

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION

Petitioner

v.

DIGITAL DOORS, INC.

Patent Owner

IPR2023-00967

U.S. Patent No. 7,313,825

PETITION FOR *INTER PARTES* REVIEW

UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104

EXPERT DECLARATION OF

DR. WILLIAM C. EASTTOM II (CHUCK EASTTOM) PH. D, D.SC.

I. INTRODUCTION

1. I have been retained by counsel for DigitalDoors, Inc. (“DigitalDoors” or “Patent Owner”) and asked to provide my opinion on the validity of claim 81 of U.S. Patent No. 7,313,825 in view of three references, U.S. Patent No. 7,010,701 (“Bossemeyer,” EX1005), U.S. Patent No. 6,985,588 (“Glick,” EX1006), and U.S. Patent No. 7,913,919 (“Carmichael,” EX1007).

2. To conduct my analysis, I reviewed the ’825 Patent, Bossemeyer, Glick, and Carmichael. I also reviewed the Petition for *Inter Partes* Review and the accompanying Declaration of Dr. Erez Zadok (EX1003). A full list of the materials that I reviewed is attached as Appendix A.

II. BACKGROUND AND QUALIFICATIONS

3. My name is William C. Easttom II (Chuck Easttom). I have 30 years of experience in the computer science industry including extensive experience in cybersecurity. I have authored 41 computer science books, including textbooks used at over 60 universities around the world.

4. I hold a Doctor of Science degree in Cyber Security from Capitol Technology University (Dissertation topic “A Comparative Study of Lattice Based Algorithms for Post Quantum Computing”). I also hold a Doctor of Philosophy (Ph.D.) in Technology (Dissertation topic “The Effects of Complexity on Carbon Nanotube Failures”) from Capitol Technology University, and a Doctor of

Philosophy (Ph.D.) in computer science from the University of Portsmouth (Dissertation topic “A Systematic Framework for Network Forensics Using Graph Theory). I also hold three master’s degrees (one in Applied Computer Science, one in Education, and one in Systems Engineering). I am an inventor with 25 computer science patents.

5. I also hold over 70 industry certifications, including several related to computer security. I am also experienced in database management and data mining.

6. I am a Distinguished Speaker for the Association of Computing Machinery (ACM) and a Senior Member of the Institute for Electrical and Electronics Engineering (IEEE) and a Senior Member of the Association of Computing Machinery (ACM). The IEEE is the world’s largest and most preeminent engineering organization. Among other activities, the IEEE creates industry standards including hardware, software, and other engineering and computer science standards. I am also a Distinguished Visitor of the IEEE. I have been a member of the IEEE Software & Systems Engineering Standards Committee for several years. I worked on the DevOps 2675 standards group from 2017 to 2019. I am also currently the Vice Chair of the IEEE p23026 Standards Group “Systems and Software Engineering -- Engineering and Management of Websites for Systems, Software, and Services Information.” I am also a Member of the IEEE Engineering in Medicine and Biology Standards Committee, Standard for a Unified Terminology

for Brain-Computer Interfaces P2731, from 2020 to present. I chair one of the subgroups.

7. I am an adjunct lecturer at Georgetown University, teaching graduate courses in *Requirements Engineering* and *Cryptography*. I am also an adjunct professor at Vanderbilt University teaching graduate computer science courses, including a course in *quantum computing* and a graduate course in *digital forensics*.

8. During the time period of 1996 to 2000, I worked for Boeing Aerospace on software for the NATO AWACS program, Alegis Systems Group as a Sr. Software Engineer, and as Director of Academic computing for Southeastern Oklahoma State University. While working at NATO AWACS, data security was a key concern. When I was working at Alegis Systems Group, I was developing software for banks. This provided me with an understanding of financial software and transactions. Due to personally identifiable information, financial information, and other sensitive information being processed, security was a substantial concern. While working as Director of Academic computing for SOSU, I was responsible for all cybersecurity for the university including authentication and authorization methods.

9. From 2007 to 2009, I worked extensively with medical software including Electronic Medical Records (EMR) and medical billing. Furthermore, my

second masters degree included a semester research project in electronic medical software.

10. In addition to the summary, I have provided here, I describe my qualifications, issued patents, publications, and experience as an expert witness in greater detail in my curriculum vitae (“CV”), EX2005.

III. MATERIAL CONSIDERED

11. In forming my opinions, I have considered the following:

- U.S. Patent 7,313,825, EX1001
- The petition for IPR2023-00967
- All exhibits to that petition.
- The expert declaration of Dr. Erez Zadok, EX1003
- All exhibits to that declaration
- Any references cited in this declaration.

IV. SUMMARY OF OPINIONS

12. Claim 81 of the '825 Patent includes an “extraction” step and a “reconstruction” step. Neither step, however, is present in either the Bossemeyer or Glick references, as detailed below, the only references that Petitioner relies upon to satisfy those limitations.

13. Both the Bossemeyer and Carmichael references are from afield dramatically divergent, both from the technology of the challenged patent, as well

as from Glick. Bossemeyer and Carmichael are in the field of smart card applications. EX1005, 1:6-10; EX1007, Abstract. Glick concerns ways of controlling access to copyrighted digital information, including via geographic limitations. EX1006, 2:4-6, 3:43-46. The '825 Patent concerns data security for systems with large amounts of data, like email systems, browser programs, and telecommunications programs, and specifically for securing that data on portable computing devices. EX1001, 1:23-29, 7:38-43. Persons of skill in the art of the '825 Patent would not have looked to Bossemeyer or Carmichael, nor would one working with Bossemeyer or Carmichael have looked to Glick's field of art for combinations with Bossemeyer or Carmichael, as the petition and Dr. Zadok contend. Moreover, because these references come from such different fields, combining them would not have made sense for a variety of practical reasons.

V. REFERENCES AT ISSUE

14. As noted above, the field of the '825 Patent concerns data security for systems with large amounts of data, like email systems, browser programs, and telecommunications programs. EX1001, 1:23-29, 7:38-43. More specifically, it concerns the processing, distribution, and secure storage of files/documents/data objects across telecommunications networks. EX1001, 1:23-53. Its prime focus is "securing data in a computer system." EX1001, 8:10. The '825 Patent specification describes securing data on a single computer, or a plurality of computers linked over

a LAN or WAN in a manner that is flexible and programmable by the user EX1001, 6:59-63, 7:3-15. For these reasons, the lead PTO's lead Class for it is 726, "Information Security." Within that class, the USPTO subclass is 27 for "Access Control" for such information security systems. The USPTO describes that subclass as "Subject matter comprising means to control data tampering by limiting access to authorized entities or processes."¹ The challenged '825 Patent claim is a method claim where "security sensitive words, characters, data objects or icons [are] extracted" from an original set of data, and later reconstructing the original "data" in the presence of appropriate security clearance.

