

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

PROXENSE, LLC
Patent Owner.

U.S. Patent No. 10,698,989
Issue Date: June 30, 2020
Title: Biometric Personal Data Key (PDK) Authentication

Inter Partes Review No.: IPR2025-00600

**DECLARATION OF STEPHEN GRAY IN SUPPORT OF
PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 10,698,989**

Mail Stop “PATENT BOARD”
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. MY BACKGROUND, QUALIFICATIONS, AND PROFESSIONAL EXPERIENCE	2
III. MATERIALS CONSIDERED	5
IV. RELEVANT LEGAL STANDARDS	6
A. Patent and Prosecution History	7
B. Presumption of Validity and Burden of Proof	8
C. Claim Construction.....	8
D. Prior Art.....	8
E. Anticipation	9
F. Obviousness.....	10
V. LEVEL OF ORDINARY SKILL IN THE ART	13
VI. SUMMARY OF OPINIONS	15
VII. OVERVIEW OF THE '989 PATENT	15
A. Disclosure	15
B. Prosecution History	19
C. Effective Filing Date	20
VIII. CLAIM CONSTRUCTION	20
IX. LEVEL OF ORDINARY SKILL IN THE ART	22
X. DETAILED EXPLANATION OF HOW CHALLENGED CLAIMS ARE UNPATENTABLE.....	22
A. Ground 1: Claims 1-9 are Unpatentable Over Ludtke and Baird	22

1.	Ludtke	22
2.	Baird.....	26
3.	Motivation to Combine	29
4.	Detailed Analysis	33
a.	Claim 1.....	33
	[1pre] “A method comprising:”	33
	[1a] “receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones;”	33
	[1b] “persistently storing biometric data and the ID code on the smartphone,”	39
	[1c] “wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user;”	41
	[1d] “receiving, at the smartphone, scan data from a biometric scan using the smartphone;”	41
	[1e] “comparing, using the smartphone, the scan data to the biometric data;”	42
	[1f] “determining whether the scan data matches the biometric data; and”	43
	[1g] “responsive to a determination that the scan data matches the biometric data, wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third- party trusted authority”	43

	[1h] “a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code”	51
	[1i] “wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.”	52
b.	Claim 2.....	53
	[2pre] “The method of claim 1, further comprising: [2a] receiving a request for biometric verification, and responsive to a determination that the scan data does not match the biometric data, indicating the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code”	53
c.	Claim 3.....	54
	[3pre] “The method of claim 1, [3a] wherein completing the transaction includes accessing an application.”	54
d.	Claim 4.....	55
	[4pre] “The method of claim 1, [4a] wherein the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code includes the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party.”	55
e.	Claim 5.....	57
	[5pre] “A smartphone comprising:”	57

[5a] “a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority, and biometric data,”	57
[5b] “wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user,”	58
[5c] “the ID code uniquely identifying the smartphone among a plurality of smartphones,”	58
[5d] “the persistent storage storing the biometric data and the ID code,”	58
[5e] “the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the smartphone”	58
[5f] “a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage,”	59
[5g] “the validation module having a scan pad to capture scan data from a biometric scan,”	60
[5h] “the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; and”	60
[5i] “a wireless transceiver that, responsive to a determination that the scan data matches the biometric data, sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority,”	60

	[5j] “a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code,”	61
	[5k] “wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.”	61
g.	Claim 6.....	62
	[6pre] “The smartphone of claim 5, [6a] wherein the ID code is transmitted to the third-party trusted authority over a network.”	62
h.	Claim 7.....	62
	[7pre] “A system, comprising:”	62
	[7a] “a smartphone that persistently stores biometric data and an ID code,”	63
	[7b] “wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan data of a legitimate user,”	63
	[7c] “and the ID code is received from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones,”	63
	[7d] “the smartphone configured to indicate that a biometric authentication is requested,”	63
	[7e] “the smartphone configured to wirelessly send the ID code to the third-party trusted authority for authentication responsive to determining that scan data from a biometric scan performed using the smartphone	

	matches the biometric data of the legitimate user,”	64
	[7f] “wherein a transaction is completed responsive to successful authentication of the ID code by the third-party trusted authority,”	64
	[7g] “wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account; and”	64
	[7h] “the third-party trusted authority operated by a third party,”	64
	[7i] “the third-party trusted authority storing a plurality of legitimate ID codes and authenticating the ID code received based on a comparison of the ID code received and the legitimate ID codes included in the plurality of the legitimate ID codes.”	65
i.	Claim 8.....	65
	[8pre] “The system of claim 7, [8a] wherein the smartphone receives an authentication request, and in response, requests biometric scan from a user to generate the scan data and, when the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code.”	65
k.	Claim 9.....	66
	[9pre] “The system of claim 7, [9a] wherein completing the transaction includes accessing an application.”	66
B.	Ground 2: Claims 1-9 Are Unpatentable Over Burger and Baird	66

1.	Burger.....	66
2.	Motivation to Combine	71
3.	Detailed Analysis	74
a.	Claim 1.....	74
	[1pre] “A method comprising:”	74
	[1a] “receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones;”	74
	[1b] “persistently storing biometric data and the ID code on the smartphone,”	75
	[1c] “wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user”	78
	[1d] “receiving, at the smartphone, scan data from a biometric scan using the smartphone;”	78
	[1e] “comparing, using the smartphone, the scan data to the biometric data;”	80
	[1f] “determining whether the scan data matches the biometric data; and”	82
	[1g] “responsive to a determination that the scan data matches the biometric data, wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third- party trusted authority,”	83
	“third-party trusted authority”	87

	[1h] “a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code,”	90
	[1i] “wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.”	93
b.	Claim 2.....	94
	[2pre] “The method of claim 1, further comprising: [2a] receiving a request for biometric verification, and responsive to a determination that the scan data does not match the biometric data, indicating the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code.”	94
c.	Claim 3.....	96
	[3pre] “The method of claim 1, [3a] wherein completing the transaction includes accessing an application.”	96
d.	Claim 4.....	97
	[4pre] “The method of claim 1, [4a] wherein the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code includes the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party.”	97
e.	Claim 5.....	99
	[5pre] “A smartphone comprising:”	99

[5a] “a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority, and biometric data,”	99
[5b] “wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user,”	99
[5c] “the ID code uniquely identifying the smartphone among a plurality of smartphones,”	99
[5d] “the persistent storage storing the biometric data and the ID code,”	99
[5e] “the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the smartphone;”	99
[5f] “a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage,”	100
[5g] “the validation module having a scan pad to capture scan data from a biometric scan,”	100
[5h] “the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; and”	100
[5i] “a wireless transceiver that, responsive to a determination that the scan data matches the biometric data, sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority,”	101

	[5j] “a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code,”	101
	[5k] “wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.”	101
f.	Claim 6.....	101
	[6pre] “The smartphone of claim 5, [6a] wherein the ID code is transmitted to the third-party trusted authority over a network.”	101
g.	Claim 7.....	102
	[7pre] “A system, comprising:”	102
	[7a] “a smartphone that persistently stores biometric data and an ID code,”	102
	[7b] “wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan data of a legitimate user,”	102
	[7c] “and the ID code is received from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones,”	102
	[7d] “the smartphone configured to indicate that a biometric authentication is requested,”	102
	[7e] “the smartphone configured to wirelessly send the ID code to the third- party trusted authority for authentication responsive to determining that scan data from a biometric scan performed using the smartphone	

	matches the biometric data of the legitimate user,”	102
	[7f] “wherein a transaction is completed responsive to successful authentication of the ID code by the third-party trusted authority,”	103
	[7g] “wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account; and”	103
	[7h] “the third-party trusted authority operated by a third party,”	103
	[7i] “the third-party trusted authority storing a plurality of legitimate ID codes and authenticating the ID code received based on a comparison of the ID code received and the legitimate ID codes included in the plurality of the legitimate ID codes.”	103
h.	Claim 8.....	104
	[8pre] “The system of claim 7, [8a] wherein the smartphone receives an authentication request, and in response, requests biometric scan from a user to generate the scan data and, when the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code.”	104
i.	Claim 9.....	104
	[9pre] “The system of claim 7, [9a] wherein completing the transaction includes accessing an application.”	104

I. INTRODUCTION

1. I have been retained by Apple Inc. (“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. 10,698,989 (“the ’989 patent,” Ex. 1001). The application for the ’989 patent was filed February 20, 2016, and 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.

4. I have been asked by Petitioner to provide my opinion on whether the claims of the ’989 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 ’989 patent. In performing my analysis, I have been asked to assume that the priority date of the ’989 patent 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. MY BACKGROUND, QUALIFICATIONS, AND PROFESSIONAL EXPERIENCE

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

7. I am competent to write this declaration.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

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

16. 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.

17. 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.

III. MATERIALS CONSIDERED

18. In preparing this declaration and formulating my opinions, I have considered, relied upon, and applied my own knowledge, background and experience in the relevant field. I have also considered the viewpoint of a POSITA in the field, as of the relevant time frame. I also reviewed the '989 Patent (EX1001), the file history of the '989 Patent (EX1002), and each of the documents cited herein, and I have considered these documents in light of the general knowledge in the art as of December 20, 2004.

19. Among other things, the documents and materials I reviewed and considered include:

Exhibit #	Description
1001	U.S. Patent No. 10,698,989 (the “’989 Patent”)
1002	Prosecution History of the ’989 Patent
1005	U.S. Patent No. 7,188,110 to Ludtke et al. (“Ludtke”)
1006	U.S. Patent Application Publication No. 2006/0075230 to Baird, III et al. (“Baird”)
1007	U.S. Patent Application Publication No. 2005/0050367 to Burger et al. (“Burger”)
1008	<i>Samsung Electronics America, Inc. v. Proxense, LLC</i> , IPR2021-01448, Paper 12 (Feb. 28, 2022)
1009	<i>Proxense, LLC v. Samsung Electronics Co., Ltd.</i> , Case No. 6:21-CV-00210-ADA, Dkt. No. 43, Claim Construction Order (W.D. Tex. Jan. 18, 2022)
1011	<i>Google LLC v. Proxense, LLC</i> , IPR2024-00233, Paper 10 (Jul. 23, 2024)
1012	<i>Google LLC v. Proxense, LLC</i> , IPR2024-00234, Paper 10 (Jul. 23, 2024)
1013	<i>Samsung Electronics America, Inc. v. Proxense, LLC</i> , IPR2021-01447, Paper 12 (Feb. 28, 2022)
1014	Office communication in <i>Ex parte</i> reexamination, App. No. 90/015,054 (office action rejecting all claims).
1015	EP 1478152 to Nishida et al. (“Nishida”)

IV. RELEVANT LEGAL STANDARDS

20. I am not a lawyer, and therefore I offer no opinions on the law.

Nonetheless, I have been informed and understand that certain legal standards are relevant to my analysis. In preparing and expressing my opinions and considering

the subject matter of the '989 Patent, I rely on certain basic legal principles that counsel have explained to me, as summarized below.

A. Patent and Prosecution History

21. I have been informed that a patent includes a specification, one or more drawings, and one or more claims. I have been informed that the specification provides a written description of the patented invention, the drawings illustrate the invention, and the claims define the scope of the invention. I understand that the file history includes the back and forth communication between a patent applicant and the United States Patent and Trademark Office (“USPTO” or “Patent Office”) during the application process, including the application itself, as well as office actions filed by the USPTO examiner and responses filed by the applicant.

22. I have been informed and understand that a patent is to be understood from the perspective of a person having ordinary skill in the art (“POSITA”). Such an individual is considered to possess normal skills and knowledge in a particular technical field (as opposed to being a genius). I have been informed and understand that in considering what the claims of a patent require, what was known prior to that patent, what a prior art reference discloses, and whether an invention is obvious or not, one must use the perspective of such a POSITA.

B. Presumption of Validity and Burden of Proof

23. I have been informed and understand that an issued patent claim is presumed to be valid. I have further been informed that establishing a patent claim to be unpatentable in an *inter partes* review proceeding requires proof by “preponderance of the evidence,” which I understand means proof that it is more likely than not that the claim is unpatentable.

C. Claim Construction

24. I have been informed and understand that the first step in an unpatentability analysis involves construing claims, as necessary, to determine their scope. Counsel has informed me that claim terms are given their plain and ordinary meaning as would be understood by a POSITA in the relevant art. Because the meaning of a claim term may not be readily apparent, I understand that I may look to those sources available to the public that show what a POSITA would have understood a claim term to mean. These include, in order of importance, the words of the claims themselves, the patent specification, the prosecution history, and, finally, evidence outside the patent like dictionaries, textbooks, or other resources that may inform the meaning of the claim terms.

D. Prior Art

25. I am told that the second step in an unpatentability analysis involves comparing the construed claim language against the disclosures of the prior art.

26. I have been informed that prior art to the '989 Patent includes patents and printed publications in the relevant art that predate the priority date of the alleged invention recited in the '989 Patent. For purposes of this declaration, I have been asked to apply December 20, 2004, the purported effective filing date of the '989 Patent, as the priority date.

27. I have further been informed and understand that a person of ordinary skill in the art is presumed to know the relevant prior art.

28. I have been informed and understand that a patent claim may be declared unpatentable if it is anticipated by, or rendered obvious in view of, prior art.

E. Anticipation

29. I have been informed that, to anticipate a claim under 35 U.S.C. § 102, a reference must teach or disclose every element of the claim either expressly or inherently to a person having ordinary skill in the relevant art. I have also been informed that, to be an inherent disclosure, the prior art reference must necessarily disclose the limitation, and the fact that the reference might possibly practice or contain a claimed limitation is insufficient to establish that the reference inherently teaches the limitation.

F. Obviousness

30. I have been informed that a patent claim is not patentable under 35 U.S.C. § 103 if the differences between the patent claim and the prior art are such that the claimed subject matter as a whole would have been obvious at the time the claimed invention was made to a person having ordinary skill in the relevant art. Obviousness, as I have been informed and understand, is based on the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and, to the extent that they exist, certain objective indicia of non-obviousness.

31. I have been informed that whether there are any relevant differences between the prior art and the claimed invention is to be analyzed from the view of a person of ordinary skill in the relevant art at the time of the invention. As such, my opinions below as to a person of ordinary skill in the art are as of the time of the invention, even if not expressly stated as such; for example, even if stated in the present tense.

32. In analyzing the relevance of the differences between the claimed invention and the prior art, I have been informed that I must consider the impact, if any, of such differences on the obviousness or non-obviousness of the invention as a whole, not merely some portion of it. The person of ordinary skill faced with a

problem is able to apply his or her experience and ability to solve the problem and also look to any available prior art to help solve the problem.

33. I have been informed and understand that a single prior art reference can render a patent claim obvious under 35 U.S.C. § 103 if any differences between that reference and the claims would have been obvious to a person of ordinary skill in the art.

34. Alternatively, I have been informed and understand that a prior art reference may be combined with other references to disclose each element of the invention under 35 U.S.C. § 103. Thus, the teachings of two or more references may be combined in the same way as disclosed in the claims, if such a combination would have been obvious to one having ordinary skill in the art. I have been informed and understand that a reference may also be combined with the knowledge of a person of ordinary skill in the art, and that this knowledge may be used to combine multiple references.

35. I have been informed that a precise teaching in the prior art directed to the subject matter of the claimed invention is not needed. I have been informed that one may take into account the inferences and creative steps that a person of ordinary skill in the art would have employed in reviewing the prior art at the time of the invention. For example, if the claimed invention combined elements known in the prior art and the combination yielded results that were predictable to a

person of ordinary skill in the art at the time of the invention, then this evidence would make it more likely that the claim was obvious. On the other hand, if the combination of known elements yielded unexpected or unpredictable results, or if the prior art teaches away from combining the known elements, then this evidence would make it more likely that the claim that successfully combined those elements was not obvious.

36. I have been informed that there are recognized, exemplary, rationales for combining or modifying references to show obviousness of claimed subject matter. Some of the rationales include the following: combining prior art elements according to known methods to yield predictable results; simple substitution of one known element for another to yield predictable results; use of a known technique to improve a similar device (method or product) in the same way; applying a known technique to a known device (method or product) ready for improvement to yield predictable results; choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art; and some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the

prior art reference or to combine prior art teachings to arrive at the claimed invention.

37. I have been informed that objective indicia can be important evidence regarding whether a patent is obvious or nonobvious, if it has an appropriate nexus to the claimed invention, *i.e.*, is a result of the merits of a claimed invention (rather than the result of design needs or market-pressure advertising or similar activities). Such indicia include: commercial success of products covered by the patent claims; a long-felt need for the invention; failed attempts by others to make the invention; copying of the invention by others in the field; unexpected results achieved by the invention as compared to the closest prior art; praise of the invention by the infringer or others in the field; the taking of licenses under the patent by others; expressions of surprise by experts and those skilled in the art at the making of the invention; and the patentee proceeded contrary to the accepted wisdom of the prior art.

V. LEVEL OF ORDINARY SKILL IN THE ART

38. I have been informed and understand that a POSITA is a hypothetical person who is presumed to be aware of all pertinent prior art, thinks along conventional wisdom in the art, and is a person of ordinary creativity.

39. I understand there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including (1) the levels of education and

experience of persons working in the field at the time of the invention; (2) the sophistication of the technology; (3) the types of problems encountered in the field; and (4) the prior art solutions to those problems.

40. I have been informed by Apple's counsel that the earliest priority date for the '989 Patent is December 20, 2004, the date on which the initial provisional application was filed.

41. Based on the technologies disclosed in the '989 Patent, I believe that a POSITA would include someone who had, at the priority date of the '989 Patent, 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.

42. Based on these criteria, as of the relevant time frame for the '989 Patent, I possessed at least such experience and knowledge of a POSITA, and am qualified to opine on the '989 Patent.

43. For purposes of this declaration, in general, and unless otherwise noted, my statements and opinions, such as those regarding my experience and the understanding of a POSITA generally (and specifically related to the references I consulted herein), reflect the knowledge that existed in the field as of December

20, 2004. Unless otherwise stated, when I provide my understanding and analysis below, it is consistent with, refers to, and applies the level of a POSITA as of the priority date of the '989 Patent.

VI. SUMMARY OF OPINIONS

44. As described in detail below, based on my review of the '989 Patent and its prosecution history, the other materials I have considered, and my knowledge and experience, I offer the following opinions in this declaration:

45. Claims 1-9 are invalid at least as obvious over Ludtke and Baird.

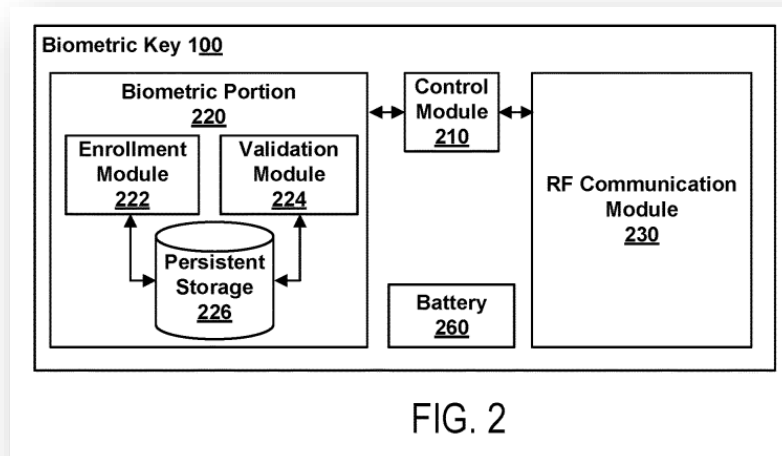
46. Claims 1-9 are invalid at least as obvious over Burger and Baird.

VII. OVERVIEW OF THE '989 PATENT

A. Disclosure

46. The '989 Patent, titled "Biometric Personal Data Key (PDK) Authentication," issued on June 30, 2020. EX1001, (10), (45), (54). The '989 Patent relates to "authentication responsive to biometric verification of a user being authenticated." EX1001, 1:35-38, 2:9-11, 3:66-4:1.

47. The '989 Patent describes a "biometric key" as illustrated in Figure 2, including a biometric module, a control module, and an RF module. EX1001, FIG. 2, 4:60-64.



