UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,

Petitioner,

v.

PROXENSE, LLC,

Patent Owner.

Case No. IPR2024-00234
U.S. Patent No. 9,298,905

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 '905 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, 3-7, 9, 10, and 12-18 Are Obvious in View of Ludtke. 31

1. Independent claim 1 31

a. [1preamble]: "A method comprising:" 31

b. [1a]: "persistently storing biometric data of a legitimate user and an ID code on an integrated device" 32

c. [1b]: "responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;" 34

d. [1c]: "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;" 35

e. [1d]: "responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted uthority; and" 36

f. [1e]: "responsive to receiving an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction." 44

2. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code." 46

3. Claim 4: "The method of claim 1, wherein the biometric data includes data from 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." 47

4. Claim 5: "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." 47

5. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application" 49

6. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account." 51

7. Independent Claim 9 52

a. [9preamble]: "An integrated device comprising:" 52

b. [9a]: "a persistent storage media that persistently stores biometric data of a user and an ID code".....52

c. [9b]: "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 the ID code for comparison by a third-party trusted authority aginst one or more previously registered ID codes maintained by the third-party trusted authority; and" 52

d. [9c]: "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based n the comparison of the ID code and allowing the user to—complete a financial transaction." 54

8. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network."..... 55

9. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."..... 56

10. Independent claim 13 56

a. [13preamble]: "A system, comprising:".....56

b. [13a]: "an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code;" 57

c. [13b]: "an authentication circuit that receives the [I]D code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and" 57

d. [13c]: "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes." 59

11. Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware deice cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code."..... 59

12. Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob." 64

13. Claim 16: "The system of claim 11, wherein the biometric data includes data based on 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." 64

14. Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account." 64

15. Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application." 64

B. Ground 2: Claims 2 and 11 Are Obvious in View of Ludtke and Kon 64

1. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the ID code." 65

2. Claim 11: "The integrated device of claim 7, wherein an age verification is registered in association with the ID code." 69

XII. CONCLUSION.....69

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. 9,298,905 ("the '905 patent," Ex. 1001). The application for the '905 patent was filed October 23, 2015, and claims priority to U.S. patent application Ser. No. 13/710,109 filed December 10, 2012, which claims priority to U.S. patent application Ser. No. 11/314,199, filed December 20, 2005, which claims the benefit of U.S. Provisional Application No. 60/637,538, filed on December 20, 2004, and of U.S. Provisional Application No. 60/652,765, filed on February 14, 2005. Ex. 1001, cover page.

4. I have been asked by Petitioner to provide my opinion on whether the claims of the '905 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 '905 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 and 9-18 of the ’905 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 and 9-18 of the ’905 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. 9,928,905 to Giobbi ("the '905 patent")
Ex. 1002	File History of U.S. Patent No. 9,928,905
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.,* 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.*, Case No. 6:21-cv-00210, Dkt. No. 149, Memorandum in Support of Claim Construction Order (W.D. Tex. Dec. 28, 2022)
Ex. 1012	U.S. Patent Application Publication No. 2003/0023882 to Udom ("Udom")
Ex. 1013	U.S. Patent Application Publication No. 2002/0019811 to Lapsley et al. ("Lapsley")

Exhibit	Description
Ex. 1014	*Proxense, LLC v. Google LLC*, Case No. 6:23-cv-00320, Dkt. No. 1, Complaint (W.D. Tex. May 2, 2023)
Ex. 1015	*Proxense, LLC v. Google LLC*, Case No. 6:23-cv-00320, Preliminary Infringement Contentions (W.D. Tex. July 24, 2023)
Ex. 1016	U.S. Patent Application Publication No. 2002/0049806 to Gatz et al. ("Gatz")
Ex. 1017	*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. 1018	*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. 1019	Decision on Petition, *Ex Parte* Reexamination, No. 90/015,053 (January 3, 2023)
Ex. 1020	Order Granting Request for Ex Parte Reexamination, Ex Parte Reexamination No. 90/015,053 (Aug. 2, 2022)
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 ’905 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 and 9-18 of the ’905 patent from the perspective of a person of ordinary skill in the art at the ’905 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 '905 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 '905 PATENT

A. Overview

46. The '905 patent was filed on October 23, 2014, and claims priority to U.S. Patent Application Ser. No. 13/710,109 filed December 10, 2012, which claims priority to U.S. patent application Ser. No. 11/314,199, filed December 20, 2005, which claims the benefit of U.S. Provisional Application No. 60/637,538, filed on December 20, 2004, and of U.S. Provisional Application No. 60/652,765, filed on February 14, 2005. Ex. 1001, cover page. The '905 patent generally relates to "authentication responsive to biometric verification." Ex. 1001, 1:21-24.

47. Figure 6 illustrates a process for "verifying a subject" using a biometric key. Ex. 1001, 7:63-65. 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," at which point a "code" is sent to a trusted key authority (steps 640, 650). Ex. 1001, 7:67-8:2.