15. The petition's primary/lead reference is Bossemeyer. Bossemeyer describes its technical field as "smart card applications and, more particularly, to a network arrangement to provide access to an architecture that supports a variety of advanced smart card applications." EX1005, 1:7-11. "Smart cards" are "substitute, replacement, or consolidation cards" for credit/debit/ATM cards as well as car rental, hotel, and airline membership cards. EX1005, 1:17-20, 27-31. They hold "much more information" than conventional magnetic stripe cards and "often include some 'intelligence' such as a microprocessor." EX1005, 1:34-38. Despite

¹<https://web.archive.org/web/20061001073748/http://www.uspto.gov/web/patents/classification/uspc726/defs726.htm>, EX2009.

that fact and the additional storage on the Central Database Server, the information communicated between the reader and the server is limited, nothing like the size of media files. Bossemeyer discloses the smart cards authentication code and possibly the merchant's authentication code being transmitted. EX1005, 4:50-54. That would be a very small amount of data, just a few bytes. Bossemeyer also discloses pointers to data. EX1005, 2:58-63. In fact, Bossemeyer emphasizes reducing the amount of information which must be stored or transferred to each smart card. EX1005, 2:60-63.

16. The USPTO's lead Class for Bossemeyer is 713, "Electrical Computers and Digital Processing Systems: Support." Its subclass within that Class of support for electrical computers and digital processing systems is 201, "for computer network security in general or in combination with nominal cryptography."² Bossemeyer teaches a network connecting a smart card reader terminal through a phone network or the internet to a central storage server. EX1005, Figs. 1 and 2.

17. The petition's secondary reference is Glick, "System and method for using location identity to control access to digital information." The disclosed

²<https://web.archive.org/web/20050422055224/http://www.uspto.gov/web/patents/classification/uspc713/defs713.htm>, EX2010.

invention relates to controlling the distribution of and access to copyrighted digital information using a location attribute in order to address “widespread copyright piracy.” EX1006, 1:9-12, 2:13-14. Its goal was to overcome issues with unauthorized distribution of copyrighted material and digital rights management by allowing access to the digital information only at a specific geographic location. EX1006, 3:43-46. Specifically, Glick teaches geo-locking digital information, such as music files (e.g., MP3), software, literary works, commercial transaction files, text files, Video/graphics, paging messages, cell phone conversation and commerce, and digital film stored on diskette, CD-ROM, tape, fixed or removable hard disk, DVD/CD-ROMs, flash memory/disks, EEPROMs, etc. EX1006, 12:56-63. The PTO’s lead Class for Glick is 380, “Cryptography.” Within that class, the USPTO subclass is 258 for “Position dependent or authenticating.” The USPTO describes that subclass as “Subject matter wherein cryptographic protection is based upon or validates the spatial location of a transmitter or receiver.”³

18. A POSITA would immediately note that the Bossemeyer and Carmichael are in a dramatically different field from both ’825 Patent and Glick. This is clear in the patents’ own descriptions as well as in the USPTO classifications.

³<https://web.archive.org/web/20050205203531/http://www.uspto.gov/web/patents/classification/uspc380/defs380.htm>, EX2011.

As I discuss in more detail below, a POSITA working in the '825 Patent's field would not have looked to the field of Bossemeyer or Carmichael. Nor would someone working in the field of one of those two smart-card references have looked to the field of Glick for solutions. It is also most probable that a POSITA in one of these fields would not be a POSITA in the other. This is described in more detail later in this declaration.

VI. POSITA

19. The petitioner has asserted that “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 August 2, 2002. Less professional experience can be substituted by additional education, and vice versa.” Pet., 11.

20. For the purposes of this declaration, I will use that definition of a POSITA without conceding that it is necessarily correct.

VII. ANALYSIS

A. Extraction and Reconstruction in the Challenged Claims

21. I understand that the Petitioner has challenged the validity of independent claim 81 of the '825 Patent. I present that claim below, with the language most relevant to this petition highlighted:

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

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

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

22. At least these two critical elements are absent from both Bossemeyer and Glick, the only references for which the petition relies upon them.

B. Absence of Extraction and Reconstruction in Bossemeyer

23. As explained briefly above, Bossemeyer concerns “smart card applications using a smart card in combination with a smart card terminal.” EX1005, Abstract. One example of the state of smart-card technology at the time of Bossemeyer and the original application that led to the ’825 Patent is an academic

paper written by Major McClannan, in which he discusses his perspective that the U.S. Airforce Reserve should consider implementing smart cards.⁴ What is noteworthy is that in 2001 this was still technology that even the U.S. Air Force reserve had not implemented. Knowledge of this technology was quite specific and was not widely known or used at the time.

24. In Bossemeyer's smart-card setup, a smart card reader/terminal would connect through a network central office of a standard public-switched telephone network to a central database server accessible to different merchants, as shown in Bossemeyer's Figure 1:

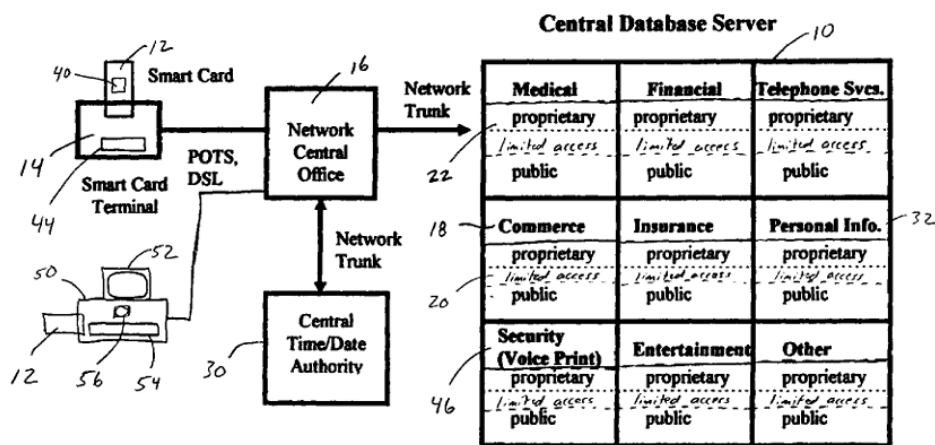


Figure 1

See also EX1005, 2:4-12.