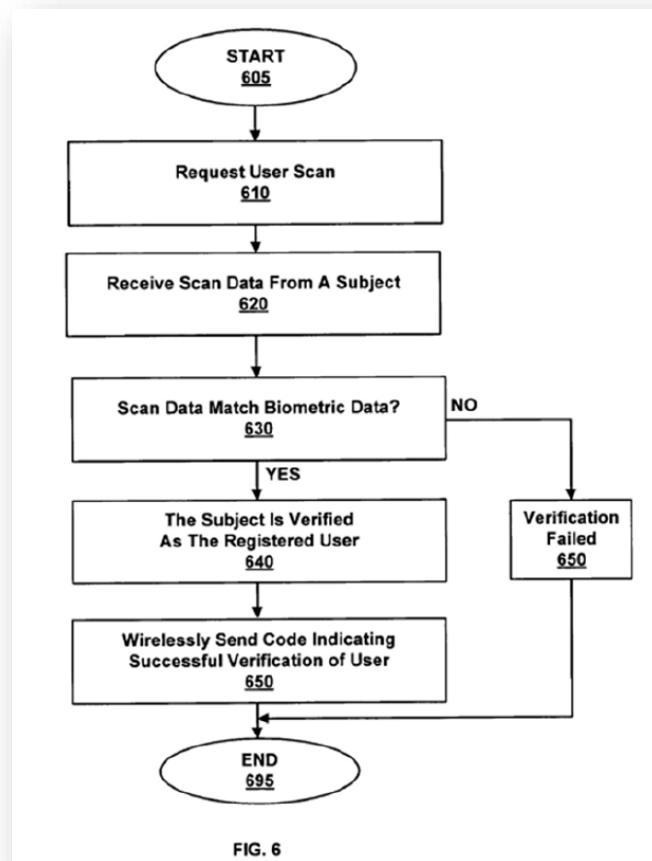
EX1001, FIG. 2. The biometric key “provid[es] authentication information for a biometrically verified user.” EX1001, 4:19-20; 4:10-12 (describing “biometric verification using a fingerprint” and “other types of biometric data”).

48. The biometric key is integrated into another device (“integrated device”), such as a “mobile phone (e.g. a cellular phone or smartphone).” EX1001, 4:26-31. The integrated device includes storage to store a code such as a device identifier (ID) and biometric data for a user. EX1001, 2:12-15. For biometric verification, the integrated device compares the user’s biometric scan against the stored biometric data, and if the scan data matches the biometric data, wirelessly sends the code to an “authentication module” for authentication. EX1001, 2:16-29, 2:50-67.

49. The ’989 Patent discloses that “the code is registered with a trusted authority” and “can be authenticated to a third party by the trusted authority.”

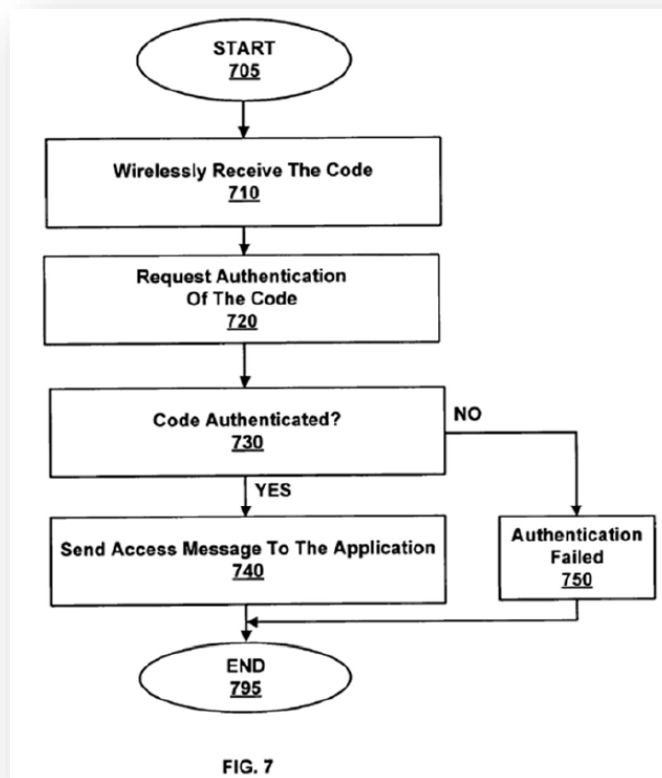
EX1001, 2:44-46. The “code uniquely identifies the integrated device” and “indicates that the biometric verification was successful.” EX1001, 2:46-47.

50. Figure 6 illustrates a process for “verifying a subject” using a biometric key. EX1001, 8:21-22, FIG. 6. The device receives biometric scan data (e.g., fingerprint scan) from the user (step 620). EX1001, FIG. 6. If the scan data matches “previously-stored biometric data,” (step 630), the user is “verified” (step 640), and the “code” is sent to a trusted key authority (step 650). EX1001, 8:25-32, FIG. 6.



EX1001, FIG. 6.

51. Once the code is received, as illustrated in Figure 7, the trusted key authority determines whether the code is “authentic” (step 730). EX1001, 8:37-40, 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). EX1001, 8:40-43, FIG. 7. If authentication is unsuccessful, authentication fails (step 750) and “the message to the application indicates that the user should be denied access.” EX1001, 8:44-47, FIG. 7.



EX1001, FIG. 7.

B. Prosecution History

52. During prosecution, the Examiner repeatedly rejected the claims as obvious over various prior art, and for non-statutory double patenting in view of U.S. Patent Nos. 8,886,954, 8,352,730, and the then-pending application that issued as U.S. Patent No. 9,298,905.¹ EX1002, 398-411, 478-492, 883-897, 970-986, 1025-1042, 1080-1095, 1160-1172.

53. Following Applicant's unsuccessful attempts to amend the claims to distinguish over the prior art, the Examiner suggested certain amendments to "place them in better condition for allowance." EX1002, 073. Pursuant to the Examiner's suggestions, Applicant's sole amendment to the claims was to replace the term "mobile phone" with the term "smartphone." EX1002, 066-070.

54. The Examiner subsequently allowed the claims, stating in the reasons for allowance: "[N]o parts of the cited arts teach or suggest limitations such as

¹ Each of these patents has been the subject of respective IPR proceedings before the Board. *See* IPR2021-01444, IPR2024-00232, IPR2024-00775, IPR2024-0133, IPR2024-01486, IPR2024-00233, IPR2024-00846, IPR2024-01334, IPR2024-01485, IPR2021-01447, IPR2024-00234, IPR2024-00776, and IPR2024-01335. The '905 Patent was also subject to an ex parte reexamination, Serial No. 90/015,053, where the patentee disclaimed the patent.

persistently storing biometric data of a legitimate user and an ID code on the smartphone, wherein the ID code is received from a third-party trusted authority, the ID code uniquely identifies the smartphone from a plurality of smartphones.” EX1002, 070-071.

55. The '989 Patent is also the subject of a pending *ex parte* reexamination proceeding, Serial No. 90/015,054, where all claims currently stand rejected.

C. Effective Filing Date

56. The '989 Patent application was filed on February 20, 2016, claiming priority to a provisional application filed December 20, 2004. EX1001, (22), (63), (60), 1:7-19. I understand that for purposes of this proceeding only, Petitioner assumes, and has asked me to assume, that the effective filing date of the '989 Patent is December 20, 2004.

VIII. CLAIM CONSTRUCTION

56. The Challenged Claims of the '989 Patent are construed herein “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b). “[C]laim terms need only be construed to the extent necessary

to resolve the controversy.” *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011). I understand that Petitioner maintains that the prior art references relied on in this Petition meet or disclose each of the claim terms under any reasonable construction. That is consistent with my opinions as set forth herein.

57. I am informed and understand that the Board previously construed the term “*third-party trusted authority*”² as recited in the ’989 Patent and related patents to mean “a trusted authority that is an entity separate from the parties to a transaction.” *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01448 (“the Samsung IPR”), Paper 12 (EX1008), 11; EX1011, 9-12; EX1012, 9-11.

58. I understand that in the litigation related to the Samsung IPR, *Proxense, LLC v. Samsung Electronics Co., Ltd.*, No. 6-21-CV-00210 (W.D.Tex.), the court construed the term “*ID code*” in the ’989 Patent as “a unique code identifying a device.” EX1009, 3. In the same IPR proceedings concerning related patents, although the Patent Owner requested that the Board adopt the court’s construction of “*ID code*,” the Board declined because it did not find it necessary to provide an express construction. *See* EX1011, 12; EX1012, 11.

² Claim language appears in *italics* throughout this Declaration.

59. Because the prior art in the subject Petition discloses each of these prior constructions, and the plain and ordinary meaning of all terms, I understand that Petitioner submits that no claim terms need be construed to resolve unpatentability. This is consistent with my opinions as set forth herein.

IX. LEVEL OF ORDINARY SKILL IN THE ART

60. A POSITA at the time of the alleged invention or priority date of the '989 Patent 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.

X. DETAILED EXPLANATION OF HOW CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1-9 are Unpatentable Over Ludtke and Baird

1. Ludtke

61. Ludtke is titled "Secure and Convenient Method and Apparatus for Storing and Transmitting Telephony-Based Data," and was filed December 11, 2000. I am informed that Ludtke qualifies as prior art, and was not cited or applied to reject any claims during prosecution of the '989 Patent. EX1001, (56); EX1002.

62. Ludtke discloses systems and methods of authorizing a user to conduct a transaction using biometric authentication for a "privacy card" and/or

“digital wallet” (each also referenced as a “transaction device”). EX1005, Abstract, 3:32-36, 6:36-44. The transaction device includes a processor, memory, and fingerprint recognition technology. EX1005, 5:60-64, FIG. 7A. The device persistently stores “authorized fingerprint recognition samples,” a device ID corresponding to the transaction device, and a public key infrastructure (“PKI”). EX1005, 11:66-12:7, 14:19-21, 38:26-29. The biometric device can use other techniques, such as a “retinal scan, voice, DNA, hand profile, face recognition, etc.,” instead of or in addition to fingerprints. *Id.*, 35:61-64.

63. When an authorized user attempts to use the transaction device, *e.g.*, at a point of sale (“POS”) terminal, other “service,” or “web-based transaction,” the user is “prompted to supply a fingerprint recognition sample.” EX1005, 1:22-38, 14:33-42, 18:45-55, 28:15-62. The sample is compared to stored fingerprints and if the sample is recognized, the user is authorized for the device. EX1005, 14:40-46.

64. Once authorized, a “secure communications session” to a “transaction processing clearing house”³ [TPCH] is opened, “requesting a transaction,” and the POS terminal provides to the TPCH the transaction record that it received from the

³ Also interchangeably referred to in Ludtke as “transaction privacy clearing house.” *See* EX1005, 6:37-38.

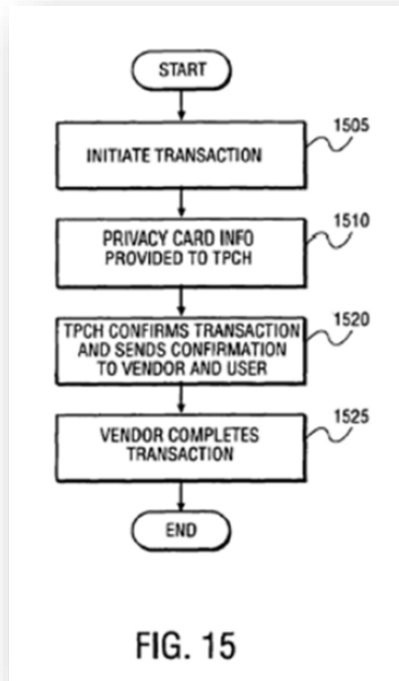
web browser *and the unique ID*⁴ of the transaction device.” EX1005, 29:5-12; 27:12-13 (“Privacy card information is provided to TPCH, step 1510.”), 34:25-27 (explaining that “necessary secure transaction communication with the TPCH [includes] providing the transaction data and its device ID.”). The TPCH is a trusted third-party agent, separate from the transaction device, personal POS terminal and the back-end transacting entity (*e.g.*, vendor). EX1005, 7:42-48, 9:26-34, FIG. 6.

65. Ludtke 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.” EX1005, 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.

66. 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

⁴ Throughout this Declaration, supplied emphases are indicated in *bold italics*.

“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.” EX1005, 29:12-23, FIG. 15.



EX1005, FIG. 15.

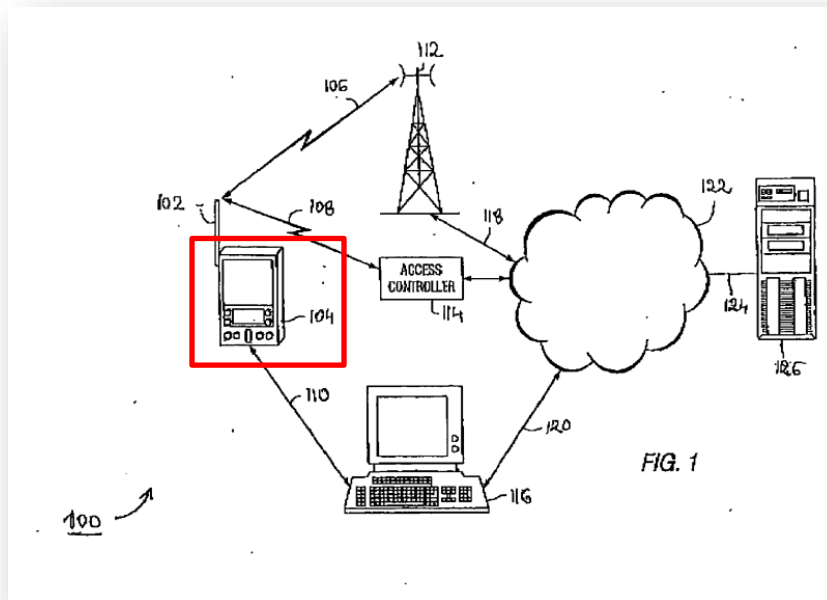
67. Based on the law as explained to me, it is my opinion that Ludtke is analogous art to the '989 Patent because it is directed to the same field of endeavor—i.e., user authentication methods and systems for networked communications devices. Even if Ludtke were not directed to the same field of endeavor (it is), at a minimum it is reasonably pertinent to the problem the inventor

of the '989 Patent was trying to solve—namely, “providing systems and methods for authentication responsive to biometric verification of a user being authenticated.” *Compare* EX1001, 1:35-38, 2:10-12, *with* Ludtke, 1:59-61.

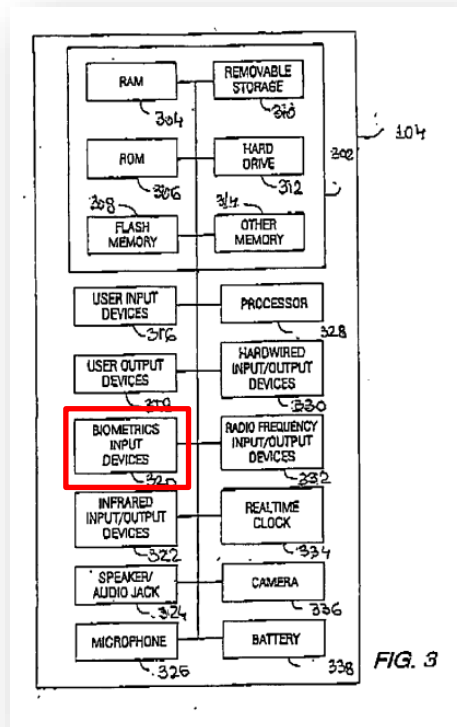
2. Baird

68. Baird is titled “Apparatus and Method for Authenticating Access to a Network Resource Using Multiple Shared Devices,” filed October 5, 2004, and was published April 6, 2006. I am informed that Baird qualifies as prior art and was not cited or applied to reject any claims during prosecution of the '989 Patent. EX1001, (56); EX1002.

69. Baird “relates to means and methods for secure access to network resources” that “allow users to be authorized to authenticate through a single given mobile device.” EX1006, Abstract, [0001], [0005]. An overall architecture for Baird is shown in FIG. 1:



EX1006, FIG. 1 (annotated). Baird describes a biometric key integrated into the device 104, as shown in FIG. 3:



EX1006, FIG. 3 (annotated).

70. Baird discloses that “[d]evice 104 further comprises at least one user input device 316 such as keyboard, pen input, or touch screen, at least one user output device 318, such as a display screen, Braille output or a video output jack, **“at least one biometrics input device, such as a fingerprint reader**, infrared input/output devices 320 for communicating with, for instance, computer 116, speaker/audio jacks 324, and a microphone or an audio input jack 326 for providing audio input, especially voice, to device 104.” EX1006, [0033]. Baird further discloses that “[s]ingle device 104 is upgraded with additional elements that allow the device 104 to operate as a trusted device, that is, a device requiring user

authentication. The user proves his or her identity to the device 104 in various ways using one or more multiple techniques. They include the use of a password, *biometrics input*, and physical possession of the single device.” EX1006, [0034]. Baird describes that its device 104 comprises “*at least one biometrics input device, such as a fingerprint reader*” which be used for user authentication. EX1006, [0034]. The device 104 can be “*a ‘smart’ cell phone*” or “*smart phone.*” EX1006, [0031], [0079].

71. Based on the law as explained to me, Baird is analogous art to the ’989 Patent because it is directed to the same field of endeavor: user authentication methods and systems for networked communications devices. Even if Baird were not directed to the same field of endeavor (it is), at a minimum it is reasonably pertinent to the problem the inventor of the ’989 Patent was trying to solve—namely “providing systems and methods for authentication responsive to biometric verification of a user being authenticated.” *Compare* EX1001, 1:35-38, *with* EX1006, [0001], [0004]-[0006].

3. Motivation to Combine

72. A POSITA would have found it obvious and would have been motivated to combine the teachings of Ludtke and Baird with a reasonable expectation of success.

73. Ludtke describes a system that authorizes a user to conduct a transaction using a “biometric device” (also called a “transaction device”) such as a privacy card and/or digital wallet. More specifically, Ludtke discloses systems and methods of authorizing a user to conduct a transaction using a “biometric device,” that employs fingerprint recognition technology for biometric verification in conjunction with an ID code. EX1005, Abstract, 3:32-36, 5:60-64, 6:36-44. Ludtke states that the “privacy card” (transaction device) is “configured to be sized for easy carrying and use” and is thus portable. EX1005, 11:64-65. Ludtke teaches that some of the data storage requirements of its transaction device can be offloaded to “another portable device such as a cell phone,” assuming that such other portable device is “always or typically in the proximity of the transaction device.” EX1005, 34:19-24. A POSITA considering these teachings in Ludtke would have recognized that since the transaction device might “always or typically” be in proximity to a cell phone, and both devices are portable, it would often be inconvenient for the user to carry multiple devices.

74. Baird provides a technical solution to the problem. Baird teaches integrating a biometric input and transaction device into a smart phone and combining multiple authentication features in a single smart phone EX1006, [0002] (“the single mobile device performs authentication and login to multiple resources using separate passwords or authentication credentials”), [0031], [0079].

As Baird states, the user “proves his or her identi[t]y” to the (“‘smart’ cell phone”) device through a “biometrics input device, such as a fingerprint reader.” EX1006, [0031]-[0034]. A POSITA looking at Baird would have recognized that incorporating the “transaction device” and biometric transaction authentication features of Ludtke into a “smartphone” with biometric authentication as taught by Baird would be advantageous because it reduces the number of devices that a user would need to carry. Similar to Ludtke, Baird stresses that “single device 104 is upgraded with additional elements that allow device 104 to operate as a trusted device, that is, a device requiring user identification.” EX1006, [0034]. Indeed, integrating an IC card into a cell phone and adding features to increase user convenience was well-known as of the priority date of the ’989 Patent. EX1015, [0002], [0004] (“Portable terminals such as mobile units proposed heretofore also include those equipped with a chip element having the function of the IC card described above, as an IC chip.”), [0018] (“The present invention lifts the limit on the number of application programs operable with the noncontact IC chip, and improves the convenience of the mobile unit”).

