UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,

Petitioner,

v.

PROXENSE, LLC,

Patent Owner.

Case No. IPR2024-00233
U.S. Patent No. 8,886,954

DECLARATION OF STEPHEN GRAY

TABLE OF CONTENTS

I. INTRODUCTION 1

II. SUMMARY OF OPINIONS 2

III. QUALIFICATIONS AND BACKGROUND 2

IV. MATERIALS CONSIDERED 6

V. LEGAL STANDARDS 8

A. Level of Ordinary Skill 9

B. Prior Art 10

C. Anticipation 10

D. Obviousness 11

VI. THE ’954 PATENT 16

A. Overview 16

VII. CLAIM CONSTRUCTION 18

VIII. LEVEL OF ORDINARY SKILL IN THE ART 20

IX. THE PRIOR ART 21

A. Ludtke (U.S. Patent No. 7,188,110) 22

B. Kon (U.S. Patent Application Publication No. 2002/0046336) 25

X. GROUNDS OF UNPATENTABILITY 30

XI. THE CHALLENGED CLAIMS ARE UNPATENTABLE BASED ON THE PRIOR ART 31

A. Ground 1: Claims 1, 2, 4-7, 10, 12, 13, 15, 16, 18, 19, and 22-27 Are Obvious in View of Ludtke. 31

1. Independent claim 1 31

a. [1preamble]: “A method comprising:” 31

b. [1ai]: "persistently storing biometric data of a user [in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered] and" 32

c. [1aii]: "[persistently storing] a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device [in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered] and" 35

d. [1aiii]: "[persistently storing] a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;" 37

e. [1b]: "responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;" 44

f. [1c]: "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;" 45

g. [1d]: "responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes from the plurality of codes and the other data values for authentication to a third party that operates a trusted authority, wherein the one or more codes and other data values include[] the device ID code; and" 45

h. [1e]: "receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application 51

2. Claim 2: "The method of claim 1, wherein the one or more codes and the other data values are transmitted to the trusted authority over a network." 55

3. Claim 4: "The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful." 55

4. Claim 5: "The method of claim 1, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition."....57

5. Claim 6: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."....57

6. Claim 7: "The method of claim 1, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account." 59

7. Claim 10: "The method of claim 1, further comprising establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication."....60

8. Independent Claim 12 60

   a. [12preamble]: "An integrated device comprising:" 60

   b. [12ai]: "a persistent storage media that stores biometric data of a user, and"....60

   c. [12aii]: "a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device, and" 60

d. [12aiii]: "a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered;" 61

e. [12b]: "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends one or more codes and other data values from the plurality of codes and other data values for authentication by a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and" 61

f. [12c]: "a radio frequency communication module that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allowing the user access to an application." 63

9. Claim 13: "The integrated device of claim 12, wherein the one or more codes and the other data values are transmitted to the trusted authority over a network." 64

10. Claim 15: "The integrated device of claim 12 comprising: an LED to be activated for requesting the biometric scan." 64

11. Independent Claim 16 66

a. [16preamble]: "A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:" 66

b. [16a]: "wirelessly receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and other data values comprises the device ID code uniquely identifying an integrated device associated with a

biometrically verified user, the device ID code being registered with a trusted authority for authentication, the trusted authority operated by a third party" 68

c. [16b]: "requesting authentication of the integrated device using the one or more codes and other data values by the trusted authority;" 71

d. [16c]: "receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party; and" 71

e. [16d]: "in response to receiving the access message, allowing the biometrically verified user access to the application." 71

12. Claim 18: "The method of claim 16, further comprising: establishing a secure communications channel with the integrated device, wherein the one or more codes and other data values associated with the biometrically verified user is received from the integrated device." 72

13. Claim 19: "The method of claim 16, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account." 72

14. Independent claim 22 72

a. [22preamble]: "A system, comprising:" 72

b. [22ai]: "an integrated hardware device that stores biometric data of a user" 73

c. [22aii]: "and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated hardware device" 73

d. [22aiii]: "and a secret decryption value in a tamper proof format written to a storage element in the integrated hardware device that is not capable of being subsequently altered,".....74

e. [22aiv]: "and that wirelessly sends one or more codes and other data values from the plurality of codes and other data values, wherein the one or more codes and other data values include the device ID code; and" 74

f. [22b]: "an authentication circuit that receives the one or more codes and other data values and sends the one or more codes and other data values to a third party that operates a trusted authority for authentication, and that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allows the user to access an application." 75

15. Claim 23: "The system of claim 22, wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from the user to generate scan data." 76

16. Claim 24: "The system of claim 22, wherein when the integrated hardware device cannot verify scan data as being from the user, the integrated hardware device does not send the one or more codes and other data values.".....78

17. Claim 25: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.".....80

18. Claim 26: "The method of claim 1, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial

recognition, a signature recognition and a voice recognition.”.....80

19. Claim 27: “The method of claim 1, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.” 80

B. Ground 2: Claims 3, 14, and 17 Are Obvious in View of Ludtke and Kon 80

1. Claim 3: “The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code.”.....80

2. Claim 14: “The integrated device of claim 12, wherein an age verification is registered in association with the device ID code.”.....85

3. Claim 17: “The method of claim 16, further comprising: registering a date of birth or age with the agent.”.....85

XII. CONCLUSION.....85

I. INTRODUCTION

1. I have been retained by GOOGLE LLC ("Petitioner") as an independent expert consultant in this proceeding before the United States Patent and Trademark Office.

2. I am over 21 years of age and, if I am called upon to do so, I would be competent to testify as to the matters set forth herein.

3. I understand that this proceeding involves U.S. Patent No. 8,886,954 ("the '954 patent," Ex. 1001). The application for the '954 patent was filed December 10, 2012, and claims priority to U.S. Patent Application Ser. No. 11/314,199, filed December 20, 2005, which claims the benefit of provisional applications filed on December 20, 2004, and February 14, 2005. Ex. 1001, cover page.

4. I have been asked by Petitioner to provide my opinion on whether the claims of the '954 patent would have been obvious to a person of ordinary skill in the art at the time of the earliest possible priority date of the '954 patent. In performing my analysis, I have been asked to assume that the priority date is December 20, 2004. My opinions are set forth below.

5. Throughout this declaration, I refer to specific pages, figures, and/or line numbers of various exhibits. These citations are illustrative and are not

intended to suggest that they are the only support for the propositions for which they are cited.

II. SUMMARY OF OPINIONS

6. This declaration considers claims 1-7, 10, 12-19, and 22-27 of the ’954 patent. Below, I set forth the opinions I have formed, the conclusions I have reached, and the bases for these opinions and conclusions. I believe the statements contained in this declaration to be true and correct to the best of my knowledge.

7. Based on my experience and knowledge of the art at the time of the applicable priority date, it is my opinion that claims 1-7, 10, 12-19, and 22-27 of the ’954 patent would have been obvious based on the asserted grounds discussed below.

8. I am being compensated for my time at my normal hourly rate. My compensation is in no way contingent upon the nature of my findings, the presentation of my findings in testimony, or the outcome of this proceeding.

III. QUALIFICATIONS AND BACKGROUND

9. I believe that I am well qualified to serve as a technical expert in this matter based upon my qualifications, discussed in detail below.

10. I am competent to write this declaration.

11. I am an independent consultant. All of my opinions stated in this declaration are based on my own personal knowledge and professional judgment.

In forming my opinions, I have relied on my knowledge and experience in designing, developing, and deploying distributed client/server systems, graphical user interfaces, website platforms, e-commerce systems, and digital image processing systems, and on the documents and information referenced in this declaration. I am over 18 years of age and, if I am called upon to do so, I am competent to testify as to the matters set forth herein.

12. In formulating my opinions, I have relied upon my training, knowledge, and experience in the relevant art. Provided as Exhibit 1004 is a copy of my current curriculum vitae, which details my education and experience, and a list of all other cases in which, during the previous four years, I testified as an expert at trial or by deposition. The following provides a brief overview of some of my experience that is relevant to the matters set forth in this declaration.

13. Since the mid-1970s, I have designed, developed, and deployed computing systems and products that operate in server, client, and network environments. As such, I have acquired expertise and am an expert in the areas of distributed computing architecture and design, graphical user interfaces, operating systems, distributed data management, local area and wide area networks, and the various programming languages used in the development of those systems and products. I have been employed by or retained as a consultant, including as a litigation consultant, for numerous companies such as Burroughs, FileNet, Fujitsu,

Marriott Corporation, MCI, Northern Telecom, Olivetti, TRW, and Xerox, as well as other companies.

14. During my career I have had a variety of assignments relating to distributed processing. For example, as the Chief Technology Officer for NTN Communications, I was responsible for the technologies related to the broadcast of online trivia games to 3,500 remote sites in North America. The trivia game broadcast used a variety of image technologies.

15. My practical experience regarding mobile device computing software includes development at NTN Communications of a multiplayer game system operating over mobile phones where issues of data synchronization, event handling and centralized control of distributed devices was required.

16. As my curriculum vitae shows, much of my career has been spent as a software development professional. As a software development professional, I have had numerous occasions to write, modify, analyze, and otherwise review bodies of source code. I have analyzed source code written in several variants of C, SQL, COBOL, PHP, Python, RPG, variants of Basic, Java, Perl, several Assembler languages, and others. For example, as an individual contributor at Xerox during the mid-1980s to 1990, I evaluated the quality of source code from third party software providers for possible inclusion in the Xerox product line. Also, as another example, I evaluated the source code of several application software

packages for completeness and maintainability for possible inclusion into the NTN Communications product line in 2000-2001. During my early career, I spent time maintaining source code written by others. In each of these assignments, I analyzed the source code to identify the data structures, logical flow, algorithms and other aspects.

17. I have developed and presented numerous public and in-house courses in computer systems technology, including relating to distributed computing applications for IBM MVS, UNIX, Linux, IBM OS/2, Microsoft Windows, and related networking technologies.

18. I also have professional experiences related to computerized authentication including authentication responsive to biometric verification of a user being authenticated.

19. While consulting for Xerox in the mid 1990s, I worked on the design of systems for multi-level authentication for distributed product configuration software products.

20. In the early 2000s I served as a technical advisor to SiCommNet which was an e-Commerce Internet start-up. SiCommNet developed and sold a product for procurement in public agencies. One of the functions that the system provided was for suppliers to confidentially respond to Requests for Proposals (RFP) posted on the e-Commerce site. A need arose for authentication and

encryption of these responses. I led the analysis and prototyping of several different approaches including PKI, certificates, tokens and biometrics.

IV. MATERIALS CONSIDERED

21. In forming my opinions, I have reviewed the following documents and any other document cited in this declaration.

Exhibit	Description
Ex. 1001	U.S. Patent No. 8,886,954 ("the '954 patent")
Ex. 1002	File History of U.S. Patent No. 8,886,954
Ex. 1005	U.S. Patent No. 7,188,110 to Ludtke et al. ("Ludtke")
Ex. 1006	U.S. Patent Application Publication No. 2002/0046336 to Kon et al. ("Kon")
Ex. 1007	*Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01444, Paper 11 (PTAB Feb. 28, 2022).
Ex. 1009	*Proxense, LLC v. Samsung Electronics Co., Ltd., et al.*, Case No. 6:21-cv-00210, Dkt. No. 43, Claim Construction Order (W.D. Tex. Jan. 18, 2022).
Ex. 1010	*Proxense, LLC v. Samsung Electronics Co., Ltd., et al.*, Case No. 6:21-cv-00210, Dkt. No. 149, Memorandum in Support of Claim Construction Order (W.D. Tex. Dec. 28, 2022).
Ex. 1011	U.S. Patent Application Publication No. 2003/0023882 to Udom ("Udom")
Ex. 1012	U.S. Patent Application Publication No. 2002/0019811 to Lapsley et. al. ("Lapsley")
Ex. 1013	*Proxense, LLC v. Google LLC, et al.*, Case No. 6:23-cv-00320, Dkt. No. 1, Complaint (W.D. Tex. May 2, 2023)

Exhibit	Description
Ex. 1014	*Proxense, LLC v. Google LLC*, Case No. 6:23-cv-00320, Preliminary Infringement Contentions (W.D. Tex. July 24, 2023).
Ex. 1015	*CERTIFICATION REPORT No. P165: Sony FeliCa Contactless Smart Card RC-S860*, UK IT Security Evaluation and Certification Scheme (Mar. 2002)
Ex. 1016	U.S. Patent Application Publication No. 2002/0049806 to Gatz et al. ("Gatz")
Ex. 1017	U.S. Patent Application Publication No. 2006/0034492 to Siegel et al. ("Siegel")
Ex. 1018	U.S. Patent Application Publication No. 2001/0036297 to Ikegami et al. ("Ikegami")
Ex. 1019	*Proxense, LLC v. Google LLC*, Case No. 6:23-cv-00320, Dkt. No. 45, Proxense's Responsive Claim Construction Brief (W.D. Tex. Dec. 1, 2023).
Ex. 1020	*Proxense, LLC v. Google LLC*, Case No. 6:23-cv-00320, Dkt. No. 45, Proxense's Expert Transcript (W.D. Tex. Dec. 18, 2023).
Ex. 1021	*Proxense, LLC v. Google LLC*, Case No. 6:23-cv-00320, Dkt. No. 50, Proxense's Sur-Reply Claim Construction Brief (W.D. Tex. Jan. 5, 2023).

22. I have also relied on my education, experience, research, training, and knowledge in the relevant art, and my understanding of any applicable legal principles described in this declaration.

23. All the opinions contained in this declaration are based on the documents I reviewed and my knowledge and professional judgment. My opinions

have also been guided by my understanding of how a person of ordinary skill in the art would have understood the claims of the ’954 patent.

24. I reserve the right to supplement and amend any of my opinions in this declaration based on documents, testimony, and other information that becomes available to me after the date of this declaration.

V. LEGAL STANDARDS

25. I am not a lawyer. My understanding of the legal standards to apply in reaching the conclusions in this declaration is based on discussions with counsel for Petitioner, my experience applying similar standards in other patent-related matters, and my reading of the documents submitted in this proceeding. In preparing this declaration, I have tried to faithfully apply these legal standards to the challenged claims.

26. I have been informed that there are two ways in which prior art may render a patent claim unpatentable. First, I have been informed that the prior art can “anticipate” a claim. Second, I have been informed that the prior art can render a claim “obvious” to a person of ordinary skill in the art. I understand that a claim is patentable if it was not anticipated and would not have been obvious in view of the prior art as of the effective filing date of the patent.

27. I have been informed that a dependent claim is a patent claim that refers back to another patent claim. I have been informed that a dependent claim includes all the limitations of the claim to which it refers.

28. I have been asked to provide my opinions as to whether the cited prior art discloses or renders obvious claims 1-7, 10, 12-19, and 22-27 of the '954 patent from the perspective of a person of ordinary skill in the art at the '954 patent's earliest priority date in 2004, as described in more detail below.