⁴ "Implementing Smart Cards Into the Air Force Reserve" at

<https://apps.dtic.mil/sti/pdfs/ADA406328.pdf>, EX2012.

25. That central database server's memory was partitioned, with different types of information stored separately in different areas of the memory. EX1005, Fig. 1, 2:13-36. Some of the information, such as personal medical information, would be considered private or proprietary. EX1005, 2:27-36. Bossemeyer's Figure 3 shows varied levels of privacy related to different types of data:

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

FIG. 3

26. Bossemeyer's setup worked like this. A user's smart card stored pointers to different areas of the central server's memory. EX1005, 2:58-60. When a user put the card in the merchant's reader device, the reader would read those pointers. If the card had pointers to the private/proprietary portions of the server memory, that data from that portion of the memory would then be sent back to the location of the merchant's smart-card reader/terminal. EX1005, 4:3-6. Effectively, the pointers on the smart card provided the key to access that private data. EX1005,

3:18, 63-66. A customer in a store would pick up an item to purchase, go to checkout, and present his or her smart card. The smart card terminal or reader reads information stored on the smart card. EX1005, 3:39-41. The smart card terminal then communicates with a remote server to obtain information to complete the transaction, and the customer can then leave with the item. EX1005, 3:43-51. Other examples of the type of transactions that Bossemeyer's smart card system facilitates are payments at gas stations, grocery stores, department stores, and hotels. EX1005, 1:19-21, 5:16. For in-person transactions like these, speed and ease of the transaction are important.

27. The petition and Dr. Zadok point to two different parts of Bossemeyer to argue that it teaches extraction of some data from a larger whole. First is the discussion at column 2, lines 17-33 and 40-47 of Bossemeyer, which discusses the partitioned memory and what kind of information the central database stores. Second are Figures 1 and 3, which further discuss that notion of partitioned memory and merely illustrate the kinds of information stored in the central database server.

28. The problem is that neither of these Bossemeyer citations relates to extracting some data from a larger whole. The '825 Patent's claim element in question here is the method-type step of extracting some data from an original "data." Yet Bossemeyer is entirely silent as to where the information stored in the central server, the form it takes before it gets to the central database server, or how

the different pieces of information end up in the different partitioned areas of memory. The petition and Dr. Zadok seem to assume that the pieces of information come from some pre-existing collection of “data” from which individual pieces of information are removed for storage, but Bossemeyer never talks about such a collection or suggests that the pieces of information were removed from a larger collection before they were stored in the individual partitioned areas of memory. In other words, Bossemeyer is entirely silent about the steps that the challenged ’825 Patent claim details, what is happening to the data from processing (the extraction step) through storage. In Bossemeyer, pieces of information are already in storage.

29. The petition and Dr. Zadok try to find extraction in Bossemeyer’s description of “partitioned” memory, but a partitioned memory does not imply or suggest extraction. A partitioned memory was and is well known in the art. It merely refers to memory with different areas reserved for different types of information. Dr. Zadok’s own evidence supports this conclusion. He points to the definition of “parse” on a page from a Microsoft technical dictionary. EX. 1003, ¶168. But he doesn’t mention the definition of “partition,” the word he’s relying on from Bossemeyer, found on that same page. EX. 1003, ¶168. It defines “partition” as “[a] logically distinct portion of memory or a storage device that functions as though it were a physically separate unit.” EX1023, 25. That same dictionary that Dr. Zadok attaches also separately defines “disk partition” in a similar manner, as “[a] logical

compartment on a physical disk drive. A single disk might have two or more logical disk partitions, each of which would be referenced with a different disk drive name.” EX1023, 6. That definition is consistent with multiple contemporary sources.^{5, 6} A “partition” and “partitioning” in the art, therefore, refer to the logical separation of different areas of memory.

30. Bossemeyer’s Figures 1 and 3 show partitioned memory with different locations for different kinds of information. Its repeated references to “partitions” in the server memory are consistent with that understanding. *See, for example*, EX1005, 2:40 “partitions in the database”; 2:59-60 “partitions of the central database server”; 3:58-60 “The desired application is then selected which relates to a memory partition of the central database server”; 3:65-66 “access to the relevant partitioned memory portions of the central database server”; 4:17-18 “pointers to relevant data

⁵ Posey, B. (2000). All about partitions: The right FAT can save your waste. Retrieved from <https://www.techrepublic.com/article/all-about-partitions-the-right-fat-can-save-your-waste>, EX2013.

⁶ Walker, M. (2000). Splitting Your PC Data Across Multiple Drives & Partitions. Retrieved from <https://www.soundonsound.com/techniques/splitting-your-pc-data-across-multiple-drives-partitions>, EX2014.

within the partitioned central database server”; 4:43-44 “FIG. 3 shows a schematic diagram of the partitioned server database.”

31. The petition and Dr. Zadok don’t discuss any of these definitions or any of these instances of “partition” in the patent. Instead, they point to a single use of the term in a verb form, “partitioning,” “a centralized partitioned database server which partitions information.” EX1005, 2:17-18. They infer from that statement that partitioning means taking a large data set and extracting portions of that data set. But that isn’t what “partitioning” means in this context, as is clear from the way that term was used by those in the art at the time, and from the way it is used everywhere else in Bossemeyer. “Partitioning” is merely referring to the act by the memory partitions of keeping different pieces of information separate from each other, not removing some pieces of data from a larger whole. Another technical dictionary from this time frame that defines “partition” as a verb (the earlier-cited dictionaries don’t) as this one Bossemeyer snippet does is consistent, making clear that “partitioning” merely means sectioning up the memory, not extracting one piece of data from a larger whole: “Partition: Before a hard disk can be used for the first time, it must be partitioned and then formatted. Partitioning is a software function that

involves dividing the storage space into usable sections, with each section assigned a letter as though it were a separate drive.”⁷