75. And a POSITA would have had a reasonable expectation of success in making such combination. Both Ludtke and Baird relate to controlling access to network resources by utilizing biometric authentication, such as through a fingerprint scan, and their systems contain overlapping features and functionality.

For example, Ludtke and Baird use overlapping hardware in their respective systems, such as fingerprint scanners, display screens, input devices, persistent memory, wireless communications elements, and speakers in a palm-sized form factor. An embodiment of Ludtke's "transaction device" (privacy card) includes a "display," a "data input mechanism" which is "preferably a touch mechanism," a "fingerprint recognition pad," and even an "audio output." EX1005, FIG. 7C. Similarly, Baird teaches a device including a "user input device," an output device which can include a "display screen," a "fingerprint reader," and speakers and "audio input, especially voice." EX1006, FIG. 3. Also, both Ludtke's and Baird's systems and devices can facilitate "e-commerce." Baird's smartphone can conduct secure "transactions" at "an on-line e-commerce site." EX1006, [0021], [0034]. Similarly, Ludtke describes that "[t]he user connects to and performs transactions" with an "eCommerce system" through its "transaction device." EX1005, 3:14-47. Given the overlap in features and functionality, a POSITA would have recognized that modifying Ludtke's system according to the teachings of Baird required only basic hardware/software modifications and routine skill. For example, because the constituent hardware components are largely the same, a POSITA would have realized that the smartphone of Baird could be modified to incorporate Ludtke's "privacy card" with a firmware/software interface between such components. The implementation of these components together (memory, display, fingerprint

scanner, wireless communication elements) was known and was certainly within the ordinary skill of a POSITA at the time.

76. Combining the teachings of Ludtke and Baird would have involved combining prior art elements according to known techniques to yield predictable results.

4. Detailed Analysis

a. Claim 1

[1pre] “*A method comprising:*”

77. To the extent limiting, Ludtke discloses [1pre]: “The system *and method* of the present invention enables a user to conduct electronic commerce transactions without compromising the user’s personal identification information and identity....” EX1005, 3:14-36.

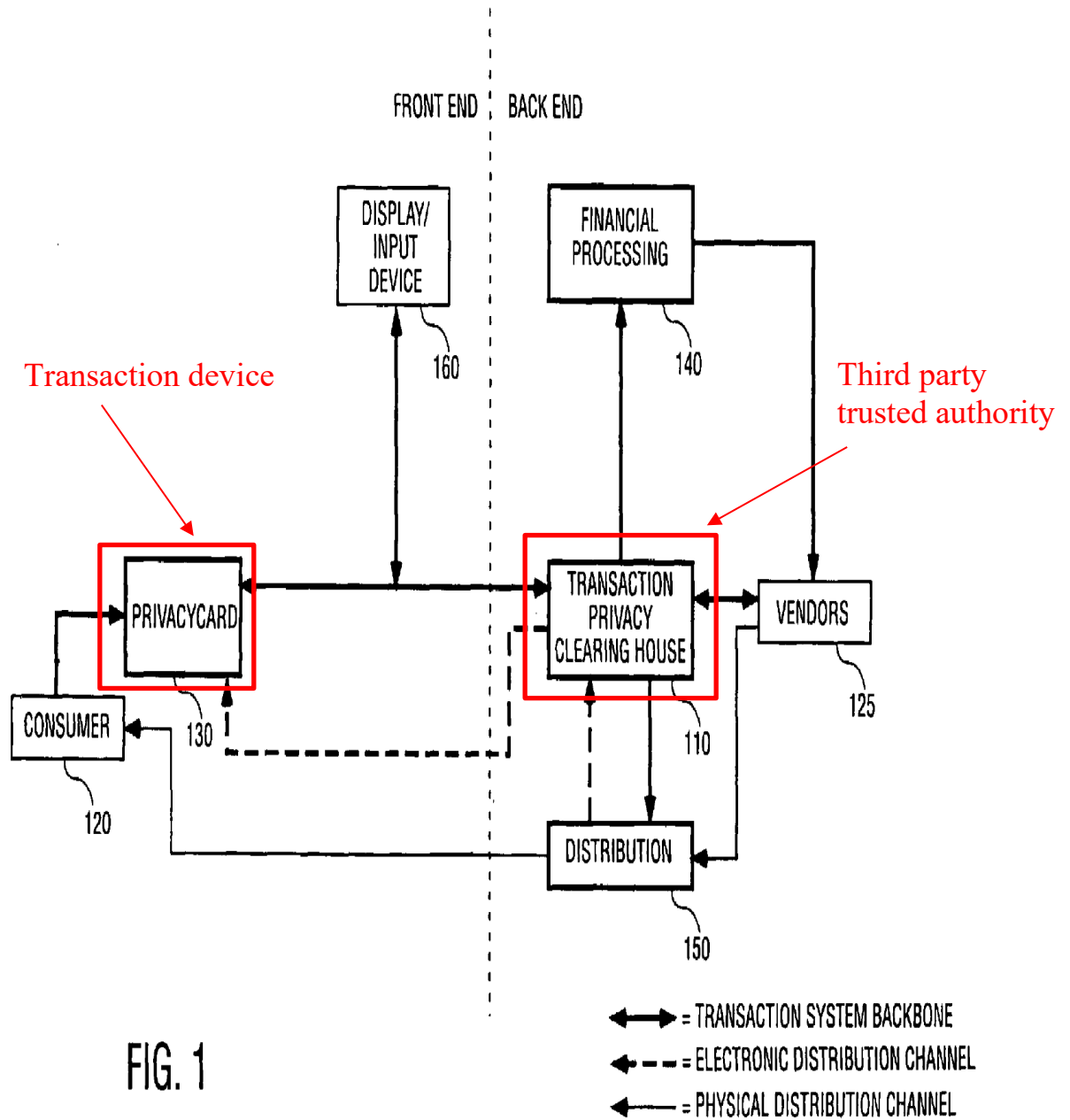
[1a] “*receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones;*”

78. Ludtke in view of Baird discloses [1a].

79. Ludtke discloses “*receiving...an identification (ID) code from a third-party trusted authority*” because in Ludtke a “unique identifier (ID)” or “globally unique silicon ID (GUID) 764” (“*identification (ID) code*”) is assigned to the “transaction device” by a “single trusted” and “highly secured” transaction privacy clearing house (TPCH) (“*third-party trusted authority*”). EX1005, FIGS. 1, 7A-C, 8, 9A-B, 10, 11, 3:32-46, 4:48-50, 6:36-51, 10:64-67, 11:63-12:7, 13:39-43,

29:10-15, 34:25-27. This “unique / device ID” is used by the transaction device in conjunction with the TPCH to conduct transactions, such as e-commerce transactions. *Id.* FIG. 1 of Ludtke and accompanying text show how the TPCH interacts with the transaction device:

COMMERCE GENERAL ARCHITECTURE



EX1005, FIG. 1 (annotated). The TPCCH controls assignment and delivery of the unique identifier to the user device as seen, e.g., in FIG. 11.

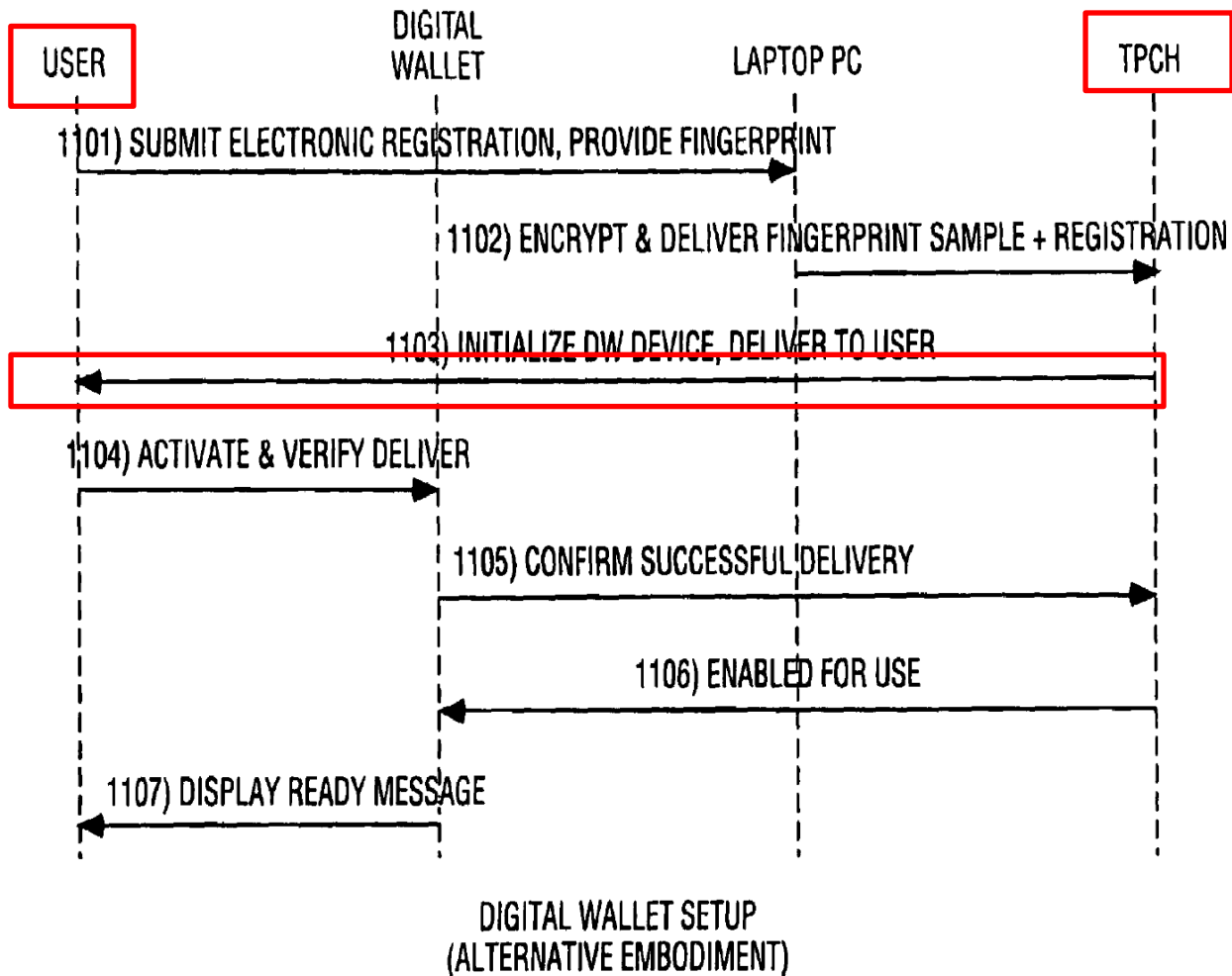


FIG. 11

EX1005, FIG. 11 (annotated). “At step 1103 the processing facility *creates a new transaction device* and personalizes it with the fingerprint and other data that was collected during registration. The processing facility *delivers the transaction device* to the user.” EX1005, 20:15-18. The “processing facility” is part of the TPOCH. *Id.*, 20:12-14.

80. Consistent with the Board’s construction of “*third-party trusted authority*,” Ludtke describes that the TPOCH is a “trusted” entity separate from the

parties to the transaction, i.e., the user and the “external retailers and vendors” that complete the transaction. EX1005, 4:48-50, 9:35-39, FIG. 6; EX1011, 20-24; EX1012, 19-24.

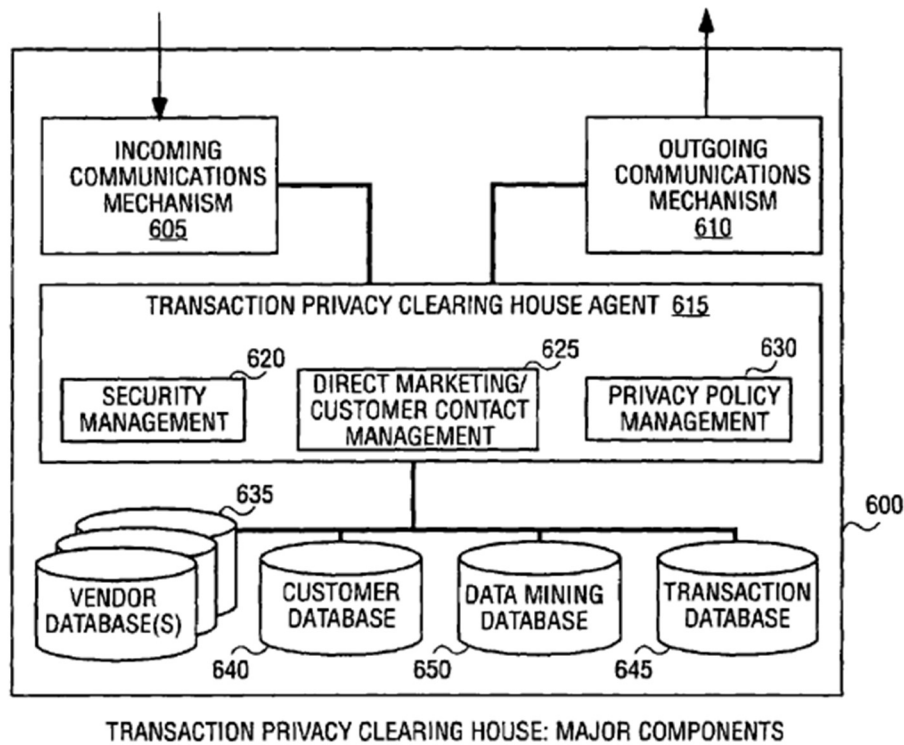


FIG. 6

EX1005, FIG. 6.

81. Ludtke further discloses that the separation between the TPCH, vendors, and the POS on which the user/transaction device is performing a transaction “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 TPOCH to function “as the middleman of the distribution channel.” EX1005, 7:44-48, 9:26-59. Accordingly, the TPOCH is a third-party trusted authority.

82. Baird teaches that a transaction device can be a secure “‘smart’ cell phone” or “smart phone” (“*smartphone*”) for conducting e-commerce transactions over a network. EX1006, [0031], [0079]. As discussed in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate the “transaction device” using biometric authentication taught in Ludtke (*e.g.*, “privacy card,” “digital wallet”) into Baird’s “smart phone.” Moreover, as a POSITA would have understood, Ludtke’s “transaction device” could be pre-installed into a smartphone by the TPOCH before delivery to a user or could be inserted into the smartphone by the user as a card device, such that the unique identifier (ID) (“*identification (ID) code*”) is received “at the smartphone.” EX1015, [0004] (“Portable terminals such as mobile units proposed heretofore also include those equipped with a chip element having the function of the IC card described above, as an IC chip.”).

83. Ludtke in view of Baird discloses “*the ID code uniquely identifying the smartphone among a plurality of smartphones*” because Ludtke describes the “globally unique silicon ID (GUID) 764 is used to identify” the transaction device “among other existing transaction [devices],” where the transaction device can be

integrated into Baird's "smart phone." EX1005, 13:39-43; EX1006, [0031].

Additionally, the TPCD can "maintain a copy" of "unique transaction device ID values" so that "whenever a transaction arrives with one of these values, the TPCD knows *which transaction device*, and hence which user, the transaction it associated with." EX1005, 30:23-27. Thus, Ludtke discloses that the "ID code" is associated with a specific "transaction device."

[1b] "*persistently storing biometric data and the ID code on the smartphone,*"

84. Ludtke in view of Baird discloses [1b].

85. Ludtke discloses "*persistently storing biometric data*" on the "transaction device." For example, "[t]he user identity info block 760...may contain the authorized fingerprint recognition samples." EX1005, 14:19-21. Additionally, "[t]he user is prompted to supply a fingerprint recognition sample. This [user authentication block of the transaction device] captures the sample, and carries out a recognition algorithm against the authorized samples *that are stored in the user identity block* [of the transaction device]..." *Id.*, 14:33-46. Fingerprints are "biometric data." *Id.*, 4:66-5:1.

86. Ludtke explains that "[t]he fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data," such that fingerprint image data" can be written "into write-once memory" ("*persistent stor[age]*"). EX1005, 19:9-40.

87. Ludtke further discloses “*persistently storing the ID code*” because it describes the transaction device storing the “unique ID value[]” in its “permanent memory” and containing the “globally unique silicon ID (GUID),” as shown, e.g., in FIG 7B. EX1005, 21:8-11, 30:20-23, FIG. 7B.

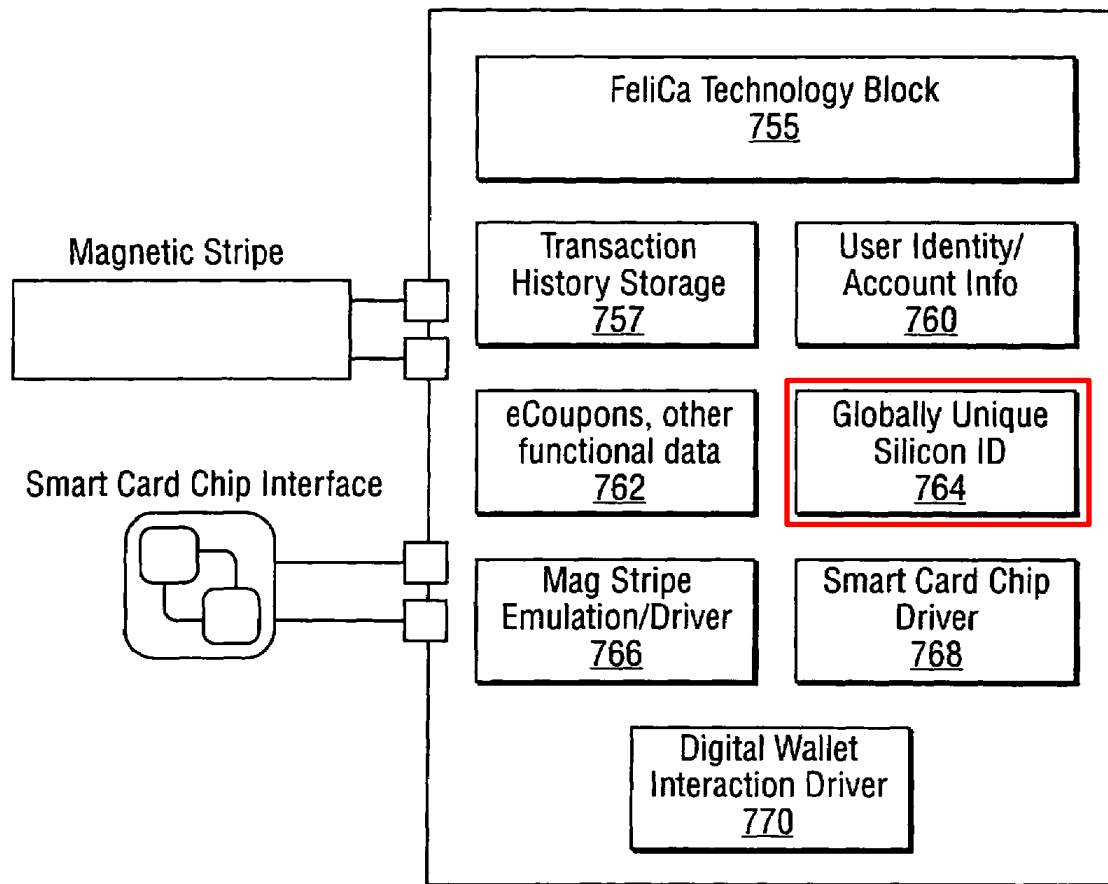


FIG. 7B

EX1005, FIG 7B (annotated).

88. Baird discloses a “*smartphone*” into which a POSITA would have found obvious to integrate Ludtke’s “transaction device,” as discussed in the

“Motivation to Combine” section. EX1006, FIGS. 3, 4, [0031]-[0033], [0079].

When integrated as such, the unique silicon ID for the transaction device is stored “*on the smartphone*” so that the device can be identified when communicating with other network resources.

