IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Giobbi	
U.S. Patent No.: 9,298,905	Examiner: To Be Assigned
Issued: March 29, 2016	Art Unit: To Be Assigned
Application No.: 14/521,982	
Filed: October 23, 2014	
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION	**REQUEST FOR *EX PARTE* REEXAMINATION UNDER 37 C.F.R. § 1.510**

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Pursuant to 35 U.S.C. § 302 and 37 C.F.R. §§ 1.510 et seq., Samsung Electronics America, Inc. ("Samsung" or "Requestor") requests *ex parte* reexamination of claims 1-18 (the "Challenged Claims") of U.S. Patent No. 9,298,905 ("the '905 patent," Exhibit 1001), entitled "Biometric Personal Data Key (PDK) Authentication." The '905 patent issued on March 29, 2016, from Application No. 14/521,982, which was filed on October 23, 2014.

Patent Owner has asserted the '905 patent against Samsung and Samsung's parent, Samsung Electronics Co., Ltd., in *Proxense, LLC v. Samsung Electronics Co., Ltd., et. al.*, Case No. 6:21-CV-00210-ADA (W.D. Tex.). Because the '905 patent is involved in concurrent litigation, the Patent Office should accord the requested reexamination "priority over all other cases." MPEP § 2261.

TABLE OF CONTENTS

Page

I. INTRODUCTION 19

II. REQUIREMENTS FOR *EX PARTE* REEXAMINATION UNDER 37 C.F.R. § 1.510 20

A. Payment of Fees – 37 C.F.R. § 1.510(a) 20

B. Statement Pointing Out Each Substantial New Question of Patentability Based on Prior Art Patents and Printed Publications – 37 C.F.R. § 1.510(b)(1) 21

C. Identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited prior art – 37 C.F.R. § 1.510(b)(2) 21

D. Copies of the Cited Prior Art Presented- 37 C.F.R. § 1.510(b)(3) 22

E. Copy of the Patent for Which Reexamination Is Requested- 37 C.F.R. § 1.510(b)(4) 22

F. Certification of Service on the Patent Owner- 37 C.F.R. § 1.510(b)(5) 22

G. Certification of Statutory Estoppel Provisions - 37 C.F.R. § 1.510(b)(6) 23

III. PROCEDURAL HISTORY 23

A. Prosecution History of the '905 Patent 24

B. The IPR filed against the '905 Patent 25

IV. THIS REQUEST SHOULD NOT BE DENIED BASED ON DISCRETIONARY ISSUES 25

V. LEVEL OF SKILL IN THE ART 28

VI. CLAIM CONSTRUCTION 29

A. "third party trusted authority" (claim 1) 30

VII. PRIORITY DATE OF THE '905 PATENT 31

VIII. OVERVIEW OF THE TECHNOLOGY 32

IX. OVERVIEW OF THE PRIOR ART 33

A. Ludtke (Ex. 1005) 33
B. Okereke (Ex. 1006) 35
C. Robinson (Ex. 1007) 36
D. Scott (Ex. 1008) 37
1. A POSITA Would Have Been Motivated to Combine the Teachings of the Ludtke, Okereke, and Robinson 38
2. A POSITA Would Have Been Motivated to Combine the Teachings of Ludtke, Scott, and Robinson 38
X. DETAILED EXPLANATION OF THE PROPOSED REJECTIONS 39
A. SNQ 1: Ludtke in combination with Okereke Renders Claims 1, 3-10, and 12-18 Obvious 40
1. The Proposed Combination 40
(a) The Prior Art Discloses the Claim Limitations 40
(b) A POSITA Would be Motivated to Combine Ludtke and Okereke 42
2. Claim 1 46
(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device" 46
(b) [1b] "responsive to receiving a request for biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;" 49
(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;" 52
(d) [1d] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and 54

(e) [1e] "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction." 58

3. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code." 60

4. Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition." 60

5. Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob." 60

6. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application." 61

7. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account." 61

8. Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data." 62

9. Claim 9: 63

(a) [9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;" 63

(b) [9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and" 63

(c) [9c] "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third - party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction." 63

10. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network." 64

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob." 64

12. Claim 13: 65

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating

that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and" 65

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes." 65

13. Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code."....66

14. Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob." 68

15. Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition." 68

16. Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account." 68

17. Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application." 68

B. SNQ 2: Ludtke in combination with Okereke and Robinson Renders Claims 2 and 11 Obvious 68

1. The Proposed Combination....68
(a) The Prior Art Discloses the Claim Limitations....68
(b) A POSITA Would have been Motivated to Combine Robinson with Ludtke and Okereke....69
2. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the ID code."....70
3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the ID code....71
C. SNQ 3: Ludtke in combination with Scott Renders Claims 1, 3-10, and 12-18 Obvious....71
1. The Proposed Combination....71
(a) The Prior Art Discloses the Claim Limitations....71
(b) A POSITA Would be Motivated to Combine Ludtke and Scott....74
2. Claim 1....79
(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device"....79
(b) [1b] "responsive to receiving a request for biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;"....81
(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;"....82
(d) [1d] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and....82

(e) [1e] "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction." 82

3. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code." 83

4. Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition." 83

5. Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob." 83

6. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application." 83

7. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account." 84

8. Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data." 84

9. Claim 9: 84

(a) [9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;" 84

(b) [9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and" 84

(c) [9c] "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third - party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction." 85

10. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network." 85

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob." 85

12. Claim 13: 86

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating

that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and" 86

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes." 86

13. Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code." 87

14. Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob." 87

15. Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition." 87

16. Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account." 88

17. Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application." 88

D. SNQ 4: Ludtke in combination with Scott and Robinson Renders Claims 2 and 11 Obvious 88

1. The proposed combination 88
(a) The Prior Art Discloses the Claim Limitations 88
(b) A POSITA Would have been Motivated to Combine Robinson with Ludtke and Scott 89
2. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code. 90
3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the device ID code. 91
XI. REAL PARTIES OF INTEREST 91
XII. CONCLUSION 91

TABLE OF ATTACHMENTS AND EXHIBITS

Attachments

(1) Certificate of Service to Patent Owner
(2) Ex. 1011 Form PTO/SB/08a (Information Disclosure Statement)

Exhibits

The '905 patent, Declaration, and Prosecution History

Ex. 1001	U.S. Patent No. 9,298,905 ("'905 patent")
Ex. 1002	File History of the '905 patent
Ex. 1003	Expert Declaration of Dr. Benjamin Goldberg
Ex. 1004	CV of Dr. Benjamin Goldberg

Prior Art

Ex. 1005	U.S. Patent No. 7,188,110 ("Ludtke")
Ex. 1006	U.S. Patent Publication No. 2003/0196084 ("Okereke")
Ex. 1007	U.S. Patent Publication No. 2003/0177102 ("Robinson")
Ex. 1008	International Publication Number WO 99/56429 ("Scott")

Other

Ex. 1009	Decision Denying Institution of *Inter Partes* Review, Paper No. 12, IPR2021-01447 (February 28, 2022)
Ex. 1010	Claim Construction Order in *Proxense, LLP v. Samsung Electronics Co., Ltd*, Case No. 6:21-CV-00210 (W.D. Tex.) Dkt. 43.
Ex. 1011	Form PTO/SB/08a (Information Disclosure Statement)
Ex. 1012	Introduction to Public Key Technology
Ex. 1013	Security Issues for Contactless Smart Cards
Ex. 1014	Smart Card Alliance Web Site
Ex. 1015	Smart Card Alliance Contactless Payment and the Retail Point of Sale

LISTING OF CLAIMS

CLAIM	LIMITATION
1a	A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device;
1b	responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;
1c	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
1d	responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and
1e	responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction.
2	The method of claim 1, further comprising: registering an age verification for the user in association with the ID code.
3	3. The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code.

CLAIM	LIMITATION
4	4. The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.
5	The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.
6	The method of claim 1, wherein completing the financial transaction includes accessing an application.
7	The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.
8a	The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification; and
8b	responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data.

CLAIM	LIMITATION
9a	An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;
9b	a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and
9c	a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction.
10	The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network.
11	The integrated device of claim 7, wherein an age verification is registered in association with the ID code.
12	The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

CLAIM	LIMITATION
13a	A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and
13b	the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes.
14	The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code.
15	The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.
16	The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal

CLAIM	LIMITATION
	scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.
17	The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.
18	The system of claim 11, wherein completing the financial transaction includes accessing an application.

I. INTRODUCTION

The challenged claims are directed to conventional technology to prevent unauthorized use of a wireless device by verifying both biometric information and the device itself. None of the concepts in the '905 patent were new when the patent was filed; they are clearly disclosed in prior art references that together disclose each and every element of the challenged claims. Moreover, all of the concepts in the patents were used for various different applications for years before the '905 patent was filed. Nevertheless, Patent Owner has launched a lawsuit against Samsung, alleging infringement of technology far newer and more innovative than the technology described in the challenged claims.

The lawsuit against Samsung involves five patents, all relating to similar technology. After the lawsuit against Samsung was filed, Samsung filed IPRs against all five asserted patents. Two of the IPRs were instituted (against US Patent Nos. 9,049,188 and 9,235,700) and are currently pending. The Board denied institution, however, on the '905 patent and two additional related family members: U.S. Patent Nos. 8,352,730 and 10,698,989. In the decisions not to institute the IPRs, the Board found merit in the Patent Owner's argument (which Samsung did not foresee, as it contradicted Patent Owner's claim construction arguments in litigation) that the prior art did not disclose a "third party trusted authority." The

present petition addresses Patent Owner's new argument with different prior art, and therefore presents substantial new questions of patentability.

This Request presents several substantial new questions of patentability. All four SNQs rely primarily on a new reference (Ludtke) that was cited neither during prosecution of either the '905 patent or any of its parents nor in the prior IPR petition regarding the '905 patent. Specifically, SNQ 1 relies on a combination of Ludtke and Okereke, neither of which was presented in the IPR. SNQ 2 relies on a third reference for a single limitation found in a handful of dependent claims. SNQs 3 and 4 rely on a combination of Ludtke and Scott, and while the Scott reference was presented in the IPR, it is cited here only as a secondary reference. Like SNQ 2, SNQ 4 relies on a third reference for a single limitation in a number of dependent claims. Respectfully, these combinations present substantial new questions of patentability that have not been considered by either the PTO or the PTAB.

II. REQUIREMENTS FOR *EX PARTE* REEXAMINATION UNDER 37 C.F.R. § 1.510

This request for *ex parte* reexamination of the '905 patent satisfies each requirement of 37 C.F.R. § 1.510.

A. Payment of Fees – 37 C.F.R. § 1.510(a)

Requestor authorizes the Patent and Trademark Office to charge Deposit Account No. DA505708 for the fees set in 37 C.P.R. § 1.20(c)(1) for reexamination.

B. Statement Pointing Out Each Substantial New Question of Patentability Based on Prior Art Patents and Printed Publications – 37 C.F.R. § 1.510(b)(1)

A detailed discussion of pertinent new teachings in the prior art references that present substantial new questions of patentability is provided in Section IX.

C. Identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited prior art – 37 C.F.R. § 1.510(b)(2)

Samsung respectfully requests reexamination of claims 1-18 of the '905 patent based on the following proposed rejections:

SNQ 1: Ludtke in combination with Okereke renders obvious claims 1, 3-10, and 12-18 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 2: Ludtke in combination with Okereke and Robinson renders obvious claims 2 and 11 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 3: Ludtke in combination with Scott renders obvious claims 1, 3-10, and 12-18 under 35 U.S.C. §§ 102 (b) and (e) and 35 U.S.C. § 103; and

SNQ 4: Ludtke in combination with Scott and Robinson renders obvious claims 2 and 11 under 35 U.S.C. §§ 102(a), (b), and (e) and 35 U.S.C. § 103.