32. That snippet that the petitioner and Dr. Zadok point to at Bossemeyer 2:17-18 about “partition[ing] information” cannot be understood to mean that some set of data is arriving at the central database server, which then intelligently breaks that data set up and puts different pieces in different reserved areas. Bossemeyer provides no description or suggestion of such an extraction process, in contrast to the extensive discussion of that kind of process in the ’825 Patent. For example, the ’825 Patent explains that its “invention extracts, disperses, via a controlled release of data segments to storage locations, and permits reconstruction utilizing security protocols to provide a security system for data.” EX1001, 1:26-29. It describes “establishing a group of security sensitive words, characters, icons, data streams or data objects, filtering the data input from a data input device and extracting the security sensitive data.” EX1001, 8:10-14. It provides a variety of other examples, like “[t]he method and the computer media containing programming instructions includes filtering data from the data input computer, extracting security sensitive words, phrases, characters, icons, or data objects and forming Subsets of extracted data and remainder data. The subsets of extracted data are stored in one or more

⁷ Prentice Hall’s Illustrated Dictionary of Computing 3rd Edition (1998), EX2006.

computer memories in the network identified as extracted stores. The remainder data is also stored in the network if necessary.” EX1001, 8:67-9:8. Another example is the description of how “the invention operates as a credit card or financial data scrubber. The e-mail data has one or more security sensitive words, characters or icons and the method ... extracts the security sensitive words, characters or icons from said e-mail data to obtain extracted data and remainder data.” EX1001, 10:3-12.

33. A POSITA would have understood that the extraction process of the ’825 Patent is vastly different than the act of “partitioning,” either as used in Bossemeyer or as used in the art at the time as the variety of technical dictionaries cited above demonstrate.

34. In fact, everywhere that Bossemeyer uses “partitioned” as a verb in relation to information, it makes clear that it’s referring to that piece of information merely being stored in a different, partitioned area of memory, thereby kept separate from other pieces of information:

- “[A] merchant may require a user’s credit information to determine whether to accept the user’s credit for a particular dollar amount.

This information *may be partitioned* in the limited access region 20 of commercial transaction applications 18.” EX1005, 2:23-27 (emphasis added).

- “Private or proprietary information *is partitioned* such that the owner of the information has control over how the information is transferred and used.” EX1005, 2:28-30 (emphasis added).

35. For at least these reasons, Bossemeyer’s reference to partitioned memory cannot be understood to mean extracting parts of data from a larger whole as claimed in the ’825 Patent.

36. The petition separately contends that “a POSITA would have understood that Bossemeyer’s method can parse the received information into private and non-private elements.” Pet., 38. There are numerous problems with this contention.

37. First, it’s notable that the petition switches to the word “parse,” even though Bossemeyer never uses that term. As noted above, Dr. Zadok’s declaration at ¶168 cites to the Microsoft definition of “parse,” a term which is absent in Bossemeyer, while ignoring the definition of “partition,” which is in Bossemeyer and appears on the very same dictionary page and contradicts his argument. EX1023, 25.

38. While the petition and Dr. Zadok discuss “parse” as if it were found in Bossemeyer, their citation for support is inexplicably to a reference that isn’t even part of this petition, U.S. Publication No. 2004/0148290 (“Merenda,” EX1008). In the midst of the discussion of Bossemeyer, at page 38, the petition introduces the

concept of “parse” with a citation, but that citation is to EX1008, Merenda, not Bossemeyer. I know that the Petitioner has filed other IPR petitions based on Bossemeyer and the Merenda references against other of Respondent’s patents, and this discussion of parse and the citation to Merenda appears in those petitions. It appears that the discussions of “parse” in the brief and the Dr. Zadok declaration are the result of the same mistake by both the lawyers for the petitioner and Dr. Zadok, copying the other petition.

39. It is, therefore, unclear how the petitioner can argue that a POSITA would have understood Bossemeyer to imply extraction with the word “parse” when neither Bossemeyer, nor Carmichael, nor Glick ever uses “parse” (or “extracting,” for that matter).

40. I also understand that to argue that something is inherent, the petitioner must make clear that the missing element is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. “Extraction” is not inherent merely because there is partitioned memory. In my experience, data often is loaded to partitioned memory without a prior extraction step. For example, when one downloads a file from the Internet, that individual file (be it image, Adobe PDF, etc.) is downloaded to the user’s hard disk without any extraction process. As another example, when one is typing a Microsoft Word document and saves the document, that document is saved to the users partitioned

hard disk without any extraction process. Indeed, Dr. Zadok’s reference to the definition of a “disk partition” (discussed above, ¶29) illustrates that such partitioning needs to occur before the disk can be used for storage. But if the petitioner’s inherency argument were right, that would mean that every time one stored data on a disk, it would first need to undergo an “extraction” process (because the memories of all disks are partitioned before use). That obviously is not the case.

41. The Petition concludes this section on page 38 discussing a fictitious “user’s medical data file,” suggesting that such a file would have multiple pieces of information that would need to be extracted. But Bossemeyer never describes a file like this or refers to any kind of file with multiple pieces of information, and I don’t find any evidence of either in the petition or Dr. Zadok’s report. And when they present a modified version of Bossemeyer’s Figure 3 on page 39 of the Petition and ¶169 of Dr. Zadok’s declaration, it still doesn’t suggest “extraction” of some pieces of information from a larger file or set of data. Even this modified figure, and the specification text they quote, merely states that these different pieces of information are stored in separate partitioned areas of the memory. But none of this evidence from Bossemeyer suggests that, prior to being stored in the partitioned areas of memory, these different pieces of information were part of a large “file.”

42. I turn now to reconstruction, a separate claim element that is absent from Bossemeyer. I first note that without an extraction step, by definition in the

context of the claim, there can be no reconstruction step. If something is never pulled apart, it cannot be reconstructed.

43. Pages 53-56 of the petition and ¶¶211-219 of Dr. Zadok's declaration seek to find reconstruction in Bossemeyer. Both point exclusively to the same four quotes from Bossemeyer and Bossemeyer's Figure 3. But none of those sources suggests, implies, or teaches reconstruction.

44. The four quotes they use all essentially say the same thing. When the smart card, with its stored data pointers, is inserted in the reader, those data pointers then point to the requested information in the central database server. That server then makes that information available by allowing access/sending it back to the smart card terminal. That is all these quotes state (emphasis shown comes from the petition and Zadok's declaration):

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... 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.

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. ***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, 4:59-65.

FIG. 3 provides one example of the type of information accessible within or through the server 200. As mentioned above, information 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.