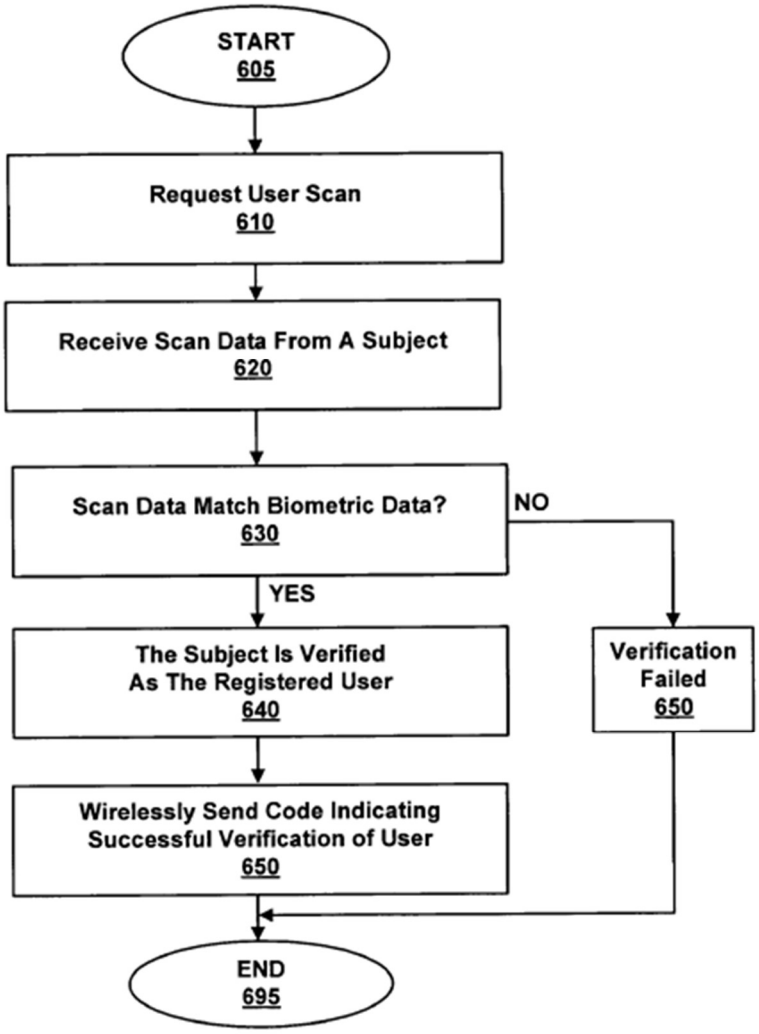


FIG. 6

Ex. 1001, FIG. 6.

48. Once the code is received, as illustrated in Figure 7, the trusted key authority authenticates the code, i.e., determines whether the code is "authentic" (step 730). Ex. 1001, 8:12-18, 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, 8:12-18, 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, 8:18-20, FIG. 7.

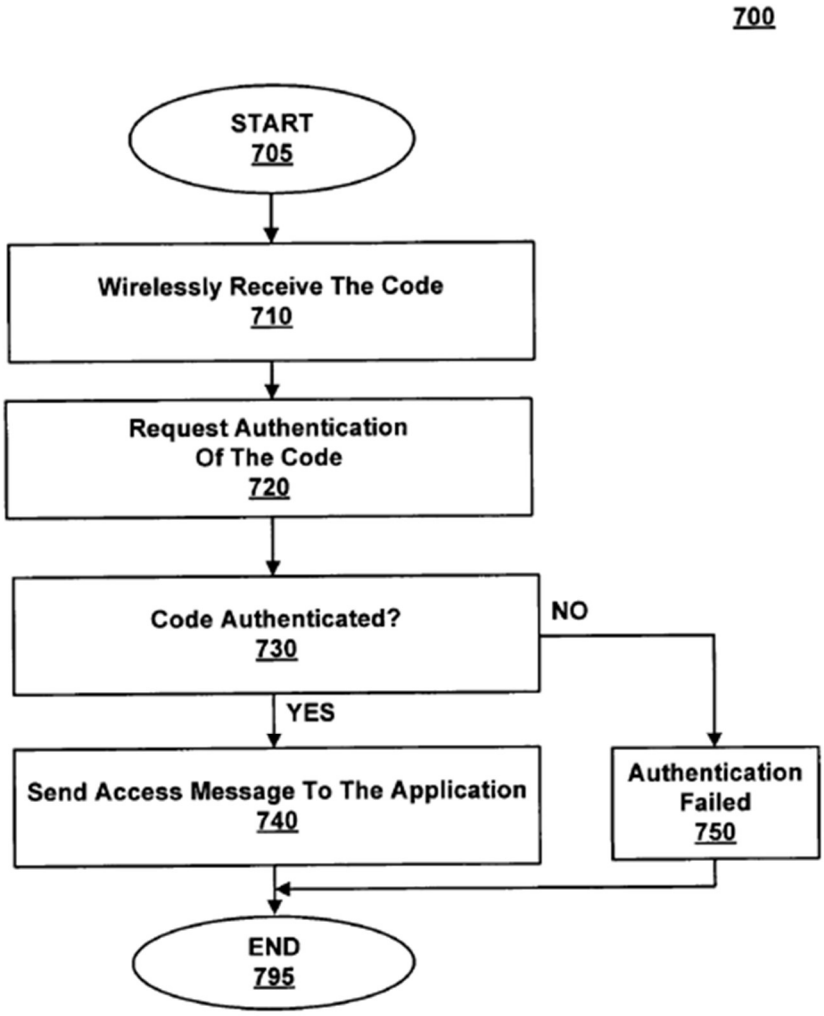


FIG. 7

Ex. 1001, FIG. 7.

VII. CLAIM CONSTRUCTION

49. I have been instructed that the "intrinsic record" includes the '905 patent itself, including the claims, description, and figures (Ex. 1001), and the '905 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 institution decision, the Patent Trial and Appeal Board ("Board") "interpreted" the term "third-party trusted authority" as recited in the '905 patent "to mean a trusted authority that is an entity separate from the parties to a transaction." Ex. 1007 at 14.

52. I also understand that in a previous district court litigation, *Proxense, LLC v. Samsung Electronics Co., Ltd.*, Case No. 6:21-cv-00210, two terms from the ’905 patent were construed by the court (Exs. 1009-1010):

- 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.

53. 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 ’905 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

54. In rendering the opinions set forth in this declaration, I have been asked to consider the ’905 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.

55. 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.

56. I met the criteria for a POSITA at the effective filing date of the '905 patent.

IX. THE PRIOR ART

57. In forming my opinions, I found the following prior art relevant when considering whether the claims of the '905 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. 1012	U.S. Patent Application Publication No. 2003/0023882 to Udom ("Udom")

Exhibit	Description
Ex. 1013	U.S. Patent Application Publication No. 2002/0019811 to Lapsley et. al ("Lapsley")
Ex. 1016	U.S. Patent Application Publication No. 2002/0049806 to Gatz et al. ("Gatz")

58. As explained below, in my opinion, claims 1-7 and 9-18 of the '905 patent would have been obvious based on Ludtke and Kon in the combinations discussed below.