A detailed explanation of the pertinence and manner of applying the cited prior art to claims 1-18 of the '905 patent is provided in Section X.

D. Copies of the Cited Prior Art Presented- 37 C.F.R. § 1.510(b)(3)

A copy of every patent or printed publication relied upon as a basis of unpatentability are submitted as exhibits in conjunction with this request for reexamination. In addition, a Form PTO/SB/08a is attached hereto as Exhibit 1011. A full list of exhibits appears on page 11.

E. Copy of the Patent for Which Reexamination Is Requested- 37 C.F.R. § 1.510(b)(4)

A copy of the '905 patent is attached to this Request as Exhibit 1001.

F. Certification of Service on the Patent Owner- 37 C.F.R. § 1.510(b)(5)

The signature on this request certifies that a copy of the request has been served in its entirety on PO's representative at the address provided for in 37 C.F.R. § 1.33(c). Specifically, PO's representative was served by first-class U.S. mail on June 8, 2022, addressed to:

Patent Law Works/Proxense
Greg Sueoka
310 East 4500 South, Suite 400
Salt Lake City, UT 84107

The Requester has also provided courtesy copies to PO's counsel in the aforementioned litigation by first-class U.S. mail on June 8, 2022, addressed to:

Hecht Partners
David Hecht
125 Park Avenue, 25th Floor
New York, NY 10017

Susman Godfrey
Brian Melton
1000 Louisiana St, Suite 5100
Houston, TX 77002

G. Certification of Statutory Estoppel Provisions - 37 C.F.R. § 1.510(b)(6)

Samsung certifies that the statutory estoppel provisions of 35 U.S.C. §§ 315(e)(1) and 325(e)(1) do not prohibit it from filing this ex parte reexamination request.

Requestor previously filed one petition for *inter partes* review against the '905 patent. *See* IPR2021-01447. The petition was denied institution.

III. PROCEDURAL HISTORY

Requestor is unaware of any co-pending Patent Office proceedings involving the '905 patent. This is the first reexamination request challenging the claims of the '905 patent.

The '905 patent claims priority to two provisional patents: U.S. Patent Application Nos. 60/637,538, filed on Dec. 20, 2004, and 60/652,765, filed on Feb. 14, 2005. The '905 patent is a continuation of application no. 13/710,109, filed on Dec. 10, 2012 (now, U.S. Pat. No. 8,886,954), which is a continuation of application no. 11/314,199, filed on Dec. 20, 2005 (now, U.S. Pat. No. 8,352,730). The application that led to the '905 patent was filed on October 23, 2014. The '905 patent issued on March 29, 2016.

A. Prosecution History of the '905 Patent

The '905 patent was filed on October 23, 2014 and claimed the benefit of application no 60/637,538 filed on December, 2004. Ex. 1002 at 482-83, 486.

On June 12, 2015, after lengthy exchange regarding various formalities, the U.S. Patent & Trademark Office (hereinafter "Patent Office") issued the first non-final Office Action rejecting claims 2-18 under 35 U.S.C 103 in light of Hsu et al. (US 6,041,410) in view of Saito et all (US 20040129787) as well as non-statutory double patenting in light of US Patent No. 8,886,954. Ex. 1002 at 94-109.

After amendment and an examiner-initiated interview to suggest terminal disclaimers the Patent Office issued a Notice of Allowance on December 16, 2015. Ex. 1002 at 37-47 and 76-80.

B. The IPR filed against the '905 Patent

Samsung previously filed an IPR against the '905 patent. IPR2021-01447. The IPR presented four grounds. The first two grounds were based on the Scott reference, combined with others. The third ground was based on the Berardi reference in combination with others. The PTAB denied institution of the first two grounds based on its belief that none of the cited prior art disclosed a "third party trusted authority" with respect to claim 1. *See, e.g.*, IPR2021-01447, Paper 12 at 20-26. The PTAB denied institution on the third ground for unrelated reasons. *See, e.g.*, IPR2021-01447, Paper 12 at 27-30.

IV. THIS REQUEST SHOULD NOT BE DENIED BASED ON DISCRETIONARY ISSUES

Patent Owner may argue that this request should be denied in accordance with § 325(d) based on the Federal Circuit's decision in *In re Vivint, Inc.*, 14 F.4th 1342 (Fed. Cir. 2021). That case, however, does not apply here. In *Vivint*, the Requestor filed an *Ex Parte* Reexam request after filing a series of vexatious IPR petitions, the last of which the Board found was an "undesirable, incremental" attack on the Patent Owner. The Board reasoned that allowing such practices "risks harassment of patent owners and frustration of Congress's intent in enacting [the AIA]," and therefore denied the petition. *Id.* at 1346.

Notwithstanding that denial, the Requestor in *Vivint* filed a reexam request that ultimately resulted in cancellation of the challenged claims. On review, the Federal Circuit reversed the CRU's decision to grant the reexam, finding that the request, just like the denied IPR petition, was an abusive filing. The Federal Circuit noted that the vast majority of the reexam was a copy of the denied IPR petition, and the Court concluded that the Director's finding that the IPR petition was abusive should have likewise applied to the reexam request. Specifically, the Court found that the reexam "copied, word-for-word, two grounds from the [denied IPR petition]--the very petition deemed 'a case of undesirable, incremental petitioning.'" *Id.* at 1353. And, for the portions that were not copied, the EPR "used prior Board decisions as a roadmap to correct past deficiencies." *Id.*

The facts here are distinguishable. ***First***, and most importantly, Samsung's previous IPR petition was not a series of "serial" petitions that were "undesirable, incremental petitions." There was only a single prior IPR filed on the '905 patent.

Second, this request is not a "word-for-word" copy of the denied IPR petition. To the contrary, the first SNQ in this request includes *completely new* art that was not seen in either prosecution or the prior IPR. In all four SNQs presented in this reexam, the primary reference, Ludtke, is completely new and was not considered during prosecution or presented in the previously filed IPR. Although

the Scott reference was previously used in the prior IPR, it is used here only as a secondary reference in two SNQs. Similarly, the Robinson reference, which was used for a very specific limitation found in a handful of dependent claims, is also used for that same limitation in the dependent claims. Notably, the Board did not disagree that Robinson teaches that limitation.

Third, this reexam is not using the prior, denied '905 IPR petition as a "roadmap" to correct past deficiencies. In *Vivint*, the requestor copied, word-for-word, two grounds in their entirety, which the Board had already found to be vexatious harassment. Even in the portions that were not copied, the Board found that the same or similar prior art was used. Here, Samsung's request presents entirely new proposed SNQs of rejection. There are ***no*** SNQs that are "word-for-word" copies of the IPR grounds, and indeed, the primary reference that forms the vast basis for the rejections is entirely different and thus do not, and could not, use the prior IPR petition denial as a "roadmap."

Fourth, each of the above patents and publications are prior art to the Asserted Patents, and as mentioned above, the grounds of rejection outlined in this Request raise substantial new questions of patentability, because the reference combinations used to establish these grounds provide teachings not previously considered by the Office. None of the reference combinations used to establish the

grounds for rejection in this Request, nor the grounds themselves, were advanced by the Examiner during prosecution of the applications that matured into the Asserted Patents.

Further, the references are also non-cumulative because, as discussed in more detail below, the prior art reference individually and/or in combination disclose each and every limitation of the challenged claims—including the challenged independent claims that were allowed over the considered prior art.

For these reasons, the present request should not be denied pursuant to the CRU's discretionary powers.

V. LEVEL OF SKILL IN THE ART

The '905 patent claims priority to two provisional applications filed on December 20, 2004, and February 14, 2005. A person of ordinary skill in the art ("POSITA") at that time would have had a bachelor's degree in computer science or electrical engineering (or an equivalent degree) with at least three years of experience in the field of encryption and security (or an equivalent). More education could compensate for less experience and vice versa. Ex. 1003 at ¶13. Each of the arguments below is made from the standpoint of a POSITA in the field of the '905 patent. Requestor's expert, Dr. Benjamin Goldberg, was at least a POSITA at the time of the alleged invention. *Id.*; Ex. 1004.

VI. CLAIM CONSTRUCTION

The USPTO construes claims in accordance with their "broadest reasonable interpretation" ("BRI") in light of the claim language and specification. *In re Reuter*, 670 F.2d 1015, 1019 (C.C.P.A. 1981); *In re Smith International, Inc.*, 871 F.3d 1375, 1381, 1382-83 (Fed. Cir. September 26, 2017). This is as true in reexamination proceedings as it is during original prosecution. *In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004); *In re ICON Health & Fitness, Inc.*, 496 F.3d 1374, 1379 (Fed. Cir. 2007). The USPTO broadly interprets claims during examination of a patent application because the applicant may "amend his claims, the thought being to reduce the possibility that, after the patent is granted, the claims may be interpreted as giving broader coverage than is justified." *In re Prater*, 415 F.2d 1393, 1404-05 (C.C.P.A. 1969). According to the Federal Circuit, "[t]his approach serves the public interest by reducing the possibility that claims, finally allowed, will be given broader scope than is justified. Applicants' interests are not impaired since they are not foreclosed from obtaining appropriate coverage for their invention with express claim language." *In re Yamamoto*, 740 F.2d 1569, 1571-72 (Fed. Cir. 1984) (*citing In re Prater*, 415 F.2d at 1405 n.31). The same policy underpinning the use of the broadest-reasonable-interpretation standard in initial examination, justifies its application in reexamination. *Id.*

Since the filing of the IPR, the District Court has issued a claim construction order construing terms as follows:

Claims	**Term**	**Construction**
1-3, 8-11,13-14	"ID code"	A unique code identifying a device
1, 9, 13	"access message"	A signal or notification enabling or announcing access

Ex. 1010 at 3. In addition to these terms, the Court also construed a number of terms as having their "plain meaning." *Id.* Although the terms above have been construed according to the *Phillips* standard, Requestor has applied these constructions in the discussion below, as the Broadest Reasonable Interpretation encompasses the *Phillips* standard. Accordingly, if the prior art meets the limitations construed according to the *Phillips* standard, it meets the limitations construed according to BRI.

A. "third party trusted authority" (claim 1)

In the previous IPR, the PTAB construed the term "third party trusted authority" as "an entity or party separate from the principal parties to a transaction." Ex. 1009, IPR2021-01447, Paper 12 at 13. In considering the prior art in light of its construction of the term, the PTAB found that Petitioner did not "explain[] sufficiently why Lapsley's DPC is a third-party trusted authority, what entities the DPC is a third-party relative to, or what application is being permitted to access in

the asserted combination." *Id.* at 24.[1] The Patent Owner argued that the DPC in Lapsley (which Petitioner pointed to as the "third party trusted authority") actually acted as a "cloud based digital wallet," and further that the purchaser did not access the digital wallet using a "fob" or "phone," but rather a device in the store where they were purchasing something. Ex. 1009 at p. 23-24. Based on these arguments, the PTAB found that the "the DPC is the resource to be accessed" and that "it is a party to the transaction, rather than a third party." *Id.* The PTAB further observed that during prosecution, the applicant explained that a "user []prov[ing] to the same institution that authenticates the fingerprint information that the user is who he purports to be' does not satisfy the 'third party' limitation." *Id.* at 24.

Requestor has applied this construction, in light of the Board's observations and analysis, to the prior art below.