29. I have been informed that in *inter partes* review proceedings, such as this one, the party challenging the patent bears the burden of proving unpatentability by a preponderance of the evidence. I understand that a preponderance of the evidence means "more likely than not."

30. For the purposes of this declaration, I have been asked to provide my opinions on issues regarding unpatentability. I have been informed of the following legal standards, which I have applied in forming my opinions.

A. Level of Ordinary Skill

31. I have been informed that a person of ordinary skill in the art is determined by considering several factors, including the (i) type of problems encountered in the art; (ii) prior art solutions to those problems; (iii) rapidity with which innovations are made; (iv) sophistication of the technology; and (v) educational level of active workers in the field.

32. I have been instructed to assume that a person of ordinary skill in the art is not a specific real individual but rather a hypothetical individual having the qualities reflected by the factors discussed above.

B. Prior Art

33. I have been advised and understand that the information used to evaluate whether an invention was new and not obvious when made is generally referred to as "prior art." I understand that prior art includes patents and printed publications that existed before the earliest priority date or the earliest filing date of the patent (which I have been informed is also called the "effective filing date"). I have been informed and understand that a patent or published patent application is prior art if it was filed before the earliest filing date of the claimed invention and that a printed publication is prior art if it was publicly available before the earliest filing date.

C. Anticipation

34. I have been informed that under 35 U.S.C. § 102, a patent claim is unpatentable for anticipation if the claimed subject matter was patented or described in a printed publication before the effective filing date of the claimed invention. I have been informed that this is referred to as unpatentability by anticipation. I have been informed that a patent claim is anticipated under § 102 if a single prior art reference discloses all limitations of the claimed invention.

D. Obviousness

35. I have been informed that for obviousness under 35 U.S.C. § 103, a patent claim is unpatentable if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art to which said subject matter pertains at the time the invention was made. I have been informed that this is referred to as unpatentability by obviousness.

36. I have been informed that an obviousness analysis includes the following considerations:

a. Determining the scope and content of the prior art;

b. Ascertaining the differences between the prior art and the claims at issue;

c. Resolving the level of ordinary skill in the pertinent art; and

d. Considering evidence of secondary indicia of nonobviousness (if available).

37. I have been informed that the relevant time for considering whether a claim would have been obvious to a person of ordinary skill in the art is the time of invention. For my obviousness analysis, counsel for Petitioner instructed me to assume that the date of invention for the challenged claims is December 20, 2004. My opinions would not change if I assumed a later date of invention.

38. I have been informed that a reference may be modified or combined with other references or with a person of ordinary skill in the art's own knowledge if the person would have found the modification or combination obvious. I have also been informed that a person of ordinary skill in the art is presumed to know all the relevant prior art, and the obviousness analysis may take into account the inferences and creative steps that a person of ordinary skill in the art would employ.

39. I have been informed that whether a prior art reference renders a patent claim obvious is determined from the perspective of a person of ordinary skill in the art. I have also been informed that, while there is no requirement that the prior art contain an express suggestion to combine known elements to achieve the claimed invention, and while a suggestion to combine known elements to achieve the claimed invention may come from the prior art as a whole or individually and may consider the inferences and creative steps a person of ordinary skill in the art would employ, as filtered through the knowledge of one skilled in the art, obviousness grounds cannot be sustained by mere conclusory statements and must include some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.

40. In determining whether a prior art reference could have been combined with another prior art reference or other information known to a person

having ordinary skill in the art, I have been informed that the following principles may be considered:

a. A combination of familiar elements according to known methods is likely to be obvious if it yields predictable results;

b. The substitution of one known element for another is likely to be obvious if it yields predictable results;

c. The use of a known technique to improve similar items or methods in the same way is likely to be obvious if it yields predictable results;

d. The application of a known technique to a prior art reference that is ready for improvement to yield predictable results;

e. Any need or problem known in the field and addressed by the reference can provide a reason for combining the elements in the manner claimed;

f. A person of ordinary skill often will be able to fit the teachings of multiple references together like a puzzle; and

g. The proper analysis of obviousness requires a determination of whether a person of ordinary skill in the art would have a "reasonable expectation of success"—but not "absolute predictability" of success—in achieving the claimed invention by combining prior art references.

41. I have been informed that, when a work is available in one field, design alternatives and other market forces can prompt variations of it, either in the same field or in another. I have been informed that if a person of ordinary skill in the art could have implemented a predictable variation and would have seen the benefit of doing so, that variation is likely to have been obvious. I have been informed that, in many fields, there may be little discussion of obvious combinations, and in these fields, market demand—not scientific literature—may drive design trends. I have been informed that, when there was a design need or market pressure and there are a finite number of predictable solutions, a person of ordinary skill in the art would have had a good reason to pursue those known options.

42. I have been informed that the law permits the application of "common sense" in examining whether a claimed invention would have been obvious to a person skilled in the art. For example, I have been informed that combining familiar elements according to known methods and in a predictable way may suggest obviousness when such a combination would yield nothing more than predictable results. I understand, however, that a claim is not obvious merely because every claim element is disclosed in the prior art, and that a party asserting obviousness must still provide a specific motivation to combine or modify the

references as recited in the claims and explain why one skilled in the art would have reasonably expected to succeed in doing so.

43. I have been informed that there is no rigid rule that a reference or combination of references must contain a "teaching, suggestion, or motivation" to combine references. But I also understand that the "teaching, suggestion, or motivation" test can be a useful guide in establishing a rationale for combining elements of the prior art. I have been informed that this test poses the question as to whether there is an express or implied teaching, suggestion, or motivation to combine prior art elements in a way that realizes the claimed invention, and that it seeks to counter impermissible hindsight analysis.

44. I am not aware of any evidence of secondary considerations that would support a determination of nonobviousness of the claimed subject matter in the '954 patent.

45. I have been informed that, in an obviousness analysis, prior art must be analogous to the patent being considered. I have been informed that a prior art reference is considered to be analogous, or in the same field of art, if the reference is either (1) in the same field of endeavor as the challenged patent, regardless of the problems the challenged patent and the prior art address; or (2) reasonably pertinent to the particular problem being solved by the challenged patent.

VI. THE ’954 PATENT

A. Overview

46. The ’954 patent was filed on December 10, 2012, and claims priority to U.S. Patent Application Ser. No. 11/314,199, filed December 20, 2005, which claims the benefit of provisional applications filed on December 20, 2004, and February 14 2005. Ex. 1001, cover page. The ’954 patent generally relates to “authentication responsive to biometric verification.” Ex. 1001, 1:19-22.

47. Figure 6 illustrates a process for “verifying a subject” using a biometric key. Ex. 1001, 7:60-62. As shown in Figure 6, the device receives biometric scan data, such as a fingerprint scan, from the user (step 620). Ex. 1001, FIG. 6. If the scan data matches “previously-stored biometric data,” (step 630), the user is “verified” (step 640), at which point a “code” is sent to a trusted key authority (step 650). Ex. 1001, 7:64-8:4, FIG. 6.

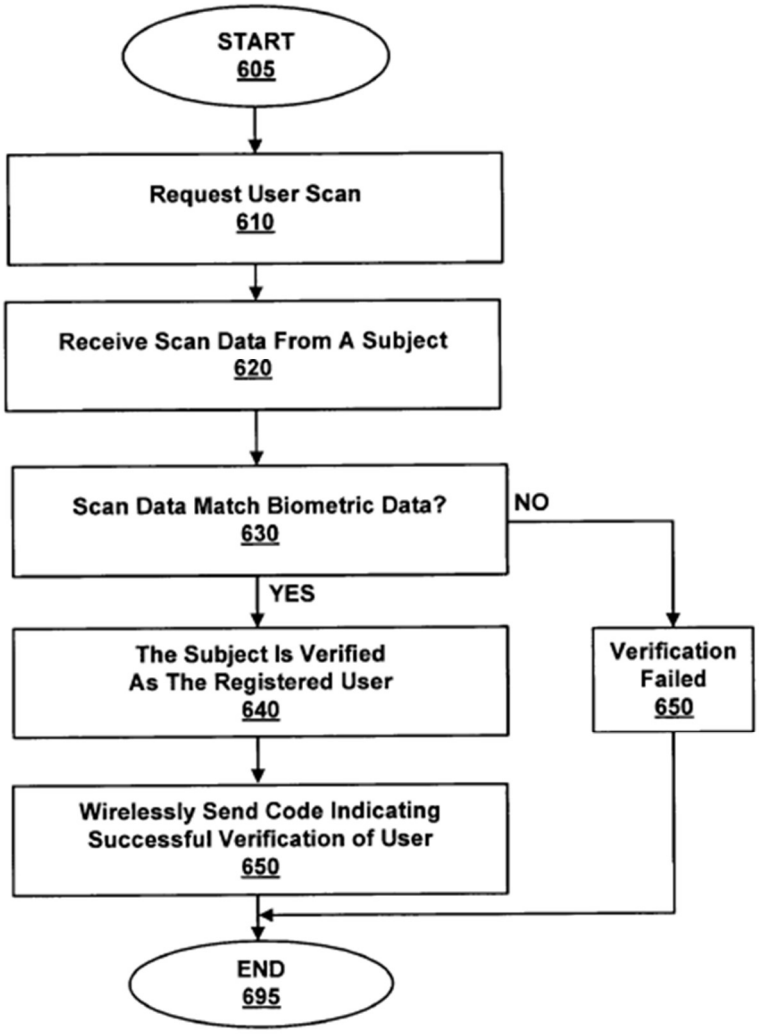


FIG. 6

Ex. 1001, FIG. 6.

48. Once the code is received, as illustrated in Figure 7, the trusted key authority determines whether the code is "authentic" (step 730). Ex. 1001, 8:5-12, FIG. 7. "If authentication is successful, the trusted key authority sends an access message to [an] application to allow user access and/or provide additional information from the profile" (step 740). Ex. 1001, 8:12-15, FIG. 7. If authentication is not successful, authentication fails (step 750) and "the message to

the application indicates that the user should be denied access." Ex. 1001, 8:15-17, FIG. 7.

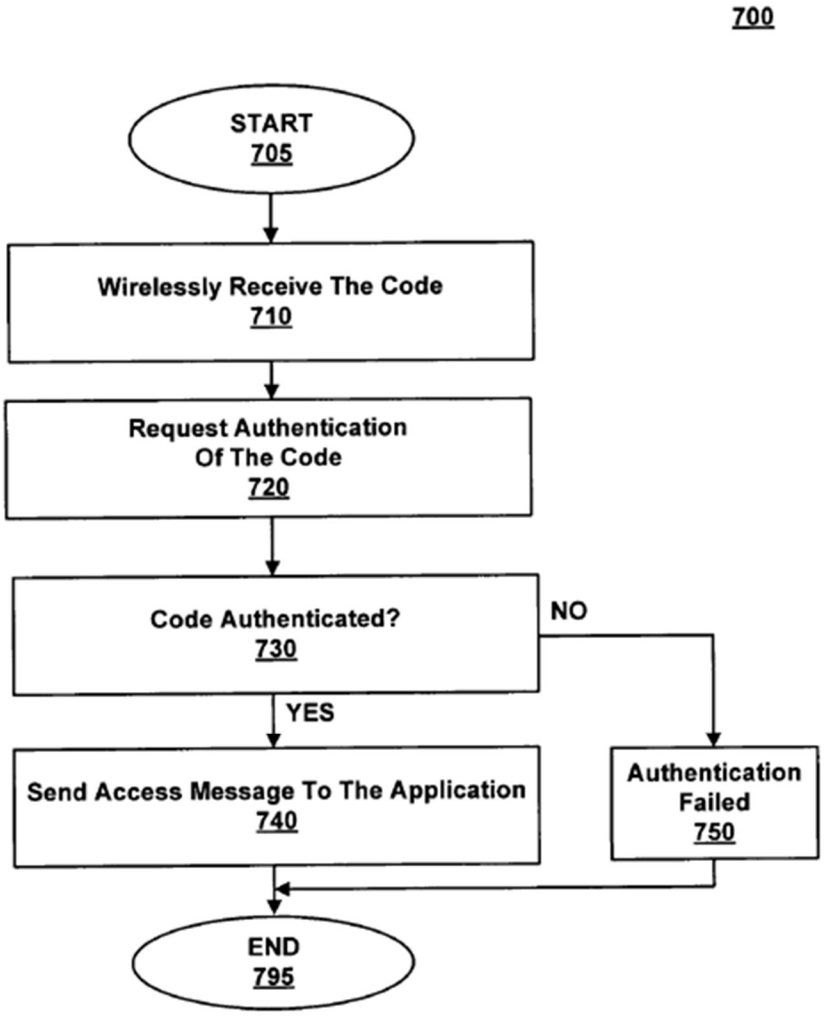


FIG. 7

Ex. 1001, FIG. 7.

VII. CLAIM CONSTRUCTION

49. I have been instructed that the "intrinsic record" includes the '954 patent itself, including the claims, description, and figures (Ex. 1001), and the '954 patent's prosecution history, which I understand is the record of proceedings at the

U.S. Patent and Trademark Office ("Patent Office") concerning the patent (Ex. 1002). I understand that, like the claims and written description, the prosecution history provides evidence to a person of ordinary skill in the art of how the inventor intended their patent to be understood and how the Patent Office understood the patent. I understand that the inventor is permitted to apply a special definition to the terms or to limit the scope of claim terms in their patent claims, which may differ from the term's plain and ordinary meaning. That special definition or limitation on scope may be provided in the patent's written description, the patent's prosecution history, or both.

50. I understand that claim interpretation may also be informed by "extrinsic evidence" (that is, evidence outside of the patent record itself). I have been informed that extrinsic evidence may include dictionaries, technical treatises, and other materials evidencing the meaning of a claim term and the understanding held by a person of ordinary skill in the art in the relevant time period.

51. I understand that in a previous district court litigation, *Proxense, LLC v. Samsung Electronics Co., Ltd., et al*., Case No. 6:21-cv-00210, two terms from the '730 patent, to which the '954 patent claims benefit, were construed by the court (Exs. 1009-1010):

- Device ID Code – "[a] unique code identifying a device;" and

- Access Message – "[a] signal or notification enabling or announcing access."

Ex. 1009, 3; Ex. 1010, 15, 20.

52. I have been asked for the purposes of this declaration to apply these constructions and the plain and ordinary meaning of the claim terms as they would have been understood by a person of ordinary skill in the art at the earliest priority date of the '954 patent. It is my opinion that the prior art relied on in the Petition discloses each of these prior constructions, and the plain and ordinary meaning of all terms.

VIII. LEVEL OF ORDINARY SKILL IN THE ART

53. In rendering the opinions set forth in this declaration, I have been asked to consider the '954 patent's claims and the prior art through the eyes of a person of ordinary skill in the art (which I may also refer to as "one skilled in the art," "skilled artisan," "POSITA," or similar variations). I have considered factors such as the educational level and years of experience of those working in the pertinent art, the types of problems encountered in the art, the teachings of the prior art, patents and publications of other persons or companies, and the sophistication of the technology.