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

59. 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 '905 patent.

60. 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.

61. 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, 18:45-50, 18:52-55. The sample is compared to stored fingerprints and if the sample is recognized, the user is "authorized to access the data and functionality of the device." Ludtke, 14:40-46.

62. 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, 28:15-18, 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, 1:22-31, 1:37-38, 14:33-40, 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. Once the transaction device authorizes the user based on the matching biometric information, the personal POS terminal "opens a secure communications session" with a transaction public clearing house ("TPCH") and "provides the transaction record that it received from the web browser *and the unique ID of the transaction device*." Ludtke, 29:5-12; *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 personal POS terminal, and the back-end transacting entity. Ludtke, 7:42-48, 9:26-42, FIG. 6.

63. Ludtke also discloses an alternate embodiment in which the POS "functionality of providing secure communication and transactions with the Transaction Privacy Clear ing 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.

64. Next, "[t]he 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.

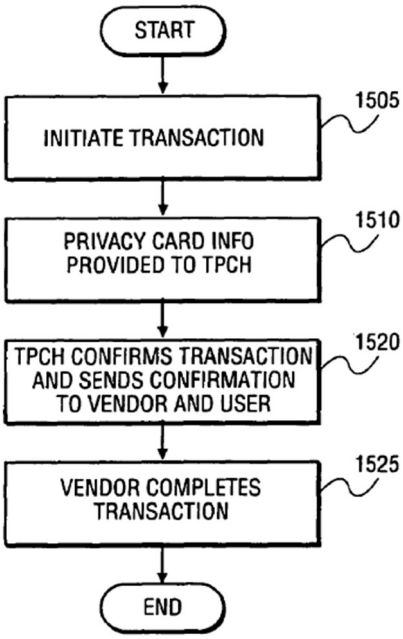


FIG. 15

Ludtke, FIG. 15.

65. Ludtke is directed to the same technical field as the '905 patent: user authentication methods and systems. *Compare* Ex. 1001, 1:62-64, *with* Ludtke, 1:59-61.

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

66. 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 '905 patent.

67. 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], [0174], [0178], [0194] (explaining that a public key certificate ("PKC") includes the ID of the user device), [0226]-[0229] (explaining that a person identification certificate ("IDC") includes the PKC).

68. 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).

69. 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

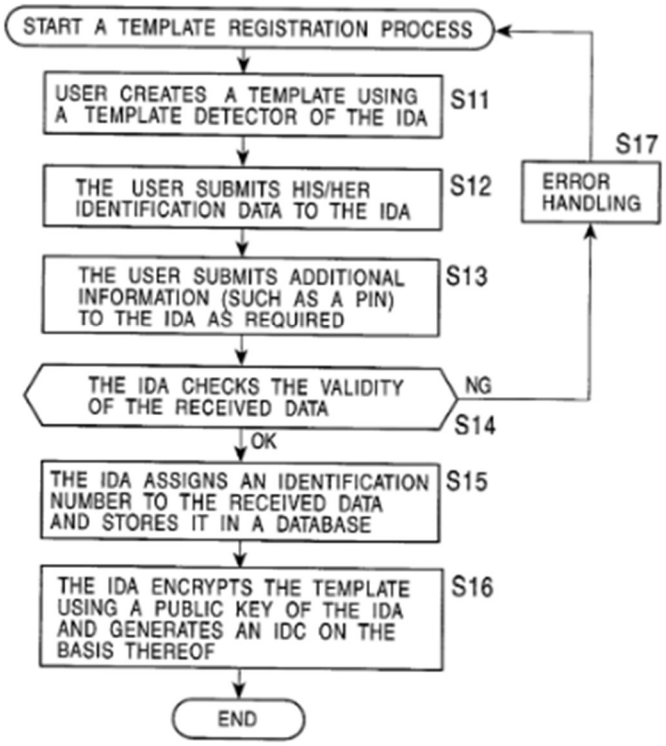
subject which supplies services is described" (emphasis added)), [0234] ("[A]n arbitrary attribute of [a] user, such as an *age*, sex, address, [or] telephone number, is encrypted *as required to identify the user*." (emphases added)), [0241] ("The person identification certificate (IDC) described above 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).

70. Kon is directed to the same technical field as the '905 patent: user authentication methods and systems. *Compare* Ex. 1001, 1:62-64, *with* Kon, [0020], [0034].

X. GROUNDS OF UNPATENTABILITY

71. 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 and 9-18 of the '905 patent would have been obvious to one of ordinary skill in the art.

72. In particular, it is my opinion that claims 1-7 and 9-18 of the ’905 patent would have been obvious to a person of ordinary skill in the art at the earliest priority date of the ’905 patent, based on the combinations shown below:

Ground	Claim(s) Challenged	35 U.S.C. §	Reference(s)
1	1, 3-7, 9, 10, and 12-18	103	Ludtke
2	2 and 11	103	Ludtke and Kon

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

A. Ground 1: Claims 1, 3-7, 9, 10, and 12-18 Are Obvious in View of Ludtke.

1. Independent claim 1

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

73. 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.

74. 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 is used” or “a digital wallet” (integrated devices). Ludtke, 3:32-36.

b. [1a]: "persistently storing biometric data of a legitimate user and an ID code on an integrated device"

75. Ludtke discloses [1a] because the privacy card and/or digital wallet (integrated device) stores "authorized fingerprint recognition samples" (biometric data of the legitimate user) in a "user identity/account information block 760" or "write-once memory, or other memory that is protected from accidental modification" (persistent storage) (Ludtke, 13:27-29, 14:19-21, 19:9-14, 19:29-40, FIGS. 7B-7C) and a "unique transaction device ID value[]" (ID code) in its "permanent memory." Ludtke, 13:20-22.