VII. PRIORITY DATE OF THE '905 PATENT

The '905 patent claims priority to two provisional applications: U.S. Patent Application No. 60/637,538, filed December 20, 2004, and U.S. Patent Application No. 60/652,765, filed on February 14, 2005. Although Requestor does not concede that all 18 claims are entitled to one or both of the priority dates of the provisional

[1] Lapsley was the prior art reference that was relied upon for the "third party trusted authority" limitation in the IPR.

applications, all prior art references relied on in this petition date back to before December 20, 2004, and therefore, no further determination needs to be made regarding the priority date.

VIII. OVERVIEW OF THE TECHNOLOGY

The '905 patent relates to integrated wireless devices in a generic "computerized authentication" system that is used to gain access to devices, applications, or accounts through a biometric validation procedure. Ex. 1001 at 1:21-24, 1:49-54. The integrated device validates a user's biometric scan against biometric data stored on the device. *Id.* at 1:62-2:5. After validation using the biometric scan, a code stored on the device is transmitted to indicate that the user's identity has been verified. *Id.* The device transmits the code to a third-party trusted authority that determines if the code is authentic by checking it against a list of legitimate integrated device codes. *Id.* at 6:37-42. If the code is authentic, the user is allowed access to the device, application, or account they seek access to. *Id.* at 2:37-42. The '905 patent purports to solve for users the problem of having to "memorize or otherwise keep track of the[ir] credentials." *Id.* at 1:33-35. The patent also purports to solve the problem of illegitimate users "us[ing] a stolen access object to enter a secured location because the user's identity is never checked." *Id.* at 1:46-48.

IX. OVERVIEW OF THE PRIOR ART

A. Ludtke (Ex. 1005)

U.S. Patent No. 7,188,110 ("Ludtke") was filed on December 11, 2000. It issued on March 6, 2007. It is therefore prior art under 35 U.S.C. § 102(e) (pre-AIA).

Titled "Secure and Convenient Method and Apparatus for Storing and Transmitting Telephony-Based Data," Ludtke discloses a method of identifying an authorized user with a biometric device and enabling the authorized user to access private information. Ex. 1005 at Abstract. Ludtke recognizes both the need to ensure the integrity of financial information and the privacy of the user. *Id.* at 1:11-21.

The system disclosed in Ludtke is strikingly like the system disclosed in the '905 patent. The Ludtke system allows transactions through an eCommerce system through a "transaction device" that has a unique identifier (ID). *Id.* at 3:34-35. The transaction device can be a privacy card or a digital wallet or both. *Id.* at 3:35-39. This transaction device is a wireless device that is carried and maintained by a user. *See, e.g., id.* at 5:40-44. The transaction device includes a highly secured memory that can provide a transaction processing clearing house (TPCH) the necessary information to authorize a transaction. *Id.* at 3:40-45. The Ludtke system is described in Figure 1:

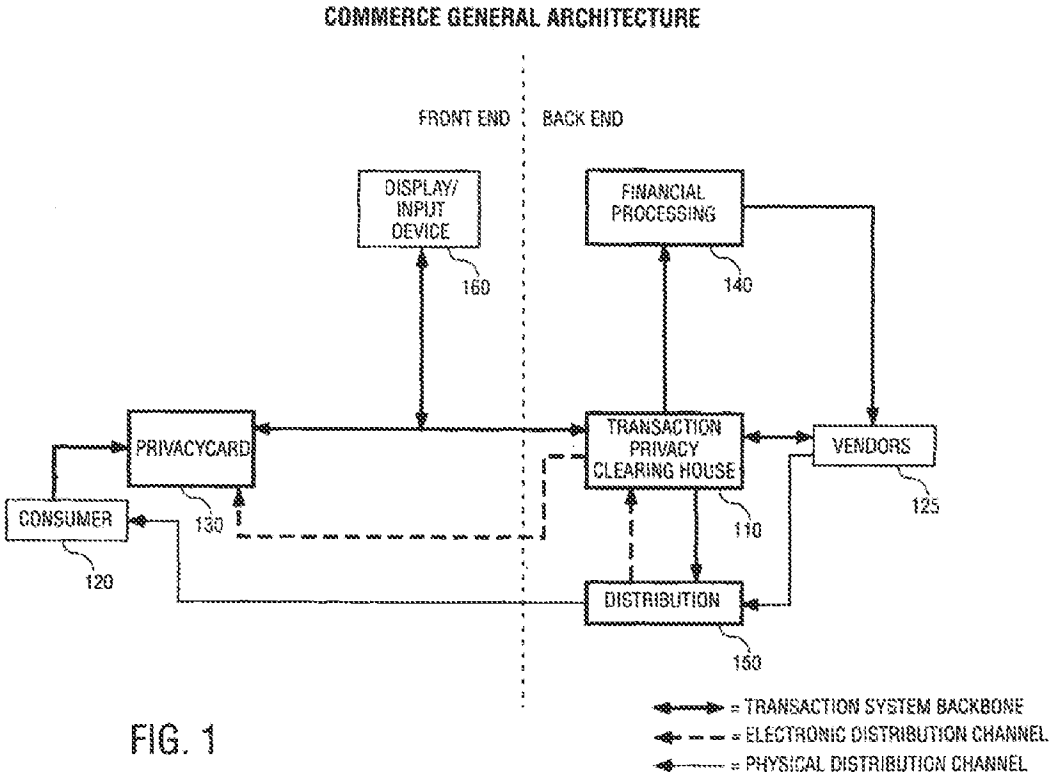


FIG. 1

As demonstrated in this figure, the Consumer 120 uses a transaction device 130 (in this figure, shown as a privacy card). The consumer wishes to purchase something from a vendor 125. The transaction device provides information to the TPCH for authorization for the transaction between the consumer and vendor to be performed. *Id.* at 6:36-44. The TPCH is not part of the transaction, but rather functions as a third-party middleman of the transaction. *Id.* at 7:44-46. This ensures that sensitive information is not shared with the vendor. *Id.* at 7:46-48.

Recognizing the need to protect the authorization of a user, Ludtke also discloses the use of fingerprint recognition as part of the digital wallet. *Id.* at 18:16-17. This biometric verification occurs before any transaction can take place, and therefore authorizes the user before the transaction device authorizes the device with the TPCH. *Id.* at 25:65-26:9; Ex. 1003 at ¶¶37-41.

B. Okereke (Ex. 1006)

U.S. Publication No. 2003/0196084 ("Okereke") was filed April 11, 2003. It published October 16, 2003. It is therefore prior art under 35 U.S.C. § 102(a) (pre-AIA).

Okereke describes a "system and method for allowing users of wireless and mobile devices to participate in Public Key Infrastructure[PKI]" and also indicates that it "facilitates secure remote communications." Ex. 1006 at Abstract. Okereke states that "systems that perform electronic financial transactions or electronic commerce must protect against unauthorized access to confidential records and unauthorized modification of data." *Id.* at ¶3.

In setting up communications for a mobile device, Okereke specifically teaches that "a unique identifier for the wireless product to be employed is passed [sic] at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other

device capable of remote wireless communication. The unique identifier can be a serial number or SIM." *Id.* at ¶25.

Okereke describes the PKI: "With PKI, a public and private key are created simultaneously using the same algorithm by a certificate authority. Information encrypted by the private key can only be decrypted with the corresponding public key. The private key is given only to the requesting party, and the public key is made publicly available as part of a digital certificate in a directory that all parties can access. The private key is never shared with anyone or sent across the network." *Id.* at ¶ 7. Therefore, the private key is secret information. Ex. 1003 at ¶¶42-45.

C. Robinson (Ex. 1007)

U.S. Publication No. 2003/0177102 ("Robinson") was filed February 19, 2003. It published September 18, 2003. It is therefore prior art under 35 U.S.C. § 102(a) (pre-AIA).

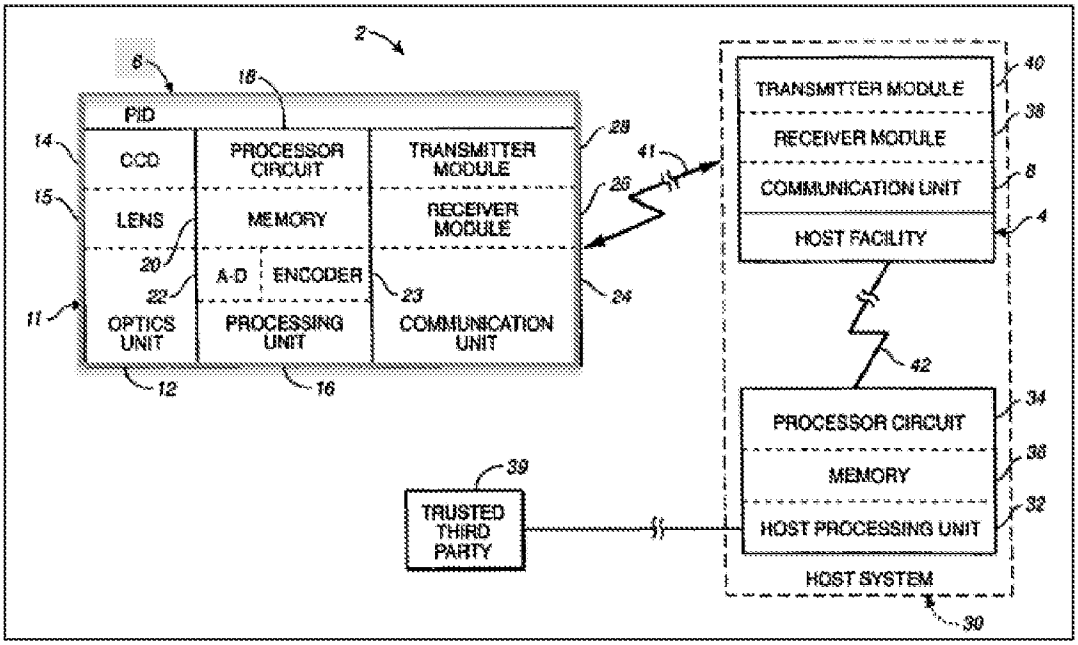
Robinson discloses that a central database 102 holds information related to users to authenticate a user's age to access an age restricted area, for example. Ex. 1007 at ¶¶27-28, 32, 66-67, Fig. 1. The central database 102 stores age verification records related to individuals seeking age verification (called "presenters"), including information such as a user's age, date of birth, government ID number, biometric template, and at least one ID number that identifies the presenter within the system. *Id.* Prior to using the age-verification system, an individual presents

biometric and age-verifying information. *Id.* at ¶¶13-15. Robinson further discloses that age-verifying information is associated with at least one ID number (SID) identifying the user; Ex. 1003 at ¶¶46-47.

D. Scott (Ex. 1008)

International PCT Application WO 99/56429 ("Scott") was filed on April 26, 1999. It was published on November 4, 1999. The International Publication Date is November 4, 1999, making it prior art under 35 U.S.C. § 102(b) (pre-AIA).

Scott discloses a method for verifying a user during authentication of an integrated device (*e.g.*, personal identification device ("PID") 6), in order to, for example, provide secure access to protected resources such as a hotel room or a point-of-sale transaction. Ex. 1008 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12; *see* claims [1A]-[1H] *infra*.



Ex. 1008 at Fig. 1[2]; Ex. 1003 at ¶48.

1. A POSITA Would Have Been Motivated to Combine the Teachings of the Ludtke, Okereke, and Robinson

Ludtke, Okereke, and Robinson all relate to protecting confidential information, communication over wireless networks, and the use of biometric information to protect this communication. All three references relate to communications for the purpose of financial transactions. Ex. 1005 at 4:54-56, 6:51-67; Ex. 1006 ¶3; Ex. 1007 ¶¶31-32, 47, Fig.1. A POSITA would naturally consider the teachings of Ludtke, Okereke, and Robinson in order to get a full understanding of the available options for secure communications and would have been motivated by this to combine the references' teachings. As explained in detail below, a POSITA would have considered applying the teachings of Okereke and Robinson to the teachings of Ludtke.