[1c] “*wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user;*”

89. Ludtke discloses [1c].

90. Ludtke discloses “*wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user*” because, as addressed in [1b], Ludtke expressly discloses using a fingerprint scan as biometric data. EX1005, 4:66-5:1 (“authentication may be achieved by using . . . a biometric solution (e.g., fingerprint recognition)”).

[1d] “*receiving, at the smartphone, scan data from a biometric scan using the smartphone;*”

91. Ludtke in view of Baird discloses [1d].

92. Ludtke discloses “*receiving...scan data from a biometric scan*” because Ludtke discloses validating a user by prompting the user to “supply a fingerprint recognition sample” and receiving a fingerprint sample (“*receiving...scan data*”) from a fingerprint recognition pad (“*from a biometric scan*”). EX1005, 14:33-54;16:47-49. In operation, 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.” EX1005, 14:40-46.

93. Baird discloses a “*smartphone*” which includes “at least one biometrics device, such as a fingerprint reader.” EX1006, FIG. 3; [0031]-[0033]. As discussed in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate Ludtke’s “transaction device” into Baird’s “*smartphone*” and as such, the scan data is “*receiv[ed] at*” and “*using the smartphone.*”

[1e] “*comparing, using the smartphone, the scan data to the biometric data;*”

94. Ludtke in view of Baird discloses [1e].

95. Ludtke discloses “*comparing...the scan data to the biometric data*” in that it describes that after “the user is prompted to supply a fingerprint recognition sample,” the transaction device “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.*” EX1005, 14:40-46, 16:47-49.

96. Baird discloses a “smartphone” into which a POSITA would have found obvious to integrate Ludtke’s “transaction device,” as discussed in the “Motivation to Combine” section, and as such, the step of “*comparing*” would be performed “*using the smartphone.*” EX1006, FIGS. 3, 4, [0031]-[0033], [0079].

Indeed, Baird itself discloses that “the device 104 [functions] as a trusted device, that is, a device requiring user authentication. The user proves his or her identify [sic] to the device 104 in various ways using one or more multiple techniques,” which can include using “biometrics input.” EX1006, [0034]. Moreover, in Baird, “[a] credentials database is stored in the device If a biometric device is being used, their identification specifications are stored also in the credentials database, and are used when the user authenticates to the device.” EX1006, [0074].

[1f] “*determining whether the scan data matches the biometric data; and*”

97. Ludtke discloses [1f].

98. Ludtke discloses “*determining whether the scan data matches the biometric data*” in that it describes that the fingerprint scanner “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.*” EX1005, 3:38-39, 14:40-46, 16:47-49. Baird also discloses that the “user proves his or her identify [sic] to the device” using, e.g., biometric input. EX1006, [0034].

[1g] “*responsive to a determination that the scan data matches the biometric data, wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority*”

99. Ludtke and Baird disclose or render obvious [1g] because Ludtke discloses the transaction device sending the transaction device ID (“*ID code*”) to

the “single trusted” and “highly secured” TPC (“*third-party trusted authority*”) for validation/confirmation using, e.g., “wireless or cellular signals” (“*wirelessly*”) once a fingerprint match is identified, and Baird describes that the transaction device can be implemented on a “*smartphone*.” EX1005, 5:63-64, 7:46-48, 9:26-59, 28:50-29:12, 30:23-27; EX1006, [0031], [0079].

100. First, Ludtke determines whether the “*scan data matches the biometric data*” (as explained for [1b] and [1c]) and “*send[s] the transaction device ID*” to the TPC “*responsive to*” a match determination between the scan data and stored data.

101. When “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.” EX1005, 28:15-40. “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....” EX1005, 28:13-56.

102. The POS asks the transaction device to “validate the user” and the user is “prompted to supply a fingerprint recognition sample.” EX1005, 1:22-38,

14:33-42, 18:45-55, 28:57-62. The sample is compared to stored fingerprints and if the sample is recognized, the user is authorized. EX1005, 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 TPCCH, requesting a transaction” and “provides the transaction record that it received from the web browser *and the unique ID of the transaction device.*” EX1005, 28:50-29:12; 27:12-13 (“[p]rivacy card information is provided to TPCCH, step 1510.”), 34:25-27 (explaining that “necessary secure transaction communication with the TPCCH, providing the transaction data *and its device ID.*”).

103. 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]. EX1005, 14:40-46; 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...[a]uthentication may be achieved by using . . . a biometric solution (e.g., fingerprint recognition).”).

104. Ludtke 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.” EX1005, 28:41-45. Thus, Ludtke also discloses

communicating the device ID directly from the transaction device to the TPCCH responsive to a “match” between the scan data and stored data.

105. *Second*, Ludtke discloses sending the transaction device ID “*wirelessly*.” Ludtke discloses that “the TPCCH is located at a secure location” and “embodied as a secure server.” EX1005, 9:26-34. The TPCCH receives incoming communications, including the transaction ID, using an “incoming communications mechanism 605” using “wireless or cellular signals.” EX1005, 9:35-42.

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

107. As Ludtke explains, the TPCCH 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. EX1005, 9:35-39, FIG. 6. Indeed, Ludtke explains, “[t]he 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.” EX1005, 9:35-39. That the vendors and transaction device are “external” to the TPCCH confirms that the TPCCH is a third party, and not a party to the transaction itself.

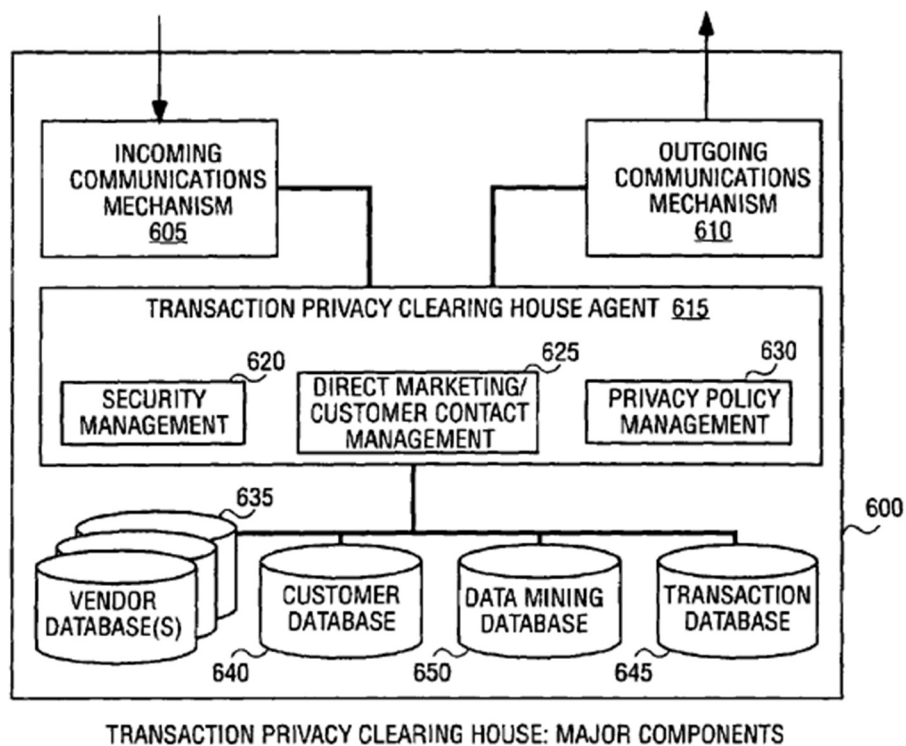


FIG. 6

EX1005, FIG. 6.

108. This is consistent with the Board’s construction that “third-party trusted authority” is a “trusted authority that is an entity separate from the parties to the transaction” EX1008, 11. It is also consistent with Patent Owner’s agreement—in IPR proceedings involving related patents—that “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.” EX1013, 13-15.

Indeed, the Board differentiated the prior art cited in 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.*” EX1013, 24.

109. Here, to the extent Patent Owner might argue that the TPCCH of Ludtke is similar to the mapping in the prior IPR, Patent Owner is wrong. Ludtke expressly identifies the TPCCH as external to the parties to the transaction, capable only of communication with the parties. The TPCCH remains independent of the user, POS, and “external” vendors. Moreover, Ludtke discloses that the TPCCH “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 TPCCH is not the vendor/retailer, or even the user’s financial institution (not a principal party to the transaction, and therefore a third party). EX1005, 29:43-46. Ludtke further discloses that the separation between the TPCCH, vendors, and the POS on which the user/transaction device is performing a transaction “ensures that only authorized entities are allowed access to data and that only authorized transaction devices can execute transactions against a user’s account,” allowing the TPCCH to function “as the middleman of the distribution channel.” EX1005 7:44-48, 9:26-59. Accordingly, the TPCCH is a third-party trusted authority.

110. The TPCB includes databases for storing the transaction ID and linking the user to the transaction ID. EX1005, 10:15-45, 33:37-41. For example, the “customer database” “holds information regarding each customer of the TPCB” and links the “actual user identity information” to “the digital aliases provided by the transaction device,” i.e., the transaction device ID. EX1005, 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. EX1005, 10:19-45, 33:37-41 (“Whenever the user carries out a transaction using the system, vendors receive only the transaction device ID *in the transaction record.*”).

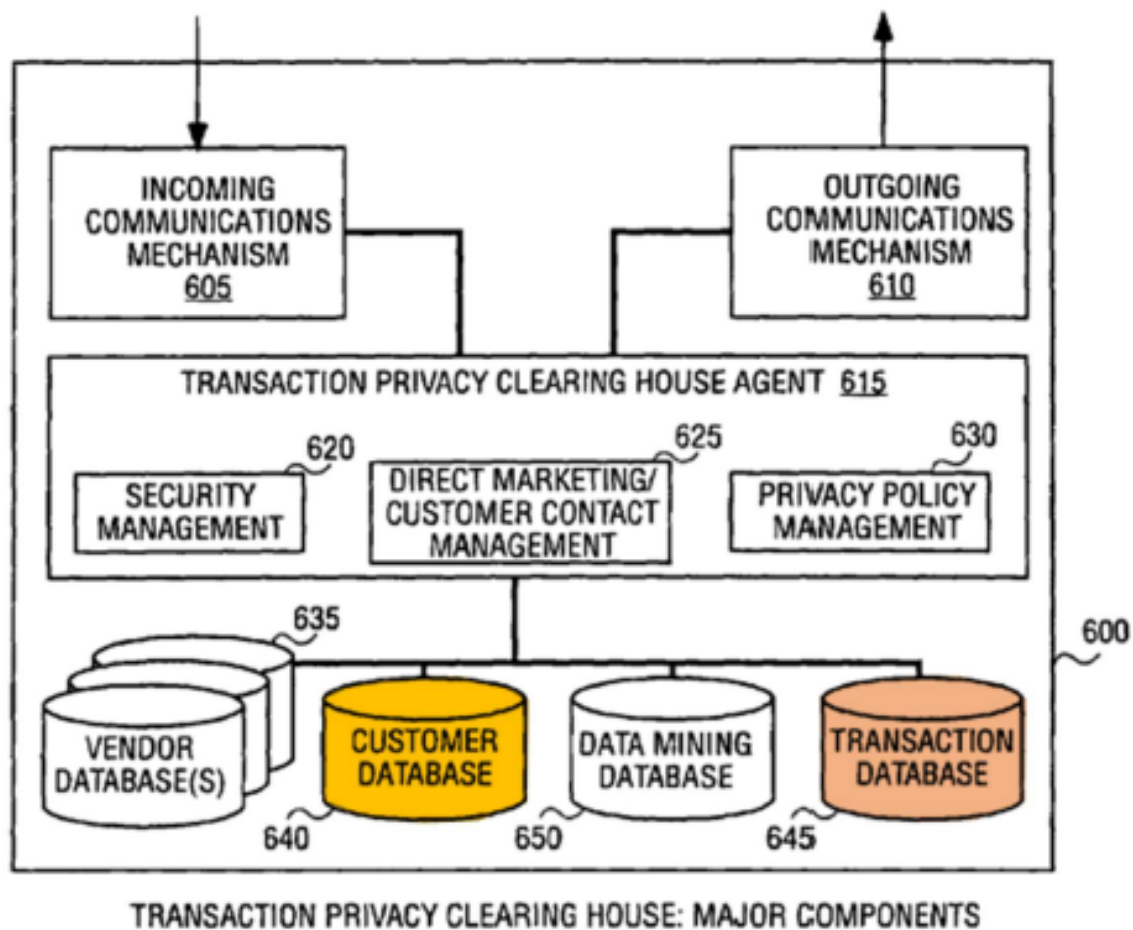


FIG. 6

EX1005, FIG. 6 (annotated).

111. 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. Thus, Ludtke discloses

storing device ID codes. As a POSITA would have understood, this would include the unique silicon ID for the transaction device (and/or smartphone) so that the hardware device can be identified when communicating with other network resources.

112. Moreover, a POSITA would have understood from this language that the TPOCH compares the received transaction device ID to one or more transaction IDs stored in the customer databases. EX1005, 29:12-14, 30:23-27. As discussed in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate Ludtke’s “transaction device” into Baird’s “*smartphone*,” such that the resulting smartphone device performs the functionality discussed for Ludtke’s device.

[1h] “*a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code*”

113. Ludtke discloses [1h].

114. Ludtke discloses “*a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code*” because after the TPOCH authenticates the transaction device ID (“*ID code*”), the transaction device receives an indication of “approval of the transaction to be performed” from the TPOCH, which allows the user to complete a “purchase” or “shopping activity” (“*transaction*”). EX1005, 6:36-44, 28:26-29:23. *See also* analysis for [1g], above.

[1i] “*wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.*”

115. Ludtke discloses [1i].

116. Ludtke discloses “*the transaction being completed*” that includes “*accessing*” at least a “*web site*” and a “*financial account.*” For “*web site*,” Ludtke describes that “the user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID).” EX1005, 3:32-35. FIG. 17 of Ludtke describes a “typical web-based transaction” in which “the user may either navigate to a **web page** [web site] by using the facility of the web browser, or by triggering a shopping activity using the transaction device.... The user triggers the purchase, usually by clicking “Buy!” or similar button in the web browser.” EX1005, 28:13-40. “The personal POS terminal provides the transaction record that it received from the web browser and the unique ID of the transaction device. The TPCCH uses the unique ID of the transaction device to process the transaction.” EX1005, 29:11-14. For “*financial account*,” Ludtke describes, e.g.: “[t]he 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.” EX1005, 5:49-52.

b. Claim 2

[2pre] *“The method of claim 1, further comprising: [2a] receiving a request for biometric verification, and responsive to a determination that the scan data does not match the biometric data, indicating the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code”*

117. Ludtke in view of Baird discloses [2pre] as discussed for claim 1.

118. Ludtke in view of Baird teaches or suggests [2a].

119. Ludtke discloses *“receiving a request for biometric verification”*

because the “transaction device requests the user to authenticate himself, for example, by fingerprint recognition.” EX1005, 27:28-30. As discussed in [1e] and [1f], Ludtke discloses that the transaction device can make *“a determination that the scan data does not match the biometric data.”* See [1e], [1f]. Ludtke describes that its transaction device “carries out a recognition algorithm against the authorized [fingerprint] samples that are stored in the user identity block” and “[i]f a match is found, the user is authorized to access the data and functionality of the device.” EX1005, 14:33-46. On the other hand, if a match is not found, “an error message is output and the DW [digital wallet] returns to checking to see if a fingerprint has been detected.” EX1005, 39:47-59. Based on this disclosure, a POSITA would understand that if no match is found for the biometric input, this *“indicat[es]”* that the transaction device *“cannot verify the scan data as being from the legitimate user,”* and any transaction is canceled so that it is unnecessary for

the transaction device to send its ID code (“*does not send the ID code*”) to the TPCH; *see also* FIG. 31 (outputting “error message” if no match).

120. As discussed in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate Ludtke’s “transaction device” into Baird’s “*smartphone*” such that the resulting smartphone device performs the functionality discussed for Ludtke’s device.

c. Claim 3

[3pre] “*The method of claim 1, [3a] wherein completing the transaction includes accessing an application.*”

121. Ludtke in view of Baird discloses [3pre] as discussed for claim 1.

122. Ludtke in view of Baird teaches “*wherein completing the transaction includes accessing an application.*” According to the ’989 patent, an application “can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, a financial account (e.g. a savings account, credit line, etc.) and the like.” EX1001, 6:42-47.

123. Ludtke describes that for some transactions, the transaction device accesses a web browser. EX1005, 20:51-53 (transaction device “can interact with a web browser, providing the necessary digital wallet identification information to the browser or other network software”). Ludtke further discloses that a “software agent” on the transaction device “can interact with other agents on other platforms (on PC’s or DTV’s, on web servers, etc.)” in relation to electronic coupons, direct

marketing, and the like. EX1005, 15:15-35. A POSITA would have understood that each of the “web browser,” “software agent,” and “other agents” in Ludtke is computer software and thus an “*application*.”

124. Baird describes that access to applications can be restricted, e.g.: “if the user needs to access an application on a server on the network or Internet, the device should transparently authenticate to that application using passwords, or Public Key Infrastructure (PKI) certificates, or whatever other credentials the application requires.” EX1006, [0088]. Based on this disclosure, a POSITA would have understood that with the integration of Ludtke’s “transaction device” into Baird’s “*smartphone*,” where access to applications are restricted, “*completing the transaction includes accessing an application*.”

d. Claim 4

[4pre] “*The method of claim 1, [4a] wherein the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code includes the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party.*”

125. Ludtke in view of Baird discloses [4pre] as discussed for claim 1.

126. Ludtke discloses [4a].

127. As discussed in [1h], Ludtke discloses “*the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code.*” See [1h].

128. Ludtke further discloses “*the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party*” in that the TPOCH (*third-party trusted authority*) sends the vendor in an e-commerce transaction an indication that the transaction has been approved (i.e. that the ID code for the user’s device was authenticated). See FIG. 15 of Ludtke, below:

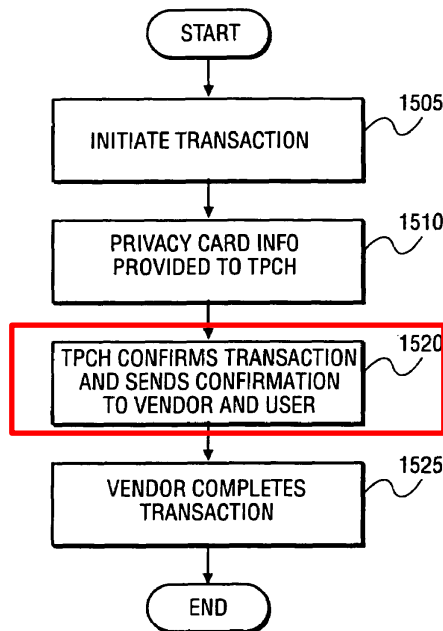


FIG. 15

EX1005, FIG. 15 (annotated). Ludtke explains: “[a]t step 1505, the user initiates the transaction. This transaction may be one over the Internet or through a retail store or bank.” EX1005, 27:4-16. “Privacy card information,” which includes the unique device ID, “is provided to TPOCH, step 1510.” *Id.* “The TPOCH, at step 1520, confirms the transaction and provides the confirmation to the vendor and the user.”

Id. A POSITA would have found it obvious to integrate Ludtke’s “transaction device” into Baird’s “*smartphone*” such that the resulting smartphone device performs the functionality discussed for Ludtke’s device.

e. **Claim 5**

[5pre] “*A smartphone comprising:*”

129. To the extent limiting, Ludtke in view of Baird discloses [5pre] because Ludtke discloses a transaction device which Baird teaches can be integrated into a “*smartphone*.” See [1a], [1b].

[5a] “*a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority, and biometric data,*”

130. Ludtke discloses [5a].

131. As discussed in [1a]-[1b], Ludtke discloses a permanent memory (“*persistent storage*”) of a transaction device “*that receives an identification (ID) code from a third-party trusted authority, and biometric data.*” See [1a], [1b].