54. Taking the factors described in the Legal Standards – Level of Ordinary Skill section into consideration, it is my opinion that a POSITA at the

time of the purported invention would have had at least a bachelor's degree in Computer or Electrical Engineering or an equivalent engineering discipline, and at least three years of experience in the field of encryption and security, or the equivalent. Additional education could substitute for professional experience, and significant work experience could substitute for formal education.

55. I met the criteria for a POSITA at the effective filing date of the '954 patent.

IX. THE PRIOR ART

56. In forming my opinions, I found the following prior art relevant when considering whether the claims of the '954 patent would have been obvious to a person of ordinary skill in the art.

Exhibit	Description
Ex. 1005	U.S. Patent No. 7,188,110 to Ludtke et al. ("Ludtke")
Ex. 1006	U.S. Patent Application Publication No. 2002/0046336 to Kon et al. ("Kon")
Ex. 1011	U.S. Patent Application Publication No. 2003/0023882 to Udom ("Udom")
Ex. 1012	U.S. Patent Application Publication No. 2002/0019811 to Lapsley et. al ("Lapsley")
Ex. 1015	*CERTIFICATION REPORT No. P165: Sony FeliCa Contactless Smart Card RC-S860*, UK IT Security Evaluation and Certification Scheme (Mar. 2002)
Ex. 1016	U.S. Patent Application Publication No. 2002/0049806 to Gatz et al. ("Gatz")

Exhibit	Description
Ex. 1017	U.S. Patent Application Publication No. 2006/0034492 to Siegel et al. ("Siegel")
Ex. 1018	U.S. Patent Application Publication No. 2001/0036297 to Ikegami et al. ("Ikegami")

57. As explained below, in my opinion, claims 1-7, 10, 12-19, and 22-27 of the '954 patent would have been obvious based on Ludtke and Kon in the combinations discussed below.

A. Ludtke (U.S. Patent No. 7,188,110)

58. Ludtke issued as U.S. Patent No. 7,188,110 on March 6, 2007, and was filed on December 11, 2000. Ludtke, cover page. I understand and have been asked to assume that Ludtke is prior art to the '954 patent. Ludtke discloses systems and methods of authorizing a user to conduct a transaction using a "biometric device" (also called a "transaction device") such as a privacy card and/or digital wallet. Ludtke, Abstract, 3:32-36, 6:36-44. The transaction device includes a processor, memory, and fingerprint recognition technology. Ludtke, 5:60-64, FIG. 7A. Ludtke stores "authorized fingerprint recognition samples," a device ID corresponding to the privacy card, and a public key infrastructure ("PKI") key on the transaction device. Ludtke, 11:66-12:7, 14:19-21, 38:26-29. Ludtke also indicates that the biometric device can use other techniques, such as a

"retinal scan, voice, DNA, hand profile, face recognition, etc.," instead of or in addition to fingerprints. Ludtke, 35:61-64.

59. When an authorized user attempts to use the transaction device, e.g., at a point of sale ("POS") terminal, or other "service," the user is "prompted to supply a fingerprint recognition sample" as an initial security measure. Ludtke, 1:22-31, 1:37-38, 14:33-40. The sample is compared to stored fingerprints, and if the sample is recognized, the user is authorized. Ludtke, 14:41-46.

60. In one embodiment, "the transaction device is used to trigger shopping activity," such as a "web-based transaction using a transaction device such as a privacy card and/or digital wallet and a personal POS terminal" by "clicking on a 'Buy' or similar button in the web browser." Ludtke, 28:26-40. The POS asks the transaction device to "validate the user" and the user is "prompted to supply a fingerprint recognition sample" as an initial security measure. Ludtke, 1:23-30, 1:37-38, 14:33-40, 18:45-50, 18:52-55. The sample is compared to stored fingerprints, and if the sample is recognized, the user is authorized.
Ludtke, 14:41-46. Once the transaction device authorizes the user based on the matching biometric information, the personal POS terminal "opens a secure communications session to the TPCH, requesting a transaction," and "provides the transaction record that it received from the web browser *and the unique ID of the transaction device*." Ludtke, 29:5-10 (emphasis added); *see also* Ludtke, 27:12-13

("Privacy card information is provided to TPCH, step 1510."), 34:25-27 (explaining that "necessary secure transaction communication with the TPCH [includes] providing the transaction data *and its device ID*." (emphasis added)). The TPCH is a trusted third-party agent, separate from the transaction device, personal POS terminal, and the back-end transacting entity (e.g., vendor). Ludtke, 7:42-48, 9:26-34.

61. Ludtke also discloses an alternate embodiment in which the POS "functionality of providing secure communication and transactions with the Transaction Privacy Clearing House (TPCH)," described above, "can be integrated into the digital wallet directly." Ludtke, 28:41-45. Thus, Ludtke also discloses communicating the device ID directly from the transaction device to the TPCH responsive to a "match" between the scanned biometric data (fingerprint) and stored data.

62. Next, Ludtke performs two steps 1) authenticating the transaction device and 2) completing a purchase transaction with a vendor via a third party authority. "The TPCH uses the unique ID of the transaction device to process the transaction. After validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCH issues a transaction confirmation back to the personal POS terminal" that "reflects the transaction confirmation back to … the transaction device. The transaction device

may display a transaction confirmation to the user and may additionally record the transaction in its local storage." Ludtke, 29:12-24, FIG. 15.

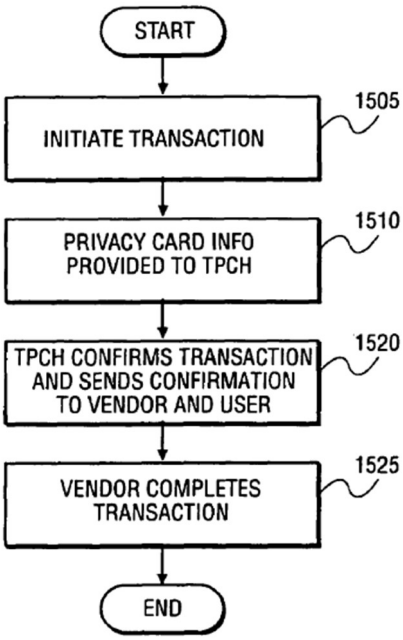


FIG. 15

Ludtke, FIG. 15.

63. Ludtke is directed to the same technical field as the '954 patent: user authentication methods and systems. *Compare* Ex. 1001, 1:19-21, *with* Ludtke, 1:59-61.

B. Kon (U.S. Patent Application Publication No. 2002/0046336)

64. Kon was published as U.S. Patent Application Publication No. 2002/0046336 on April 18, 2002, and was filed on August 30, 2001. Kon, cover

page. I understand and have been asked to assume that Kon is prior art to the ’954 patent.

65. Kon discloses authenticating a user transaction “in response to a request from a user device.” Kon, [0174]. Like Ludtke, Kon uses the user’s biometric information, which includes “fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information,” and “the ID of a user device” (device ID) to authorize a user and their corresponding device to conduct a transaction. Kon, [0060], [0173], [0178], [0194] (explaining that the public key certificate (“PKC”) includes the ID of the user device), [0026]-[0229] (explaining that a person identification certificate (“IDC”) includes the PKC).

66. Kon’s authenticating information is stored in an IDC, illustrated in Figure 5. Kon, FIG. 5, [0194] (explaining that the PKC “Subject” field includes the ID of the user device), [0217], [0226]-[0229] (explaining that the IDC includes “Subject Template Info” where “data representing biometric information such as a fingerprint of the user is stored,” and “Subject PKC Info” containing the PKC information).

FIG. 5

	Item	Description
Indis-pensable Items	Version	Version
	Serial Number	Identification Number
	signature algorithm Identifier algorithm parameters	Signature algorithem Algorithm Parameters
	Issuer	Name of the identification authority (in the form of a distinguished name)
	Validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date
	Subject	Name of the subject to be certificated (in a DN form)
Extended Items	subject Template Info encrypt Type encrypt Unique ID encryption Algorithm parameter validity subject Template Source subject Template	Template information • encrypt Type • The unique ID or the certificate number of a public key certificate used for encryption • Algorithm • parameter • Validity period (start date, expiration date) • Type of the template • Template
	Subject PKC info subject PKC serial Number subject PKC Unique ID	Information about the public key certificate of the subject • Certificate number of the subject public key certificate • Unique ID of the subject of the subject public key certificate
	Issuer Unique ID	Unique ID of the issuer
	Subject Unique ID	Unique ID of the subject
	Public Key Certificate	Public key certificate
	Issuer Alt Name	Alternative name of the issuer
	subject Directory Attributes	Personal information (encrypted as required) information used to authenticate subject Age, sex, etc.

Kon, FIG. 5 (annotated, excerpted).

67. Kon further discloses that the user's personal information, including the user's age, is registered for incorporation in the IDC (e.g., in the "Extended" field section) in association with the device ID (located in the "Subject" field). Kon, [0194] ("Subject is a field in which the name of a subject or a user is described. More specifically, for example, *the ID of a user device* or the ID of a

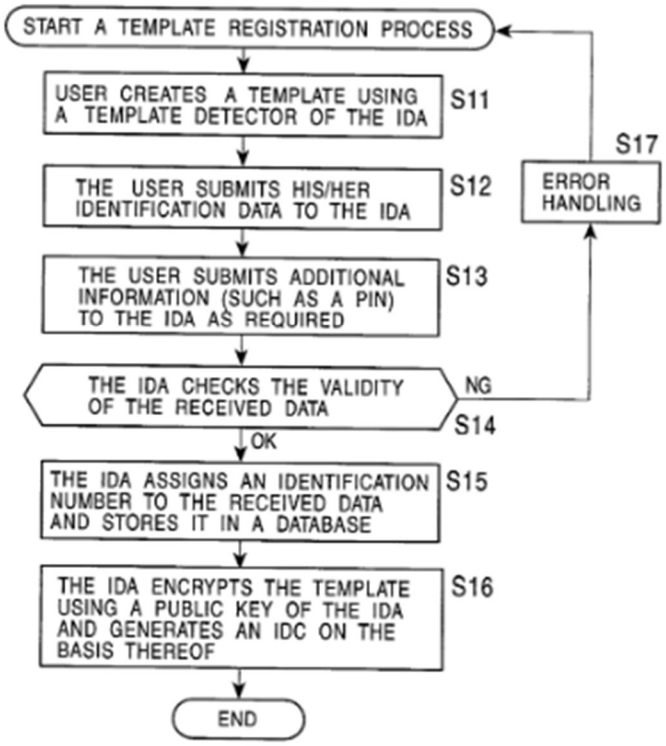
subject which supplies services is described." (emphasis added)), [0234] ("[A]n arbitrary attribute of [a] user, such as an *age*, sex, address, [or] telephone number, is encrypted *as required to identify the user*." (emphases added)), [0241] ("The person identification certificate (IDC) described above includes information (template information) used to identify a person. An example of template information is biometric information…. Personal identification information other than biometric information is also usable. Specific examples of such personal identification information includes a seal, *a passport, a driver's license*, and a card." (emphasis added)), [0264] ("To effectively *register* a person identification certificate (IDC), a person to be certified with a person identification certificate (IDC) first presents sampling information to register his/her template." (emphasis added)), [0265] ("FIG. 9 illustrates a flow in terms of registration of a template and creation of an IDC. Registration of a template is performed on the basis of information (sampling information) acquired using an apparatus capable of acquiring personal information in one of the various forms described earlier."), FIGS. 5 and 9.

FIG. 5

	Item	Description
Indis-pensable Items	Version	Version
	Serial Number	Identification Number
	signature algorithm Identifier algorithm parameters	Signature algorithem Algorithm Parameters
	Issuer	Name of the identification authority (in the form of a distinguished name)
	Validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date
	Subject	Name of the subject to be certificated (in a DN form)
Extended Items	subject Template Info encrypt Type encrypt Unique ID encryption Algorithm parameter validity subject Template Source subject Template	Template information • encrypt Type • The unique ID or the certificate number of a public key certificate used for encryption • Algorithm • parameter • Validity period (start date, expiration date) • Type of the template • Template
	Subject PKC info subject PKC serial Number subject PKC Unique ID	Information about the public key certificate of the subject • Certificate number of the subject public key certificate • Unique ID of the subject of the subject public key certificate
	Issuer Unique ID	Unique ID of the issuer
	Subject Unique ID	Unique ID of the subject
	Public Key Certificate	Public key certificate
	Issuer Alt Name	Alternative name of the issuer
	subject Directory Attributes	Personal information (encrypted as required) information used to authenticate subject Age, sex, etc.

Kon, FIG. 5 (annotated, excerpted) (illustrating registered user information).

FIG. 9



Kon, FIG. 9 (illustrating process for registering user identification information).

68. Kon is directed to the same technical field as the ’954 patent: user authentication methods and systems. *Compare* Ex. 1001, 1:19-21, *with* Kon, [0020], [0034].

X. GROUNDS OF UNPATENTABILITY

69. Based on my review of the materials set forth above, including my application of the knowledge of a person of ordinary skill in the art, it is my opinion that claims 1-7, 10, 12-19, and 22-27 of the ’954 patent would have been obvious to one of ordinary skill in the art.

70. In particular, it is my opinion that claims 1-7, 10, 12-19, and 22-27 of the ’954 patent would have been obvious to a person of ordinary skill in the art at the earliest priority date of the ’954 patent, based on the combinations shown below:

Ground	Claim(s) Challenged	35 U.S.C. §	Reference(s)
1	1, 2, 4-7, 10, 12, 13, 15, 16, 18, 19, and 22-27	103	Ludtke
2	3, 14, 17	103	Ludtke and Kon

XI. THE CHALLENGED CLAIMS ARE UNPATENTABLE BASED ON THE PRIOR ART

A. Ground 1: Claims 1, 2, 4-7, 10, 12, 13, 15, 16, 18, 19, and 22-27 Are Obvious in View of Ludtke.

1. Independent claim 1

a. [1preamble]: “A method comprising:”

71. To the extent limiting, Ludtke discloses [1preamble] because Ludtke discloses “[a] method of identifying an authorized user with a biometric device and enabling the authorized user to access private information” using a “transaction device” such as a privacy card and/or digital wallet (integrated device). Ludtke, Abstract, 3:32-36.

72. Ludtke explains that “[t]he user connects to and performs transactions with [an] eCommerce system through a transaction device which has a unique

identifier (ID)" such as "a privacy card" or "a digital wallet" (integrated devices). Ludtke, 3:32-36.

b. [1ai]: "persistently storing biometric data of a user [in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered] and"

73. Ludtke discloses [1ai] because its transaction device, like a privacy card and/or digital wallet (integrated device), stores "authorized fingerprint recognition samples" (biometric data of the user) in a "user identity/account information block 760" or "write-once memory" (persistent storage). Ludtke, 13:27-29, 14:19-21, 19:9-14, 19:29-40, FIGS. 7B-7C.