2. A POSITA Would Have Been Motivated to Combine the Teachings of Ludtke, Scott, and Robinson

Ludtke, Scott, and Robinson also relate to protecting confidential information over wireless networks, using biometric information to protect sensitive information, and also relates to financial information. Ex. 1005 at

[2] Annotations are added to figures unless indicated otherwise.

4:54-56, 6:51-67; Ex. 1007 ¶¶31-32, 47, Fig.1; Ex. 1008 at 10:24-32, 18:29-19:20. Therefore, a POSITA would have combined the Scott reference with Ludtke and Robinson for the same reasons above with respect to Okereke. In fact, a POSITA would have considered all of these references in trying to develop a process of secure communications.

X. DETAILED EXPLANATION OF THE PROPOSED REJECTIONS

As shown in detail below, claims 1-18 of the '905 patent are unpatentable under 35 U.S.C. § 103 in light of the prior art references and combinations of references presented below. The following rejections should be adopted in their entirety:

SNQ 1: Ludtke in combination with Okereke renders obvious claims 1, 3-10, and 12-18 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 2: Ludtke in combination with Okereke and Robinson renders obvious claims 2 and 11 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 3: Ludtke in combination with Scott renders obvious claims 1, 3-10, and 12-18 under 35 U.S.C. §§ 102 (b) and (e) and 35 U.S.C. § 103; and

SNQ 4: Ludtke in combination with Scott and Robinson renders obvious claims 2 and 11 under 35 U.S.C. §§ 102(a), (b), and (e) and 35 U.S.C. § 103.

A. SNQ 1: Ludtke in combination with Okereke Renders Claims 1, 3-10, and 12-18 Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 1 relies on Ludtke as the base reference, which discloses a mobile device used for performing financial transactions. Ludtke discloses all of the limitations in claims 1, 3-10, and 12-18 except the "unique Device ID" and storage of "secret information." Specifically, Ludtke discloses the system as shown below in figure 1:

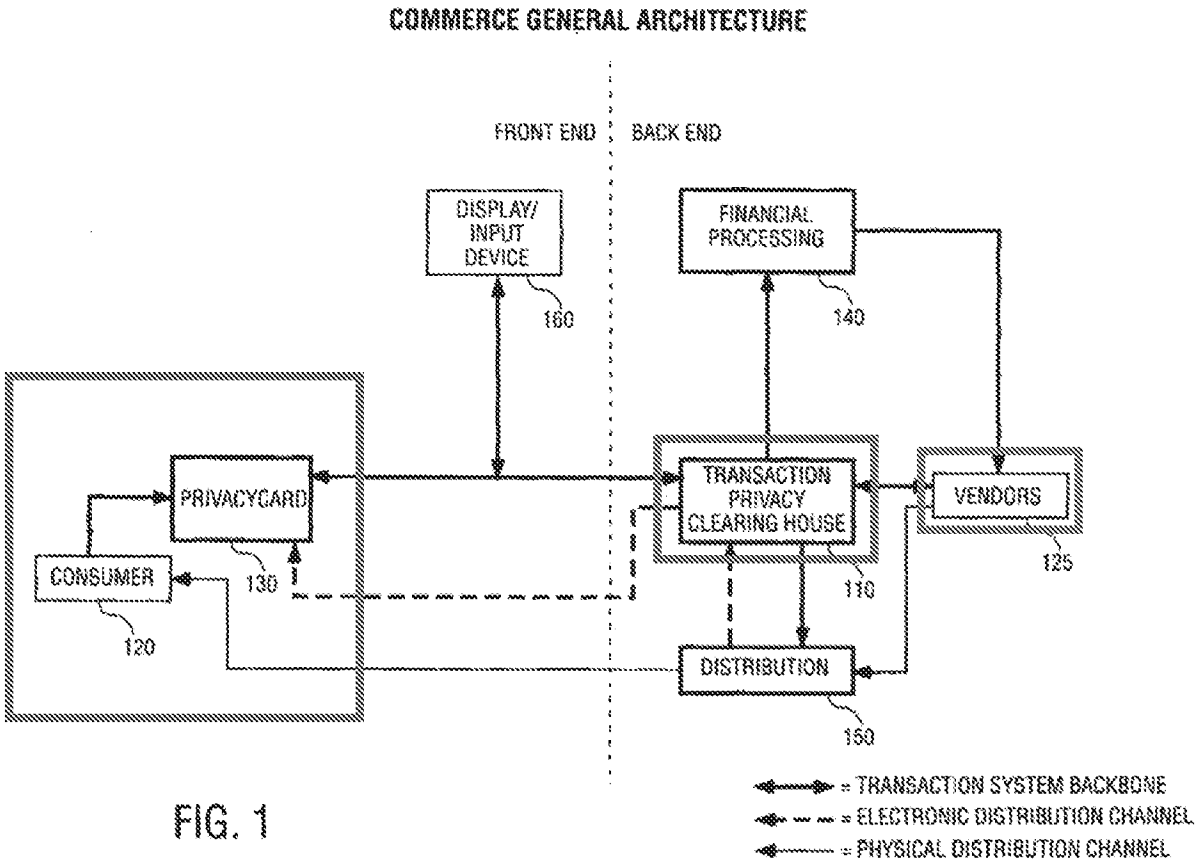


FIG. 1

Figure 1 shows one embodiment of the system in Ludtke. Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. The transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card, and digital wallet. *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a fingerprint and other biometric information. Ludtke's transaction device includes and discloses a persistent, tamper proof storage. Ludtke also discloses the process to authenticate a financial transaction between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110, which is a third party, independent of the consumer 120 and the vendor 125. Ludtke emphasizes the third-party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

The claims require storage of "secret information" in the user's device. Although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (*id.* at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (*id.* at 3:45-47; 5:30-31, 6:45-49). Okereke discloses this "secret information."

Specifically, Okereke discloses a "secret key" that is maintained by the user, and can be used to encrypt and decrypt information communicated to the user. Ex. 1006 at ¶ 25.

The claims also require an "ID code" that identifies the user's device that is communicated to the third party trusted authority for authorization of the device. Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for authorization, but Ludtke does not explicitly indicate that this "transaction device information" is unique. Okereke, however, does disclose this device ID code information, in the form of a unique serial number or SIM number for the user device. *Id*; Ex. 1003 at ¶¶196-198.

(b) A POSITA Would be Motivated to Combine Ludtke and Okereke

The scope and content of the prior art would have motivated a POSITA to combine Ludtke and Okereke. As explained above, Ludtke discloses almost all of the limitations of the claims except for "secret information" and the "unique" nature of a device ID.

Ludtke discloses a persistent, tamper-proof memory, and a POSITA would have been motivated to combine the secret key disclosed in Okereke with the system disclosed in Ludtke. Ex. 1003 at ¶¶ 199-206. A POSITA would have

already known, as of the priority date of the '905 patent, that encryption using a secret key such as that as part of PKI would have been obvious when communicating confidential information. *Id.*

POSITAs specifically recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. *Id.* The use of secret information to perform this type of encryption was well-known ***decades*** before the filing date of the '905 patent, and was a well-established, well-known method for implementing encryption. *Id.* Public Key Cryptography, which later developed into PKI encryption years before the '905 patent, was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. *Id.* POSITA recognized that such encryption is important to many applications, including financial information where it is particularly important to keep the information secret. *Id.* POSITA would therefore recognize that the use of PKI encryption, which is disclosed in Okereke, would make the system of Ludtke even more secure. *Id.* Okereke simply demonstrates this knowledge prior to the '905 patent's priority date.

Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a

financial transaction. A POSITA would have combined the teachings of Okereke's unique Device ID with Ludtke's system. As discussed above, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. A POSITA would have recognized that such transaction device information necessarily includes unique device identifiers such as a serial number or a SIM. Ex. 1003 at ¶¶199-206. Okereke explicitly discloses this fundamental information. Ex. 1006 at ¶25.

A POSITA would have been motivated to combine Ludtke and Okereke because they are both in the same field of endeavor. *Id.* Indeed, both references are in the same field of endeavor as the '905 patent, *i.e.*, authentication of a user and device, including use of biometric information, for the purpose of exchanging sensitive information over a network. *See* Ex. 1001 at 1:21-24 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ex. 1005 at Abstract ("A method of identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network is disclosed"); Ex. 1006 at Title ("System and method for secure wireless communication using PKI"); *id.* ¶31 ("In order to begin using the system via wireless device, the user may be required to provide

additional forms of authentication to the CPS, such as password or biometric signature.").

A POSITA would also have reasonably expected the combination of Ludtke and Okereke to succeed and yield predictable results. Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at 6:38-51. Given this disclosure in Ludtke, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret information in Ludtke's memory and using the unique device ID disclosed in Okereke as the transaction device information. A POSITA would have expected this to yield the predictable result of the option to use PKI-compliant encryption and decryption with a private key (secret information), as well as the ability to ensure authentication of an authorized device using unique device identifying information such as a serial number or SIM, and would have expected this combination to succeed. Ex. 1003 at ¶¶199-206.

For example, Ludtke describes a protected memory to keep the type of important and sensitive information described in Okereke. Ex. 1005 at 19:37-40. Moreover, a POSITA would be familiar with the PKI-compliant encryption system because it had long been used as a way to encrypt and decrypt information and

share such information only for authorized users. Implementing such a system with Ludtke would have been logical and obvious to a POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. It would make sense to a POSITA to use the type of information identified in Okereke in the Ludtke system to further complement Ludtke's features. *Id.*

2. Claim 1

(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device"

Ludtke and Okereke disclose this limitation.

An integrated device, biometric data, and an ID code: Ludtke discloses an integrated device, *e.g.*, Ludtke's "transaction device." Ex. 1005 at 3:32-35. Ludtke's transaction device provides a number of different "integrated" functions, including maintaining bills and bill paying on the device (*id.* at 4:4-6), online shopping (*id.* at 4:7-35), and downloading and accessing electronic catalogs (*id.* at 4:36-39). The transaction device includes a number of hardware options such as a magnetic stripe generator (*id.* at 3:49-51), a screen (*id.* at 55-57), and a bar code reader (*id.* at 3:61-63).

Ludtke explains that the "transaction device enhances security by ***authenticating the user of the card prior to usage***..." *Id.* at 4:62-65. This authentication can be performed by PIN code entry, or by other technologies such

as a biometric solution. *Id.* at 4:65-5:1. The biometric information ensures that the user is indeed legitimate.

Ludtke also specifically discloses authentication of a device through the use of "transaction device information." *Id.* at 6:36-44. A POSITA would recognize that this transaction device information necessarily includes unique device IDs, such as serial numbers and SIMs. Ex. 1003 at ¶¶208-212. But this knowledge of a POSITA is further embedded within Okereke. *See* Ex. 1005 at 6:36-44, *see also* Ex. 1006 at ¶30. As explained above in detail, a POSITA would have been motivated to combine the disclosure of Ludtke with the disclosure in Okereke.

Okereke also discloses a method for verifying a user during authentication of an integrated device. Okereke discloses wireless and mobile devices which are integrated devices. Ex. 1006 at Abstract. "The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication." *Id.* at ¶25.