Ludtke further discloses that the memory or storage of the transaction device “*having an input*” because Ludtke describes that the device may include, e.g., a “magnetic stripe” or “smart card chip interface” that can be used to input/output information for storage into memory. EX1005, FIG. 7B, 13:18-61. A POSITA would have understood that Ludtke’s “transaction device” could either be pre-installed into Baird’s “*smartphone*” for delivery to a user by the TPCB or could be inserted by the user as a card into the smartphone.

[5b] “wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user,”

132. Ludtke discloses [5b].

133. See analysis for [1c].

[5c] “the ID code uniquely identifying the smartphone among a plurality of smartphones,”

134. Ludtke in view of Baird discloses [5c].

135. See analysis for [1a].

[5d] “the persistent storage storing the biometric data and the ID code,”

136. Ludtke in view of Baird discloses [5d].

137. See analysis for [1b].

[5e] “the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the smartphone”

138. Ludtke in view of Baird discloses [5e].

139. As discussed in [1b] and [5a], Ludtke discloses or teaches “*the persistent storage having an output configured to provide a first set of biometric data and the ID code.*” See [1a], [5a].

140. Ludtke and Baird teach or suggest that biometric data and ID code are “*for use on the smartphone*” because Ludtke describes that its transaction device “carries out a recognition algorithm against the authorized samples that are stored in the user identity block” and the “globally unique silicon ID (GUID) is used to identify the [transaction device] among other existing [transaction

devices],” while Baird teaches that the integrated device can be implemented in a “smart phone.” EX1005, FIGS. 7B, 7C, 14:33-46, 13:39-43, 34:26-28, 29:10-14; EX1006, [0031], [0079]. As discussed in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate Ludtke’s “transaction device” into Baird’s “*smartphone*.”

[5f] “a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage,”

141. Ludtke alone or in view of Baird teaches or suggests [5f].

142. Ludtke suggests a “*validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage*”

because it describes the transaction device may include a “user authentication mechanism” or “user authentication block” that is capable of “**validating** that the user interacting with the device is an authorized user” by prompting the user to “supply a fingerprint recognition sample” and “car[ying] out a recognition algorithm against the authorized samples that are **stored in the user identity block...**” (“*receive the biometric data from the persistent storage*”), where “[i]f a match is found, the user is authorized to access the data and functionality of the device.” EX1005, 5:60-64 (“user authentication mechanism such as a fingerprint recognition or other mechanism may be built directly into the card”), 14:13-46, 16:47-49; *see also* [1d]-[1f]. As a POSITA would have understood, the “transaction device” taught in Ludtke could either be pre-installed into Baird’s

“*smartphone*” for delivery to a user, or could be inserted by the user as a card into the smartphone. EX1015, [0004].

[5g] “*the validation module having a scan pad to capture scan data from a biometric scan,*”

143. Ludtke and Baird each disclose [5g].

144. Ludtke discloses “*the validation module having a scan pad to capture scan data from a biometric scan*” because Ludtke describes that the user authentication block uses a “fingerprint recognition pad” (“*scan pad*”) which allows the block to “*capture*” a fingerprint recognition sample (“*scan data from a biometric scan*”). EX1005, 14:33-46; *see also* [1d]-1[f]. Likewise, Baird discloses a “fingerprint reader” for the user to “prove[] his or her” identity to the device. EX1006, FIG. 3, [0034].

[5h] “*the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; and*”

145. Ludtke discloses [5h].

146. *See* analysis for [1d]-[1f], [5f]-[5g].

[5i] “*a wireless transceiver that, responsive to a determination that the scan data matches the biometric data, sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority,*”

147. Ludtke in view of Baird discloses [5i].

148. *See* analysis for [1g].

149. Additionally, Ludtke teaches or suggests a “*wireless transceiver*” because Ludtke describes that its “transaction device is an interactive device with communications capabilities,” which can both transmit and receive information using, e.g., “wireless or cellular signals.” EX1005, 23:26-28 (“encoded encrypted image . . . is *transmitted* to the POS terminal” from the transaction device), 33:46-48 (“transaction device...can *receive* messages via the TPCCH in a variety of ways, including wireless”).

150. Likewise, Baird also teaches that a “radio or transceiver within the device 104 bi-directionally communicates via an antenna 112 with a radio or transceiver at a base station.” EX1006, [0021]. As discussed in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate Ludtke’s “transaction device” into Baird’s “*smartphone*.”

[5j] “*a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code,*”

151. Ludtke discloses [5j].

152. See analysis for [1h].

[5k] “*wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.*”

153. Ludtke discloses [5k].

154. See analysis for [1i].

g. Claim 6

[6pre] “*The smartphone of claim 5, [6a] wherein the ID code is transmitted to the third-party trusted authority over a network.*”

155. Ludtke in view of Baird discloses [6pre] as discussed for claim 5.

156. Ludtke discloses [6a].

157. Ludtke discloses “*the ID code is transmitted to the third-party trusted authority*” because the “transaction device information” (“*ID code*”) “is provided to the TPC 110” (“*third-party trusted authority*”), which “then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.”

EX1005, 6:41-44; *see also id.*, FIG. 15; 27:9-13.

158. Ludtke further discloses that transmission occurs “*over a network*” because “[t]he TPC 110 may be embodied as a secure server connected to the transaction device in some form of direct connection or alternately a form of indirect connection over the Internet or point of sale networks.” EX1005, 9:30-34. As discussed in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate Ludtke’s “transaction device” into Baird’s “*smartphone.*”

h. Claim 7

[7pre] “*A system, comprising:*”

159. To the extent limiting, Ludtke alone or in view of Baird discloses [7pre].

160. Ludtke discloses “systems” for authorizing biometric access to a transaction device and a third-party trusted authority. EX1005, claim 15-16, FIGS 1-9B.

161. Baird similarly discloses an “apparatus...for authenticating access to a network resource” utilizing biometric authentication. EX1007, (54).

[7a] “a smartphone that persistently stores biometric data and an ID code,”

162. Ludtke in view of Baird discloses [7a].

163. See analysis for [1b], [5a], [5d].

[7b] “wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan data of a legitimate user,”

164. Ludtke discloses [7b].

165. See analysis for [1c], [5b].

[7c] “and the ID code is received from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones,”

166. Ludtke in view of Baird discloses [7c].

167. See analysis for [1a], [5c].

[7d] “the smartphone configured to indicate that a biometric authentication is requested,”

168. Baird discloses [7d].

169. Baird discloses “the smartphone configured to indicate that a biometric authentication is requested” because it describes its device, which can be implemented as a smart phone, as “requiring user authentication,” where the “user

proves his or her identify to the device 104 in various ways using one or more multiple techniques,” including the use of “biometrics input.” EX1006, [0031], [0034], [0079].

[7e] ***“the smartphone configured to wirelessly send the ID code to the third-party trusted authority for authentication responsive to determining that scan data from a biometric scan performed using the smartphone matches the biometric data of the legitimate user,”***

170. Ludtke in view of Baird discloses [7e].

171. See analysis for [1g], [5i].

[7f] ***“wherein a transaction is completed responsive to successful authentication of the ID code by the third-party trusted authority,”***

172. Ludtke in view of Baird discloses [7f].

173. See analysis for [1g], [1h], [5j].

[7g] ***“wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account; and”***

174. Ludtke discloses [7g].

175. See analysis for [1i], [5k].

[7h] ***“the third-party trusted authority operated by a third party,”***

176. Ludtke discloses [7h].

177. See analysis for [1g].

[7i] “the third-party trusted authority storing a plurality of legitimate ID codes and authenticating the ID code received based on a comparison of the ID code received and the legitimate ID codes included in the plurality of the legitimate ID codes.”

178. Ludtke discloses or renders obvious [7i] because it describes that the “single trusted” and “highly secured” TPCCH (“*third-party trusted authority*”) contains a “copy” of “unique transaction device IDs” (“*plurality 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 (“*authenticating the ID code received based on a comparison of the ID code received and the legitimate ID codes included in the plurality of the legitimate ID codes*”). EX1005, FIG. 6, 3:40-43, 4:48-50, 6:36-50, 10:15-18, 28:26-29:23, 30:20-27.

i. Claim 8

[8pre] “The system of claim 7, [8a] wherein the smartphone receives an authentication request, and in response, requests biometric scan from a user to generate the scan data and, when the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code.”

179. Ludtke in view of Baird discloses [8pre] as discussed for claim 7.

180. Ludtke in view of Baird discloses [8a].

181. See analysis for claim 2.

k. Claim 9

[9pre] “*The system of claim 7, [9a] wherein completing the transaction includes accessing an application.*”

182. Ludtke in view of Baird discloses [9pre] as discussed for claim 7.

183. Ludtke discloses or teaches [9a].

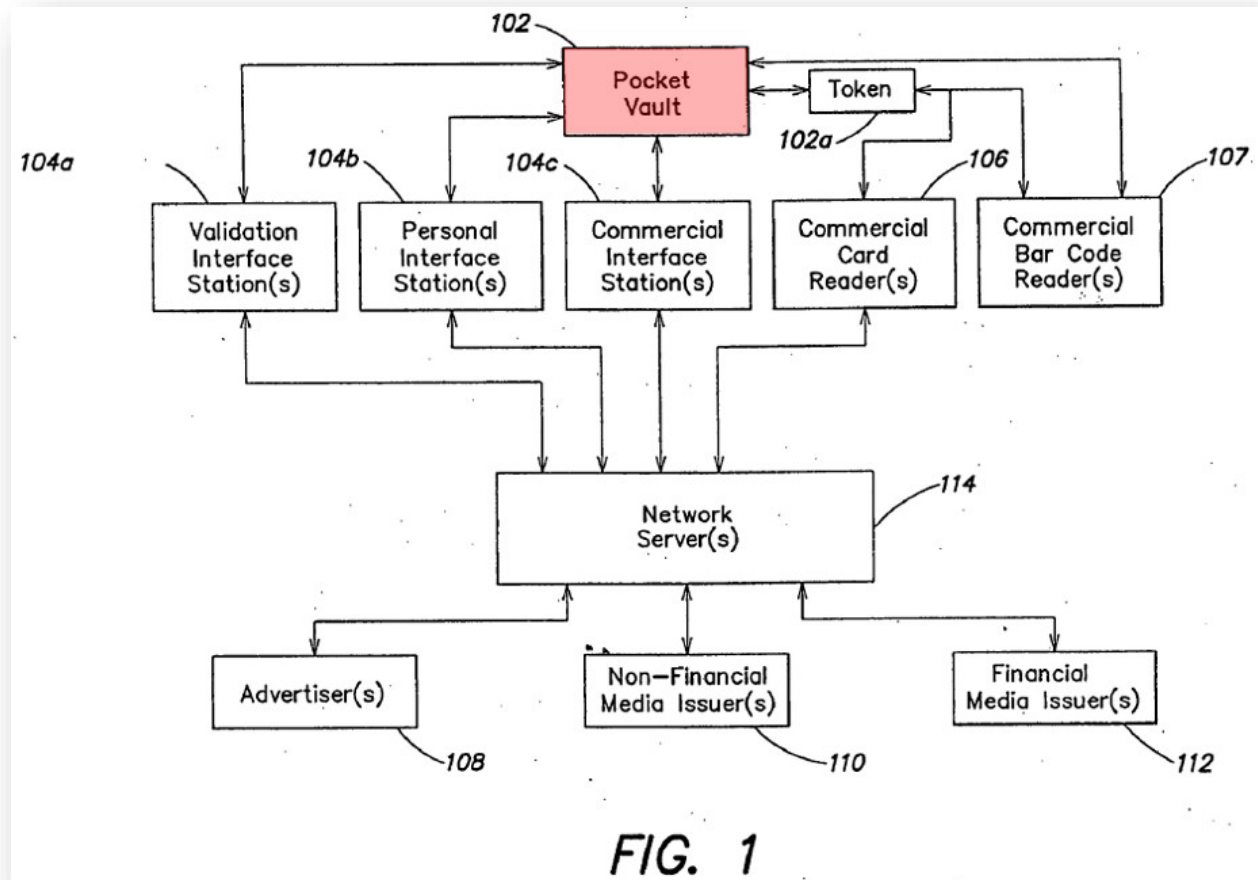
184. *See* analysis for claim 3.

B. Ground 2: Claims 1-9 Are Unpatentable Over Burger and Baird

1. Burger

185. Burger was filed September 30, 2004 and published March 3, 2005. I am informed that Burger qualifies as prior art. Burger discloses a portable electronic authorization device called a “Pocket Vault,” which is “used for producing, distributing, storing, and using the typical contents of a person’s wallet, as well as the multiple, separate transaction authorization devices.” EX1007, [0051], [0093]. Burger’s system enables “individuals to replace nearly all of the paper and plastic contents of their wallets and all of their other transaction authorization implements with a single, hand-held portable electronic authorization device. The system may include the portable electronic authorization devices, removable morphing tokens or cards associated with such devices.” EX1007, [0093]. Beneficially, “the system may eliminate virtually all of the distribution costs and security concerns associated with paper and plastic media.” EX1007, [0093].

186. Burger's Figure 1 shows a system 100 in which the Pocket Vault can be used. EX1007, [0051].

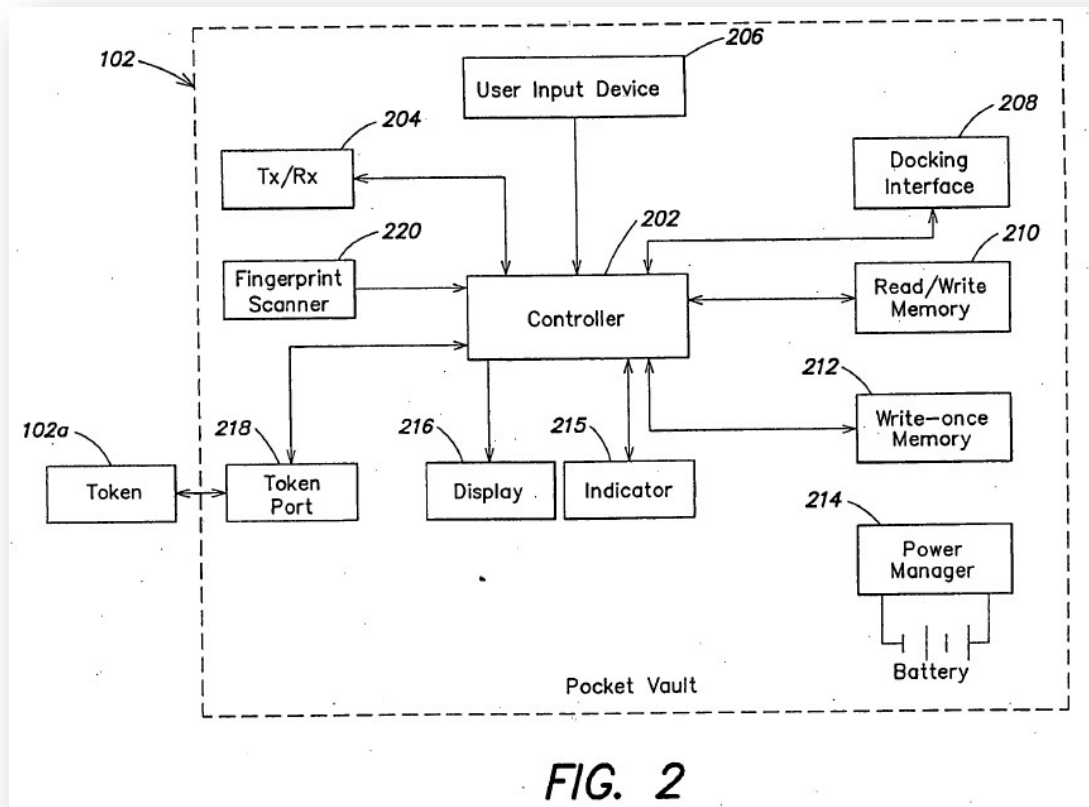


EX1007, FIG. 1 (annotated).

187. As shown in Figure 1, Burger's system 100 includes the Pocket Vault 102, an associated token 102a, network server(s) 114, interface stations 104a-c, commercial card and bar code reader(s) 106, 107, and computers 108, 110, and 112 operated by one or more advertisers, non-financial media issuers, and financial media issuers. EX1007, [0096]-[0097].

188. An example of the Pocket Vault 102 is shown in Figure 2. Pocket Vault 102 includes “a controller 202,...a transceiver 204, a user input device 206, a docking interface 208, a read/write memory 210, a write-once memory 212, a power manager 214, an indicator 215, a display 216, a token port 218, and a fingerprint scanner 220, all coupled to the controller 202.” EX1007, [0118]. Pocket Vault 102 may also “include a hard-wired memory (not shown) to store device serial numbers and key operating system and encryption software components.” EX1007, [0118]. A POSITA would have understood that device serial numbers are generally used to identify a device, and, for a device such as the Pocket Vault, would have included a Pocket Vault ID (chip ID).

189. Memory 210 can include a high-security section used to “store value-based or value-linked media such as debit and credit cards and certain ID information such as driver’s licenses, passports, building security passes, etc.” EX1007, [0129].



EX1007, FIG. 2.

190. The controller 202 includes “a low-power multiprocessor or microcomputer having an on-board SRAM and/or flash memory.” EX1007, [0122]. “The controller 202 may include a software-programmable and encryption-protected or hard-wired unique chip ID. In one embodiment, this chip ID [(Pocket Vault ID)] is released from the Pocket Vault 102 only after the fingerprint scanner 220...has successfully authenticated the identity of the holder.” EX1007, [0122].

191. Pocket Vault 102 also includes a fingerprint scanner 220. EX1007, FIG. 2. The fingerprint scanner 220 can refer to “any device capable of accurately scanning a fingerprint of an individual for comparison with one or more fingerprint images stored in memory.” EX1007, [0135]. “In addition to or in lieu of a fingerprint scanner, other biometric scanning devices may also be employed,” such as “an iris or retina scanner, an optical sensor, and/or a voiceprint.” EX1007, [0135].

192. “[A]uthentication information used to validate the holder’s identity (e.g., the stored fingerprint and/or PIN code) is stored within the to-be-accessed device,” the Pocket Vault, “and the validation is performed in its entirety on-board the same device, such that the user-specific authentication information never leaves the device in which it is stored. Thus, using this technique, the likelihood that such information will be intercepted by unauthorized third parties may be reduced significantly.” EX1007, [0112]. Burger explains that “great care may be taken to ensure that only authorized individuals are permitted to validate Pocket Vaults 102 by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, after it has been confirmed that the holder’s authentication information has been properly stored in the Pocket Vault 102, a trust relationship may be established between the network server 114 and the Pocket Vault 102. This relationship may involve, for example, the registration of a unique

encrypted chip ID of the Pocket Vault 102 with the network server 114 through a secure Internet connection, the distribution of a digital certificate (e.g., a PKI certificate) to the Pocket Vault 102, and the grant of authority to the Pocket Vault 102 to permanently store the Pocket Vault holder's authentication information."

EX1007, [0114]. "Because of the creation of the above-described trust relationships, each Pocket Vault 102 and each interface station 104 may communicate securely with the network server 114." EX1007, [0116].

193. Based on the law as explained to me, it is my opinion that Burger is analogous art to the '905 Patent because it is directed to the same field of endeavor—i.e., user authentication methods and systems for networked communication devices. Even if Burger were not directed to the same field of endeavor (it is), at a minimum it is reasonably pertinent to the problem the inventor of the '989 Patent was trying to solve—namely, "providing systems and methods for authentication responsive to biometric verification of a user being authenticated." *Compare* EX1001, 1:62-64, *with* EX1007, Abstract, [0002], [0007].

2. Motivation to Combine

194. A POSITA would have found it obvious and been motivated to combine the teachings of Burger and Baird with a reasonable expectation of success.