76. The '905 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, 2:43-50, 4:6-16 (emphasis added). The '905 patent further describes a "biometric key" as including the elements recited in Figure 2, including a biometric module, a control module, and an RF module. Ex. 1001, FIG. 2, 4:42-5:64. 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 .

77. 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 Technology block 774.").

78. Ludtke further 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).

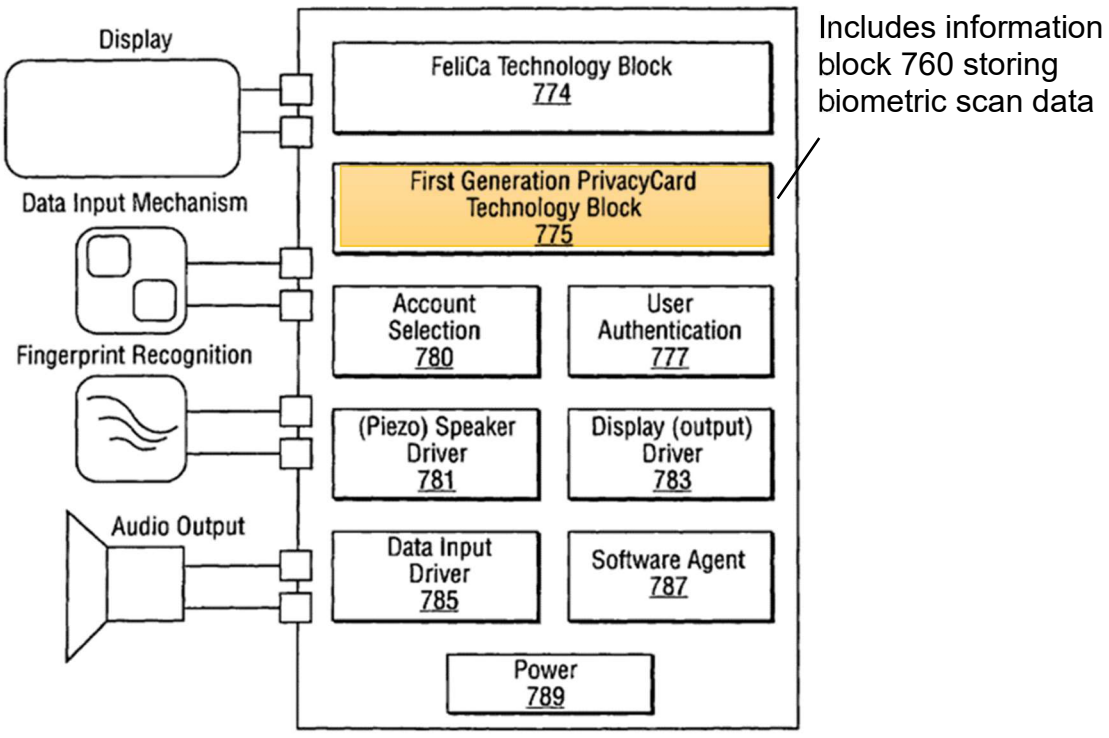


FIG. 7C

Ludtke, FIG. 7C (annotated).

79. Ludtke further discloses that 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.

80. Ludtke's stored device ID, like "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. 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.

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

81. 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 sensor) in response to the prompt (request for biometric verification). Ludtke, 14:33-42.

82. In Ludtke, the privacy card user authentication[1] 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 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).

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

83. 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.

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

e. [1d]: "responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and"

84. Ludtke discloses or renders obvious [1d] because Ludtke discloses transferring (sending) the transaction device ID (ID code) to a "single trusted" and "highly secured" transaction processing clearing house (TPCH) (third-party trusted authority) for validation/confirmation using, e.g., "wireless or cellular signals" (wirelessly) once a fingerprint match is identified. Ludtke, 5:63-64, 7:46-48, 9:26-30, 9:35-42, 9:52-59, 28:50-29:14, 30:23-27.

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

86. 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 "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.

87. 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, 14:33-40, 18:45-50, 18:52-55. The sample is compared to stored fingerprints, and if the sample is recognized, the user is authorized to "access the data and functionality of the device." 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.").

88. The "confirmation that the user is authorized" is based on the match between the scan data and stored data, as explained for [1b] and [1c]. 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).

89. 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.

90. **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.

91. **Finally,** Ludtke discloses that the TPCH is a trusted third-party for validating/confirming that ID code by comparing the received transaction ID against one or more previously stored (registered) IDs.

92. As Ludtke explains, with respect to Figure 6, the TPCH is an entity separate from the parties to a transaction (third party) 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. elements 605 and 610 respectively. 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.

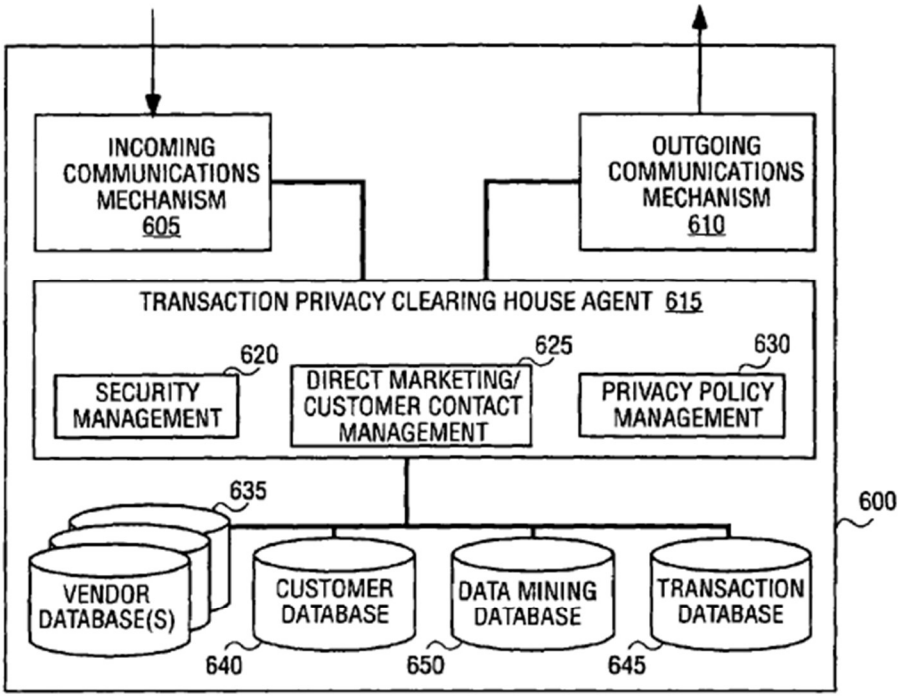


FIG. 6

93. 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 (emphasis added).