45. It appears that the petitioner is asserting that any retrieval of a subset of data is 'reconstruction', and that is inaccurate. Providing access to data, or allowing

someone to view it, is not reconstruction. Nothing in Bossemeyer suggests that the piece of data targeted by the pointer and then provided to the merchant is in any way reconstructed or combined with any other data, let alone a body of data that it was originally a part of.

46. Dr. Zadok's declaration actually concedes that Bossemeyer does not explicitly disclose reconstruction: "Although Bossemeyer does not explicitly state that the information, once reaching the terminal, is merged/reconstructed..." EX1003, ¶216. Instead, he contends that when multiple pieces of information get returned, "logical merging would have been obvious to take place for the (secure) transaction to succeed: otherwise, why retrieve disparate information from different stores, send it to a single terminal location, only to not use it in unison, resulting in a failed transaction." EX 1003, ¶216.

47. Dr. Zadok makes several unstated assumptions in his statement, and it is not clear that any of them are true, nor does Dr. Zadok cite any source, reference, or basis for these assumptions. First, he contends that merging would be necessary "for the (secure) transaction to succeed." EX 1003, ¶216. Dr. Zadok provides no explanation and cites no evidence as to why that would be the case. Whether or not that would occur would appear to be a matter of electronic financial transactions. I do not see anything in Dr. Zadok's CV that qualifies him as an expert in financial transactions. Nowhere does his CV mention financial, banking, or any related

experience, education, or training. EX1004. Conversely, in the late 1990s I worked as a senior software engineer developing financial applications for banks. It is quite clear to me that it is equally possible that each piece of data could be returned and used separately for a separate part of the transaction process without them ever being merged. There are numerous examples specifically from financial transactions. For example, if a user is withdrawing money at an ATM, all information would come from a single source (customers bank account record) with a single piece of information (balance available). As another example, for a merchant charging a credit card for a purchase, the only information the merchant would need to retrieve is whether or not the balance is equal to or greater than the available funds/credit.

48. In fact, there are reasons not to merge the data. For example, Bossemeyer explicitly discusses financial data in figure 3 including restricted data such as credit history (218) and charge accounts (220). For a merchant processing a payment transaction, the only relevant issue is whether or not the charge account has a sufficient amount open to process the charge. Since this is an existing charge account, the customers credit history is not relevant to this transaction. In the case of figure 3 in Bossemeyer, merging is strongly contraindicated. Merging bank accounts, credit history, and a digital wallet put data that Bossemeyer identifies as *restricted*, *limited*, or *unrestricted*, into the same dataset. Neither Dr. Zadok nor the petition articulate any benefit or rational for doing this. Including unnecessary

“restricted access” data like credit history is problematic for security reasons. It unnecessarily leaves that data susceptible to exposure, complicates the transaction, and combines data that Bossemeyer endeavors to keep separate.

49. Furthermore, with the data described in figure 3 of Bossemeyer, the data would be difficult if not impossible to merge. Consider the Bank Account data 220 and the Digital Wallet 210. For Bank Accounts (220 in figure 3 of Bossemeyer) banks will often use BAI2 files in transmitting information.^{8, 9} This file type has a specific format.¹⁰ Banks may also use file types such as Swift MT,¹¹ ISO 20022,¹² NACHA¹³ (National Automated Clearinghouse Association), or others. Each of these is not compatible with the others, and substantial file translation is required. The digital wallet (210 in figure 3 of Bossemeyer) will have different file formats

⁸ <https://www.moderntreasury.com/learn/bai2>, EX2015.

⁹ <https://www.sepaforcorporates.com/swift-for-corporates/bai2-format-specification/>, EX2016.

¹⁰ <https://blogs.sap.com/2015/10/20/ebs-how-to-interpret-a-bai2-file/>, EX2017.

¹¹ <https://www2.swift.com/knowledgecentre/products/Standards%20MT/publications>, EX2018.

¹² <https://www.iso20022.org/iso-20022-message-definitions>, EX2019.

¹³ <https://achdevguide.nacha.org/ach-file-overview>, EX2020.

depending on the vendor. Today, for example, Apple uses a propriety format¹⁴ called PASS¹⁵. This is also not compatible with the bank file formats, and substantial file translation is required. In 2000 the situation was even more complicated. This was before Apple iPhone and Google Android became the dominant smart phone operating systems, there were even more diverse formats for digital wallets.^{16, 17, 18,}

19

50. Not only does Bossemeyer not disclose merging of this data, but it would also take undue experimentation to do so, with no guarantee of success and

¹⁴https://developer.apple.com/library/archive/documentation/UserExperience/Conceptual/PassKit_PG/Creating.html, EX2021.

¹⁵https://developer.apple.com/library/archive/documentation/UserExperience/Reference/PassKit_Bundle/Chapters/Introduction.html, EX2022.

¹⁶https://www.usenix.org/legacy/event/ec98/full_papers/daswani/daswani.pdf, EX2023.

¹⁷https://www.gpayments.com/documents/GPayments_eWallet_Whitepaper.pdf, EX2024.

¹⁸ <https://www.maithean.com/products/wallet.html>, EX2025.

¹⁹<https://www.nytimes.com/1998/08/10/business/cybercash-s-lesson-in-web-survival.html>, EX2026.

no benefit from attempting to do so. A similar issue exists with medical data (212, 214, 216 in Bossemeyer's Fig. 3). Medical data will be in different formats depending on the nature of the data. As a few examples: HL7 (Health Level Seven)²⁰ is used for clinical and administrative data, SDA (Summary Document Architecture)²¹ is an InterSystems format used to represent patient data, EDI 837²² is used for claim data. These disparate file types would also take undue experimentation to do so, with no guarantee of success and no benefit from attempting to do so. And neither the petition nor Dr. Zadok articulate any reason one would attempt to do so. It should be noted that HL7 was first introduced in 1987.²³ The EDI format originated in the 1990s.

51. Dr. Zadok also assumes that the only way to “use” the different pieces of information would have been to merge them. Based on my extensive experience and training with data, specifically with both the medical and financial data that is

²⁰ <https://digitalhealth.folio3.com/blog/hl7-messages-examples/>, EX2027.

²¹ https://docs.intersystems.com/healthconnectlatest/csp/docbook/DocBook.UI.Page.cls?KEY=HXSDA_ch_about, EX2028.

²² <https://kasa-solutions.com/guide-to-the-837-file-format/>, EX2029.