195. Burger discloses verifying a user (a Pocket Vault holder) during authentication of a device (Pocket Vault 102) for use in transactions involving financial and/or non-financial media. EX1007, [0002], [0010], [0113], [0114], [0127]-[0128], [0553]. Burger discloses, e.g., Pocket Vault 102 including “a fingerprint scanner 220” to authenticate the identity of the holder. EX1007, [0122], [0135], FIG. 2. In operation, the Pocket Vault 102 may be interfaced with any of interface stations 104a-c, including a personal interface or docking station 104b, “so as to permit information to be uploaded from the network server 114 to the Pocket Vault 102, or to be downloaded from the Pocket Vault 102 to the network server 114.” EX1007, FIG. 1, [0100], [0102]. “There are many users of home finance software,” which “can be relatively ‘data hungry,’ and commonly require users to download checking and debit card data from their banks (or key it in manually) and to key in the details of credit card and cash purchases.” EX1007, [0102]. “All of this keying and internet file downloading from third parties may be replaced by a simple docking procedure, i.e., when the Pocket Vault 102 is interfaced with the personal docking station....” *Id.* A POSITA looking at this teaching in Burger would have recognized the inconvenience of requiring a personal docking station 104b in order for the user of Pocket Vault 102 to perform these network tasks.

196. Baird provides a technical solution to the problem. Baird teaches integrating a biometric input and transaction device into a smart phone. EX1006, [0031]-[0034], [0079]. Baird further discloses that “users that need to securely gain access to network resources, such as servers, databases, virtual private networks, etc., authenticate...through a single mobile device that is user specific,” such as a “smart phone.” EX1006, [0002]. A POSITA looking at Baird would have recognized that combining Burger’s Pocket Vault with biometric transaction authentication features into a “smartphone” as taught by Baird would be advantageous because it eliminates the need for a separate personal docking station in order to provide network access.

197. A POSITA would have had a reasonable expectation of success combining the teachings of Burger and Baird for several reasons. Both systems contain overlapping features and functionality (authentication, biometrics, display, user input, facilitating secure “transactions”), and use similar hardware, such as fingerprint scanners, display screens, input devices, and persistent memory. *See, e.g.*, EX1007, FIG. 26; EX1006, FIGS. 1, 3. Because of these complementary features and functionality, a POSITA would have recognized that modifying Burger’s system to integrate or incorporate the Pocket Vault on a smart phone for network access, as taught by Baird, required only simple hardware and software modifications and routine skill. For example, both Burger’s Pocket Vault and

Baird's "*smartphone*" include fingerprint scanners, displays, user input, memory, wireless transceivers and controllers, and these overlapping and complementary hardware elements can readily be combined together including adapted firmware/software and modifications well within the ordinary skill in the art.

198. Combining the teachings of Burger and Baird would have involved simply combining prior art elements according to known methods to yield predictable results. *KSR*, 550 U.S. at 415-421.

3. Detailed Analysis

a. Claim 1

[1pre] "*A method comprising:*"

199. To the extent limiting, Burger discloses [1pre] because it discloses systems, methods ("*A method*"), and apparatus for authentication using a Pocket Vault 102. EX1007, [0002], [0010], [0113], [0114], [0127]-[0128], [0553].

[1a] "*receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones;*"

200. Burger in view of Baird discloses [1a].

201. Burger describes that the "controller" on board the Pocket Vault "may include a software-programmable and encryption-protected or hard-wired unique chip ID" ("*identification (ID) code*"). EX1007, [0122]. As a POSITA would understand, this "unique encrypted chip ID," if hard-wired or pre-programmed into the controller, may be registered with a network server 114 ("*third-party trusted*

authority”) to establish a “trust relationship.” EX1007, [0114]. Alternatively, as a POSITA would have understood from the language “software programmable” in view of the disclosure, the “unique encrypted chip ID” (or “Pocket Vault ID”) can be “*received*” by the “smartphone” from the “trusted third party authority” if the chip ID is updated from the trusted third-party authority. EX1007, [0397], [0414]. For example, “information currently stored on a Pocket Vault” can be “updated (e.g., information may be uploaded from the network server 114),” and thus “received” from the third party trusted authority. The chip ID “*uniquely identifies*” the respective Pocket Vault among a plurality of devices. EX1007, [0151] (“list of currently authorized or registered Pocket Vaults 102, identified by chip ID”).

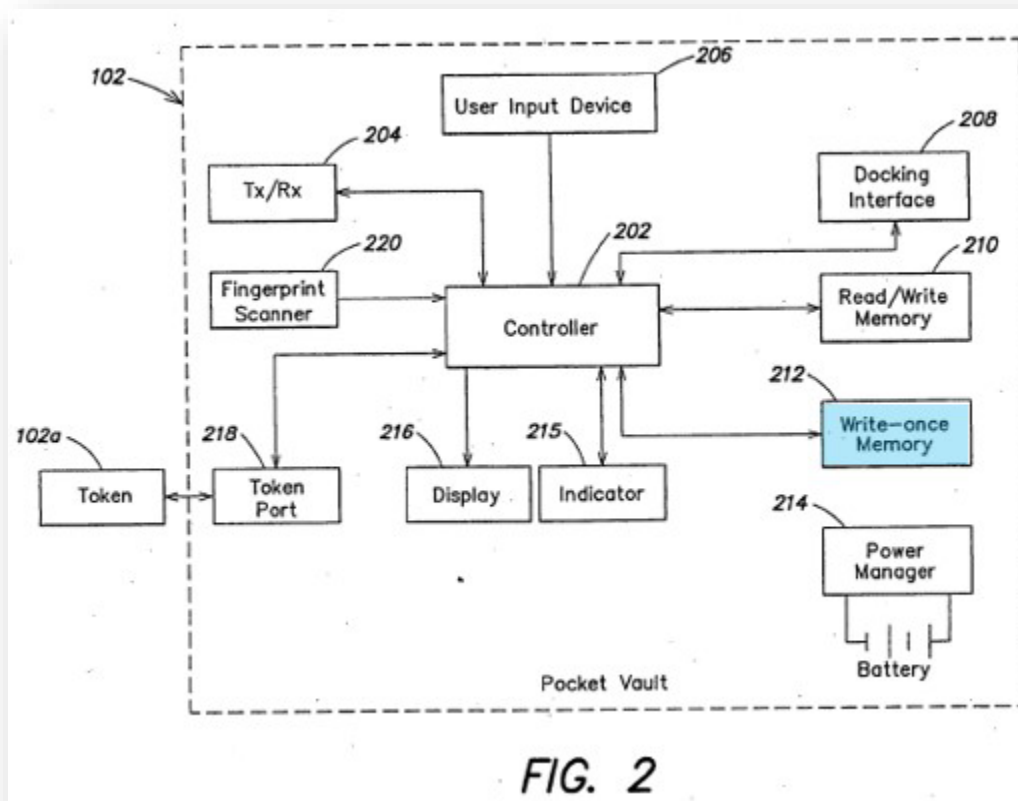
202. Additionally, Baird discloses a “*smartphone*” for conducting transactions, including e-commerce transactions. EX1006, [0031], [0079]. For the reasons discussed above in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate Burger’s “Pocket Vault” into Baird’s “*smartphone*” with biometric authentication. A POSITA would have understood that the combined Pocket Vault / smartphone would have maintained a unique identifier to distinguish that device from other devices.

[1b] “*persistently storing biometric data and the ID code on the smartphone,*”

203. Burger in view of Baird discloses [1b].

204. Burger describes that the Pocket Vault device stores authentication information, such as user fingerprints (“*storing biometric data*”), device serial numbers such as a Pocket Vault ID (“*ID code*”), and “digital certificates.” EX1007, [0112], [0129]. Indeed, Burger teaches that the network server 114 provides the PKI certificate to the Pocket Vault 102 and grants the Pocket Vault 102 authority to permanently store authentication information (“*persistently storing biometric data*”). EX1007, [0114], [0182].

205. A POSITA would have understood that a device serial number and a digital certificate are unique to the device and, thus, would have been used as a device ID to advantageously distinguish that particular device from other devices. Furthermore, Burger’s Pocket Vault includes a “write once memory 212” which “*persistently stores*” data because it permits only a single write operation and stores data in a tamper proof format. EX1007, [0127], [0128], FIG. 2. Thus, a POSITA would have understood that Burger’s Pocket Vault ID number and digital certificate renders obvious “*persistently storing...an ID code.*”



EX1007, FIG. 2.

206. Baird discloses a “*smartphone*” that uses biometric data (*e.g.*, fingerprint scanner) to authenticate a user. EX1007, FIGS. 3, 4; [0031]-[0033]. For the reasons discussed in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate Burger’s “Pocket Vault” device into Baird’s “*smartphone*,” and as such, the resulting combination device would include the unique silicon ID for the “Pocket Vault” / *smartphone* so that the device can be identified when communication with other network resources.

[1c] “wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user”

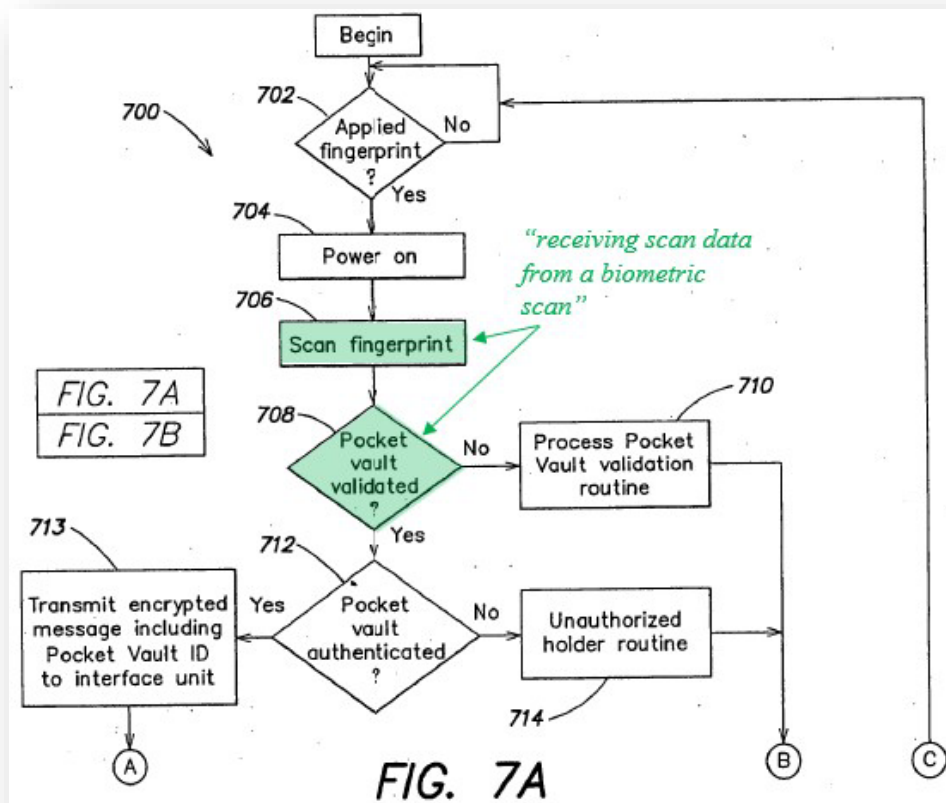
207. Burger discloses [1c].

208. Burger discloses the “*biometric data*” as being at least a “*fingerprint scan.*” EX1007, FIG. 2, [0122] (“fingerprint scanner”).

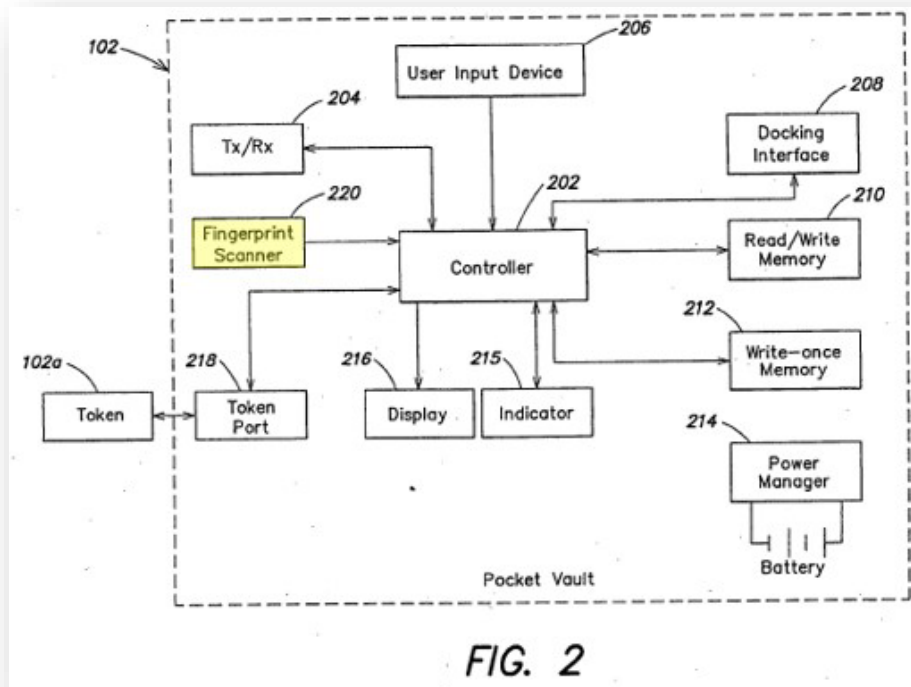
[1d] “receiving, at the smartphone, scan data from a biometric scan using the smartphone;”

209. Burger in view of Baird discloses [1d].

210. Burger discloses “*receiving...scan data from a biometric scan*” because it describes the Pocket Vault 102 receiving biometric scan data (e.g., from a fingerprint scanner 220 or retina scanner) on the handheld device when a user activates the device, as shown in FIGS. 7A and 2. EX1007, [0178]-[0180]. Thus, the Pocket Vault 102 receives biometric scan data e.g., from the fingerprint scanner 220 or retina scanner on the handheld device. EX1007, [0112], [0135], [0178]-[0182].



EX1007, FIG. 7A (annotated).



EX1007, FIG. 2 (annotated).

211. For the reasons discussed in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate Burger’s “Pocket Vault” device into Baird’s “*smartphone*.”

[1e] “*comparing, using the smartphone, the scan data to the biometric data;*”

212. Burger in view of Baird discloses [1e].

213. Burger discloses “*comparing...the scan data to the biometric data*” because it discloses that after receiving the user’s biometric scan data (e.g., fingerprints), the Pocket Vault device compares the scanned data to biometric data (e.g., fingerprints) stored in the write-once memory 212 to determine if there is a match. EX1007, [0182]-[0184], FIGS. 7A, 2.

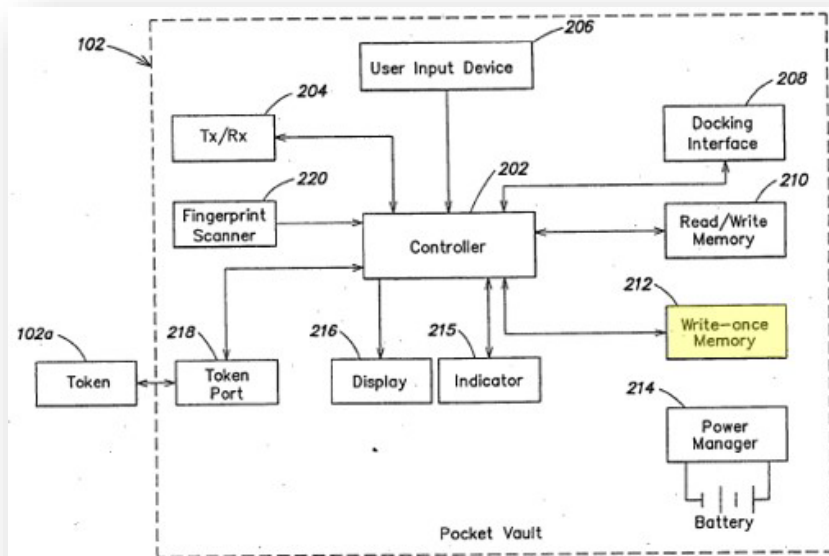
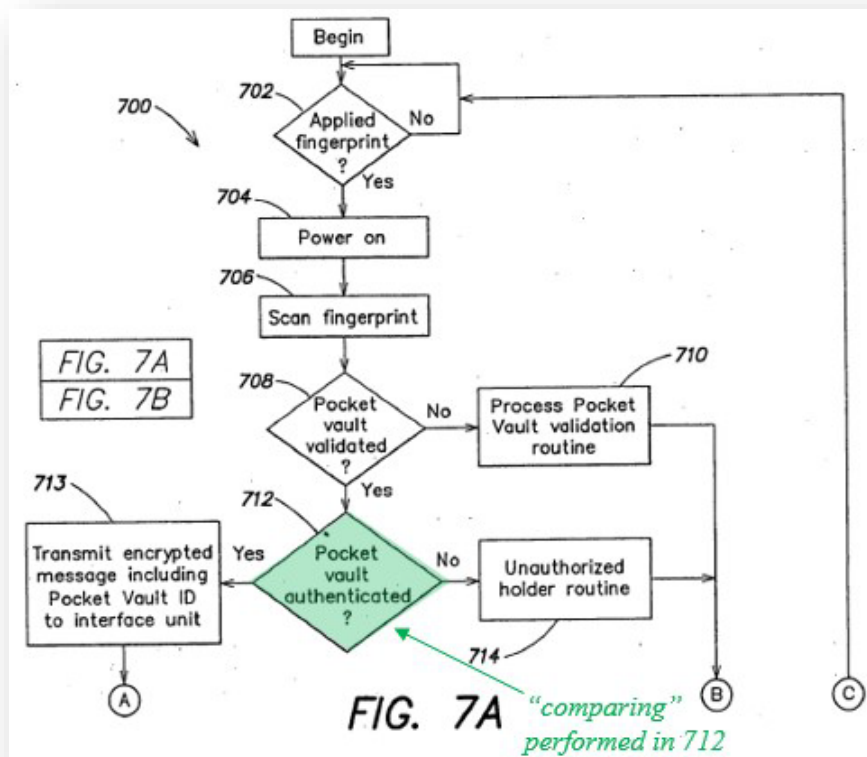


FIG. 2

EX1007, FIG. 2 (annotated).



EX1007, FIG. 7A (annotated).

214. For the reasons discussed in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate Burger’s “Pocket Vault” into Baird’s “*smartphone*.”

[1f] “*determining whether the scan data matches the biometric data; and*”

215. Burger discloses [1f].

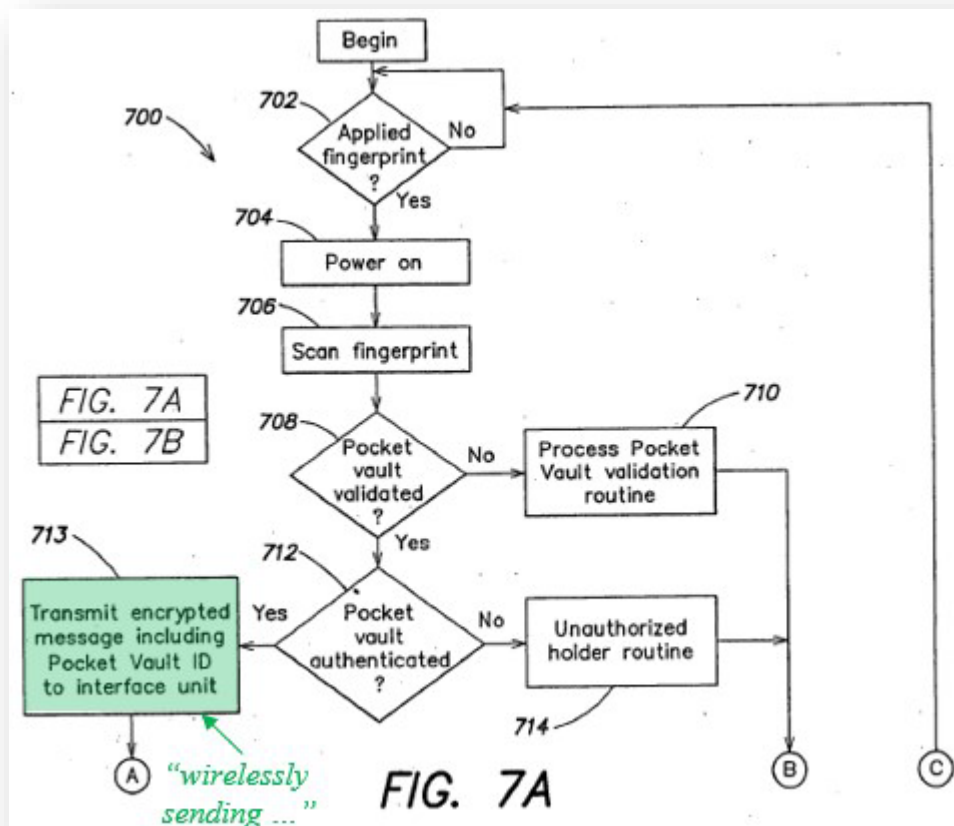
216. Burger discloses “*determining whether the scan data matches the biometric data*” because it discloses that after receiving the scan data from the biometric scan, the user’s scanned data (e.g., fingerprints) are compared to

biometric data (e.g., fingerprints) stored in the write-once memory 212 to determine if there is a match. EX1007, [0182]-[0184], FIGS. 7A, 2.