74. The '954 patent defines "integrated device" as a device, such as a mobile phone (e.g. a cellular phone or Smartphone), tablet, laptop, mp3 player, mobile gaming device, watch, key fob *or other mobile device*" "having an integrated biometric key." Ex. 1001, 2:41-48, 4:6-14 (emphasis added). The '954 patent further describes a "biometric key" as including the elements recited in FIG. 2, including a biometric module, a control module, and an RF module. Ex. 1001, FIG. 2, 4:40-5:62. Ludtke's transaction device (such as digital wallet or privacy card) likewise includes a biometric key and constitutes an integrated device consistent with this construction, as explained below.

75. Ludtke's privacy card (integrated device) has a "user identity/account information block 760 [that] *stores data* about the user and accounts that are

accessed by the card" including "the authorized fingerprint recognition samples." Ludtke, 13:27-29, 14:19-21, 14:13-18 (emphasis added) (explaining that the privacy card embodied in Figure 7C "may include those functions set forth in FIG. 7B, referred to herein as first generation privacy card technology block 775 and FeliCa[1] Technology block 774.").

76. Ludtke explains that "[t]he fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). If confirmation succeeds, the device writes the fingerprint image data *into write-once memory*" (persistent storage). Ludtke, 19:9-14, 19:29-40 (emphasis added).

[1] FeliCa is a "contactless (wireless) card execution platform." Ludtke, 11:1-5.

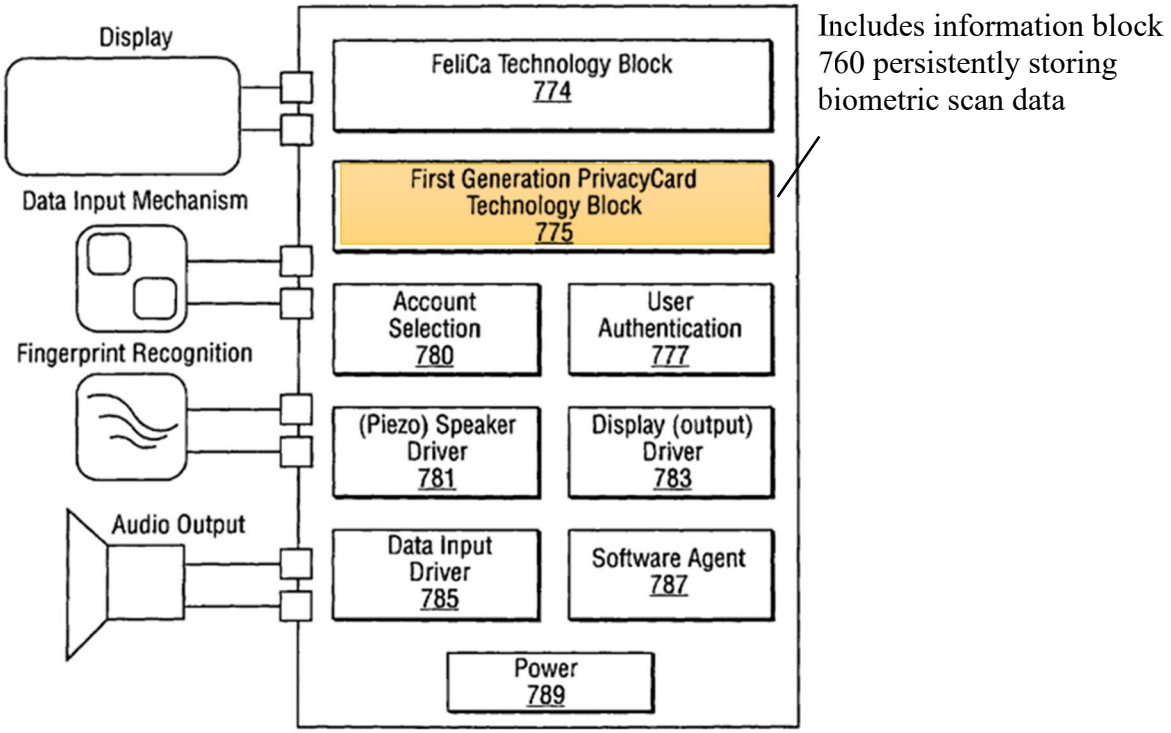


FIG. 7C

Ludtke, FIG. 7C (annotated).

77. A POSITA would have understood that Ludtke's fingerprint data is persistently stored in a tamper proof format that is unable to be subsequently altered because it is stored in "write-once memory." Ludtke, 19:9-14, 19:29-40. This is consistent with the '954 patent, which explains that "*at least some of persistent storage 226 is a memory element that can be written to once but cannot subsequently be altered.* Persistent storage 226 can include, for example, a ROM element, a flash memory element, or any other type of non-volatile storage element. Persistent storage 226, when implemented as write-once memory as disclosed in Ludtke, is itself, and stores data in, a tamper proof format to prevent

any changes to the stored data. Tamper[-]proofing increases reliability of authentication because it does not allow any changes to biometric data (i.e., allows reads of stored data, but not writes to store new data or modify existing data)." Ex. 1001, 5:22-34 (emphasis added).

c. [1aii]: "[persistently storing] a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device [in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered] and"

78. Ludtke discloses and renders obvious [1aii] because its transaction device (integrated device) stores a "unique transaction device ID value[]" (device ID code) in its "permanent memory" (persistent storage). Ludtke, 30:20-23.[2]

79. Ludtke's stored device ID, like a "globally unique silicon ID (GUID) 764[,] is used to identify the privacy card among other existing transaction cards," and thus uniquely identifies the privacy card (integrated) device. Ludtke, 13:39-41. Even if the claim language is interpreted to require storing additional

[2] Patent Owner indicated in its Sur-Reply Claim Construction Brief that "the plain and ordinary meaning of the claim term, that within this stored area are (1) codes and values uniquely identifying an integrated device or biometric key; and (2) a secret decryption value." Ex. 1021, 8. Ludtke's transaction devices likewise store a device ID and a secret decryption value, as explained below.

codes besides the "device ID code," Ludtke discloses that the device ID is stored along with other codes and data values, e.g., magnetic stripe and bar codes, which allow the transaction device to interface with a POS terminal. Ludtke, 8:63-67, 9:18-25, 23:11-19.

80. A POSITA would have understood that the transaction device ID is stored in a tamper proof format unable to be subsequently altered because it is intended to *uniquely* identify the device to which it corresponds and "contain[s] an identification that maintains the confidentiality of the user's identity." Ludtke, 10:64-67, 30:20-23. Storing the device ID in a tamper proof format, unable to be subsequently altered, would have comported with Ludtke's goal of ensuring that the device is authorized to perform certain transactions and ensuring the integrity of the confidential information. Ludtke, 30:18-27. Ludtke's use of FeliCa technology further suggests storing information in a tamper proof format because contactless smart cards implementing FeliCa were known to be tamper resistant. Ex. 1015, 21, 25.

81. Furthermore, it is my opinion that a POSITA would have been motivated and found it obvious to store the device ID in "write-once memory" to prevent modification of the transaction device ID and ensure that the ID is associated with the correct device. Ludtke uses write-once memory to store other kinds of sensitive information (e.g., biometric data as explained in [1ai], above) in

a tamper proof format unable to be subsequently altered, and a POSITA would have had a reasonable expectation of success in using the same type of memory to store the keys as well. Indeed, because Ludtke's device ID "contain[s] an identification that maintains the confidentiality of the user's identity" (Ludtke, 10:64-67), a POSITA would have understood the importance of ensuring the integrity of the device ID and would have been motivated to store it in the same format as Ludtke's fingerprint data—tamper proof and unable to be subsequently altered—to preserve its integrity.

d. [1aiii]: "[persistently storing] a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;"

82. Ludtke discloses and renders obvious [1aiii] because the transaction device uses a public key infrastructure (PKI) to verify the user, and the PKI requires the transaction device to store either a public key or a private key (secret decryption value) to decrypt encrypted data. Ludtke, 5:11-20; 38:9-14. The disclosure of Ludtke makes clear that both Ludtke's public key and private key are "secret values" that are used for decryption.

83. Ludtke discloses that the "sensitive nature of the information being transferred, such as access codes, PINs, etc.," make it "desire[able] to use a secure communication means and/or encryption to lessen the possibility of unauthorized use of the information." Ludtke, 37:39-45. To ensure the integrity of sensitive

information, Ludtke uses a PKI system to encrypt and decrypt transmitted data. Ludtke, 5:11-20; 38:9-14.

Public Key Decryption

84. In one example, the transaction device stores a secret decryption value configured as a public key. While public keys were traditionally known to various parties (and therefore not secret), Ludtke discloses using a public decryption key that is only known to the communicating parties for the purposes of exchanging sensitive data, like a password, in a one-to-one configuration where a single "public key" is distributed to correspond to a single "private key"; therefore, *both* the public and private keys of Ludtke comprise a "secret" value. Ludtke, 38:1-3 ("there may be a *one-to-one* relationship between a password and a public key"), 38:12-14 ("data that is encrypted with a private key [is] only [] capable of being decrypted with the public key[,]"), 38:25-29 ("The back-end distributes *one public key with each password* and *the biometric device stores and associates these back-end public keys with the associated password and data*. . . ." (emphasis added)). This is also consistent with Patent Owner's expert's representations in the district court that "something that is secret is typically referred to as something that's not known to the adversary" (Ex. 1020, 45:16-22), or in other words, secret values "are not available to anyone who hasn't been explicitly given the secret value." Ex. 1020, 46:11-18; *see also* Ex. 1020, 50:11-14 ("The idea behind these protocols is

that only the parties that the designer of the protocol wants would know the secret keys, and the bad guys wouldn't.").

85. Ludtke's secret public decryption key is used by the transaction device to decrypt data encrypted by the back end's private key. More specifically, "the back-end select[s] an *unused* PKI key pair (one public, one private) from its internal database of keys" then "combines the selected public key with the password data structure, adds a password ID, and encrypts this entire combination with its private session key. It then, at 2710, transmits this to the device." When the device receives the encrypted information (e.g., a Password ID), "the device *decrypts* and authenticates the incoming data *using the public session key* of the back-end system and other elements of the PKI system that are well known to those skilled in the art." Ludtke, 38:49-61 (emphasis added).

86. Accordingly, a POSITA would have understood that Ludtke stores a secret public decryption key, i.e., a secret decryption value.

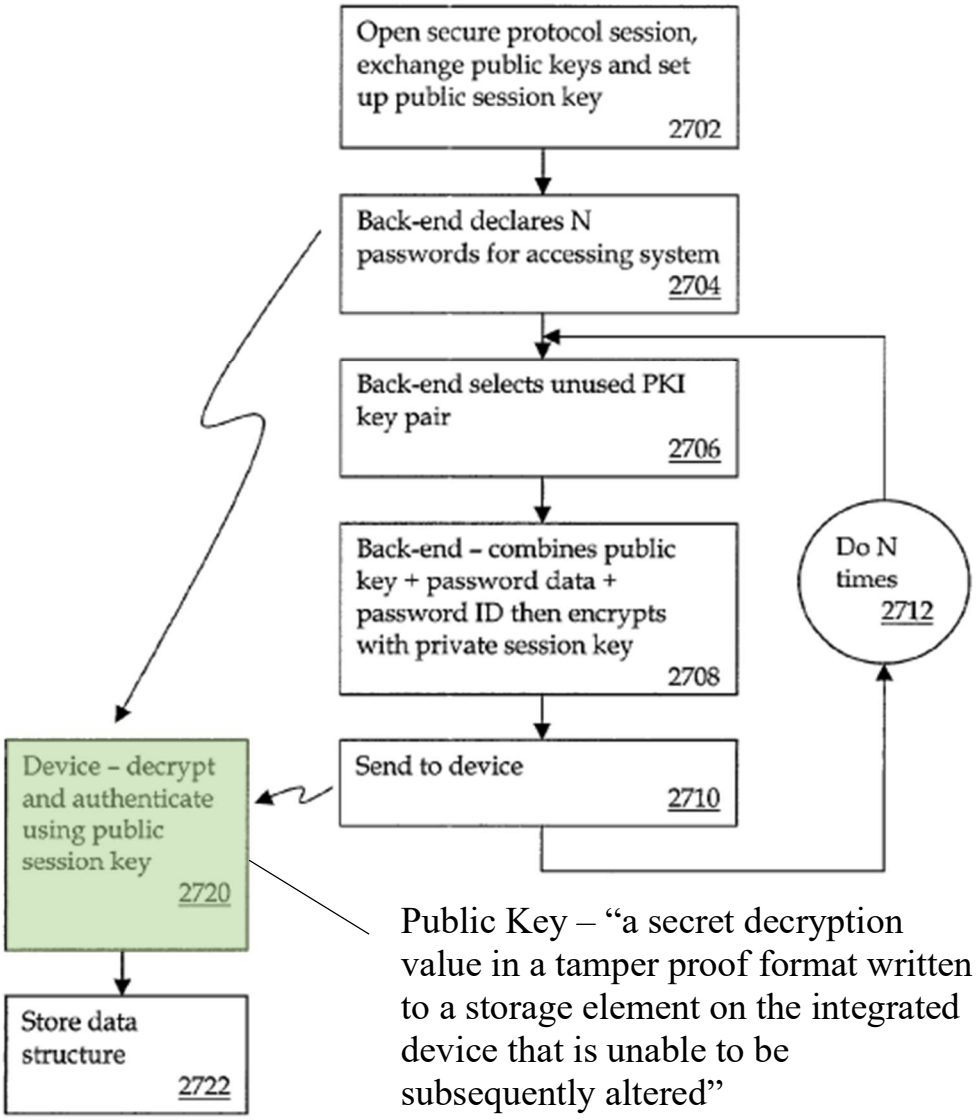


FIG. 27

Ludtke, FIG. 27 (annotated).

87. In my opinion, a POSITA would have been motivated and found it obvious to store the key in a tamper-proof format unable to be subsequently altered to comport with Ludtke's goal of generally preserving the integrity and confidentiality of sensitive information, like the key. Ludtke, 38:1-3, 9-21,

37:39-45. Because the key itself is considered sensitive and confidential information, since it grants access to additional sensitive and confidential information, if the key could be modified or tampered with, its integrity would be compromised. Indeed, the integrity of the system at large, which is intended to secure sensitive and confidential information, would also be compromised if the secret key cannot be secured.

88. Specifically, a POSITA would have been motivated and found it obvious to store the key in "write-once memory," i.e., in a tamper proof format that is unable to be subsequently altered, to prevent tampering and modification, thereby enhancing the security of the system generally and ensuring that sensitive data, like the key itself, remains secure. Ludtke uses write-once memory to store other kinds of sensitive information (e.g., biometric data as explained in [1ai], above), in a tamper proof format unable to be subsequently altered, and a POSITA would have had a reasonable expectation of success in using the same type of memory to store the keys as well.