Okereke specifically discloses authenticating the wireless device. Okereke describes a proxy server program awaiting initiation to establish secure wireless access capabilities. *Id.* at ¶25. When authentication is requested, "a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization." *Id.* "The unique identifier can be a serial number or

SIM number, for example." *Id.* Both serial numbers and SIM numbers are unique codes that identify the devices they are attached to. Ex. 1003 at ¶¶208-212. A POSITA would recognize that a serial number or SIM number is a unique identifier of a mobile device. *Id.* Once the proxy server confirms the unique identifier, it authorizes the device by sending approval to a desktop computer to make a key exchange to allow communication. *Id.*

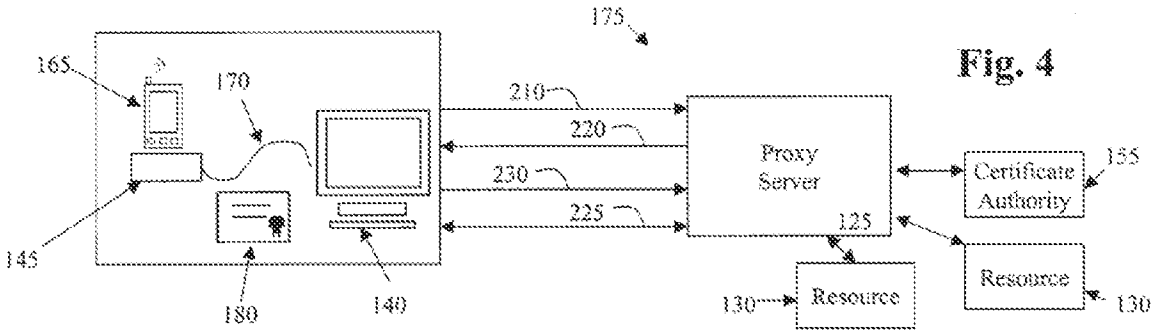


Fig. 4

Persistently storing biometric information and an ID code: Ludtke discloses a persistent storage on the integrated device. Specifically, the transaction device disclosed in Ludtke includes a process to use fingerprint data (biometric data of the user) to secure the device. Ludtke describes persistently storing the fingerprint data on the integrated device:

> The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). If confirmation succeeds, the device writes the fingerprint image data into write once memory, or other memory that is protected from accidental modification.

Id. at 19:35-40. This fingerprint data is persistently stored in a tamper-proof format that is unable to be subsequently altered (write-once memory or other memory that is protected from accidental modification). Indeed, a write-once memory will only allow writing once, therefore, the information cannot be tampered with, and cannot be modified. Ex. 1003 at ¶213. In each case, this memory is persistent storage, because the information stored is not easily re-writable. *Id.*

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

Ludtke describes receiving scan data from a biometric scan responsive to receiving a request for a biometric verification of the user. As explained above, Ludtke describes using biometric verification – including a fingerprint – to verify the user of the device. Figure 28 shows a device with a Fingerprint Identification Unit (FIU) 2806 and a touchpad 2808 for user input:

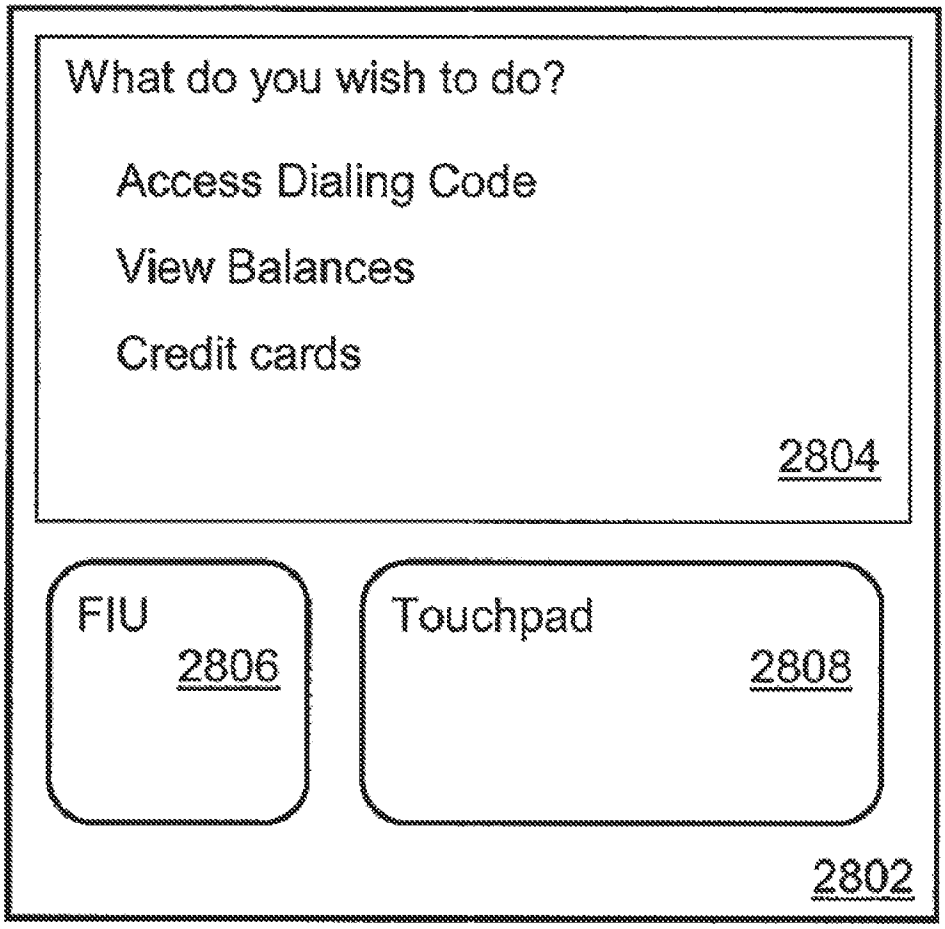


FIG. 28

Ex. 1005 at Fig. 28. "The user of the consumer access device 2802 would be authorized access to the device 2802 if the device recognized the user after the user had pressed his finger against the FIU 2806." *Id.* at 39:24-27.

A POSITA would recognize that FIU 2806 is a "biometric sensor." Ex. 1003 at ¶215. Indeed, the only way the FIU would be able to detect the fingerprint – and

determine the data present in the fingerprint – is if it was a fingerprint (or biometric) sensor. *Id.*

Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

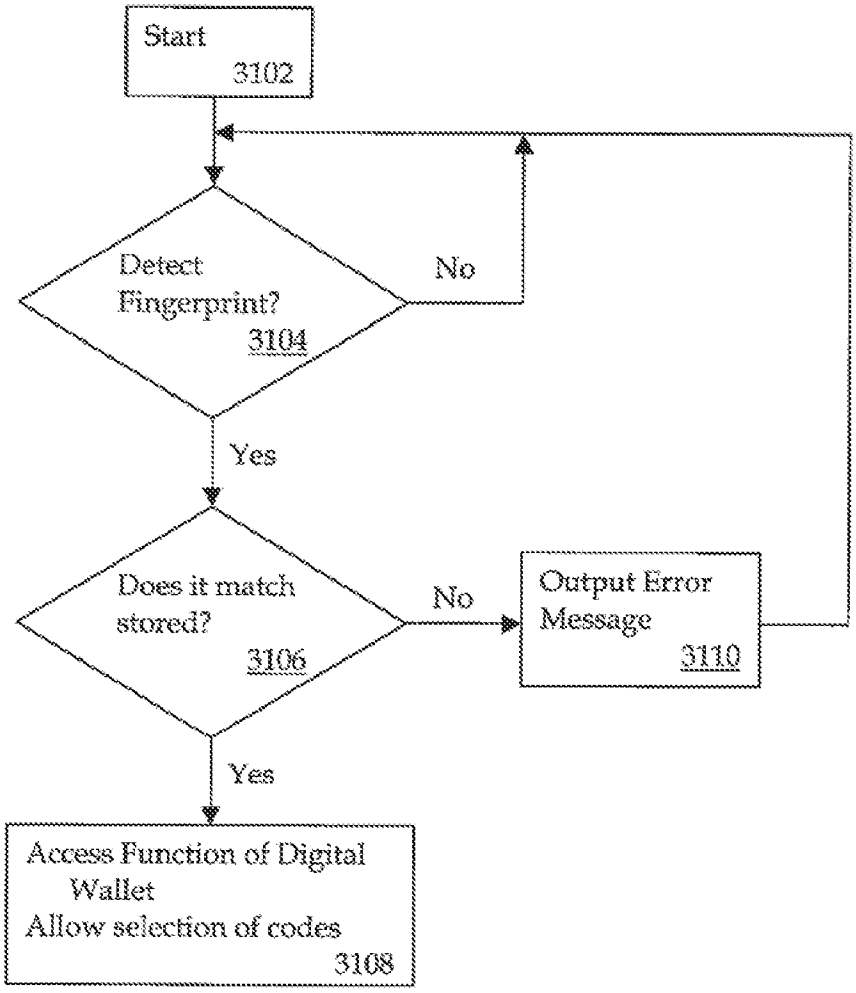


FIG. 31

Id. at Fig. 31. As can be seen in the flow chart, the device is continuously looking for a request for verification ("Detect fingerprint"). In response to that request, it will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106). *Id.* at 39:47-59.

(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;"

Ludtke also shows this limitation in Figure 31:

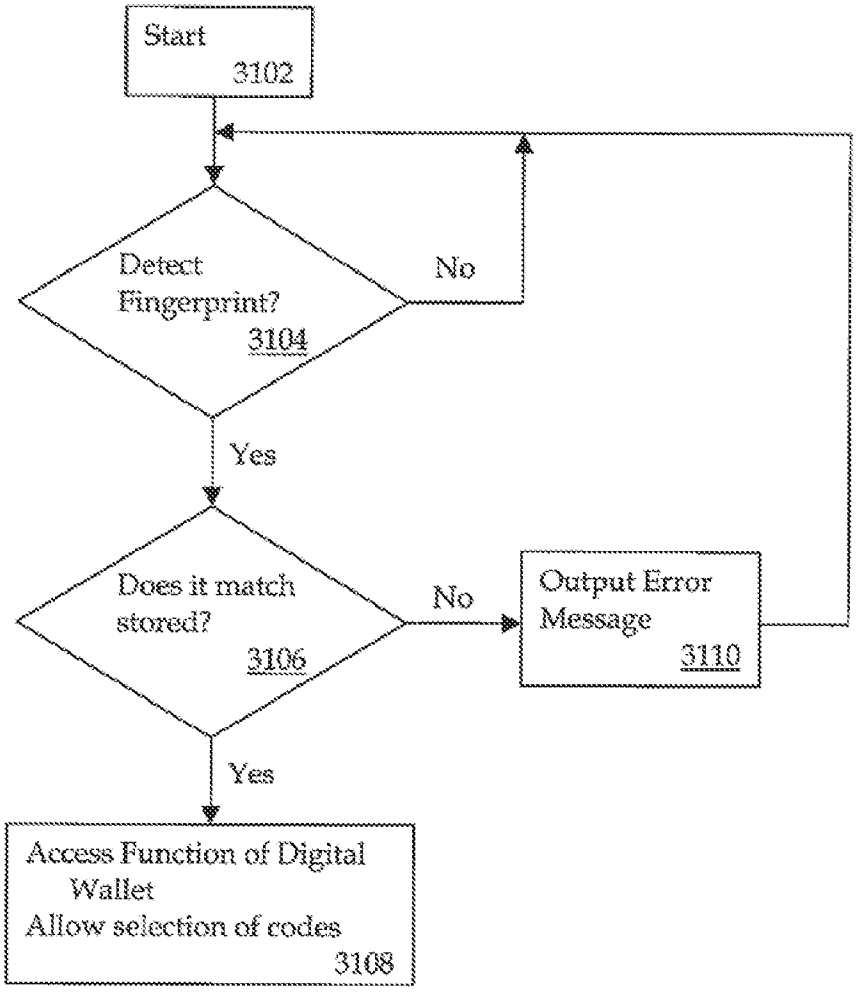


FIG. 31

Ex. 1005 at Fig. 31. Ludtke explains that if "a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW [Digital Wallet/Integrated Device] returns to checking to see if a fingerprint has been

detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes." *Id.* at 39:47-54.