[1g] “responsive to a determination that the scan data matches the biometric data, wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority,”

217. Burger in view of Baird discloses [1g].

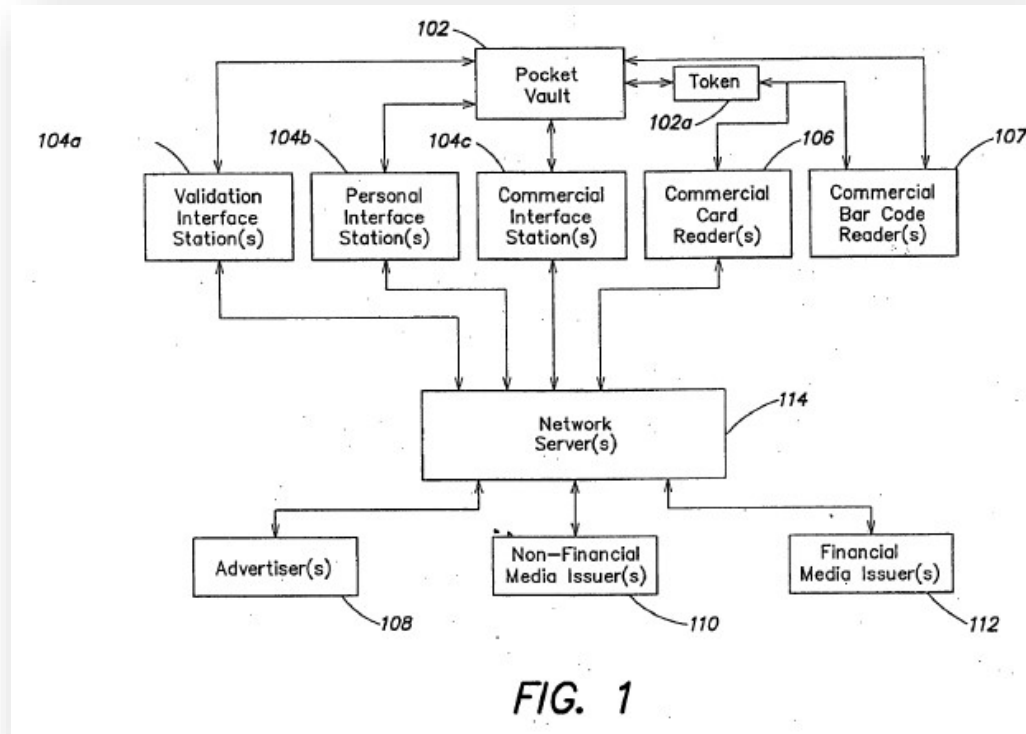
218. Burger discloses “*determination that the scan data matches the biometric data,*” because as shown in Figure 7A (step 712), Burger discloses “it is determined whether Pocket Vault 102 has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches one of the fingerprints stored in the fingerprint memory 212.” EX1007, [0183]-[0184], [0209]-[0210]. And “*responsive*” to such determination, the Pocket Vault wirelessly sends (step 713) an encrypted message including the unique Pocket Vault chip ID (“*wirelessly sending...the ID code*”). EX1007, [0186], [0114], [0122], [0146], FIG. 7A.



EX1007, FIG. 7A (annotated).

219. Burger teaches that authentication information, such as the encrypted message including the unique Pocket Vault chip ID, are transmitted to the network server 114. EX1007, [0113]-[0114]. Communication between the various network elements, e.g., between the Pocket Vault 102, interface stations 104a-c, and network server 114 can be “wireless,” and the Pocket Vault 102 can communicate directly with the network server 114. EX1007, [0099] (“[t]he connections between most of the network devices may be...*wireless*”); [0101] (“a *wireless* network such

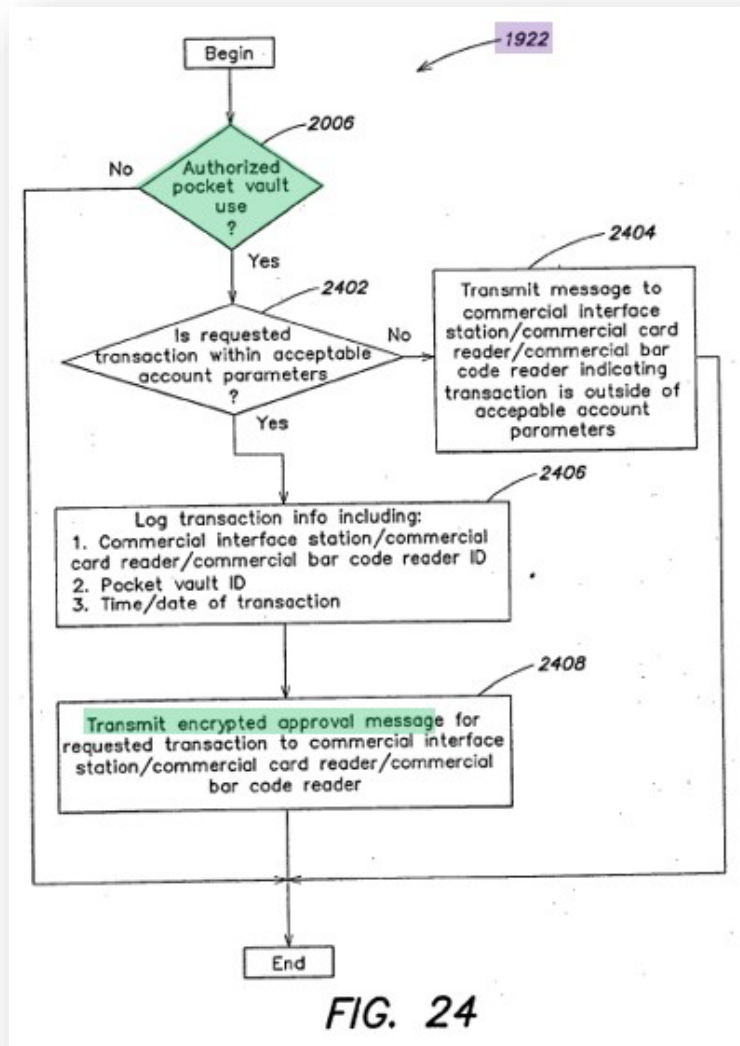
as Bluetooth may be employed to permit communication between devices on the network system”), [0097], [0123], FIG. 1.



EX1007, FIG. 1.

220. Moreover, when a user is interested in a financial transaction, the network server 114 determines whether the Pocket Vault 102 is authorized to be used, e.g., by checking whether the transmitted Pocket Vault ID matches a stored ID from among the previously registered IDs in the network server 114, and then transmits an approval message for the transaction (“*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*”).

EX1007, FIGS. 19 (steps 1920, 1922), 24 (steps 2006, 2406, 2408), 25 (steps 2502-2506), [0511]-[0529], [0182], [0145]-[0146].



EX1007, FIG. 24 (annotated).

221. For the reasons discussed in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate Burger’s “Pocket Vault” into

Baird’s “*smartphone*,” such that the resulting smartphone device performs the functionality discussed for Burger’s “Pocket Vault.”

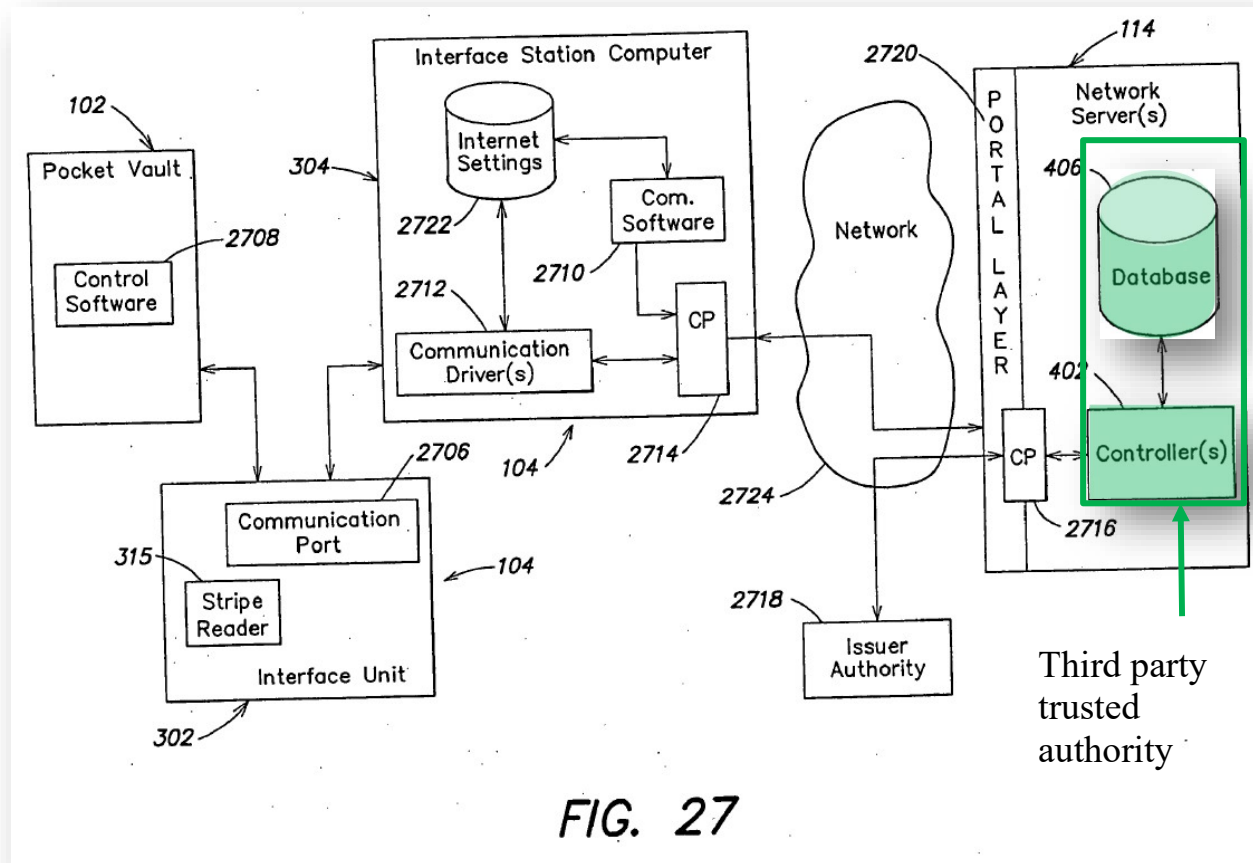
“third-party trusted authority”

222. The Board previously construed “‘third-party trusted authority’ as a trusted authority that is an entity separate from the parties to a transaction.”

EX1008, 11. Consistent with this construction, the network server 114 includes a controller 402 and database 406 that collectively are “*a third-party trusted authority*.” EX1007, [0146], [0531]-[0543], FIG. 27. The database 406 stores a list of current Pocket Vault holders, a list of currently authorized or registered Pocket Vaults 102, identified by chip ID and linked to the holder list; a list of currently authorized or registered tokens 102a, identified by chip ID and linked to the holder list (“*one or more previously registered ID codes maintained by the third-party trusted authority*”). EX1007, [0146], FIG. 4. Burger explains that “***a trust relationship*** may be established between the network server 114 and the Pocket Vault 102. This relationship may involve, for example, the registration of a unique encrypted chip ID of the Pocket Vault 102 with the network server 114 through a secure Internet connection, the distribution of a digital certificate (e.g., a PKI certificate) to the Pocket Vault 102, and the grant of authority to the Pocket Vault 102 to permanently store the Pocket Vault holder’s authentication information.” EX1007, [0114]. “Because of the creation of the above-described

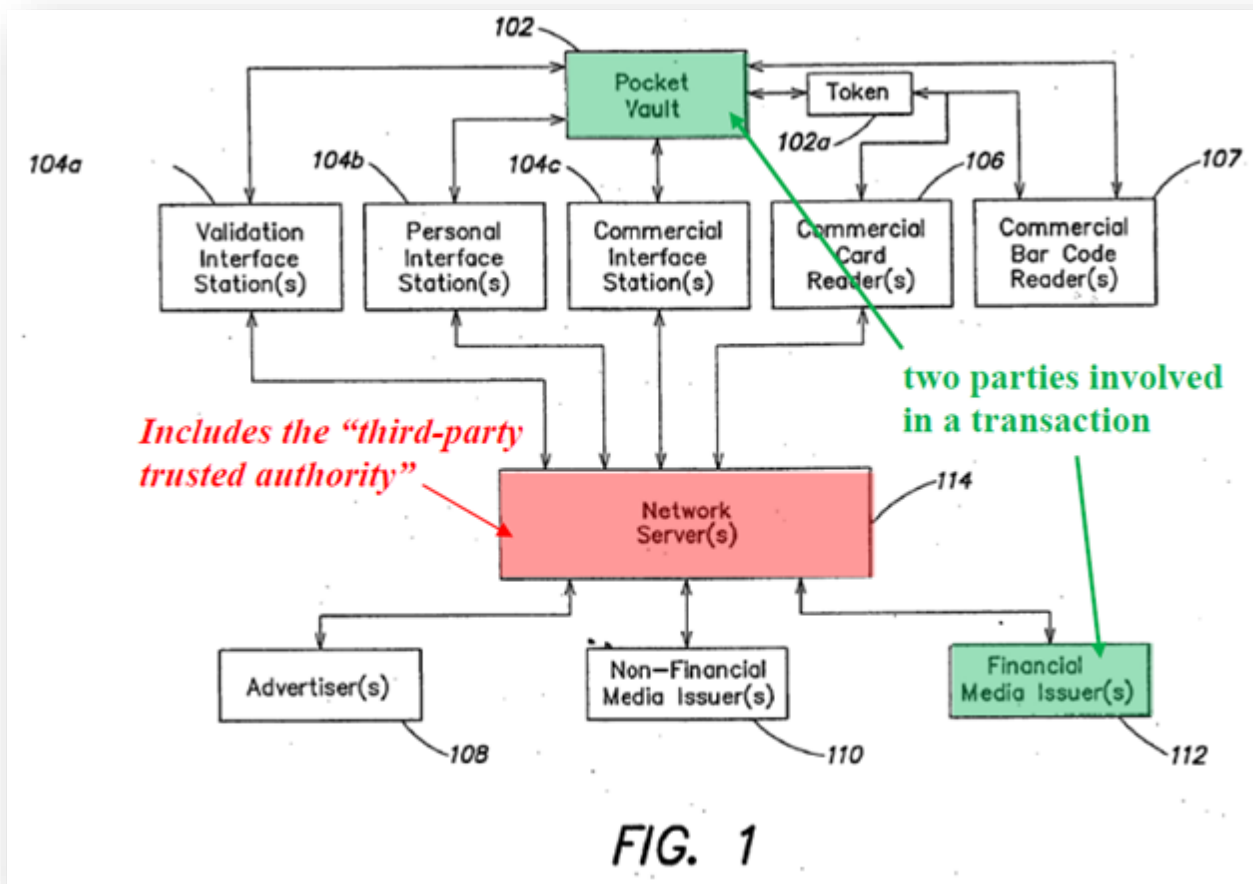
trust relationships, each Pocket Vault 102 and each interface station 104 may *communicate securely with the network server 114*, as well as with any other networked devices or sites that *require a high level of trust*.” EX1007, [0116].

223. Accordingly, it would have been obvious to a POSITA that the controller 402 and database 406 of the network server 114 can operate as “*a third-party trusted authority*” in a transaction between the Pocket Vault or Pocket Vault holder/user (e.g., *first party*) and a retailer (e.g., *second party*). EX1007, FIGS. 19, 24, 25, [0095], [0319]-[0320], [0474], [0511]-[0513], [0158].



EX1007, FIG. 27 (annotated).

224. In another example, the controller 402 and database 406 of the network server 114 may be “*a third-party trusted authority*” when there is a transaction between a Pocket Vault or Pocket Vault holder (e.g., *first party*) and an entity such as a financial media issuer 112 (e.g., *second party*). Thus, the Pocket Vault holder can obtain necessary payment information to make a payment to the retailer, and the financial media issuer can provide credit card or bank account information and charge the Pocket Vault holder’s account based on the payment amount.



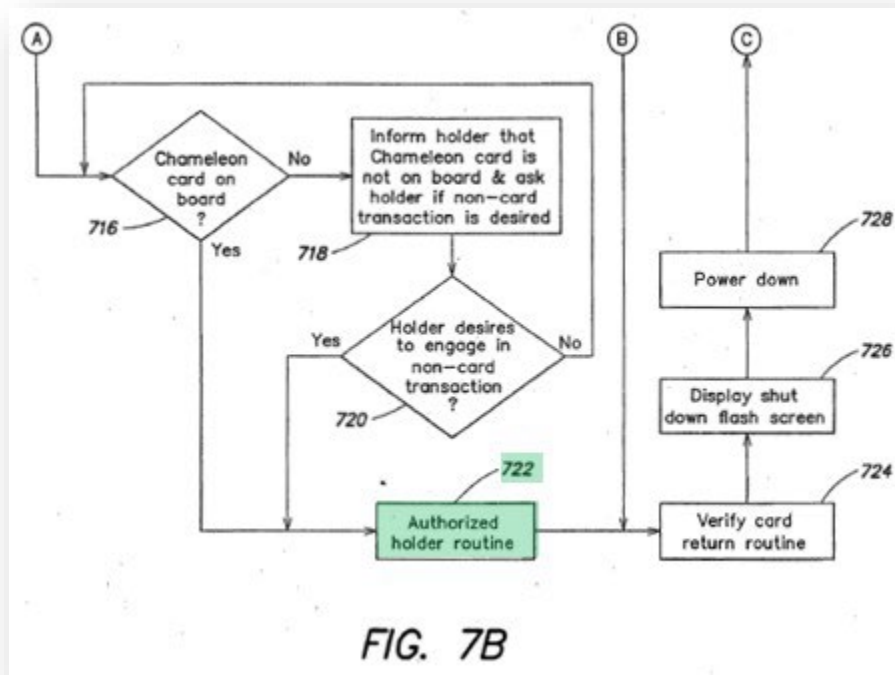
EX1007, FIG. 1 (annotated).