Private Decryption Key

89. Ludtke also discloses storing one or more private keys (secret decryption values) on the transaction device.

90. Because information that is encrypted using a public key is decrypted with a private key (Ludtke, 38:9-14), a POSITA would have also understood that

the private key stored at the transaction device is used to decrypt data encrypted using a public key—and therefore constitutes a secret decryption value.

91. A POSITA would have been motivated and found it obvious to store keys in "write-once memory," i.e., in a tamper proof format that is unable to be subsequently altered, to prevent modification and thereby enhance the security of the system, as discussed above.

Private Encryption Key

92. Patent Owner in its complaint and infringement contentions identifies a private encryption key as a "secret[] decryption value." Ex. 1013, ¶ ("Android phones must contain a secret[] decryption value (i.e., the encryption key only accessible on the user's own device)"); Ex. 1014, 15, 54. Ludtke also discloses storing a private encryption key on its transaction device.

93. For example, Ludtke explains that the transaction device may transmit a password encrypted with the device's private encryption key to the back-end for decryption. As explained in column 39, the transaction device may "choose the PKI key pairs associated" with passwords, and "inform the back-end system about this key/password relationship, passing a 'security mechanism public key' and password to the back-end." Ludtke, 39:7-12. Then, "[w]hen the back-end issues a challenge for a password with a given ID, *the device encrypts the password with its corresponding private key* and transmits [both] to the back-end" for decryption.

Ludtke, 39:13-18 (emphasis added). In another example, Ludtke the digital wallet (transaction device) sends the "DW [Digital Wallet] identification (ID) plus an encrypted message using the DW private key" so the access site (back-end) "will decrypt the message with the DW public key." Ludtke, 40:5-26.

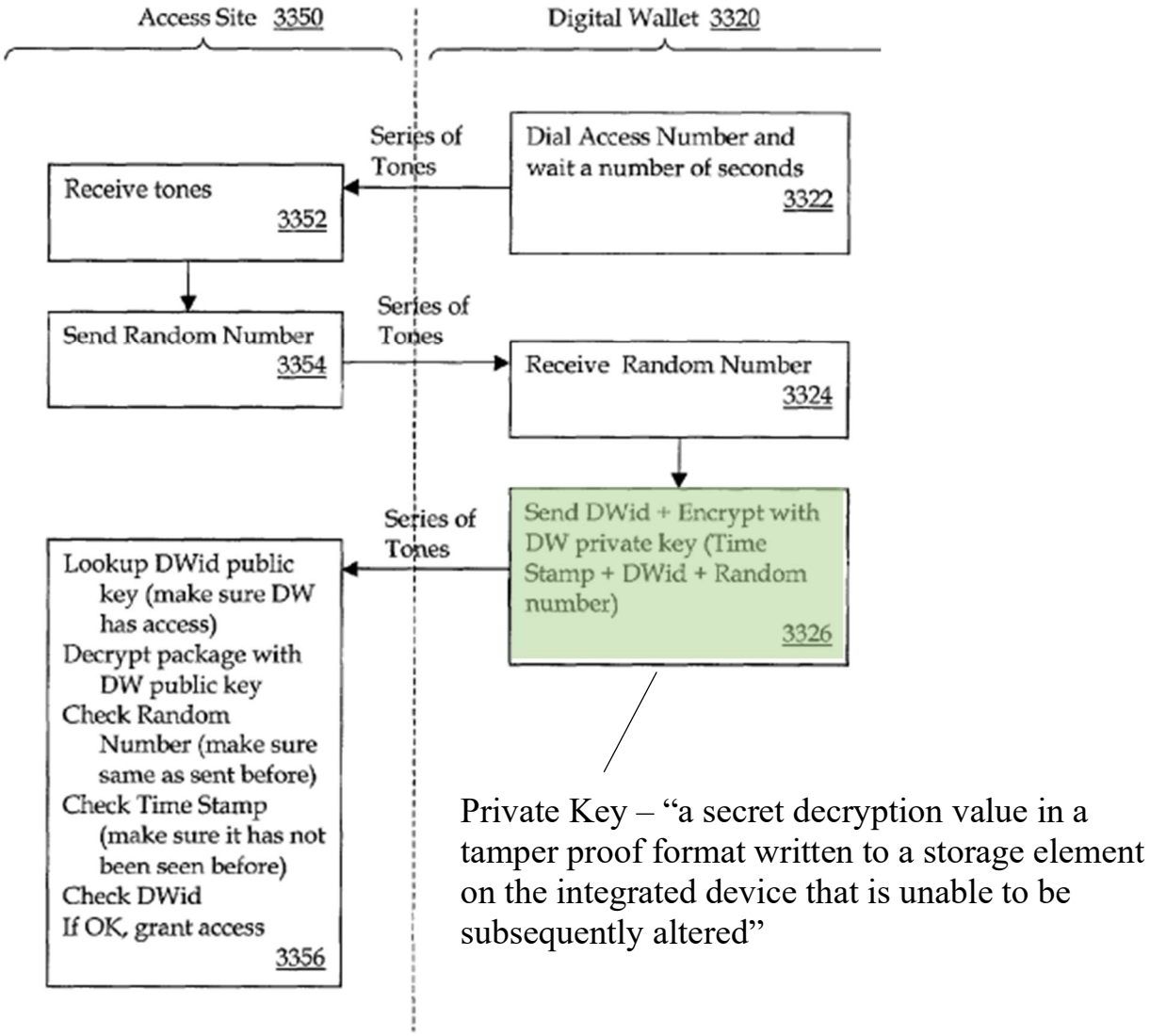


FIG. 33

Ludtke, FIG. 33 (annotated).

94. As I explained above for the private decryption key, a person of ordinary skill in the art, in my opinion, would have been motivated and found it obvious to store the key in "write-once memory," i.e., in a tamper proof format that is unable to be subsequently altered, to prevent modification and thereby enhance the security of the system, as discussed above.

e. [1b]: "responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;"

95. Ludtke discloses [1b] because Ludtke discloses "validating that the user interacting with the device is an authorized user" by prompting the user to "supply a fingerprint recognition sample" and receiving a fingerprint sample (scan data) from a "fingerprint recognition pad" (a biometric scan) in response to the prompt (request for biometric verification). Ludtke, 14:33-42.

96. In Ludtke, the privacy card user authentication[3] block 777 "includes a biometric solution" such as a fingerprint recognition pad for "validating that the user interacting with the device is an authorized user." Ludtke, 14:33-40. In operation, "the user is prompted to supply a fingerprint recognition sample," after

[3] The authentication block performs authorization that is distinct from the authentication performed by the third-party trusted authority described in [1d] below.

which the "block captures the sample[] and carries out a recognition algorithm against the authorized samples that are stored in the user identity block …. If a match is found, the user is authorized to access the data and functionality of the device." Ludtke, 14:40-46; *see also* Ludtke, 16:47-49 (explaining that the digital wallet also receives biometric scan data after prompting).

f. [1c]: "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;"

97. Ludtke discloses [1c] because, as explained in [1b], the transaction device uses a "recognition algorithm" to compare the fingerprint sample (scan data) "against the authorized samples that are stored in the user identity block" (biometric data) to determine "a match." Ludtke, 14:40-46.

g. [1d]: "responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes from the plurality of codes and the other data values for authentication to a third party that operates a trusted authority, wherein the one or more codes and other data values include[] the device ID code; and"

98. Ludtke discloses [1d] because Ludtke discloses transferring (sending) the transaction device ID (one or more codes from the plurality of codes and the other data values) to a "single trusted" and "highly secured" transaction processing clearing house (TPCH) (third-party trusted authority) over a wireless network connection using "wireless or cellular signals" (wirelessly) once a fingerprint

match is identified (responsive to a determination that the scan data matches the biometric data). Ludtke, 5:63-64, 7:46-48, 9:26-30, 9:35-42, 9:52-59, 28:50-29:14, 30:23-27.

99. **First,** Ludtke determines whether the scan data matches the biometric data (as explained for [1b] and [1c]) and sends the transaction device ID responsive to a "match" between the scan data and stored data.

100. In one embodiment, where "the transaction device is used to trigger shopping activity," such as a "web-based transaction using a transaction device such as a privacy card and/or digital wallet and a personal POS terminal," "the user may tap on an on-screen icon being displayed by the transaction device, e.g., digital wallet; and the digital wallet transmits a signal," which "causes" a "web browser" for purchasing desired content (application) "to launch." Ludtke, 28:15-18, 28:26-40. "Once a transaction has been triggered, the browser communicates with the personal POS terminal, requesting it to initiate a transaction," and "provides a transaction record, which includes all of the necessary data to support th[e] transaction, including a list of items being purchased, unit cost and quantity, the vendor who will provide the items, etc." Ludtke, 28:13-18, 28:50-56.

101. The POS asks the transaction device to "validate the user" and the user is "prompted to supply a fingerprint recognition sample" as an initial security measure. Ludtke, 1:22-31, 1:37-38, 14:41-42, 18:45-50, 18:52-55, 28:57-62. The

sample is compared to stored fingerprints, and if the sample is recognized, the user is authorized. Ludtke, 14:41-46. After the transaction device receives the fingerprint recognition sample "*to confirm [an] entire transaction and that the user is authorized*," the personal POS terminal "opens a secure communications session to the TPCH, requesting a transaction," and "provides the transaction record that it received from the web browser *and the unique ID of the transaction device*." Ludtke, 28:50-29:12 (emphases added); *see also* Ludtke, 27:12-13 ("Privacy card information is provided to TPCH, step 1510."), 34:25-27 (explaining that "necessary secure transaction communication with the TPCH" includes "providing the transaction data and [the] device ID.").

102. The "confirmation that the user is authorized" is based on the match between the scan data and stored data, as explained for [1c] and [1d]. Ludtke, 14:40-46; *see also* Ludtke, 4:62-5:1 ("The transaction device enhances security by authenticating the user of the card *prior to usage* such that if a card is lost or stolen, it is useless in the hands of an unauthorized person …. [A]uthentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g., fingerprint recognition)"(emphasis added)).

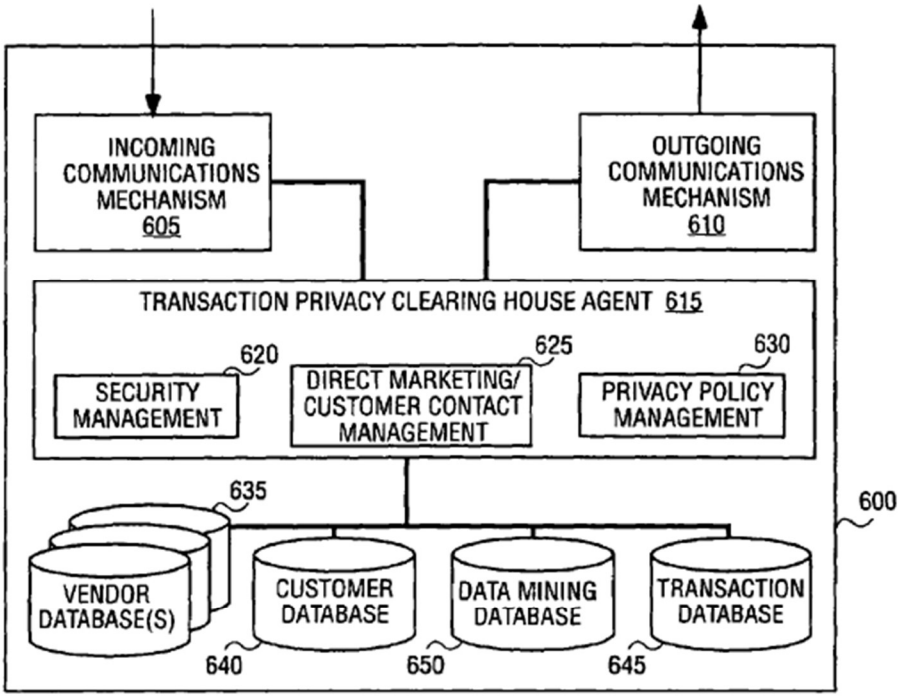
103. Ludtke also discloses an alternate embodiment in which the POS "functionality of providing secure communication and transactions with the Transaction Privacy Clearing House (TPCH)" described above "can be integrated

into the digital wallet directly." Ludtke, 28:41-45. Thus, Ludtke also discloses communicating the device ID directly from the transaction device to the TPCH responsive to a "match" between the scan data and stored data.

104. **Second,** Ludtke discloses sending the transaction device ID wirelessly. More specifically, Ludtke discloses that "the TPCH is located at a secure location" and "embodied as a secure server." Ludtke, 9:26-34. The TPCH receives incoming communications, including the transaction ID, using an "incoming communications mechanism 605" using "wireless or cellular signals." Ludtke, 9:35-42.

105. **Finally,** Ludtke discloses that the TPCH is a third party that operates a trusted authority. As Ludtke explains, with respect to Figure 6, the TPCH is an entity separate from the parties to a transaction because it is distinct from the transaction device, the POS on which the user/transaction device is performing a transaction, and the "*external* retailers and vendors" that complete the transaction. Ludtke, 9:35-39 (emphasis added), FIG. 6. Ludtke further discloses that the separation between the TPCH, vendors, and the POS on which the user/transaction device is performing a transaction "ensures secure communications among the components internal to the TPCH 600 and the entities external to the TPCH 600," and "ensures that only authorized entities are allowed access to data and that only authorized transaction devices can execute transactions against a user's account,"

thereby allowing the TPCH to function "as the middleman of the distribution channel." Ludtke, 7:46-48, 9:26-30, 9:43-59. Indeed, as Ludtke explains, "The incoming communications mechanism 605 and outgoing communications mechanism 610 are the means of communicating with *external* retailers and vendors, as well as the transaction device." *Id.* That the vendors and transaction device are "external" to the TPCH confirms that the TPCH is a third party, and not a party to the transaction itself.



TRANSACTION PRIVACY CLEARING HOUSE: MAJOR COMPONENTS

FIG. 6

106. In my opinion, this reading of "third party" is consistent with Patent Owner's previous "agree[ment] that at a 'third-party trusted authority' is *an institution or entity that is outside of the* multi-party system (*user and application or vendor*) that is being authenticated" and the Board's construction that "third-party trusted authority" is "a trusted authority that is an entity separate from the parties to the transaction, and one that is "separate from the principal parties to a transaction." Ex. 1007, 13-15 (emphases added). Indeed, the Board differentiated the prior art cited in the prior IPR2021-01447 because the purported third party authority was not a third party at all, stating "the DPC is the resource to be accessed, *but it is a party to the transaction, rather than a third party*." Ex. 1007, 24. Here, to the extent Patent Owner raises any argument that the TPCH of Ludtke is similar to the mapping in the prior IPR, I disagree, particularly because Ludtke expressly identifies the TPCH as external to the parties to the transaction, capable only of communication with the parties, as explained above. It is also my opinion that the TPCH's ability (in certain embodiments) to settle funds does not make it a "party" to the transaction because it remains independent of the user, POS, and "external" vendors. Settlement of funds is an example of the independent TPCH providing a service to other elements that are the parties to the transaction, and settlement of funds is a common practice of a clearing house (like Ludtke's TPCH), which remains a third party to the transaction. Moreover, Ludtke expressly

discloses that the TPCH "may issue a funds settlement request to a third party financial institution on behalf of the user, causing the necessary funds to be transferred to the vendor from the user's account" thus further confirming that the TPCH is not the vendor/retailer, or even the user's financial institution from which funds are withdrawn (not a principal party to the transaction, and therefore a third party). Ludtke, 29:43-46.

h. [1e]: "receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application.