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

Responsive to a determination that the scan data matches the biometric data: As explained in conjunction with limitation [1c], if the scanned fingerprint data matches the stored fingerprint, then access to functions of the integrated device, such as the digital wallet, is permitted. *Id.* at 39:47-54.

Third party trusted authority: Ludtke describes a transaction processing [or privacy] clearing house (TCPH) which is a third party trusted authority. The TPCH "may access relevant account information to authorize transactions." *Id.* at 3:40-45. Figure 1 of Ludtke shows how the TPCH is a third party:

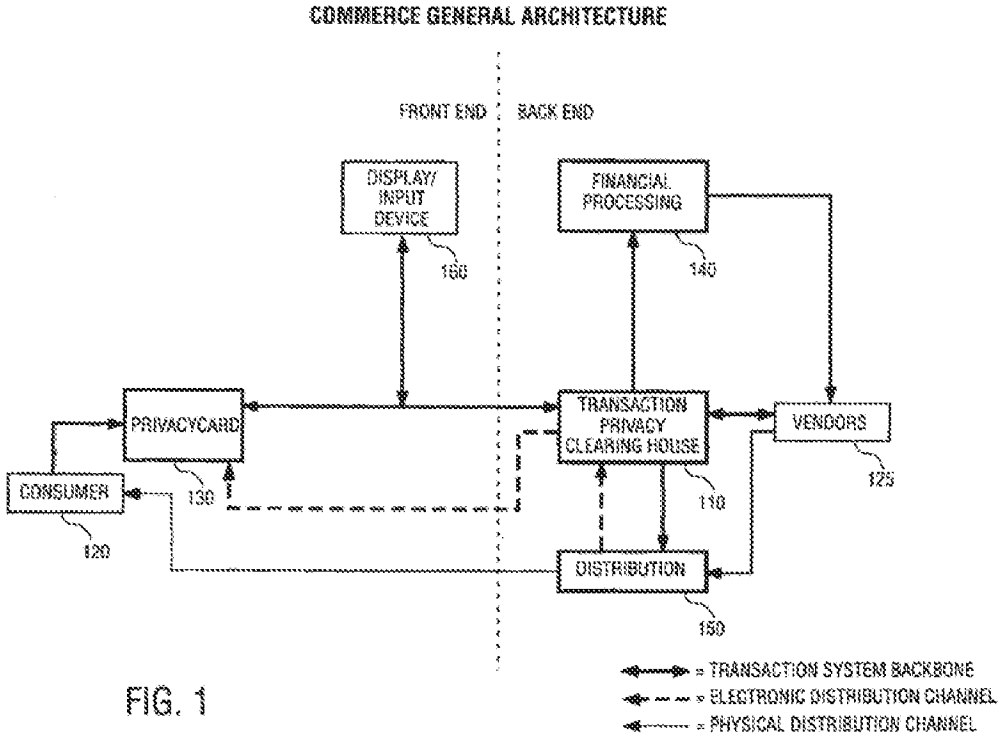


FIG. 1

Ex. 1005 at Figure 1. Figure 1 shows the commerce general architecture. *Id.* at 6:36-8:24. Figure 1 shows a consumer 120 who wishes to complete a purchase, *id.* at 6:36-64, and a vendor 125, who is selling something to the user 120. *Id.* "In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125." *Id.* at 6:36-38.

The TPCH is a third party to the transaction between the user/consumer 120 and the vendor 125. Ludtke explains that in "one embodiment of electronic distribution, the TPCH 110 functions as the middleman of the distribution channel.

This allows TPCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties." *Id.* at 7:44-48. This demonstrates that the TPCH acts as a middleman to ensure that only necessary information is exchanged between the consumer 120 and the vendor 125, but is not associated with either of them.

The TPCH is also a "trusted authority." Ludtke explains that the "transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id.* at 6:41-44. The consumer 120 and vendor 125 therefore trust the TPCH to indicate whether the transaction may be complete. Ex. 1003 at ¶¶ 219-221.

Wirelessly sending the ID code: Ludtke explains that "[t]he transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id.* at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id.* at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id.* at 9:35-42; Ex. 1003 at ¶222.

One or more previously registered ID codes maintained by the third-party trusted authority: Ludtke also explains that the "TPCH 110 maintains a secure database of transaction device information and user information. In one embodiment, the TPCH 110 interfaces to at least one financial processing system 140 to perform associated financial transactions, such as confirming sufficient funds to perform the transaction, and transfers to the vendor 125 the fees required to complete the transaction." *Id.* at 6:49-55. And as explained above, Ludtke explains that the "transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id.* at 6:41-44. Therefore, the TPCH includes previously registered information that can be compared with information from the consumer and the consumer's device so the TPCH can determine whether the consumer 120 is authorized to complete a transaction with vendor 125. Indeed, the transaction device information that the TPCH compares to the received transaction device information must be stored within the TPCH as a list of codes (and specifically, a list of ID codes), in order to perform the comparison function that is disclosed. *Id.* at 30:19-27; Ex. 1003 at ¶223.

ID Code: Ludtke does not describe the specific "transaction device information" that is provided to the TPCH 110 and that is maintained in a secure

database by the TPCH 110. *Id.* at 6:41-44. However, as discussed above, a POSITA would have been motivated to combine Ludtke with the teachings of Okereke, and would have recognized that the "transaction device information" would include a device serial number or SIM code, both of which uniquely identify the integrated device. Ex. 1003 at ¶224.

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

As indicated above, Ludtke explains that the "transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 ***and the user 120*** approval of the transaction to be performed." Ex. 1005 at 6:41-44. A POSITA would recognize that when the TPCH 110 "indicates to . . . the user 120," that indication is in the form of an access message allowing the user access to an application. Ex. 1003 at ¶225. In this case, the TPCH is allowing access to the application on the transaction device that will permit the transaction to be completed. Specifically, the TPCH is sending a signal (or a notification) to the user's device, which allows (it enables or announces) access to the application on the transaction device that will permit the transaction to be completed. Ludtke further discloses this limitation at Fig. 15, Step 1520:

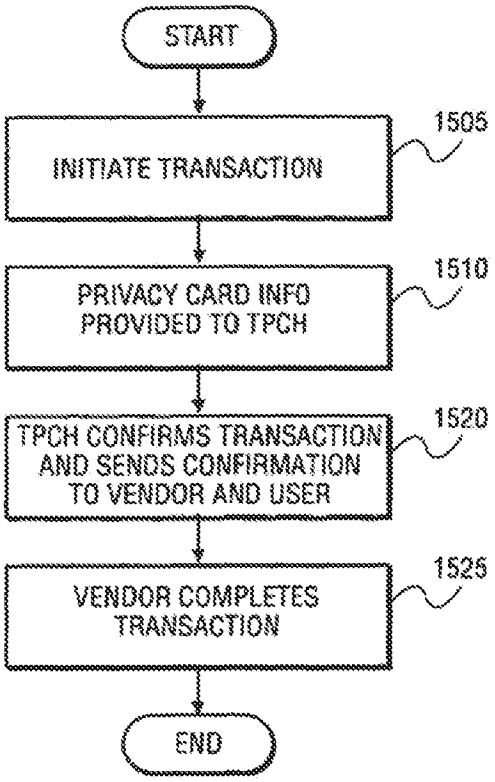


FIG. 15

Ex. 1005 at Fig. 15, *see also* Fig. 17, steps 8 and 9-1. With regard to step 1520, Ludtke teaches that the "TPCH, at step 1520, confirms the transaction and provides the confirmation to the vendor and the user. At step 1525, the vendor completes the transaction without the knowledge of the user." *Id.* at 27:13-16. The transaction, as described in Ludtke, is a financial transaction because it is a purchase from a vendor by the user. Ex. 1003 at ¶225.

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

Ludtke and Okereke disclose this limitation. As explained above, Ludtke discloses the transaction device receiving biometric information allowing access to the device and then subsequently communicates the ID code to the TPCH. Ex. at 1003 at ¶226. It is inherent that, when the ID code is sent to the TPCH, that is an indication that the biometric verification has been successful. Indeed, as the ID code will not be sent at all if biometric verification fails (Ex. 1005 at 19:35-45), the sending of the ID code itself is an "indication that the biometric verification was successful." *Id.*

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

Ludtke describes a number of different types of biometric information that may be used: "The identification by the biometric device may be achieved in a variety of ways, as discussed above. For example, biometric identification, may be, ***fingerprint***, ***retinal scan***, ***voice***, DNA, ***hand profile, face recognition***, etc." Ex. 1005 at 35:60-64; Ex. 1003 at ¶227.

5. Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet,

laptop, mp3 player, mobile gaming device, watch and a key fob."

Ludtke and Okereke disclose this limitation. POSITA would recognize that the transaction device disclosed in Ludtke, which includes a number of different iterations, including a privacy card (Ex. 1005 at 20:43-50), and a cellular telephone mechanism (*id.* at 17:3-10), would meet many of these limitations including "mobile phone," "tablet," and "key fob." Okereke explicitly states that its device may be a mobile phone. Ex. 1006 at Abstract; Ex. 1003 at ¶228.

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

Ludtke discloses this limitation. In Ludtke, access would be given applications of either computer software, a file (or both). In a number of embodiments, Ludtke describes the transaction device as including a "digital wallet" which POSITA would recognize as an application and files that allow a user to digitally store credit card and other payment information and to make transactions with that card. Ex. 1005 at 5:1-5; Ex. 1003 at ¶229.

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

Ludtke discloses this limitation. In Ludtke, access would be given applications of either computer software, a file (or both). In a number of

embodiments, Ludtke describes the transaction device as including a "digital wallet" which POSITA would recognize as files that allow a user to digitally store credit card and other payment information and to make transactions with that card. Ex. 1005 at 5:1-5; Ex. 1003 at ¶230. Moreover, a POSITA would recognize that giving access to the digital wallet is providing access to a financial account. *Id.*; Ex. 1003 at ¶230.

8. Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data."

Ludtke and Okereke disclose this limitation. For example, Ludtke discusses the process of requesting and receiving biometric information. *See supra* Section X.A.2; Ex. 1005 at 39:19-35. Ludtke then describes an embodiment where the biometric information is not needed: "Alternatively, the consumer access device, once the user has been identified may not require re-identification until the consumer access device is, for example, turned off." *Id.* at 39:35-38. A POSITA would recognize that in this embodiment, a request to authenticate the device for a financial transaction after biometric verification had occurred, but before the device was turned off is a request to send the ID code without an additional biometric

verification. Ex. 1003 at ¶231. A POSITA would recognize that in this case, the ID code would be sent without biometric verification. *Id.*

9. Claim 9:

(a) [9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;"

See Claim 1, element [1a]. Section X.A.2.a, *supra*; Ex. 1003 at ¶232.

(b) [9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and"

See Claim 1, elements [1c], [1d]. Section X.A.2.c, d, *supra*.