[1h] “a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code,”

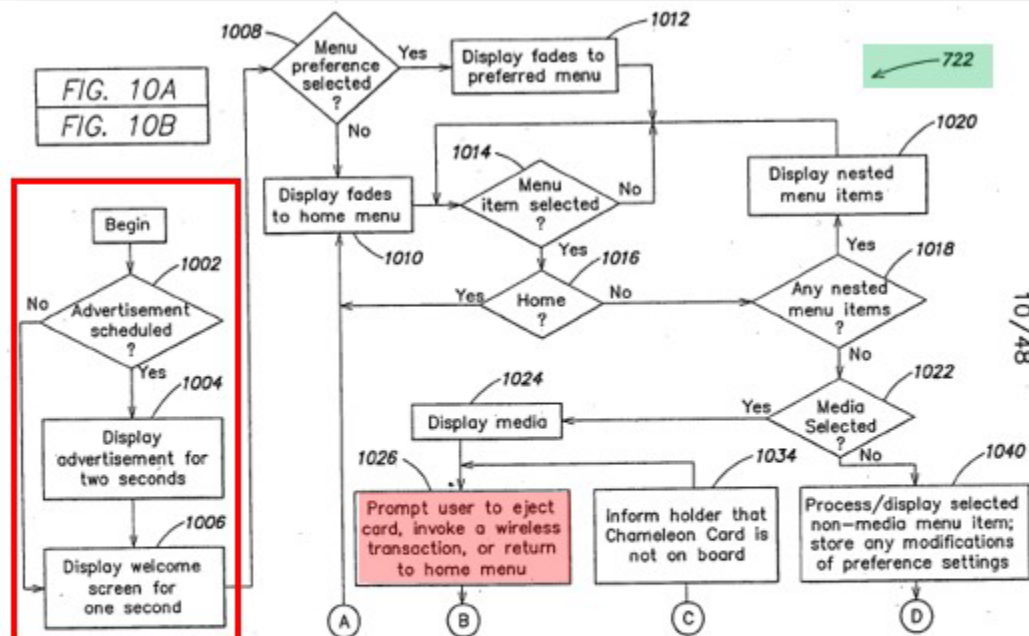
225. Burger discloses [1h] because, it describes, e.g., that after the network server 114 authenticates the Pocket Vault ID, the user is granted access to the Pocket Vault 102 and can then select a transaction from a displayed menu.

EX1007, FIGS. 7B, 10A, 19, [0320], [0189], [0095]-[0096], [0125], [0236]-[0238], [0155]-[0158]. Ultimately, the Pocket Vault 102 or associated token 102a displays credit card information to be used by a retailer and “may be used by the

Pocket Vault holder to engage in a transaction.” EX1007, [0095], [0103], [0155]-[0158], [0320]. Thus, in this manner, it would have been obvious to a POSITA that Burger discloses “a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code.” see also EX1007, FIGS. 7B, 10A, 25, 26H-K.

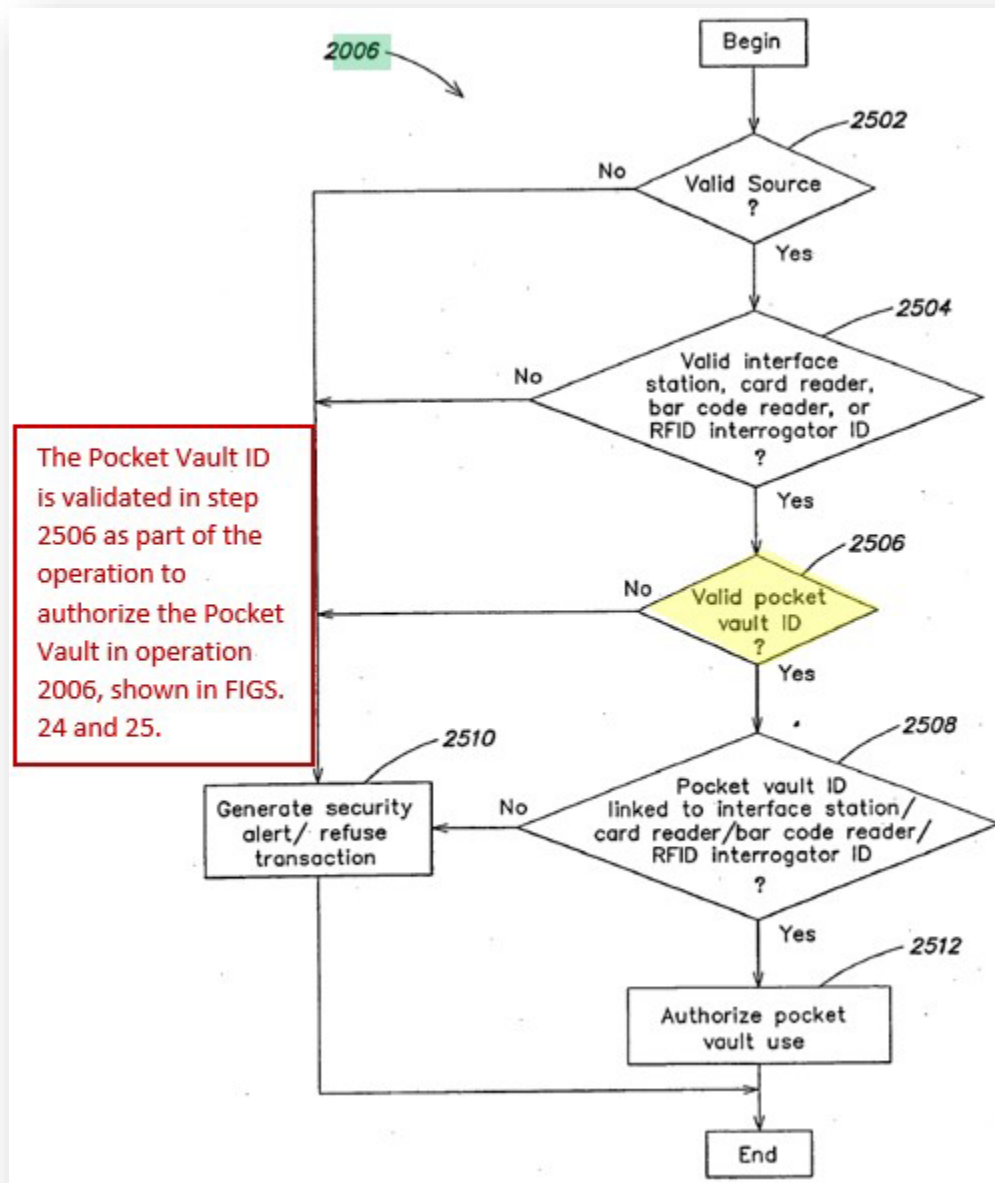


EX1007, FIG. 7B (annotated).



As part of the Authorized Holder Routine 722 in FIG. 7B, an advertisement is displayed and subsequently a user can select a wireless transaction to be conducted.

EX1007, FIG. 10A (annotated).



EX1007, FIG. 25 (annotated).

[1i] *“wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.”*

226. Burger discloses [1i].

227. Burger discloses that the Pocket Vault can be used for accessing a “financial account” or “web site.” EX1007, [0550] (Pocket Vault contains information regarding the “financial transactions engaged in”), [0679] (describing transaction of “securing a room” over a hotel’s “web site”).

b. Claim 2

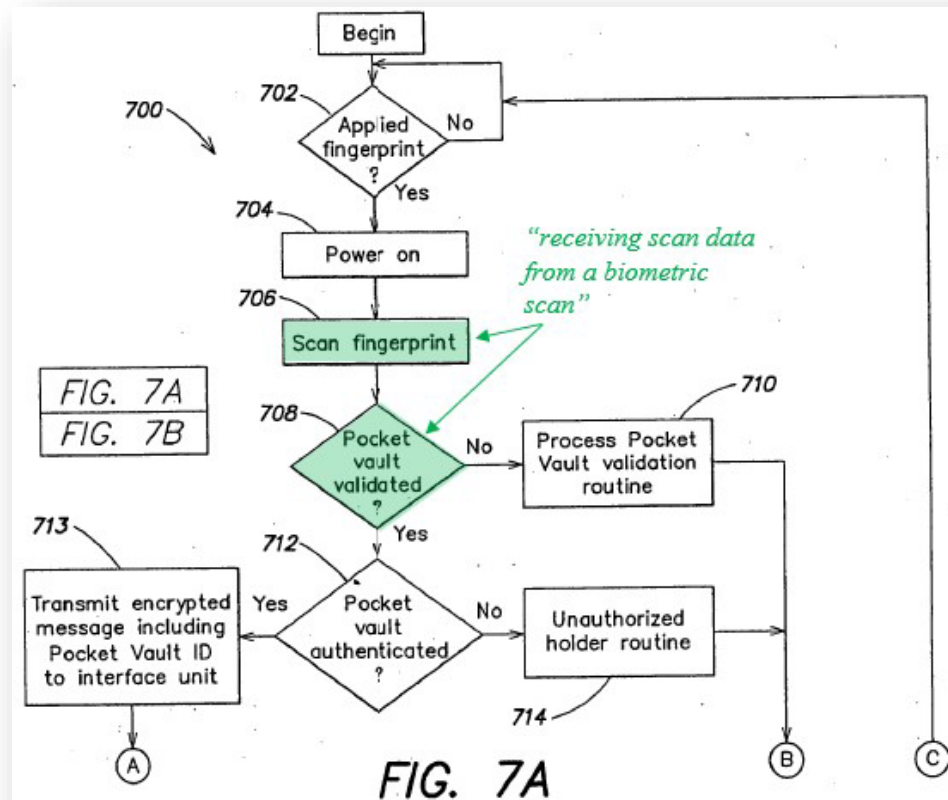
[2pre] “The method of claim 1, further comprising: [2a] receiving a request for biometric verification, and responsive to a determination that the scan data does not match the biometric data, indicating the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code.”

228. Burger in view of Baird discloses [2pre] as discussed for claim 1.

229. Burger in view of Baird discloses [2a].

230. As depicted in Burger’s FIGS. 7A and 2, a user activates the Pocket Vault by “a physical action” such as applying a fingerprint. EX1007, [0178]-[0180]. In response, the Pocket Vault’s “fingerprint scanner 220 scan[s] the applied fingerprint.” EX1007, [0181]. A POSITA would have understood that the receiving of activation data (e.g., indicating that the physical action . . . or application of the finger on the scanner 220 has occurred) corresponds to “receiving a request for a biometric verification” because a biometric verification is performed “with each attempted use of any of these devices.” EX1007, [0112].

231. As shown in FIG. 7, if authentication at step 712 is successful, Burger's system (at step 713) will "transmit encrypted message including Pocket Vault ID to interface unit." EX1007, FIG. 7A, [0186].



EX1007, FIG. 7A (annotated).

232. Otherwise, if the user is not authenticated by fingerprint matching (i.e. no match exists) at step 712 (*"a determination that the scan data does not match the biometric data, indicating the [device] cannot verify the scan data as being from the legitimate user"*), as a POSITA would have understood, the Pocket Vault **does not send its ID** to the interface unit (*"does not send the ID code"*) and the

device performs an “Unauthorized holder routine” at step 714. *See* [1g]; EX1007, FIG. 9, [0112], [0135], [0182]-[0185], [0218]-[0224].

233. As discussed in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate Burger’s “Pocket Vault” into Baird’s “*smartphone*,” such that the resulting smartphone device performs the functionality discussed for Burger’s “Pocket Vault.”

c. Claim 3

[3pre] “*The method of claim 1, [3a] wherein completing the transaction includes accessing an application.*”

234. Burger in view of Baird teaches [3pre] as discussed for claim 1.

235. Burger discloses, e.g. that the “network server 114” accessed by the Pocket Vault “stores both data *and applications that are accessible to users*” and “may serve a website, i.e., a collection of web pages and data that are available to users via a browser.” EX1007, FIG. 1, [0539]. Baird describes that access to applications can be restricted. EX1006, [0088]. Based on this disclosure, a POSITA would have understood that with the integration of Burger’s “Pocket Vault” into Baird’s “smartphone,” where access to applications is restricted, “*completing the transaction includes accessing an application.*”

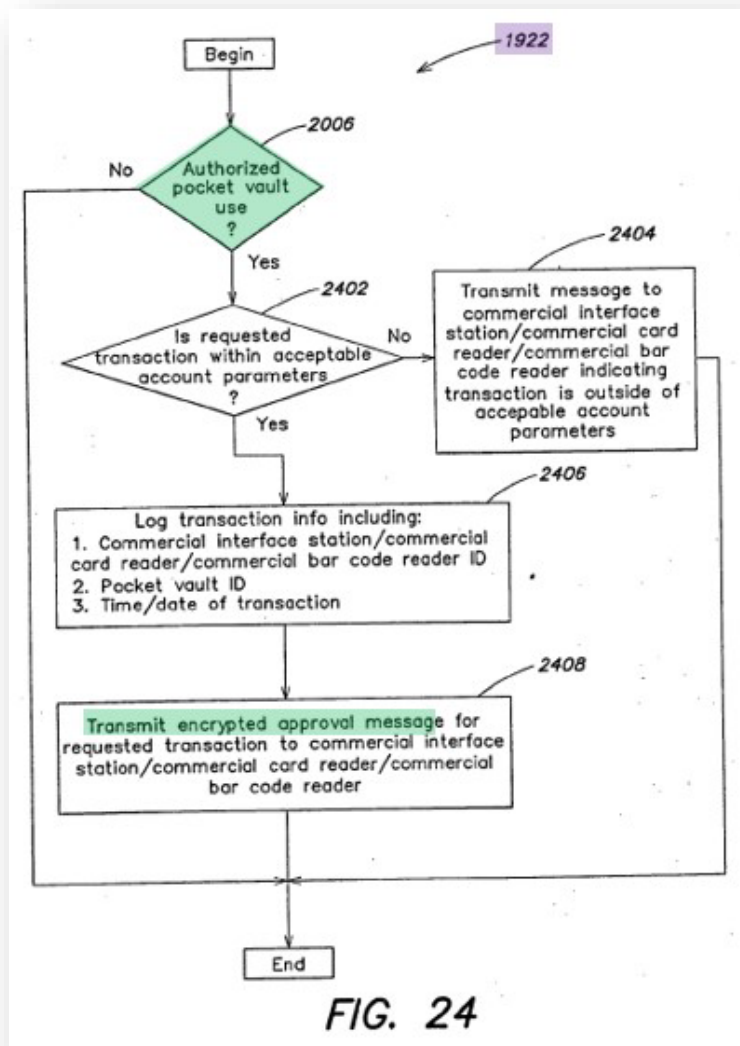
d. Claim 4

[4pre] *“The method of claim 1, [4a] wherein the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code includes the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party.”*

236. Burger in view of Baird discloses [4pre] as discussed for claim 1.

237. Burger discloses [4a].

238. Burger discloses that the network server (“*third-party trusted authority*”) authorizing a transaction may employ a routine to implement “process[ing] request to authorize transaction” as shown in FIG. 24:



EX1007, FIG. 24 (annotated). As shown, the network server (“*third-party trusted authority*”) transmits an “encrypted approval message” to “the entity with which the transaction is being attempted” (i.e., the counterparty to the transaction, which is “*another party*”). EX1007, [0518]. For the reasons discussed in the “Motivation to Combine” section, a POSITA would have found it obvious to integrate Burger’s “Pocket Vault” into Baird’s “*smartphone*.”

e. **Claim 5**

[5pre] “*A smartphone comprising:*”

239. To the extent limiting, Burger in view of Baird discloses [5pre]. See [1a], [1b].

[5a] “*a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority, and biometric data,*”

240. Burger discloses [5a].

241. See analysis for [1a]-[1b].

[5b] “*wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user,*”

242. Burger discloses [5b].

243. See analysis for [1c].

[5c] “*the ID code uniquely identifying the smartphone among a plurality of smartphones,*”

244. Burger in view of Baird discloses [5c].

245. See analysis for [1a].

[5d] “*the persistent storage storing the biometric data and the ID code,*”

246. Burger in view of Baird discloses [5d].

247. See analysis for [1b].

[5e] “*the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the smartphone;*”

248. Burger in view of Baird discloses [5e].

249. See analysis for [1b].

[5f] “a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage,”

250. Burger alone or in view of Baird teaches or suggests [5f].

251. Burger discloses or suggests the claimed “*validation module*” because it describes, e.g., that its Pocket Vault includes the capability such that “authentication information used to validate the holder’s identity (e.g., the stored fingerprint and/or PIN code) is stored within the to-be-accessed device, and the validation is performed in its entirety on-board the same device” EX1007, [0112], [0135]; *see also* [1d]-[1f]. A POSITA would have found it obvious to integrate Burger’s “Pocket Vault” into Baird’s “*smartphone*.”

[5g] “the validation module having a scan pad to capture scan data from a biometric scan,”

252. Burger discloses [5g].

253. Burger discloses a “*scan pad*” in that it describes a “fingerprint scanner 220” that is “capable of accurately scanning a fingerprint.” EX1007, [0118], [0135]; *see also* [1d]-[1e].

[5h] “the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; and”

254. Burger discloses [5h].

255. *See* analysis for [1d]-[1e], [5f]-[5g].

[5i] “a wireless transceiver that, responsive to a determination that the scan data matches the biometric data, sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority,”

256. Burger in view of Baird discloses [5i].

257. See analysis for [1g].

[5j] “a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code,”

258. Burger discloses [5j].

259. See analysis for [1h].

[5k] “wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.”

260. Burger discloses [5k].

261. See analysis for [1i].

f. Claim 6

[6pre] “The smartphone of claim 5, [6a] wherein the ID code is transmitted to the third-party trusted authority over a network.”

262. Burger in view of Baird discloses [6pre] as discussed for claim 5.

263. Burger discloses [6a].

264. Burger discloses this limitation because it describes the Pocket Vault ID (“ID code”) being transmitted to the network server over a network. EX1007, FIGS. 1, 2-3 (“Tx/Rx”), 7A, [0208], [0345], [0414].

g. Claim 7

[7pre] “A system, comprising:”

265. To the extent it is limiting, Burger alone or in view of Baird discloses [7pre]. EX1007, FIGS. 1, 2.

[7a] “a smartphone that persistently stores biometric data and an ID code,”

266. Burger in view of Baird discloses [7a].

267. See analysis for [1b], [5a], [5d].

[7b] “wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan data of a legitimate user,”

268. Burger discloses [7b].

269. See analysis for [1c], [5b].

[7c] “and the ID code is received from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones,”

270. Burger in view of Baird discloses [7c].

271. See analysis for [1a], [5c].

[7d] “the smartphone configured to indicate that a biometric authentication is requested,”

272. Baird discloses [7d].

273. See analysis for [1d], [5e].

[7e] “the smartphone configured to wirelessly send the ID code to the third-party trusted authority for authentication responsive to determining that scan data from a biometric scan performed using the smartphone matches the biometric data of the legitimate user,”

274. Burger in view of Baird discloses [7e].

275. See analysis for [1g], [5i].

[7f] “wherein a transaction is completed responsive to successful authentication of the ID code by the third-party trusted authority,”

276. Burger in view of Baird discloses [7f].

277. See analysis for [1g], [1h], [5j].

[7g] “wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account; and”

278. Burger discloses [7g].

279. See analysis for [1i], [5k].

[7h] “the third-party trusted authority operated by a third party,”

280. Burger discloses [7h].

281. See analysis for [1g].

[7i] “the third-party trusted authority storing a plurality of legitimate ID codes and authenticating the ID code received based on a comparison of the ID code received and the legitimate ID codes included in the plurality of the legitimate ID codes.”

282. Burger discloses [7i].

283. Burger discloses that the network server may contain databases and/or a registry of Pocket Vault IDs and/or digital certificates for identifying a particular Pocket Vault, among a plurality of “*legitimate ID codes*.” EX1007, FIG. 1, [0111]-[0116], [0144]-[0146], [0481].

h. Claim 8

[8pre] “The system of claim 7, [8a] wherein the smartphone receives an authentication request, and in response, requests biometric scan from a user to generate the scan data and, when the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code.”

284. Burger in view of Baird discloses [8pre] as discussed for claim 7.

285. Burger in view of Baird discloses [8a].

286. See analysis for claim 2.

i. Claim 9

[9pre] “The system of claim 7, [9a] wherein completing the transaction includes accessing an application.”

287. Burger in view of Baird discloses [9pre] as discussed for claim 7.

288. Burger discloses [9a].

289. See analysis for claim 3.

Conclusion and Declaration

The findings and opinions set forth in this declaration are based on my work and examinations to date. I may continue my examinations. I may also receive additional documentation and other factual evidence over the course of this proceeding that will allow me to supplement and/or refine my opinions. I reserve the right to add to, alter, or delete my opinions and my declaration upon discovery of any additional information. I reserve the right to make such changes as may be deemed necessary. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board (“PTAB” or “Board”) of the USPTO. I also recognize that I may be subject to cross-examination in the 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.

I declare that all statements made herein on my own knowledge are true and that all statements made on information and belief are believed to be true, and further, 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.

Dated: March 6, 2025

By:



Stephen Gray