²³ <https://www.sciencedirect.com/topics/biochemistry-genetics-and-molecular-biology/health-level-7>, EX2030.

referenced in Bossemeyer, I strongly disagree with Dr. Zadok on this point. Data operations often make use of disparate pieces of information from different sources without merging or combining them. While merging can provide benefits in specific situations, it can also cause problems including duplicate data, inconsistent data, and inaccurate data.²⁴ Problems with merging data are well known in the art.^{25, 26, 27, 28}

52. Dr. Zadok's last assumption is that merger of the different pieces of information, if it occurred, would constitute "reconstruction." But that could only be the case if those pieces of data were part of the same whole in the first place and were extracted to then later be merged. And, as I demonstrated above, Bossemeyer

²⁴ <https://dataladder.com/merging-data-multiple-sources/>, EX2031.

²⁵ https://www.tc.columbia.edu/media/centers-amp-labs/gsjp/gsjp-volume-pdfs/MergingMultipleandorDivergentDatasetsusingSPSS_AMethodReviewandTutorial.pdf, EX2032.

²⁶ <https://libguides.princeton.edu/stata-merge-append>, EX2033.

²⁷ Kadane, J. B. (2001). Some statistical problems in merging data files. *Journal of Official Statistics*, 17(3), 423.

<https://www.scb.se/contentassets/ca21efb41fee47d293bbee5bf7be7fb3/some-statistical-problems-in-merging-data-files.pdf>, EX2034.

²⁸ <https://nap.nationalacademies.org/read/24893/chapter/4>, EX2035.

is entirely silent on the nature of the data before it is found in the portioned database server. Bossemeyer does not teach that these disparate pieces of information are ever part of a larger whole. So, even if they were merged, there is no evidence that the result of that merger would constitute a “reconstruction.” Rather, at most, one might consider such a merger to be the initial construction of a new dataset with multiple pieces of information.

53. Both Dr. Zadok and the petitioner rely on Bossemeyer’s Figure 3 for the point that the central database server stores related information (e.g., medical information) in different areas of the partitioned memory, and that accessing these different areas may require different levels of security. Pet., 55-56, EX 1003, ¶218. Again, all that Figure 3 indicates is that the merchant may access different types of information. It says nothing about what the merchant does with those different pieces of information when it obtains them. Bossemeyer provides neither a statement nor a suggestion that they are merged together, let alone that they are reconstructed into a combined form that they were previously in. And neither Dr. Zadok nor the petition provide any evidence that this is the case.

54. To agree with Dr. Zadok’s opinion on “reconstruction,” one would have to imagine that transactions couldn’t occur without merging data, imagine that Bossemeyer has a merging step that it does not disclose, ignore the inherent difficulties in merging the various data types, ignore the possibility of data errors

when merging, and then assume that such merger would be the equivalent of the reconstruction of the '825, even though Bossemeyer does not disclose any extraction of the data for the data to be reconstructed from.

55. For at least these reasons, I disagree with the petition and Dr. Zadok. Bossemeyer does not satisfy the required extraction or reconstruction elements of the different challenged claims, either explicitly, inherently, or via obviousness.

C. Absence of Reconstruction in Glick

56. The petition's secondary reference is Glick, which the petition combines with Bossemeyer in Ground 1 and with Bossemeyer and Carmichael in Ground 2. The petition primarily relies on Glick for the elements of the challenged claim related to a "portable computing device locatable with current location data" and the "predetermined region based upon said current location data." I will not address whether that reference teaches these elements here.

57. Instead, I will focus on whether Glick discloses "reconstruction." As I explained above, Dr. Zadok essentially concedes that Bossemeyer does not. Both Dr. Zadok and the petition, however, briefly assert that Glick discloses reconstructs. Pet., 56; EX1003, ¶220. Because reconstruction is one of the focuses of my analysis here, I will address that point.

58. The petition includes just a single sentence asserting that Glick discloses “reconstructs”: “Glick also discloses an appliance that reconstructs requested information.” Pet., 56. That’s the full explanation.

59. The claim language itself poses the first two problems for the petitioner’s argument. The claim requires that what is getting reconstructed is “said data,” the original data. EX1001, Cl. 81. The reconstruction is “via said extracted data,” meaning the data that was previously extracted from “said data.” EX1001, Cl. 81. The first problem is that reconstruction needs to involve data that was previously extracted. But the petitioner never contends that Glick involves an extraction step. So how can Glick disclose “reconstruction via said extracted data” when Glick never discloses extraction in the first place?

60. The second problem the claim language poses relates specifically to what the petitioner contends is the “reconstruction” step in Glick: decryption. The first of the petitioner’s two cites in support of its single sentence asserting reconstruction indicates that it is arguing that decryption meets this claim element: “The appliance that receives the encrypted digital information can generate a decryption key to decrypt the digital information based on the received area parameter and the appliance location determined in accordance with any of the foregoing methods.” EX1006, 4:4-8. What is Glick decrypting? “music, literary works, photography, video, software, etc.” EX1006, 2:9-10; 5:21-24. But decrypting

these items is not “reconstruction,” because it does not involve combining data previously “extracted” from these items.

61. That fact is obvious if one understands what “decryption” entails in the art, merely “decoding - that is, translating information from an unreadable or secret format into a form in which it can be used.” Barron’s Dictionary of Computer Terms, EX2039. Prentice Hall’s Dictionary of Computing similarly defines decryption as “[t]he process of decoding information so that it can be read and manipulated.” EX2006. Nothing about “decryption” suggests “reconstruction” by adding back “said extracted data.”

62. I have authored several research papers on cryptography, a textbook on cryptography, and teach a graduate course in cryptography for Georgetown. There simply is no relation between *decryption* and *reconstructing data*.

63. Indeed, the ’825 Patent itself discusses “decryption” as separate and apart from reconstruction:

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

64. The petition’s only other citation is paragraph 220 of Dr. Zadok’s declaration, which merely states, “Glick discloses an appliance that reconstructs

requested information in an analogous manner to Bossemeyer,” followed by the same cite to column 4, lines 4-8 of Glick that I just discussed. Because Dr. Zadok elsewhere concedes that Bossemeyer doesn’t disclose “reconstructed,” EX1003, ¶216, it is unclear what Dr. Zadok is referring to or how it supports his or the petitioner’s position.

65. Dr. Zadok closes that paragraph 220 with a cite to Section VII.B of his declaration, which is his summary of the Glick reference, without any additional information or explanation. Section VII.B does not mention reconstruction, encryption, or decryption and does not cite or discuss Glick’s column 4, lines 4-8, so it is difficult to understand Dr. Zadok’s inclusion of this citation.