The "validation module" will be the portion of the smartphone, including processors and instructions that receives the scan and verifies the biometric information. Ex. 1003 at ¶234. A POSITA would recognize that the validation module would be in coupled with the memory, since the biometric information that the validation module compares with received biometric information is stored in the memory for comparison. *Id.*

(c) [9c] "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third -party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based

on the comparison of the ID code and allowing the user to—complete a financial transaction."

See Claim 1, elements [1d], [1e]. Section X.A.2.d, e, *supra*. A POSITA would recognize that because the transaction device has wireless access, it necessarily has a "radio frequency communication module," as all wireless communications occur through an RF module. Ex. 1003 at ¶235.

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

Ludtke and Okereke disclose this limitation. As explained above, Ludtke explains that "[t]he transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id.* at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id.* at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id.* at 9:35-42. Therefore, the communications described above in conjunction with claim 1 (by both Ludtke and Okereke) to the agent are transmitted over a network. Ex. 1003 at ¶236.

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone,

tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob."

See Claim 5. Section X.A.5, *supra*; Ex. 1003 at ¶237.

12. Claim 13:

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and"

See Claim 1, elements [1a], [1d], [1e]. Section X.A.2.a, d-e, *supra*. The integrated devices described above are hardware devices because they are held by the user. Ex. 1003 at ¶238. The "authentication circuit" is the portion of the hardware device, including processors and instructions that receives the scan and verifies the biometric information. *Id.*

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a

comparison of the ID code received and the legitimate codes included in the list of the legitimate codes."

See Claim 1, elements [1d], [1e]. Section X.A.2.d-e, *supra*; Ex. 1003 at ¶239.

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

See Claim 1, elements [1b], [1c]. Section X.A.2.b-c, *supra*. Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

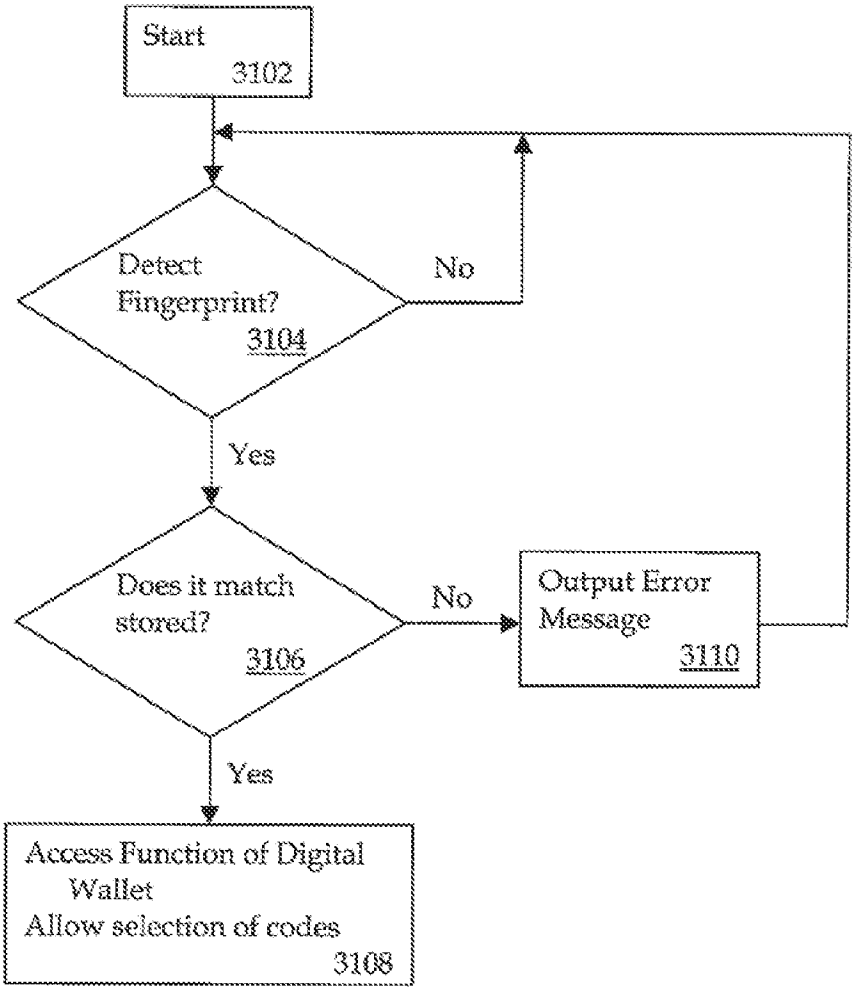


FIG. 31

Id. at Fig. 31. As can be seen in the flow chart, if the scan data does not match the stored data (i.e., the device cannot authenticate the user), it will output an error message, and not allow access to the digital wallet or selection of codes. *Id.* at 39:47-59. Ex. 1003 at ¶¶240-241.

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

See claim 5, section X.A.5, *supra*; Ex. 1003 at ¶242.

15. **Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition."**

See claim 4, Section X.A.4, *supra*; Ex. 1003 at ¶243.

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

See claim 7, Section X.A.7, *supra*; Ex. 1003 at ¶244.

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

See claim 6, Section X.A.6, *supra*; Ex. 1003 at ¶245.

B. SNQ 2: Ludtke in combination with Okereke and Robinson Renders Claims 2 and 11 Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 2 relies entirely on Ludtke and Okereke for the same reasons as outlined in SNQ 1, but also relies on Robinson for the limitations in dependent claims 2 and 11. Both of these dependent claims involve registering an age

verification. Where Ludtke and Okereke do not explicitly disclose registering an age verification, Robinson discloses the age verification in claims 2 and 11. As explained below, a POSITA would be motivated to combine the age verification disclosed in Robinson with the system disclosed in Ludtke with the secret information and unique device ID disclosed in Okereke. Ex. 1003 at ¶246.

(b) A POSITA Would have been Motivated to Combine Robinson with Ludtke and Okereke

The scope and content of the prior art would have motivated POSITA to combine Robinson with Ludtke and Okereke. Ex. 1003 at ¶¶247-250. Like both Ludtke and Okereke, Robinson discloses a way to improve security and to authenticate a user and device. Ex. 1007 at ¶¶27-29, 32, 66-67, Fig. 1.

All three of the references are therefore in the same field of endeavor, with Robinson specifically teaching improving security with an additional age-based authorization factor and to authenticate a user for age-restricted access or transactions initiated by a wireless device like Ludtke's transaction device. *Id.* at ¶9-10; Ex. 1003 at ¶¶247-250. A POSITA would have recognized that the disclosure of Ludtke welcomes this modification with its stated aim to provide, for example, secure access to restricted areas. Ex. 1005 at 2:5-8, 10:24-28. Indeed, a POSITA would have recognized that the age verification disclosed in Robinson would, for example, allow a way for the Ludtke system to ensure that the user is

old enough to conduct a transaction, access a specific financial system or application, or to enter a restricted area. *Id.*

A POSITA would also have had a reasonable expectation of success because age verification as disclosed in Robinson is a logical extension of the type of information that is exchanged. *Id.* Robinson, like Ludtke and Okereke, also discloses the use of biometric information to verify a user. Ex. 1007 at ¶39. It would be logical to modify the system of Ludtke and Okereke to also include the age of the user who was verified with biometric information. *Id.* The age would logically be registered at Ludtke's TPCH, where the age can also be kept confidential from third parties, consistent with Ludtke's goals. *Id.*

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

Ludtke in combination with Okereke disclose all of the limitations of claim 1. *See* SNQ 1, Claim 1. Section X.A.2, *supra.*

However, neither Ludtke nor Okereke expressly disclose "registering an age verification for the user" as recited in this limitation. Robinson discloses that a central database 102 holds information related to users to authenticate a user's age to access an age restricted area, for example. Ex. 1007 at ¶¶27-28, 32, 66-67, Fig. 1. The central database 102 stores age verification records related to individuals seeking age verification (called "presenters"), including information such as a

user's age, date of birth, government ID number, biometric template, and at least one ID number that identifies the presenter within the system. *Id.* Prior to using the age-verification system, an individual presents biometric and age-verifying information. *Id.* at ¶13-15. Robinson further discloses that age-verifying information is associated with at least one ID number (SID) identifying the user. Ex. 1003 at ¶252.

3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the ID code.

Ludtke in combination with Okereke disclose all of the limitations of claim 9. *See* SNQ 1, Claim 9. Section X.A.9, *supra*; Ex. 1003 at ¶253.

Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 11 for the same reasons as described in conjunction with claim 2. Section X.B.2, *supra*. Ex. 1003 at ¶254.

C. SNQ 3: Ludtke in combination with Scott Renders Claims 1, 3-10, and 12-18 Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 3 relies on Ludtke as the base reference, which discloses a mobile device used for performing financial transactions. Ludtke discloses all of the limitations in claims 1, 3-10, and 12-18 except the "unique Device ID" and storage

of "secret information." Specifically, Ludtke discloses the system as shown below in figure 1:

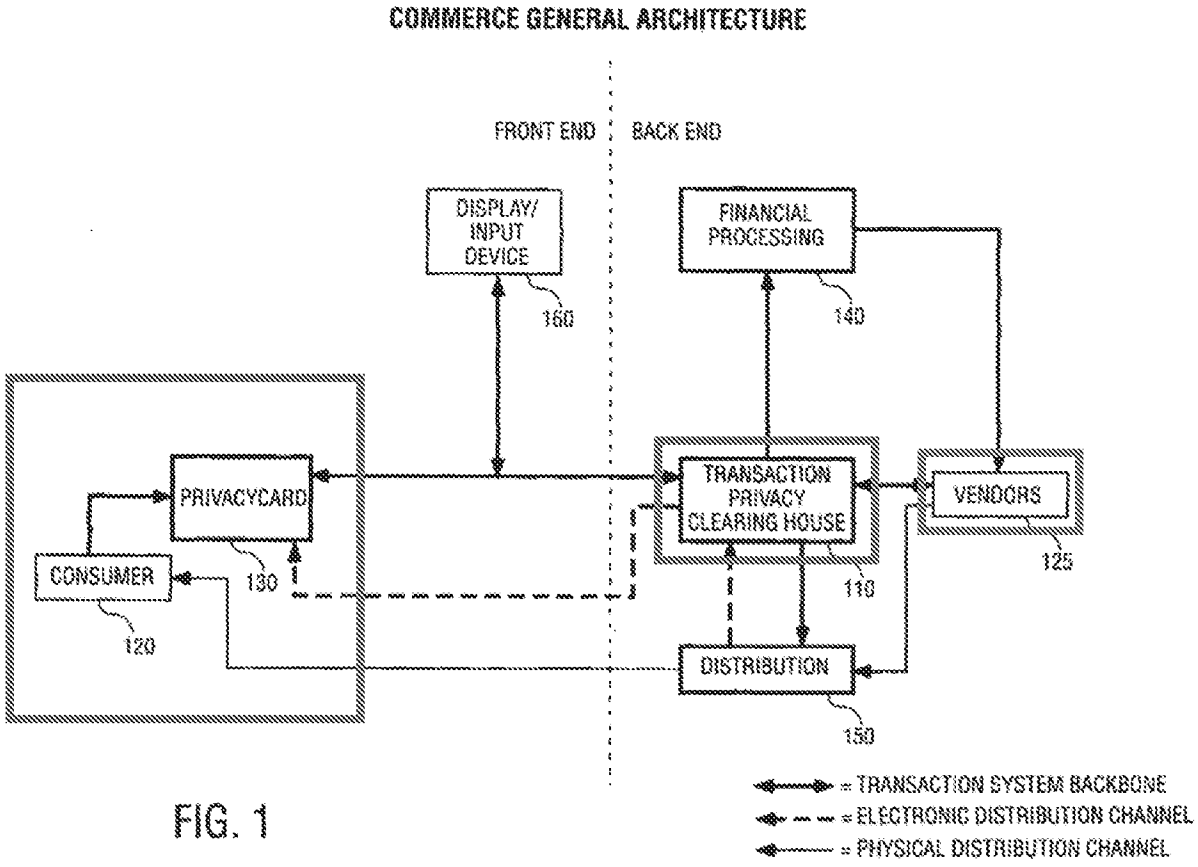


FIG. 1

Figure 1 shows one embodiment of the system in Ludtke. Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. The transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card, and digital wallet. *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a fingerprint and other biometric information.