107. Ludtke discloses or renders obvious [1e] because after the TPCH authenticates the transaction device ID (device ID code), a "web browser" webpage (application) receives an indication of "approval of the transaction to be performed" (access message indicating that the third party trusted authority successfully authenticated the ID code) from the TPCH. Ludtke, 6:41-44, 24:17-32, 28:26-40, 29:15-20. The access message also allows the user to access "content or a reference to the content" on the web page. Ludtke, 29:15-20, 29:29-30, 31:41-52.

108. Ludtke explains that, when "the transaction device is used to trigger shopping activity, the user may tap on an on-screen icon being displayed by the transaction device, e.g., digital wallet; and the digital wallet transmits a signal,"

which "causes" a "web browser" for purchasing desired content (application) "to launch." Ludtke, 28:26-40. "Once a transaction has been triggered, the browser communicates with the personal POS (application) terminal, requesting it to initiate a transaction," and "provides a transaction record, which includes all of the necessary data to support th[e] transaction, including a list of items being purchased, unit cost and quantity, the vendor who will provide the items, etc." Ludtke, 28:50-56.

109. The POS asks the transaction device to "validate the user," causing the transaction device to "display[] the transaction amount, and request[] the user to select which account to use for payment." Ludtke, 28:64-67. After selecting an account and confirming for the POS that "the entire transaction and that the user is authorized[,]" the transaction record "and the unique ID of the transaction device" are sent to the TPCH, as discussed in [1d].

110. Next, the TPCH "uses the unique ID of the transaction device to process the transaction," and "issues a transaction confirmation back to the personal POS terminal" (access message) after "validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction." Ludtke, 29:15-23. The "transaction confirmation" (access message) is "reflect[ed] … back to the web browser [(application)] and transaction device" and "[s]ecure distribution of physical (or electronic) content to the user is performed"

based on the confirmation. Ludtke, 29:15-23, 29:29-30. The distributed content includes the content itself or a reference to that content, such as a "web URL." Thus, Ludtke discloses receiving at a web browser webpage (application) a transaction confirmation (access message) that allows the user to access electronic content on the web browser (application).

111. Ludtke also discloses [1e] because Ludtke discloses downloading "new functionality," software, and services (an application) on the transaction device and accessing the service after receiving the transaction confirmation (access message) at the transaction device.

112. Ludtke's transaction device is configured to "adapt to new services and functionality, either automatically by the transaction device or manually by the user. For example, on a web site the user might click a button that causes new functionality to be *downloaded to the transaction devi*ce for access at a future time." Ludtke, 19:45-50 (explaining that the transaction device is "to be used for the initial set of services that the user requested during the registration process," and that "[o]nce the device has been initialized for secure transactions, additional services could be downloaded to the device."), 31:11-52 (describing downloaded "services and functionality" including services for purchasing a "train ticket to certain destinations" and "electronic content" from a "content provider.").

113. The transaction device can "download and store a large amount of services and functionality" and "if the transaction device finds itself in the presence of a service that is managed by an alternate system, it can download not only the service software, but also the necessary underlying 'transaction system' software." Ludtke, 31:23-26, 30-40. The downloaded functionality and software/service is an "application" within the meaning of the '954 patent, which defines "application" as "a resource that can be accessed by a verified and authenticated user." Ludtke, 18:45-50, 31:11-52; Ex. 1001, 6:18-24.

114. Ludtke further explains that "once a user has carried out a typical transaction to purchase electronic content" using the downloaded functionality—that is, after the TPCH validates the transaction device and sends a "transaction confirmation" (access message) back to the transaction device, as discussed above—a "content provider" has the content "delivered to the transaction device," thereby allowing the user to access the service(s) offered by the downloaded functionality/software. Ludtke, 29:15-20, 31:41-50. Thus, Ludtke discloses receiving at the downloaded software/functionality (application) a transaction confirmation (access message) that allows the user to access the services prescribed by the downloaded software/functionality (application).

2. Claim 2: "The method of claim 1, wherein the one or more codes and the other data values are transmitted to the trusted authority over a network."

115. Ludtke discloses claim 2.

116. As explained for [1e], the device ID and other codes are sent to the external TPCH server over a wireless network connection using, e.g., "wireless or cellular signals." Ludtke, 9:35-42, 5:63-64 ("Furthermore, the privacy card may have a wireless communication mechanism for input and output.").

3. Claim 4: "The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful."

117. Ludtke discloses claim 4 because, as discussed in [1d], sending the transaction device ID (one or more codes and the other data values) indicates that the scan data matches the biometric data (the biometric verification was successful). *See* [1d]. This is consistent with the '954 patent which explains that the act of sending the device ID indicates that biometric verification was successful. Ex. 1001, FIG. 6 ("Wirelessly Send Code Indicating Successful Verification of User"), 7:18-20 ("If the biometric verification of the user is successful, the key provides its code over the secure communications channel.").

118. As explained for [1b]-[1c], fingerprint recognition is a security measure "that limits access to the card 705 to authorized users." Ludtke, 12:23-25, 4:62-5:1 ("The transaction device enhances security by authenticating the user of

the card prior to usage such that if a card is lost or stolen, it is useless in the hands of an unauthorized person …. [A]uthentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g., fingerprint recognition).”).

119. And as explained for [1d], when the “personal POS terminal receives the transaction request, it communicates with the transaction device, *asking the transaction device to validate the user*, confirm that the user wants to make this transaction, and get the appropriate information for which account the user wants to use for payment.” Ludtke, 28:57-62 (emphasis added); [1d]. Upon receiving the request, the transaction device “validat[es] that the user interacting with the device is an authorized user” by prompting the user to “supply a fingerprint recognition sample” and receiving a fingerprint sample (biometric scan) from the “fingerprint recognition pad” in response to the prompt to generate the scan data. Ludtke, 14:33-42; [1b].

120. The transaction device user authentication block “captures the sample[] and carries out a recognition algorithm against the authorized samples that are stored in the user identity block” Ludtke, 14:40-46. Then, “[i]f a match is found, the user is authorized to access the data and functionality of the device” and “validates that the user is authorized” to conduct their transaction executed at the POS terminal (application). Ludtke, 14:40-46, 29:5-6; *see also* Ludtke, 16:47-49

(explaining that the digital wallet also receives biometric scan data after prompting).

121. Thus, communicating the device ID (one or more codes) responsive to the fingerprint (or other biometric scan) recognition, as disclosed by Ludtke, indicates that the biometric verification was successful.

4. Claim 5: "The method of claim 1, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition."

122. Ludtke further discloses claim 5 because its biometric data expressly includes a "fingerprint" as well as a "retinal scan, voice, DNA, hand profile, face recognition, etc." Ludtke, 35:61-64.

5. Claim 6: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."

123. Ludtke discloses or renders obvious claim 6.

124. Ludtke explains that the "transaction device is an interactive device with communications capabilities" that allow it to receive "messages via the TPCH in a variety of ways, including wireless, Internet, a pager system, cellular, etc." Ludtke, 33:46-49, 17:3-10. The transaction device is also configured to allow the user to "directly" "view and respond to messages" and further includes conventional computing circuity, such as a processor, memory, and "instructions"

for execution. Ludtke, 33:49-54, 11:66-12:7, 15:65-16:8, FIGS. 7A and 9A. Moreover, Ludtke expressly discloses the transaction device having "pager or cell phone functionality built-in." Ludtke, 17:65-18:4.

125. A POSITA reading Ludtke would have found the structural and functional configurations of the disclosed portable transaction device—especially its cellular and wireless adaptions, to be at least suggestive of a mobile phone. Ludtke, 9:39-41 (explaining that transaction devices may operate on "cellular signals"), 26:56-57 ("The personal POS terminal may be configured to be mobile, such that the user may take it out of the home environment."). Indeed, because the '954 patent does not specify (and the claims do not recite) the precise characteristics of the mobile phone, a POSITA would have understood that a transaction device having "built in" "cell phone functionality" *is* a mobile phone.

126. It is also my opinion that a POSITA would have been motivated and found it obvious to implement the transaction device as a mobile phone to enable the user to safely conduct financial transactions (e.g., purchases) using a single device.

127. Furthermore, it was known in the art at the time of the invention to implement biometric security features on a mobile device for financial transactions. *See, e.g.*, Udom, Abstract, [0014], [0032]-[0033] (describing a "process of verifying an individual's identity and authorizing that person to have

access to a secure resource (e.g., a bank account …) [where] the software within the CPU 104 compares data from the sensor 106 that represents a scanned biometric characteristic, to either data or data templates stored for various individuals in memory 105" and "processor 104 might just as well be comprised of a cellular telephone."); Lapsley, Abstract, [0024] (describing "biometric authorization of an electronic transaction between a consumer and a merchant us[ing] an electronic identicator and an access device" where "the access device may be a wireline telephone, a wireless telephone, a two-way pager, a personal digital assistant, or a personal computer.").

128. Thus, in my opinion, a POSITA would have reasonably expected implementing Ludtke's transaction device as a mobile phone or tablet to succeed because Ludtke already contemplates using the transaction device as a "cell phone" and such implementations were established in the art. Ludtke, 17:65-18:4.

6. Claim 7: "The method of claim 1, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account."

129. Ludtke discloses claim 7 because, as discussed in [1e], the transaction confirmation (access message) is received at a web browser that includes a user-accessible *web site*. Ludtke, 29:15-20, 29:29-30, 31:41-52. Alternatively, the

transaction confirmation is received at *software/functionality* downloaded to the transaction device, as also discussed in [1e]. Ludtke, 31:11-52.

7. Claim 10: "The method of claim 1, further comprising establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication."

130. Ludtke discloses claim 10 because, as explained for [1aiii], Ludtke discloses "establish[ing] a secure connection to a back-end system" prior to transferring (sending) the "access codes, PINs, etc.," using a public key infrastructure. Ludtke, 37:39-45.

8. Independent Claim 12

a. [12preamble]: "An integrated device comprising:"

131. Ludtke discloses [12preamble] because, as discussed for [1preamble], Ludtke discloses "a biometric device" (also called a transaction device) such as a privacy card and/or digital wallet for "enabling the authorized user to access private information over a voice network." Ludtke, Abstract, 3:32-36.

b. [12ai]: "a persistent storage media that stores biometric data of a user, and"

132. Ludtke discloses [12ai] for the reasons explained for [1ai].

c. [12aii]: "a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device, and"

133. Ludtke discloses [12aii] for the reasons explained for [1aii].

d. [12aiii]: "a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered;"

134. Ludtke discloses [12aiii] for the reasons explained for [1aiii].

e. [12b]: "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends one or more codes and other data values from the plurality of codes and other data values for authentication by a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and"

135. Ludtke discloses [12b] because the transaction device ID (ID code) is wirelessly sent to a "single trusted" and "highly secured" TPCH (third party that operates a trusted authority) using e.g., the privacy card's input/output logic which "enable[s] the privacy card to send and receive information" using "wireless or cellular signals," or the digital wallet's "wireless transmission driver" that uses the same wireless technology. Ludtke, 5:63-64, 7:46-48, 9:26-30, 9:35-42, 9:51-59, 12:10-16, 17:3-4, 28:50-29:12, 30:23-27.

136. As discussed for [1b], the privacy card includes a user authentication block 777 (validation module) for "validating that the user interacting with the device is an authorized user." Ludtke, 14:33-40. In operation, "the user is prompted to supply a fingerprint recognition sample," after which the "block captures the sample" and communicates with information block 760 (persistent

storage media that "*stores data* about the user and accounts that are accessed by the card" including "the authorized fingerprint recognition samples") to "carr[y] out a recognition algorithm against the authorized samples that are stored in the user identity block." Ludtke, 14:40-44; [1a] and [1c], above. *See also* Ludtke, 16:47-50 (explaining that the digital wallet also receives biometric scan data after prompting). Finally, "[i]f a match is found, the user is authorized to access the data and functionality of the device." Ludtke, 14:45-46.

137. Once the user/transaction device is authorized (fingerprint match identified), the transaction device ID (ID code) is wirelessly sent to a "single trusted" and "highly secured" TPCH (third party that operates a trusted authority) using, e.g., input/output logic that "enable[s] the privacy card to send and receive information" using "wireless or cellular signals," or (in the case of a digital wallet) a "wireless transmission driver" that uses the same wireless technology. Ludtke, 5:63-64, 7:46-48, 9:26-30, 9:35-42, 9:52-59, 12:10-16, 17:3-4, 28:50-29:12, 30:23-27. This is consistent with the '954 patent, which does not explain how a validation module communicates codes but does explain that an RF module wirelessly sends a code to the trusted authority. Ex, 1001, 5:49-52, 8:2-4.

f. [12c]: "a radio frequency communication module that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allowing the user access to an application."

138. Ludtke discloses [12c] because the transaction device receives an "approval of the transaction to be performed" (access message) from the TPCH via its "cellular" "wireless communication mechanism" (radio frequency communication module) that allows the user to access services and content (an application). Ludtke, 5:63-65, 6:36-44, 9:39-42, 17:3-10, 29:5-23, 29:29-30, 31:11-52, 33:46-49.

139. As discussed for [1e], the transaction device receives an indication of "approval of the transaction to be performed" (access message) from the TPCH after "validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction." The approval allows the user to access services and content, i.e., an application. Ludtke, 29:15-20, 29:29-30, 31:11-52. In one embodiment, the TPCH "issues a transaction confirmation" (access message) "back to the personal POS terminal" where it is then reflected "*back to* the web browser and *the transaction device*" and displayed to the user. Ludtke, 29:15-23 (emphases added). Alternatively, where the communication functions of the POS are integrated into the transaction device, the confirmation may be delivered to the transaction device. Ludtke, 28:41-45.

140. Ludtke further discloses that the transaction device uses a "wireless communication mechanism for input and output," including for receiving "cellular signal[]" communication output from the TPCH. Ludtke, 5:63-64, 9:39-42, 17:3-10, 33:46-49. Because the transaction device communicates using cellular technology, a POSITA would have understood that the wireless communication mechanism is a radio frequency communication module.

9. Claim 13: "The integrated device of claim 12, wherein the one or more codes and the other data values are transmitted to the trusted authority over a network."