94. The TPCH also includes various databases for storing the transaction ID and linking the user to the transaction ID. Ludtke, 10:15-22, 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, 33:39-42 ("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, 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*.") (emphasis added).

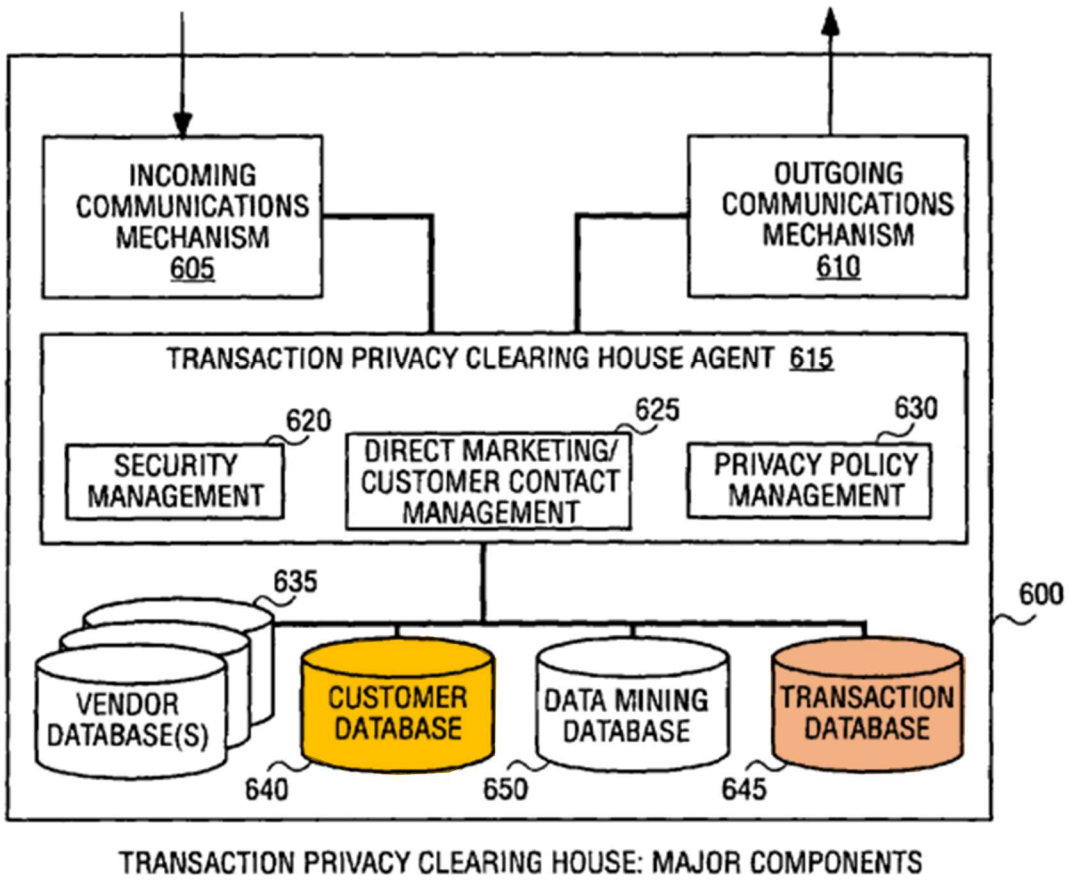


FIG. 6

Ludtke, FIG. 6 (annotated).

95. 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 it associated with." Ludtke, 30:23-27 (emphasis added). Thus, Ludtke discloses storing device ID codes.

96. A POSITA would have understood that the TPCH compares the received transaction device ID to one or more transaction IDs previously stored in the customer databases because "[t]he TPCH uses the unique ID of the transaction device to process the transaction" and "knows *which transaction device*, and hence which user, the transaction it associated with." Ludtke, 29:12-14, 30:23-27 (emphasis added).

97. It is also my opinion that a POSITA would have been motivated and found it obvious to configure the TPCH to compare the received transaction device ID to the stored transaction device ID to ascertain which customer is requesting the transaction, whether "the transaction device is in good standing[,]" and whether the "selected account" associated with the transaction ID "has sufficient funds for the transaction." Ludtke, 29:12-18, 30:23-27.

f. [1e]: "responsive to receiving an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction."

98. Ludtke discloses [1e] because after the TPCH authenticates the transaction device ID (ID code), the transaction device 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, which allows the user to complete a "purchase" or "shopping activity" (financial transaction). Ludtke, 6:36-44, 28:26-31, 28:50-62, 29:5-23.

99. As explained for [1d], 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. The TPCH (third-party trusted authority) "*uses the unique ID of the transaction device to process the transaction"* to validate the transaction device and confirm that "the selected account has *sufficient funds* for the transaction." Ludtke, 29:12-15 (emphases added). Once validated, 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).

100. The approved transaction may relate to a "purchase" made using the web browser or in a "retail situation" where "the user or a store clerk specifies the items to be purchased," i.e., a financial transaction. Ludtke, 22:9-15. *See also* Ludtke, 28:26-31("the transaction device is used to trigger shopping activity "), 28:34-35 ("The user triggers the purchase, usually by clicking on a "Buy!" or similar button in the web browser."). Thus, the approval allows the user to complete a financial transaction by receiving the items being purchased.

2. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code."

101. Ludtke discloses claim 3.

102. 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).

103. 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; [1c], above. More specifically, 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 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).

104. Ludtke discloses sending an indication that the biometric verification was successful because Ludtke sends the transaction device ID in response to successful fingerprint recognition, which indicates that the biometric verification was successful. This is consistent with the '905 patent, which does not disclose sending a distinct indication of success but discloses that sending the device ID (code) itself is an indication of successful biometric verification. Ex. 1001, 2:28-36 ("the code uniquely identifies the integrated device; the code indicates that the biometric verification was successful"), 6:10-13, 8:4-7.

3. Claim 4: "The method of claim 1, wherein the biometric data includes data from 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."

105. Ludtke further discloses claim 4 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.

4. Claim 5: "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."

106. Ludtke discloses or renders obvious claim 5.

107. Ludtke explains that the "transaction device is an interactive device with communications capabilities" that allows 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.

108. 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 '905 patent does not specify the precise nature of the mobile phone, a POSITA would have understood that a transaction device having "built in" "cell phone functionality" *is* a mobile phone.

109. 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.

110. 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.").

111. Thus, 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 as a "cell phone" and such implementations were established in the art. Ludtke, 17:65-18:4.

5. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application"

112. Ludtke discloses claim 6 because completing the purchase (financial transaction) includes accessing a financial account (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, 29:29-36; *see also* Ex. 1001, 6:20-26 (defining "application" as "resource that can be accessed by a verified and authenticated user" and identifying "a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.)" as one type of application.

113. More specifically, Ludtke discloses that completing the purchase (financial transaction), as discussed for [1e], includes confirming that the user's selected account has "sufficient funds to perform the transaction." Ludtke, 29:15-18. A POSITA would have understood that confirming "sufficient funds" necessarily requires accessing a financial account with an application to determine whether the amount of funds in the account is adequate to cover the purchase. Ludtke further discloses that once the transaction is confirmed and the purchased product (content) is distributed to the user, the TPCH "processes the settlement of funds" by, e.g., "transfer[ing] of the appropriate financial credit into the vendor's account." Ludtke, 29:29-36.

114. Thus, the method includes accessing a financial account (application) to determine fund sufficiency and withdraw the appropriate amount of funds.

6. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account."

115. Ludtke discloses claim 7 because, as explained for claim 6, completing the purchase (financial transaction) includes determining whether the user's account has "sufficient funds" and transferring the appropriate amount from the user's account to the vendor (accessing a financial account). Ludtke, 29:15-18, 29:29-36; s*ee also* Ludtke, 5:49-52 ("The transaction device may represent a single account such as a particular credit card, or it might represent multiple accounts such as a *credit card*, telephone card and *debit card*." (emphasis added)).

116. More specifically, Ludtke discloses that completing the purchase (financial transaction), as discussed for [1e], includes confirming that the user's selected account has "sufficient funds to perform the transaction." Ludtke, 29:15-18. A POSITA would have understood that confirming "sufficient funds" necessarily requires accessing a financial account with an application to determine whether the amount of funds in the account is adequate to cover the purchase. Ludtke further discloses that once the transaction is confirmed and the purchased product (content) is distributed to the user, the TPCH "processes the settlement of funds" by, e.g., "transfer[ring] of the appropriate financial credit into the vendor's account." Ludtke, 29:29-36. Thus, the method includes accessing a financial

account to determine fund sufficiency and withdraw the appropriate amount of funds.

7. Independent Claim 9

a. [9preamble]: "An integrated device comprising:"

117. Ludtke discloses [9preamble] because, as discussed for [1preamble] and [1ai], 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. [9a]: "a persistent storage media that persistently stores biometric data of a user and an ID code"

118. Ludtke discloses [9a] for the same reasons discussed for [1a].

c. [9b]: "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 the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and"

119. Ludtke discloses or renders obvious [9b] for the same reasons discussed for [1d].

120. As discussed for [1d], 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, 13:27-29, 14:19-21, 14:40-45 (emphasis added); [1a] and [1c], above; *see also* Ludtke, 16:47-49 (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.

121. Once the user/transaction device is verified (scan data matches the biometric data e.g., fingerprint match identified), the transaction device ID (ID code) is wirelessly sent to a "single trusted" and "highly secured" TPCH (third-party 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, 9:51-59, 12:10-16, 17:3-4, 28:50-29:12, 30:23-27. This is consistent with the '905 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.

122. The TPCH uses the received transaction device ID to confirm/validate that the transaction device is in "good standing" by ensuring that the received device ID matches an ID maintained in, e.g., its customer database (comparing the received ID with stored IDs), as discussed for [1d].

d. [9c]: "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction."

123. Ludtke discloses [9c] 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) after the code is authenticated (based on the comparison of the ID code). Ludtke, 5:63-64, 6:36-44, 9:39-42, 17:3-10, 29:5-23, 33:46-49.

124. As discussed for [1e], the transaction device receives an indication of "approval of the transaction to be performed" (access code) from the TPCH after the code is authenticated (based on the comparison of the ID code), and the approval allows the user access to the application to complete their purchase at the POS (financial transaction). Ludtke, 6:36-44, 28:26-31, 28:50-62, 29:5-23. 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.

125. 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 mechanism performing the wireless communication is a radio frequency communication module.

8. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network."

126. Ludtke further discloses claim 10.

127. As explained for [1e], the device ID and other codes are sent to the external server TPCH 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.").

9. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."

