in IPR proceedings. Accordingly, this factor should not be a basis for denying institution.

6. Other circumstances

The prior art presented in this Petition renders the Challenged Claim unpatentable as obvious. “[T]he PTAB will not deny institution of an IPR or PGR under *Fintiv* (i) when a petition presents compelling evidence of unpatentability.” EX1018, 2. “Compelling, meritorious challenges are those in which the evidence, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are

unpatentable by a preponderance of the evidence.” *Id.*, 4. Here, the Petition plainly shows that the ’482 Patent claims no more than the known concept of storing sensitive data in security-controlled memories. The evidence of unpatentability is compelling, and thus the PTAB should not deny institution under *Fintiv*.

As such, because the *Fintiv* factors are either neutral or weigh against discretionary denial, and institution should not be denied on discretionary factors.

B. Discretionary Denial Under 35 U.S.C. § 325(D) Is Not Appropriate

Discretionary denial under § 325(d) is not warranted because the challenges presented in this petition are neither cumulative nor redundant to the prosecution of the ’482 patent. The PTO has not previously considered Merenda or Bossemeyer. Further, the combination is not redundant to any combination of references considered during prosecution. Additionally, Dr. Zadok is an expert in the relevant art, and his analysis of the prior art has not been presented to the PTO. EX1003, ¶¶45-406. In view of the new information presented in this Petition, the Board has ample discretion to institute an IPR on the grounds presented.

VIII. Conclusion

Accordingly, Petitioner has established a reasonable likelihood that the Challenged Claims are unpatentable.

Case IPR2023-00970
U.S. Patent No. 7,552,482

Dated: June 20, 2023

Respectfully submitted,

/Theodoros Konstantakopoulos/
Theodoros Konstantakopoulos
(Reg. No. 74,155)
tkonstantakopoulos@desmaraisllp.com
DESMARAIS LLP
230 Park Ave
New York, NY 10169
212-808-1060 (telephone)
212-351-3401 (facsimile)

Counsel for Petitioner

IX. Mandatory Notices

A. Real Party-in-Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that the real party-in-interest is International Business Machines Corporation.

B. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), to the best knowledge of the Petitioner, the '482 patent is or was involved in the following case:

Case Heading	Number	Court	Date
<i>DigitalDoors, Inc.</i> ³ v. <i>International Business Machines Corporation</i>	2:22-cv-457	EDTX	Nov. 29, 2022

C. Lead and Back-up Counsel and Service Information

Lead Counsel

Theodoros Konstantakopoulos
Desmarais LLP
230 Park Ave
New York, NY 10023

Phone: (212) 351-3400
tkonstantakopoulos@desmaraisllp.com
USPTO Reg. No. 74,155

Back-up Counsel

Brian D. Matty

Phone: (212) 351-3400

³ The '482 Patent cover page (EX1001, 1) and the USPTO assignment database (<https://assignment.uspto.gov/patent/index.html#/patent/search/resultAbstract?id=7552482&type=patNum>) identify “Digital Doors, Inc.” as the assignee of the '482 Patent.

Case IPR2023-00970
U.S. Patent No. 7,552,482

Desmarais LLP
230 Park Ave
New York, NY 10023
Emily Weber
Desmarais LLP
101 California Street
San Francisco, CA 94111

bmatty@desmaraisllp.com
USPTO Reg. No. 70,358

Phone: (415) 573-1858
eweber@desmaraisllp.com
USPTO Reg. No. 79,973

Please address all correspondence to lead and back-up counsel. Petitioner consents to service in this proceeding by email at the addresses above and at IBMDigitalDoorsIPRService@desmaraisllp.com.

CERTIFICATION UNDER 37 C.F.R. § 42.24(d)

Pursuant to 37 C.F.R. § 42.24(d), Petitioner hereby certifies, in accordance with and in reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 13,997. Pursuant to 37 C.F.R. § 42.24(d), this word count excludes the table of contents, table of authorities, mandatory notices under § 42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Dated: June 20, 2023

Respectfully submitted,

/Theodoros Konstantakopoulos/
Theodoros Konstantakopoulos
(Reg. No. 74,155)
tkonstantakopoulos@desmaraisllp.com
DESMARAIS LLP
230 Park Ave
New York, NY 10169
212-808-1060 (telephone)
212-351-3401 (facsimile)

Counsel for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), the undersigned certifies that a complete copy of the foregoing materials:

- Petition for Inter Partes Review Under 35 U.S.C. § 312 and 37 C.F.R. § 42.104 of U.S. 7,552,482;
- Exhibit List;
- Exhibits 1001-1019;
- Word Count Certification Under 37 CFR § 42.24(d);
- Petitioner's Power of Attorney

was served on counsel of record for Patent Owner by filing this document through P-TACTS on June 20, 2023, and by sending this document via Federal Express Priority Overnight shipping, which is at least as fast and reliable as U.S. Priority Mail Express, to counsel of record for Patent Owner at the correspondence address indicated in Patent Center:

Robert Kain
The Concept Law Group, P.A.
6400 N. Andrews Ave
Suite 500
FT LAUDERDALE, FL 33309
UNITED STATES

Case IPR2023-00970
U.S. Patent No. 7,552,482

Dated: June 20, 2023

Respectfully submitted,

/Theodoros Konstantakopoulos/
Theodoros Konstantakopoulos
(Reg. No. 74,155)
tkonstantakopoulos@desmaraisllp.com
DESMARAIS LLP
230 Park Ave
New York, NY 10169
212-808-1060 (telephone)
212-351-3401 (facsimile)

Counsel for Petitioner