141. Ludtke discloses claim 13 for the reasons explained for claim 2.

10. Claim 15: "The integrated device of claim 12 comprising: an LED to be activated for requesting the biometric scan."

142. Ludtke discloses or renders obvious claim 15 because Ludtke's verification unit (verifier) includes a "high resolution color" or "black [and] white" "LCD screen" that is activated when the user "interacts with the device" for fingerprint recognition. Ludtke, 11:37-41, 14:54-63, 16:53-56.

143. Ludtke discloses that the "fingerprint recognition, on-card display technology" of the transaction device authentication block verification unit/verifier) "may be *enabled* via thin LCD technologies." Ludtke, 11:37-41 (emphasis added). The LCD is configured such that, when "the user interacts with the device," the LCD generates (displays) "the appropriate images." Ludtke, 14:54-63. Moreover, "[w]hen the user has selected an account, *the*

transaction device asks the user to confirm the entire transaction and that the user is authorized, for example, by entering a PIN or *providing a fingerprint recognition sample*" and "request[s] the user's attention, either via audio *or video signals, or both*." Ludtke, 28:63-29:4 (emphases added).

144. A POSITA would have understood that Ludtke's LCD, which asks the user to "provid[e] a fingerprint recognition sample" using "video signals" and "appropriate images," does so using its display, which is conventionally backlit using an LED. Ludtke, 14:54-63, 28:63-29:4; Siegel, [0041] ("[M]ost LCD panels are backlit with fluorescent tubes or arrays of light-emitting diodes (LEDs) that are built into the sides or back of the panel."); Ikegami, [0024], [0108], [0110], [0135], [0141], [0154], [0187] (describing an "authenticating apparatus" including "an instruction unit for prompting the person to be authenticated to input data" such as "biometrics information" and wherein the instruction unit prompts the user with "a light emitting element such as an LED or the like").

145. Thus, it is my opinion that Ludtke discloses activating the LCD when a fingerprint scan (biometric scan) is needed (for requesting the biometric scan), and therefore at least suggests activating an LED as part of the process because LCDs typically use LEDs to backlight their display, as further evidenced by Siegel and Ikegami. Siegel, [0041]; Ikegami, [0024], [0108], [0110], [0135], [0141], [0154], [0187].

146. It is also my opinion that a POSITA would have been motivated and found it obvious to backlight Ludtke's LCD using LEDs because "liquid crystals do not emit light" and "most LCD panels are backlit with fluorescent tubes or arrays of light-emitting diodes (LEDs) that are built into the sides or back of the panel" to achieve the desired lighting. Siegel, [0041]. A POSITA would have had a reasonable expectation of success in backlighting the LCD with LEDs since such a modification would have only required the use of routine components (LEDs) in accordance with their known and conventional use (backlighting an LCD) as taught by Siegel, and further because it was known in the art to use LEDs to prompt a user's attention for the purposes of inputting biometric information in an authentication device. Ikegami, [0024], [0108], [0110], [0135], [0141], [0154], [0187].

11. Independent Claim 16

a. [16preamble]: "A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:"

147. Ludtke discloses [16preamble] because, as explained for [1e], Ludtke discloses a method of authenticating a verified user using a POS terminal (a device with a computer processor to execute steps). Ludtke, 28:57-29:20.

148. As illustrated in Figure 14, Ludtke's POS terminal includes a processor (microprocessor 1405) configured to execute software, including

"internal driver software that executes locally to drive the wireless transceiver, software to store incoming data into memory and to control input/output to a computer (e.g., PC) coupled to the personal POS terminal," "[h]ost application software," and "user application" software stored on the POS terminal. Ludtke, 25:34-58, FIG. 14. "The personal POS terminal may also include software that is configured to communicate with the PC and the eCommerce system to perform the transaction." Ludtke, 26:23-26.

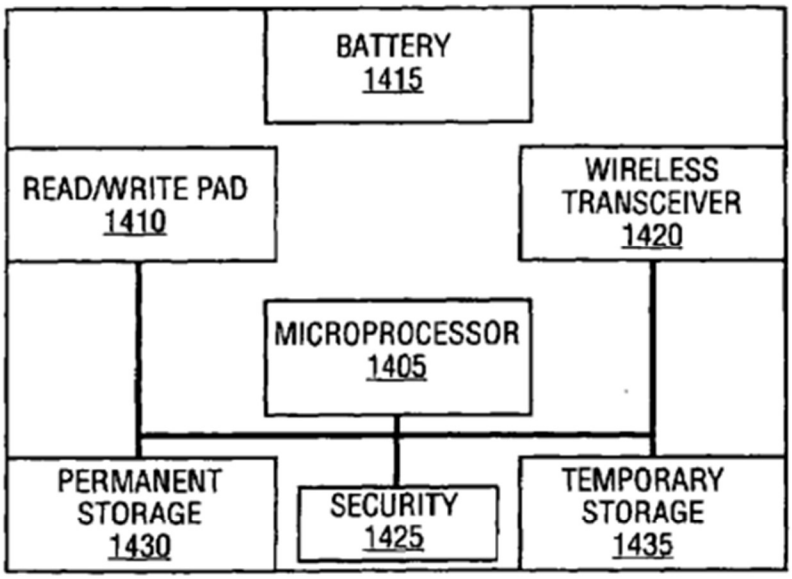


DIAGRAM OF THE MAJOR COMPONENTS OF THE PERSONAL POS, SHOWING THE DATA/ADDRESS BUS INTERCONNECT

FIG. 14

Ludtke, FIG. 14.

149. Executing the software causes the steps recited in each of [16a]-[16d] to be executed, as explained below.

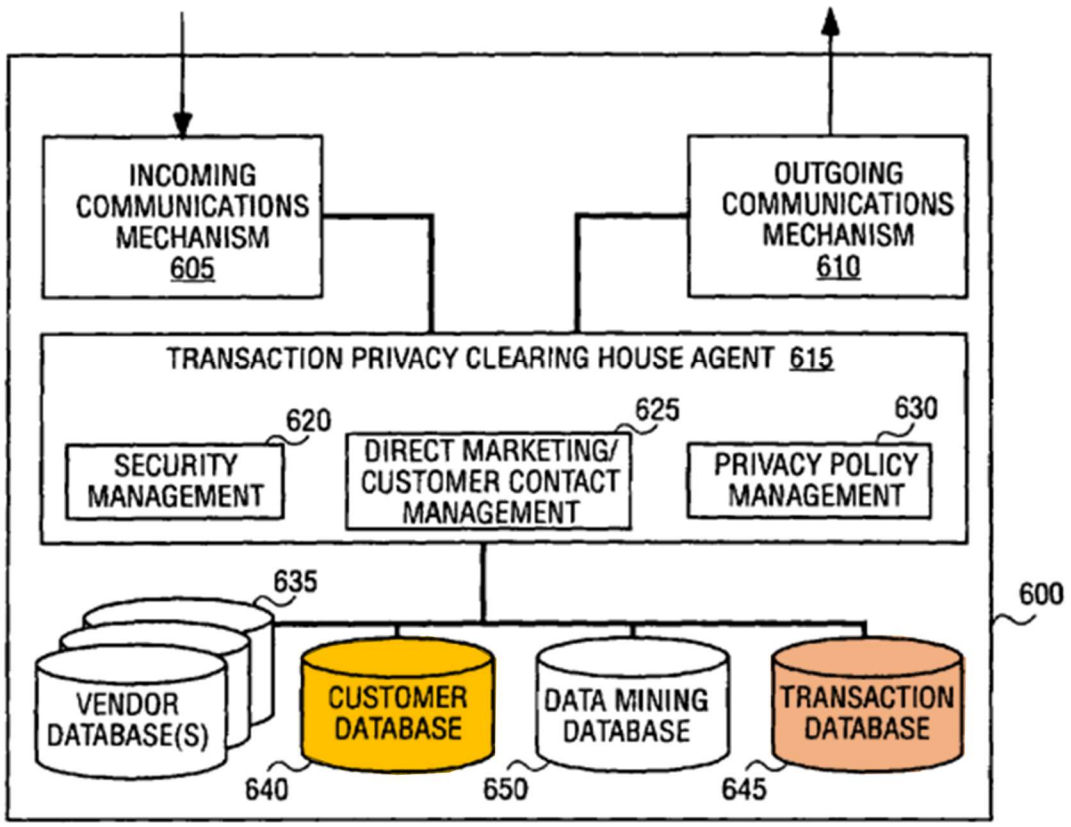
b. [16a]: "wirelessly receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and other data values comprises the device ID code uniquely identifying an integrated device associated with a biometrically verified user, the device ID code being registered with a trusted authority for authentication, the trusted authority operated by a third party"

150. Ludtke discloses [16a] because the POS terminal wirelessly receives the transaction device's device ID, as explained for [1e].

151. When Ludtke's "personal POS terminal receives the transaction request, it communicates with the transaction device, *asking the transaction device to validate the user*, confirm that the user wants to make this transaction, and get the appropriate information for which account the user wants to use for payment." Ludtke, 28:57-62 (emphasis added). The POS terminal then receives the validating information, including the transaction device's transaction device ID, so that it can "provide[] the transaction record that it received from the web browser *and the unique ID of the transaction device*" to the TPCH, as explained for [1e]. Ludtke, 28:50-29:12 (emphasis added).

152. The transaction device ID uniquely identifies the transaction device and is one of one or more codes from a plurality of codes and other data values (such as bar codes and magnetic strip information), as also explained for [1aii]. Ludtke, 3:49-53.

153. The transaction device ID is also registered with a TPCH (third party trusted authority). The TPCH includes various databases for storing the transaction ID and linking the user to the transaction ID. Ludtke, 10:15-22, 10:40-45, 33:37-41. For example, the "customer database" "holds information regarding each customer of the TPCH" and links the "actual user identity information" to "the digital aliases provided by the transaction device," i.e., the transaction device ID. Ludtke, 10:15-19, 33:38-41 ("the transaction device acts as a digital alias for its user."). The "transaction database" maintains transaction records that include the transaction device ID. Ludtke, 10:19-22, 10:40-45, 33:37-41 ("Whenever the user carries out a transaction using the system, vendors receive only the transaction device ID *in the transaction record*.")



TRANSACTION PRIVACY CLEARING HOUSE: MAJOR COMPONENTS

FIG. 6

Ludtke, FIG. 6 (annotated).

154. Ludtke further discloses that the TPCH can "maintain a copy" of "unique transaction device ID values" so that "whenever a transaction arrives with one of these values, the TPCH knows *which transaction device*, and hence which user, the transaction [is] associated with." Ludtke, 30:23-27. Thus, Ludtke discloses the device ID code being registered with the TPCH.

c. [16b]: "requesting authentication of the integrated device using the one or more codes and other data values by the trusted authority;"

155. Ludtke discloses [16b] for the reasons explained for [1e].

156. After receiving a fingerprint recognition sample "to confirm [an] entire transaction and that the user is authorized," Ludtke's personal POS terminal "opens a secure communications session to the TPCH, requesting a transaction" to request authentication of the transaction device ID (one or more codes), and "provides the transaction record that it received from the web browser and the unique ID of the transaction device." Ludtke, 28:50-29:12. The authentication "validat[es] that the transaction device is in good standing and that the selected account has sufficient funds for the transaction," and thus determines whether the transaction device ID is legitimate. Ludtke, 29:15-18.

d. [16c]: "receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party; and"

157. Ludtke discloses or renders obvious [16c] for the reasons explained for [1e].

e. [16d]: "in response to receiving the access message, allowing the biometrically verified user access to the application."

158. Ludtke discloses or renders obvious [16d] for the reasons explained for [1e].

12. Claim 18: "The method of claim 16, further comprising: establishing a secure communications channel with the integrated device, wherein the one or more codes and other data values associated with the biometrically verified user is received from the integrated device."

159. Ludtke discloses claim 18 for the same reasons discussed for claim 10.

13. Claim 19: "The method of claim 16, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account."

160. Ludtke discloses claim 19 for the reasons explained for claim 7.

14. Independent claim 22

a. [22preamble]: "A system, comprising:"

161. Ludtke discloses [22preamble] because, as illustrated in Figure 2, Ludtke discloses a system. Ludtke, Abstract, FIG. 2.

162. Ludtke's system includes the elements recited in [22ai]-[22c], such as a biometric integrated device (privacy card) and a POS terminal (authentication unit), for communication with a TPCH (third-party trusted authority), for reasons explained below.

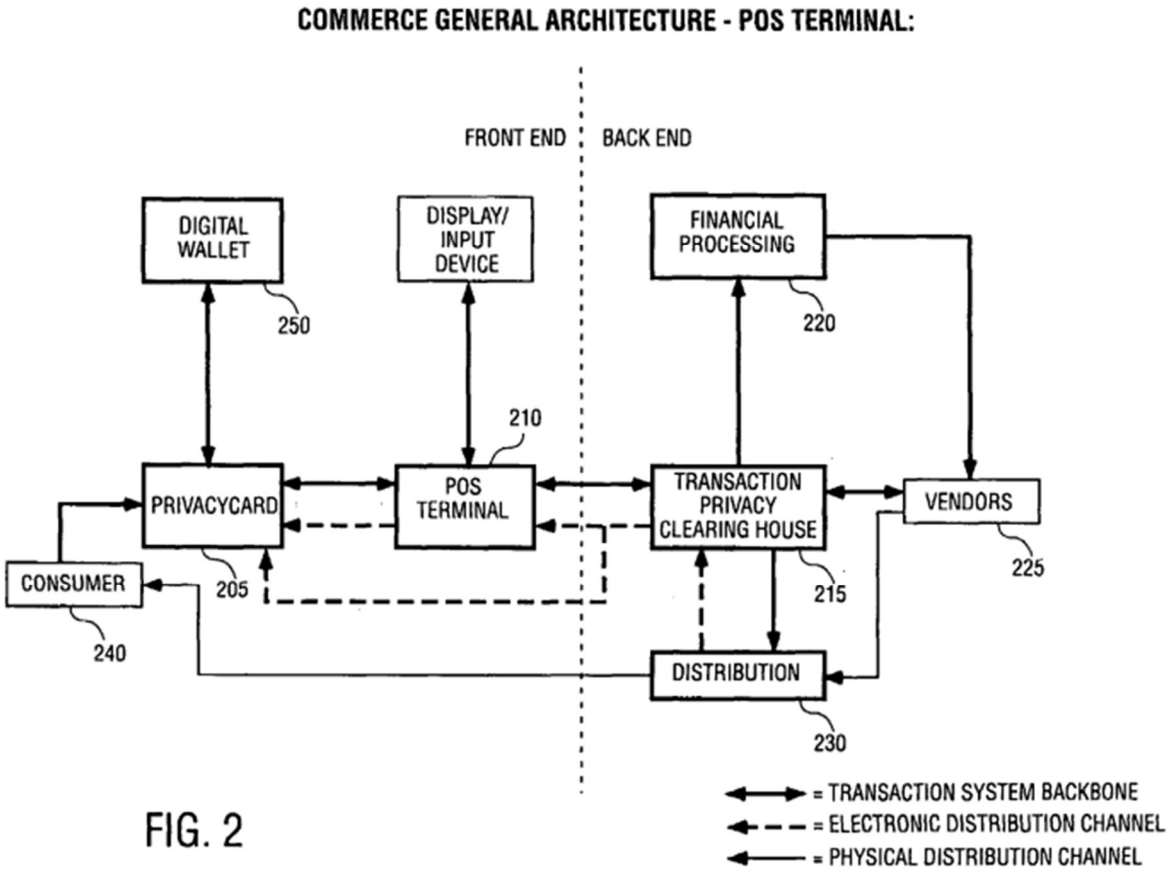


FIG. 2

Ludtke, FIG. 2.