128. Ludtke discloses or renders obvious claim 12 for the same reasons discussed for claim 5.

10. Independent claim 13

a. [13preamble]: "A system, comprising:"

129. Ludtke discloses [13preamble] because, as illustrated in Figure 2, Ludtke discloses a system. Ludtke, Abstract.

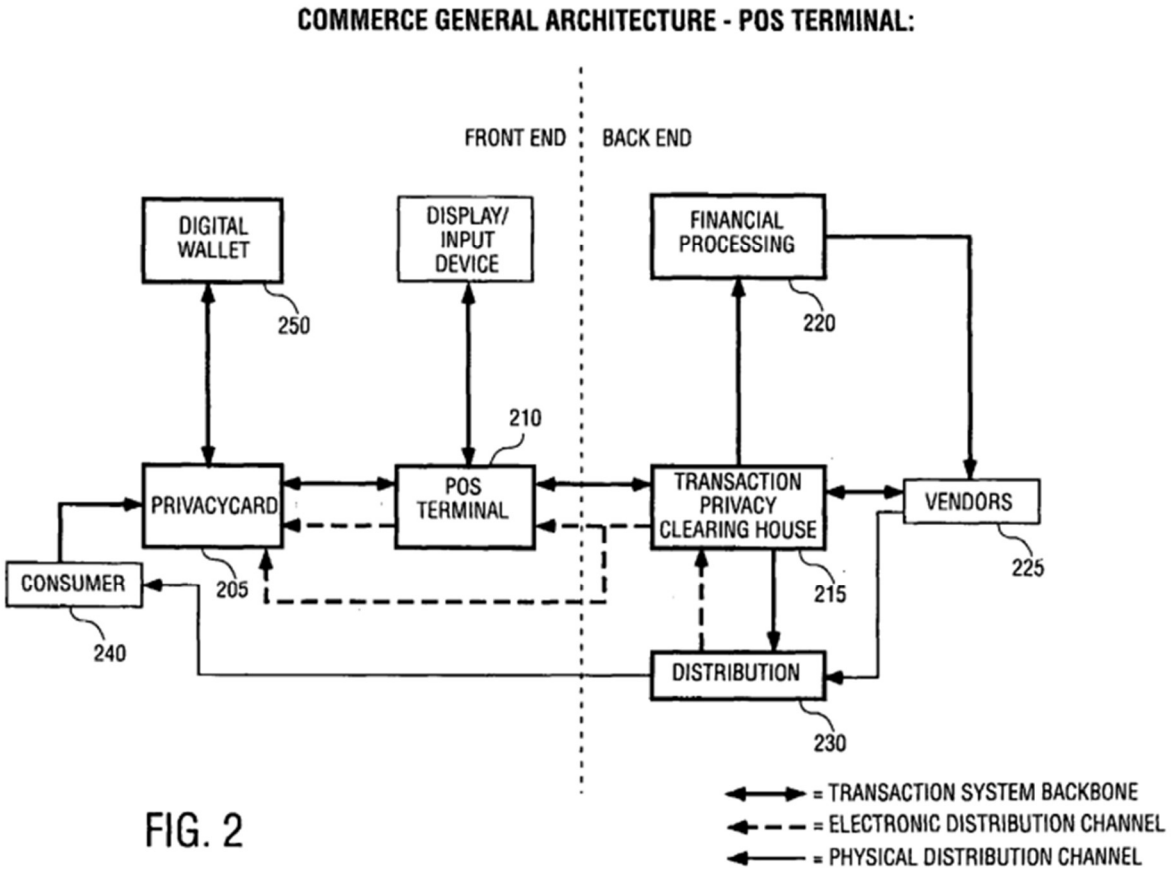


FIG. 2

Ludtke, FIG. 2.

130. The system includes the elements recited in [13a]-[13c], such as an integrated device (e.g., privacy card or digital wallet) and a POS terminal (authentication circuit), for communication with a TPCH (third-party trusted authority) for reasons explained below.

b. [13a]: "an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code;"

131. Ludtke discloses [13a] for the same reasons discussed for [1a] and [1d]. The transaction device (integrated device) of claim 1 is a hardware device such as a privacy card that wirelessly sends a transaction device ID to a POS, as discussed for [1d]. Ludtke, 5:63-64, 7:46-48, 9:26-30, 9:35-42, 9:52-59, 28:50-29:12, 30:23-27.

c. [13b]: "an authentication circuit that receives the [I]D code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and"

132. Ludtke discloses [13b] 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 complete a purchase (financial transaction). Ludtke, 28:50-29:12.

133. 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 (emphasis added). Thus, Ludtke discloses receiving the device ID and providing the device ID to a third-party trusted authority.

134. "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 third-party trusted authority successfully authenticated the ID code) "back to the

personal POS terminal," which allows the user to complete the purchase (financial transaction). Ludtke, 29:12-23; [1e], above.

d. [13c]: "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes."

135. Ludtke discloses or renders obvious [13c] because, as explained for [1d], the "single trusted" and "highly secured" TPCH (third-party trusted authority) contains a "copy" of "unique transaction device ID[s]" (list of legitimate ID codes) and confirms/validates that the transaction device is in "good standing" by ensuring that the received device ID matches an ID maintained in, e.g., the customer database. Ludtke, 3:40-43, 4:48-50, 6:36-44, 28:26-31, 28:50-62, 29:5-23, 30:20-27.

11. Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code."

136. Ludtke further discloses claim 14.

137. As explained for [1b] and [13b], the transaction device (integrated device) receives a validation request from the POS terminal (authentication request

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

138. For example, 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], above. 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; [1c], above. More specifically, 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.

139. 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, 16:47-49 (explaining that the digital wallet also receives biometric scan data after prompting).

140. 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, 4:62-65, 4:66-5:1; *see also* Ludtke, 39:50-56 ("At 3104 the [digital wallet ("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)).