66. There does not appear to be any evidence whatsoever suggesting, let alone establishing, reconstruction in Glick.

D. Lack of Combination of Bossemeyer/Carmichael with Glick

67. The petition relies on combining Glick with Bossemeyer for both grounds of the petition. For both grounds, the petition primarily relies on Glick for the elements of the challenged claim related to a “portable computing device locatable with current location data” and the “predetermined region based upon said current location data.” That means that if there would not have been a motivation to combine Glick with either or both of the smart-card references, both grounds of the challenge lack those claim elements.

68. I do not believe that a person of ordinary skill in the art would have been motivated to combine Glick with Bossemeyer.

69. Bossemeyer and Glick are from dramatically different technical fields, and a POSITA working with Bossemeyer as a foundation would not have been motivated to look for art in the far different field of Glick for solutions to problems with Bossemeyer, as the petition and Dr. Zadok contend.

70. The field of Bossemeyer, smart cards, exists to facilitate in-person transactions. EX1005, 4:42-49. Bossemeyer involves technology for storing certain types of information on the card itself, technology for authenticating/authorizing reading the data on the card, reader technology for reading data on the card, and technology enabling the reader to communicate with remote networks and sending and obtaining information from those networks. EX1005, Fig. 1, 2:4-12, 3:53-58. The problems Bossemeyer seeks to address are specific to those types of technologies. Bossemeyer, for example, addresses ways of remotely storing information that could not be stored on the card and then limiting the types of remote information returned to the reader depending on authorization. EX1005, 2:58-66. Bossemeyer teaches a network connecting a smart card reader terminal through a phone network or the internet to a central storage server. EX1005, Figs. 1 and 2. It never considers hacking attacks, for example, and a successful hacker who gained

access to Bossemeyer's central database server would have access to everything it stored.

71. Glick, on the other hand, concerns media sharing over the Internet. EX1006, 1:8-29; 2:33-53, 3:17-23. It involves technologies around encryption, "Digital Rights Management" (DRM) systems, and transferring media files. EX1006, 1:54-2:4, 2:33-53. It seeks to address the problem of access to media files by limiting access using geolocation information and encryption. EX1006, 1:27-64.

72. These two references involve different equipment and technologies and address very different problems. The different classification codes I noted earlier in my report show that the PTO reached the same conclusion. I'd also note that the Petitioner's characterization of the field as "securing security-sensitive information" is so broad, encompassing such a wide array of technologies, as to be almost meaningless. Pet., 72-73. For example, it would include encryption, dual-factor authentication, malware tools, firewall systems, tokenization (tap to pay) of financial information, blockchain, face ID, captcha, fingerprint scanners on computers, computer database technologies, cloud technologies, anti-surveillance technologies.

73. Moreover, nothing suggests adding location limitations to Bossemeyer's smart cards, and the combination would limit Bossemeyer's effectiveness. Smart cards, which include credit-card, debit-card, ATM-card, company-card, department-store-card, car-rental-cards, hotel-card, airline-card,

driver's-license, building-security-cards functionalities are meant to be portable. EX1005, 1:18-26. Limiting where they can be used based on geography, which is what the petitioner proposes to draw from Glick, would make those smart cards far less useful and desirable. Bossemeyer expressly includes airline membership, car rental, and hotel membership functionalities of its smart cards, demonstrating that these cards are intended for travel, not use only within limited geographies. EX1005, 1:20-22. Why would a customer want to have all those functionalities on a card but then not be able to use the card in a different city?

74. The petitioner's reliance on the Carmichael reference reinforces my point. Carmichael is another smart-card patent, and it includes a geo-location functionality. EX1007, Abstract. But Carmichael doesn't disclose, teach, or even hint at using geolocation information to limit use of the smart card. Instead, it characterizes the benefit that technology provides as helping to find lost or stolen cards, finding the card owner, or generating a travel log for the user. EX1007, 4:6-12. If Carmichael had seen a security benefit from limiting use based on geolocation, he would have mentioned it.

75. It is also probable that, according to Petitioner's own definition of a POSITA for purposes of this proceeding, a POSITA working in the field of the '825 Patent would not have the requisite skills or technical experience to make changes to Bossemeyer's smart card system. Smart cards are a specialized field of technology

(specialized storage on the card, specialized readers, etc.). Petitioner argues that a 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 August 2, 2002.” Pet., 11. It is quite possible for someone to complete a degree in computer science and not have any knowledge of smart cards. Again, as I noted above, smart cards were and remain a very specialized field that was not widely implemented or used during the relevant time frame.

76. It is not clear that a POSITA as identified by the petitioner would have the requisite knowledge about smart card technology to add Glick to Bossemeyer to reach the claims of the ’825 Patent, and the petition doesn’t appear to try to establish that a POSITA would have. In the petitioner’s description of a POSITA there is no mention of any knowledge of smart cards. And reviewing the curriculum at Stony Brook University, where Dr. Zadok teaches, it is quite clear that one can get a degree in computer science, computer engineering, or electrical engineering, with absolutely no training related to smart cards.²⁹ There is a passing mention of smart

²⁹<https://www.cs.stonybrook.edu/students/Undergraduate-Studies/csecourses>, EX2036.

cards in the lecture notes for “System Security,”³⁰ however it is just a passing mention. I further note that the course “System Security” is a graduate course and not one someone with a bachelor’s degree in computer science would have taken³¹. A POSITA from the university that Dr. Zadok teaches at would not have the skills to make any modifications to any smart card.

77. For these reasons, I do not believe a person of ordinary skill in the art would have looked to Glick and could have implemented Glick’s features in a Bossemeyer smart card.

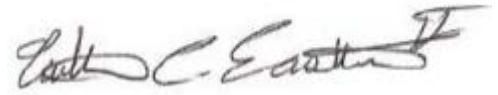
VIII. CONCLUSIONS

78. Upon completing my analysis, I have reached the following conclusions. Bossemeyer fails to disclose at least two claim elements in the challenged claim, the “extraction” element and the “reconstruction” element. A combination with Glick could not rectify that problem, and even if it could, a person of ordinary skill would not have looked to Glick or been able to combine Glick with Bossemeyer.

³⁰https://www3.cs.stonybrook.edu/~amione/CSE509_Course/materials/resources/auth_notes.pdf, EX2037.