b. [22ai]: "an integrated hardware device that stores biometric data of a user"

163. Ludtke discloses [22ai] for the reasons explained for [1ai]. Ludtke, Abstract, 3:32-36.

c. [22aii]: "and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated hardware device"

164. Ludtke discloses [22aii] for the reasons explained for [1aii].

d. [22aiii]: "and a secret decryption value in a tamper proof format written to a storage element in the integrated hardware device that is not capable of being subsequently altered,"

165. Ludtke discloses [22aiii] for the reasons explained for [1aiii].

e. [22aiv]: "and that wirelessly sends one or more codes and other data values from the plurality of codes and other data values, wherein the one or more codes and other data values include the device ID code; and"

166. Ludtke discloses [22aiv] for the reasons explained for [16a].

167. When Ludtke's "personal POS terminal receives the transaction request, it communicates with the transaction device, *asking the transaction device to validate the user*, confirm that the user wants to make this transaction, and get the appropriate information for which account the user wants to use for payment." Ludtke, 28:57-62 (emphasis added). The POS terminal then receives the validating information, including the transaction device's transaction device ID, so that it can "provide[] the transaction record that it received from the web browser *and the unique ID of the transaction device*" to the TPCH, as explained for [1e]. Ludtke, 28:50-29:12 (emphasis added).

f. [22b]: "an authentication circuit that receives the one or more codes and other data values and sends the one or more codes and other data values to a third party that operates a trusted authority for authentication, and that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allows the user to access an application."

168. Ludtke discloses [22b] because the system includes a POS terminal (authentication circuit) that (1) receives the transaction device ID from the transaction device, (2) sends the transaction ID to the TPCH (third party trusted authority) for authentication, and (3) receives an approval (access message) from the TPCH indicating that the ID was authenticated, allowing the user to access content (application) as explained in [1e]. Ludtke, 28:50-29:12.

169. Ludtke describes an exemplary transaction performed utilizing the disclosed system and illustrated in Figure 17, wherein "the transaction device is used to trigger" a purchase, such as a "shopping activity," and a POS (authentication circuit) "initiates the transaction." Ludtke, 28:11-18, 28: 22-23, 28:26-31, 28:50-52. "When the personal POS terminal receives the transaction request, it communicates with the transaction device, asking the transaction device to validate the user, confirm that the user wants to make this transaction, and get the appropriate information for which account the user wants to use for payment." Ludtke, 28:57-62. Then, the "POS terminal opens a secure communications session

to the TPCH" (third party trusted authority) and "*provides the transaction record that it received* from the web browser *and the unique ID of the transaction device*." Ludtke, 29:6-12 (emphases added). Thus, Ludtke discloses receiving the device ID and providing the device ID to a third-party trusted authority.

170. "The TPCH uses the unique ID of the transaction device to process the transaction," and "[a]fter validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCH issues a transaction confirmation" (access message indicating that the trusted authority successfully authenticated the ID code) "back to the personal POS terminal" which allows the user to access purchased content (application) by determining whether the user's account has "sufficient funds" and transferring the appropriate amount from the user's account to the vendor. Ludtke, 29:15-18, 29-36; *see also* Ex. 1001, 6:18-24 (defining "application" as "resource that can be accessed by a verified and authenticated user."

15. Claim 23: "The system of claim 22, wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from the user to generate scan data."

171. Ludtke discloses claim 23 because, as explained for [1b] and [1e], Ludtke's transaction device (integrated hardware device) receives a validation request from the POS terminal (authentication request from the authentication

circuit) and prompts the user to scan their fingerprint (requests a biometric scan) to validate the user. Ludtke, 14:33-41, 28:57-62.

172. When the "personal POS terminal receives the transaction request, it communicates with the transaction device, *asking the transaction device to validate the user*, confirm that the user wants to make this transaction, and get the appropriate information for which account the user wants to use for payment." Ludtke, 28:57-62 (emphasis added); [1e]. Upon receiving the request, Ludtke's transaction device "validat[es] that the user interacting with the device is an authorized user" by prompting the user to "supply a fingerprint recognition sample" and receiving a fingerprint sample (biometric scan) from the "fingerprint recognition pad" in response to the prompt to generate the scan data. Ludtke, 14:33-42; [1b]. Ludtke's transaction device's user authentication block "captures the sample[] and carries out a recognition algorithm against the authorized samples that are stored in the user identity block." Ludtke, 14:40-46.

173. Then, "[i]f a match is found, the user is authorized to access the data and functionality of the device" and "validates that the user is authorized" to conduct their transaction at the POS terminal. Ludtke, 14:40-46, 29:5-6; *see also* Ludtke, 16:47-50 (explaining that the digital wallet also receives biometric scan data after prompting).

16. Claim 24: "The system of claim 22, wherein when the integrated hardware device cannot verify scan data as being from the user, the integrated hardware device does not send the one or more codes and other data values."

174. Ludtke discloses or renders obvious claim 24.

175. As explained for claim 23, Ludtke's "user is prompted to supply a fingerprint recognition sample," after which the "block captures the sample," after which the "block carries out a recognition algorithm against the authorized samples that are stored in the user identity block" to determine "if … the user is authorized to access the data and functionality of the device," and whether to "validate[] that the user is authorized" to conduct the transaction at the POS terminal. Ludtke, 14:40-46, 29:5-6.

176. A POSITA would have understood that the transaction device does not send the one or more codes if it cannot verify the scan data is from the user, because the biometric scan data "is used as a security mechanism that limits access to the card 705 to authorized users," and the user is only authorized/validated "[i]f a match is found" between the scan data and "stored" "authorized samples." Ludtke, 12:23-25, 14:40-46. Indeed, a transaction device that cannot be authenticated/validated as being from the user is "useless." Ludtke, 4:62-5:1; *see also* Ludtke, 39:50-56 ("At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored

authorized fingerprint. *If a match does not occur, then at 3110 an error message is output* and the DW returns to checking to see if a fingerprint has been detected 3104." (emphasis added)).

177. Additionally, a POSITA would have been motivated and found it obvious to configure Ludtke's transaction device to not send the one or more codes and other data values if the transaction device (integrated device) cannot verify the scan data as being from the user to prevent unauthorized use of the transaction device when "lost or stolen." Ludtke, 4:62-5:1, 18:23-31.

178. Such a modification would have been within the purview of one skilled in the art, and would have only required the use of known conventional components in accordance with their known use—for example, configuring Ludtke's authorization block to output an "error" or "authentication failure" message upon failing to detect a fingerprint match, as was well known in the art. *See, e.g.*, Ludtke, 39:50-56; Kon, [0007]-[0010] (describing "a conventional process of identifying a person using biometric information," wherein a comparator transmits an "authentication failure message" "[i]f it is determined that the input data does not match with the registered information"). Accordingly, a POSITA would have been motivated to make such a modification and had a reasonable expectation of success in doing so.

17. Claim 25: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."

179. Ludtke discloses claim 25 for the reasons explained for claim 6.

18. Claim 26: "The method of claim 1, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition."

180. Ludtke discloses claim 26 for the reasons explained for claim 5.

19. Claim 27: "The method of claim 1, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account."

181. Ludtke discloses claim 27, for the reasons explained for claim 7.

B. Ground 2: Claims 3, 14, and 17 Are Obvious in View of Ludtke and Kon

182. Dependent claims 3, 14, and 17 require an age or birthdate verification. While Ludtke does not expressly disclose age or birthdate verification, Kon does (Kon [0234]). In my opinion, it would have been obvious to add Kon's age and birthdate verification to Ludtke.

1. Claim 3: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code."

183. Ludtke in combination with Kon renders obvious claim 3.

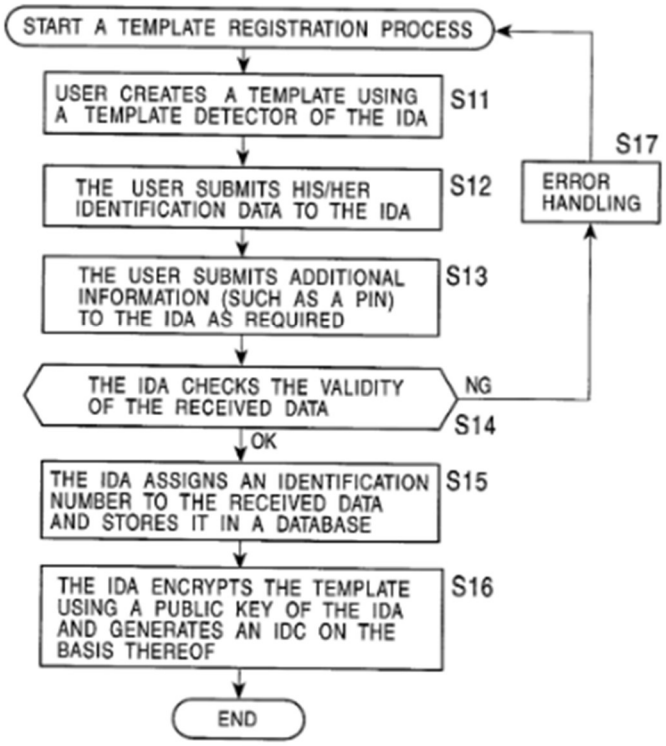
184. Kon discloses registering and storing a user's personal information, including the user's age, in association with the user device's device ID—the user's device ID is stored in a "Subject" field and the user's age is stored in a "Directory Attribute" field of a registered IDC certificate. Kon, [0194] ("Subject is a field in which the name of a subject or a user is described. More specifically, for example, *the ID of a user device* or the ID of a subject which supplies services is described" (emphasis added)), [0234] ("[A]n arbitrary attribute of a[] user, such as an age, sex, address, [or] telephone number, is encrypted as required to identify the user."), [0265] ("FIG. 9 illustrates a flow in terms of registration of a template and creation of an IDC. Registration of a template is performed on the basis of information (sampling information) acquired using an apparatus capable of acquiring personal information in one of the various forms described earlier."), FIGS. 5, 9.

FIG. 5

	Item	Description
Indis-pensable Items	Version	Version
	Serial Number	Identification Number
	signature algorithm Identifier algorithm parameters	Signature algorithem Algorithm Parameters
	Issuer	Name of the identification authority (in the form of a distinguished name)
	Validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date
	Subject	Name of the subject to be certificated (in a DN form)
Extended Items	subject Template Info encrypt Type encrypt Unique ID encryption Algorithm parameter validity subject Template Source subject Template	Template information • encrypt Type • The unique ID or the certificate number of a public key certificate used for encryption • Algorithm • parameter • Validity period (start date, expiration date) • Type of the template • Template
	Subject PKC info subject PKC serial Number subject PKC Unique ID	Information about the public key certificate of the subject • Certificate number of the subject public key certificate • Unique ID of the subject of the subject public key certificate
	Issuer Unique ID	Unique ID of the issuer
	Subject Unique ID	Unique ID of the subject
	Public Key Certificate	Public key certificate
	Issuer Alt Name	Alternative name of the issuer
	subject Directory Attributes	Personal information (encrypted as required) information used to authenticate subject Age, sex, etc.

Kon, FIG. 5 (annotated, excerpted) (illustrating registered user information).

FIG. 9



Kon, FIG. 9 (illustrating process for registering user identification information).

185. As illustrated in Figure 9, user identification registration includes submitting, by a user, their identifying information (e.g., age) (step S12), and validating (verifying) the received information (step S14) before storing it in a database. Kon, [0265]-[0266], FIG. 9. Documentation corroborating, i.e., verifying, the user's age may be supplied, including the user's passport or driver's license. Kon, [0241] ("The person identification certificate (IDC) described above includes information (template information) used to identify a person.… Specific examples of such personal identification information include[] a seal, *a passport, a*

driver's license, and a card." (emphasis added)). Thus, Kon discloses registering the user's age verification in association with the user's device ID.

186. The user's age, like the biometric information, provides another data point for identifying the user (Kon, [0241]); thus, a POSITA would have understood the benefit of using age as an identifying data point for authentication. Indeed, a POSITA would have considered age to be an especially useful identifier where, for example, a service or transaction implicates an age minimum (e.g., purchasing alcohol, cigarettes, or other age-restricted shopping content). *See e.g.*, Gatz, [0005], [0078], [0082].

187. For example, Gatz (Ex. 1015), provides one example showing how important monitoring age-restricted shopping content is, as would have been understood by a POSITA. Gatz explains that, generally, content (including shopping content) on the internet may not be appropriate for all ages. Gatz, [0005] ("As particular types of information or images contained in this uncontrolled information collection may not be suitable for certain users, it may be desirable to selectively restrict access to WWW resources."). Specifically, Gatz explains that if an account is designated to a child, it may be restricted from accessing "age-restricted shopping content" or require verification "that the associated account can access such shopping content." Gatz, [0078]; *see also* FIG. 14 (showing a user interface for accessing age-restricted shopping content). Indeed, based on the

known need to control access to certain services, age, as used by both Gatz and Kon, was a well-known way to restrict user access. Gatz, [0082].

188. Accordingly, a POSITA would have been motivated and found it obvious to register the user's age, as taught by Kon, in association with Ludtke's device ID to facilitate age prohibitive transactions because using age as criteria to restrict certain shopping content was well-known in the art at the relevant time. *See, e.g.*, Gatz, [0005], [0078], [0082] (describing the need to control access to certain services, and explaining that age may be used to restrict user access).

2. Claim 14: "The integrated device of claim 12, wherein an age verification is registered in association with the device ID code."

189. Ludtke in view of Kon renders obvious claim 14 for the reasons explained for claim 3.

3. Claim 17: "The method of claim 16, further comprising: registering a date of birth or age with the agent."

190. Ludtke in view of Kon renders obvious claim 17 for the reasons explained for claim 3.

XII. CONCLUSION

191. For the reasons set forth in Section XI, it is my opinion that one skilled in the art would have found claims 1-7, 10, 12-19, and 22-27 of the '954 patent to be obvious.

192. In signing this declaration, I understand that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in this case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

193. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: January 17, 2024

Respectfully submitted,

Stephen Gray