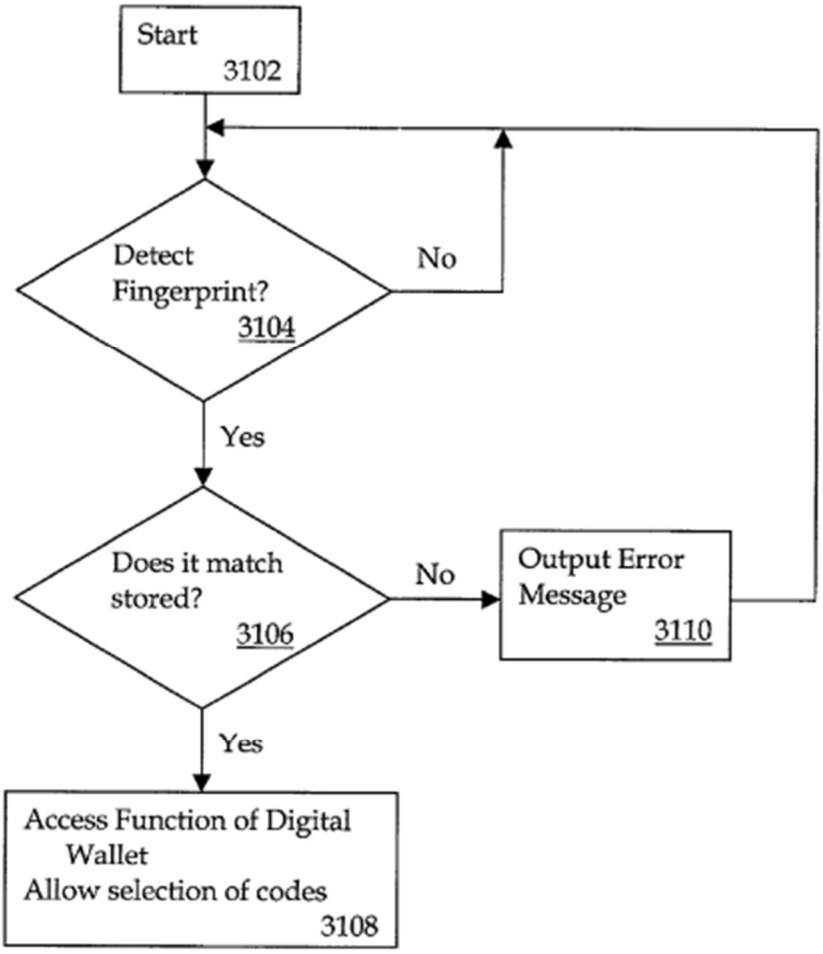


FIG. 31

141. It is also my opinion that a POSITA would have been motivated and found it obvious for security reasons to configure the 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.

142. Additionally, it is my opinion that a POSITA would have been motivated 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 for network efficiency reasons. As there would be no reason to send a message when the data is not verified, foregoing the potentially unnecessary message would conserve processing resources of the device and transmission resources of the network.

143. 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.

12. Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."

144. Ludtke discloses or renders obvious claim 15 for the same reasons discussed for claim 5.

13. Claim 16: "The system of claim 11, wherein the biometric data includes data based on 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."

145. Ludtke discloses claim 16 for the same reasons discussed for claim 4.

14. Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account."

146. Ludtke discloses claim 17 for the same reasons discussed for claim 7.

15. Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application."

147. Ludtke discloses claim 18 for the same reasons discussed for claim 6.

B. Ground 2: Claims 2 and 11 Are Obvious in View of Ludtke and Kon

148. Dependent claims 2 and 11 require an age or birthdate verification. While Ludtke does not expressly disclose age or birthdate verification, Kon does. In my opinion, it would have been obvious to add Kon's age and birthdate verification to Ludtke.

1. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the ID code."

149. Ludtke in combination with Kon renders obvious claim 2.

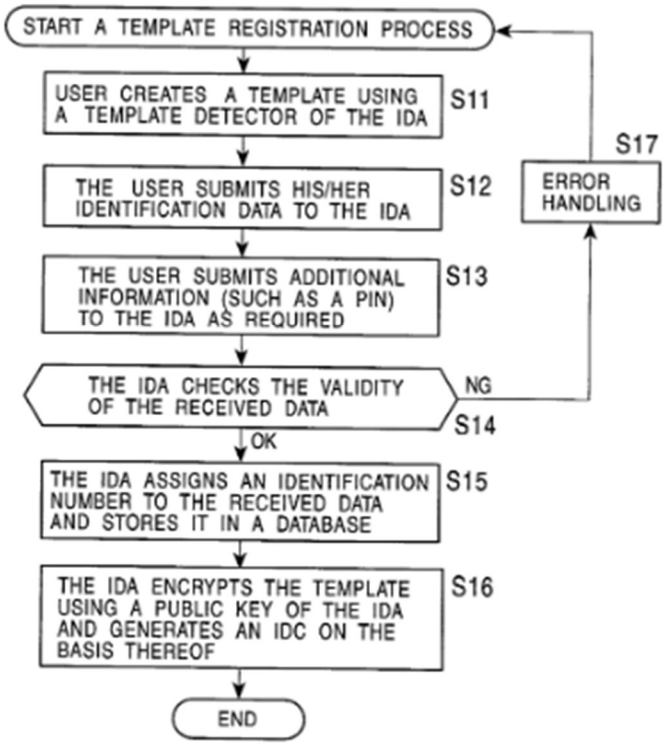
150. Kon discloses registering and storing a user's personal information, including the user's age, in association with the user's device ID—the user's device ID is stored in a "Subject" field and the user's age is stored in a "Directory Attribute" field of a registered IDC certificate. Kon, [0194] ("Subject is a field in which the name of a subject or a user is described . . . , for example, *the ID of a user device* or the ID . . . ." (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).

151. 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.

152. 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].).

153. For example, Gatz (Ex. 1016), 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." *Id.*, [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. *Id.*, [0082].

154. 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 11: "The integrated device of claim 7, wherein an age verification is registered in association with the ID code."

155. Ludtke in view of Kon renders obvious claim 11 for the reasons explained for claim 2.

XII. CONCLUSION

156. For the reasons set forth in Section XI, it is my opinion that one skilled in the art would have found claims 1-7 and 9-18 of the '905 patent to be obvious.

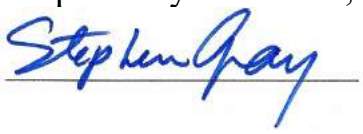
157. In signing this declaration, I understand that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in this case and that cross-examination 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.

158. 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