³¹https://www3.cs.stonybrook.edu/~amione/CSE509_Course/materials/lectures/L7_auth.pdf, EX2038.

Dated: August 29, 2023

A handwritten signature in black ink, appearing to read "Easttom II", written in a cursive style.

Dr. William C. Easttom II

APPENDIX A

MATERIALS REVIEWED

The petition for IPR2023-00967 and all exhibits to that petition

The expert declaration of Dr. Erez Zadok, EX1003 and all exhibits to that declaration

U.S. Patent No. 7,313,825

U.S. Patent No. 7,010,701 (Bossemeyer)

U.S. Patent No. 6,985,588 (Glick)

U.S. Patent No. 7,913,919 (Carmichael)

U.S. Publication No. 2004/0148290 (Merenda)

USPTO Patent Classification Code Definitions – Class 713 -

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

USPTO Patent Classification Code Definitions – Class 726 -

<https://web.archive.org/web/20061001073748/http://www.uspto.gov/web/patents/classification/uspc726/defs726.htm>

USPTO Patent Classification Code Definitions – Class 380 -

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

McClannan, Keith, *Implementing Smart Cards Into the Air Force Reserve*, Air Command and Staff College, April 2001 -

<https://apps.dtic.mil/sti/pdfs/ADA406328.pdf>

Posey, Brien, *All about partitions: The right FAT can save your waste*, Daily Tech Insider, Sep. 2000 - <https://www.techrepublic.com/article/all-about-partitions-the-right-fat-can-save-your-waste>

Walker, Martin, *Splitting Your PC Data Across Multiple Drives & Partitions*, Sound on Sound, Aug. 2000 -

<https://www.soundonsound.com/techniques/splitting-your-pc-data-across-multiple-drives-partitions>

Nader, Jonar, Prentice Hall's Illustrated Dictionary of Computing:
Internet Update (Prentice Hall 1998, Third Edition)
Dowing, Douglas, Dictionary of Computer Terms (Barron's Business Guide 1995,
Fourth Edition)

BAI2, Modern Treasury Corp., – <https://www.moderntreasury.com/learn/bai2>

BAI2 Format Specification, SEPA for Corporates, Jan. 2015 –
<https://www.sepaforcorporates.com/swift-for-corporates/bai2-format-specification/>

Maheshwari, Ajay, *EBS – How to interpret a BAI2 file*, SAP, Oct. 2015 –
<https://blogs.sap.com/2015/10/20/ebs-how-to-interpret-a-bai2-file/>

Standards MT, Swift, 2023 -
<https://www2.swift.com/knowledgecentre/products/Standards%20MT/publications>

ISO 20022 Message Definitions, ISO, Sep. 2010 – <https://www.iso20022.org/iso-20022-message-definitions>

ACH Guide for Developers, Nacha, - <https://achdevguide.nacha.org/ach-file-overview>

Pass Design and Creation, Wallet Developer Guide, Jan. 2018 –
https://developer.apple.com/library/archive/documentation/UserExperience/Conceptual/PassKit_PG/Creating.html

About Pass Files, Apple Inc., Nov. 2017 –
https://developer.apple.com/library/archive/documentation/UserExperience/Reference/PassKit_Bundle/Chapters/Introduction.html

Daswani, Neil et. al., *SWAPER00: A Simple Wallet Architecture for Payments, Exchanges, Refunds, and Other Operations*, USENIX Workshop, Aug. 1998 –
https://www.usenix.org/legacy/event/ec98/full_papers/daswani/daswani.pdf

Clark, Brent, *Electronic Wallets: Past, Present, and Future*, GPayments, 2001 –
https://www.gpayments.com/documents/GPayments_eWallet_Whitepaper.pdf

NetPay Wallet, Maithean, - <https://www.maithean.com/products/wallet.html>

Wayner, Peter, *Cybercash's Lesson in Web Survival*, The New York Times, Aug. 1998 - <https://www.nytimes.com/1998/08/10/business/cybercash-s-lesson-in-web-survival.html>

HL7 Messages Examples – Complete Guide 2023, folio3 Software Inc., - <https://digitalhealth.folio3.com/blog/hl7-messages-examples/>

About SDA, InterSystems, 2023 – https://docs.intersystems.com/healthconnectlatest/csp/docbook/DocBook.UI.Page.cls?KEY=HXSDA_ch_about

Guide to the 837 File Format, Kasa Solutions, - <https://kasa-solutions.com/guide-to-the-837-file-format/>

Denecke, Kerstin, *Biomedical Standards and Open Health Data*, Science Direct, 2021 – <https://www.sciencedirect.com/topics/biochemistry-genetics-and-molecular-biology/health-level-7>

Ibarrera, *Merging data from multiple sources*, Data Ladder, Nov. 2021 – <https://dataladder.com/merging-data-multiple-sources/>

Audette, Lillian M. et. al., *Merging Multiple and/or Divergent Datasets using SPSS: A Method Review and Tutorial*, Graduate Student Journal of Psychology 2022, Vol. 19, 2022 – https://www.tc.columbia.edu/media/centers-amp-labs/gsjp/gsjp-volume-pdfs/MergingMultipleandorDivergentDatasetsusingSPSS_AMethodReviewandTutorial.pdf

Al, Muhammad et. at., *Merge and Append Using Stata: How to Merge and Append Datasets*, Princeton University, May 2023 - <https://libguides.princeton.edu/stata-merge-append>

Kadane, Joseph B., *Some Statistical Problems in Merging Data Files*, Journal of Official Statistics, Vol. 17, No. 3, 2001 - <https://www.scb.se/contentassets/ca21efb41fee47d293bbec5bf7be7fb3/some-statistical-problems-in-merging-data-files.pdf>

Groves, Robert M. et. al., *Federal Statistics, Multiple Data Sources, And Privacy Protection*, The National Academies Press, 2017 -
<https://nap.nationalacademies.org/read/24893/chapter/4>

Department of Computer Science CSE Courses, Stony Brook University –
<https://www.cs.stonybrook.edu/students/Undergraduate-Studies/csecourses>

Lecture Notes for Chapter 3 System Security, Stony Brook University -
https://www3.cs.stonybrook.edu/~amione/CSE509_Course/materials/resources/author_notes.pdf.

Sekar, R., *CSE509 - Computer System Security*, Stony Brook University –
https://www3.cs.stonybrook.edu/~amione/CSE509_Course/materials/lectures/L7_auth.pdf