Ludtke's transaction device includes and discloses a persistent, tamper proof storage. Ludtke also discloses the process to authenticate a financial transaction between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110, which is a third party, independent of the consumer 120 and the vendor 125. Ludtke emphasizes the third party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

The claims require storage of "secret information" in the user's device. Although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (*id.* at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (*id.* at 3:45-47; 5:30-31, 6:45-49). Scott discloses this "secret information." Specifically, Scott includes an extensive discussion regarding a secret key infrastructure. Scott discloses that the device's memory 20 also stores a private key unique to each device and used for encryption, which can be "set into memory by the manufacturer." Ex. 1008 at 11:24-30, 28:13-15, 4:14-18. Scott discloses that this "private key" used by the PID 6 is never disclosed. *Id.* at 8:21-22.

The claims also require a unique "ID code" that identifies the user's device that is communicated to the third party trusted authority for authorization of the device. Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for authorization, but Ludtke does not explicitly indicate that this "transaction device information" is unique. Scott, however, does disclose a unique ID code that identifies the PID 6. Ex. 1008 at 4:9-10 ("The memory can further 10 store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including a unique ID code that identifies the device, which may be set by the device manufacturer and can be the device serial number. *Id.* at 11:11-13. Serial numbers are unique codes that identify the devices that they are attached to. Ex. 1003 at ¶¶255-258. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32.

(b) A POSITA Would be Motivated to Combine Ludtke and Scott

The scope and content of the prior art would have motivated POSITA to combine Ludtke and Okereke. As explained above, Ludtke discloses almost all of the limitations of the claims except for "secret information" and the "unique"

nature of a device ID code. Similar to Ludtke, Scott discloses authenticating a user using a "personal identification device" (PID) for protected applications such as opening a hotel room door or a conducting a point-of-sale transaction. *Id.* at 8:5-12. Scott specifically describes a system for authentication of a mobile device to protect information for financial transactions. *Id.* at 2:5-16.

Ludtke discloses a persistent, tamper proof memory, and POSITA would have been motivated to combine the secret key disclosed in Scott with the system disclosed in Ludtke. Ex. 1003 at ¶¶259-265. The secret key infrastructure disclosed in Scott is similar to that disclosed in Okereke, as discussed above. *Id.* As discussed above, a POSITA would have already known, as of the priority date of the '905 patent, that encryption using a secret key such as that disclosed in Scott would have been obvious when communicating confidential information. *Id.* A POSITA specifically recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. *Id.* The use of secret information (such as that in PKI encryption) to perform this type of encryption was well-known ***decades*** before the filing date of the '905 patent, and was a well-established, well-known method for implementing encryption. *Id.* For example, Public Key Cryptography, which later developed into PKI encryption years before the Challenged Patents,

was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. *Id.* A POSITA recognized that such encryption is important to many applications, including financial information where it is particularly important to keep the information secret. *Id.* A POSITA would therefore recognize that the use of secret information, which is disclosed in Scott, would make the system of Ludtke even more secure. *Id.* Scott simply demonstrates this knowledge prior to the '905 patent's priority date.

Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a financial transaction. A POSITA would have combined the teachings of Scott's unique Device ID with Ludtke's system. As discussed above, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. A POSITA would have recognized that such transaction device information necessarily includes unique device identifiers such as a serial number or other number that is specific to the processing unit. Ex. 1003 at ¶¶259-265. Scott explicitly discloses this fundamental information. *Id.*

A POSITA would have been motivated to combine Ludtke and Scott because they are both in the same field of endeavor. Indeed, both references are in the same field of endeavor as the '905 patent, *i.e.*, authentication of a device,

including use of biometric information, for the purpose of exchanging sensitive information over a network. *See* Ex. 1001 at 1:21-24 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ludtke at Abstract ("A method of identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network is disclosed"); Scott at Abstract ("A portable, hand-held personal identification device (6) and method for providing secure access to a host facility…"); *id.* ¶31 ("Where absolute security is essential, some host facilities employ a biometric sensor to measure a biometric trait of a person requesting access to the host facility").

A POSITA would have reasonably expected the combination of Ludtke and Scott to succeed and yield predictable results. Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at 6:38-51. Scott similarly discloses a persistent, tamper-proof memory. Scott teaches that data is stored in a memory where, after biometric enrollment, "there is no going back or editing." Ex. 1008 at 16:11-12. Given these disclosures, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret

information in Ludtke's memory and using the unique device ID disclosed in Scott as the transaction device information. A POSITA would have expected this to yield the predictable result of the option to use secret key encryption and decryption with a private key (secret information), as well as the ability to ensure authentication of an authorized device using unique device identifying information such as a serial number, and would have expected this combination to succeed. Ex. 1003 at ¶264.

For example, Ludtke describes a protected memory to keep the type of important and sensitive information described in Okereke. Ex. 1005 at 19:37-40. Moreover, a POSITA would be familiar with the secret key encryption system because it had long been used as a way to encrypt and decrypt information and share such information only for authorized users. Implementing such a system with Ludtke would have been logical and obvious to a POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. It would make sense to a POSITA to use the type of information identified in Scott in the Ludtke system to further complement Ludtke's features. Ex. 1003 at ¶265.

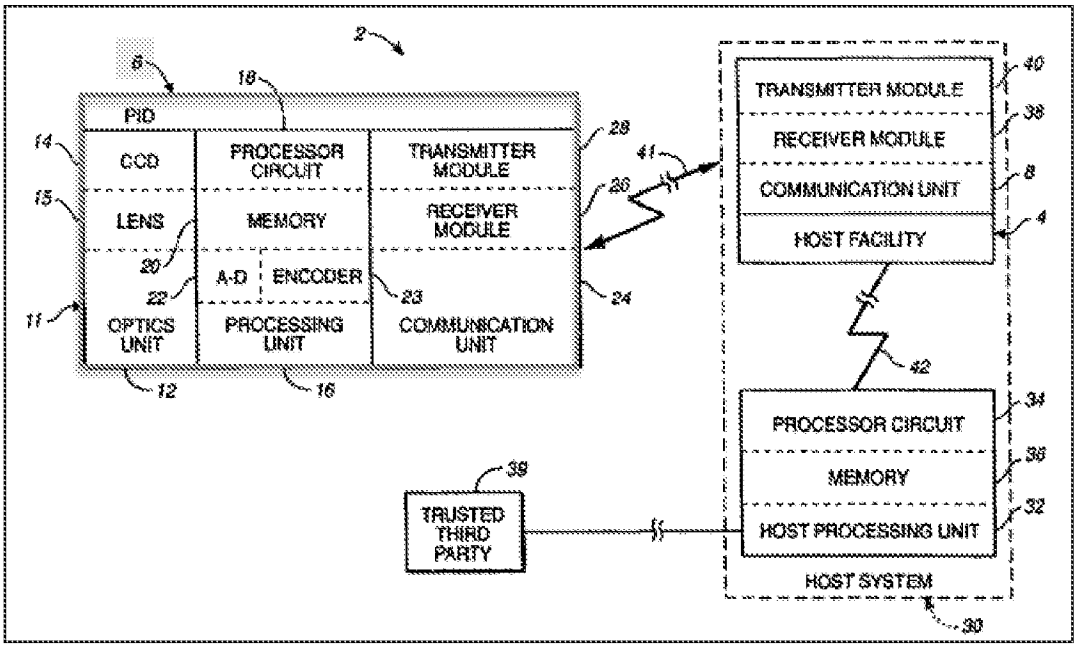
2. Claim 1

(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.a, *supra*.

As explained above in detail, a POSITA would have been motivated to combine the disclosure of Ludtke with the disclosure in Scott.

Scott also discloses a method for verifying a user during authentication of an integrated device (*e.g.*, personal identification device ("PID") 6), in order to, for example, provide secure access to protected resources such as a hotel room or a point-of-sale transaction. Ex. 1008 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12; *see* claims [1A]-[1H] *infra*.



Ex. 1008 at Fig. 1.

As explained above, Scott discloses that the memory 20 of the PID 6 persistently stores a plurality of codes and other data values including a unique ID code that identifies the PID 6. Ex. 1008 at 4:9-10 ("The memory can further store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including a unique ID code that identifies the device, which may be set by the device manufacturer and can be the device serial number. *Id.* at 11:11-13. A serial number is a unique code that identifies the device it is attached to. Ex. 1003 at ¶¶267-270. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32.

As discussed above, a POSITA would have been motivated to modify the system of Ludtke to incorporate the unique serial numbers also disclosed in Scott. Ex. 1003 ¶¶267-270; *see supra* §X.C.1. A POSITA would have been motivated to store permanent information, such as the unique device identifiers (serial number). Moreover, a POSITA would have recognized that the "transaction device information" disclosed within Ludtke could further include the unique device information in Scott, which would ensure that the information used to authenticate the device only identifies the authorized device. *Id.* A POSITA would also have stored the unique device identifiers in the persistent tamper-proof memory, because this is important information that allows authorization and sensitive communications to take place, and a POSITA would have recognized the need to take care to ensure it is not easy to tamper with and modify the information. *Id.* at ¶270.

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

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.b, *supra*. Ex. 1003 at ¶271.

(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.c, *supra*. Ex. 1003 at ¶272.

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

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.d, *supra*; Ex. 1003 at ¶273.

ID Code: Ludtke does not describe the specific "transaction device information" that is provided to the TPCH 110 and that is maintained in a secure database by the TPCH 110. Ex. 1005 at 6:36-64. However, as discussed above, a POSITA would have been motivated to combine Ludtke with the teachings of Scott, and would have recognized that the "transaction device information" would include a unique serial number, which uniquely identifies the integrated device. Ex. 1008 at 4:1-14, 5:10-21; Ex. 1003 at ¶274.

(e) [1e] "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully

authenticated the ID code, allowing the user to complete a financial transaction."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.e, *supra*; Ex. 1003 at ¶275.

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

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.3, *supra*. Ex. 1003 at ¶276.

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

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.4, *supra*. Ex. 1003 at ¶277.

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

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.5, *supra*. Ex. 1003 at ¶278.

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

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.6, *supra*. Ex. 1003 at ¶279.

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

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.7, *supra*. Ex. 1003 at ¶280.

8. **Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data."**

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.8, *supra*. Ex. 1003 at ¶281.

9. **Claim 9:**

(a) **[9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;"**

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.9.a, *supra*. Ex. 1003 at ¶282.

See also Claim 1, element [1a]. Section X.C.1.a, *supra*.

(b) **[9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against**

one or more previously registered ID codes maintained by the third-party trusted authority; and"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.9.b, *supra*. Ex. 1003 at ¶284.

See also Claim 1, elements [1c], [1d]. Section X.C.1.c, d, *supra*. Ex. 1003 at ¶285.

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

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.9.c, *supra*. Ex. 1003 at ¶286.

See also Claim 1, elements [1d], [1e]. Section X.A.1.d, e, *supra*. Ex. 1003 at ¶287.

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

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.10, *supra*. Ex. 1003 at ¶288.

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone,

tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.11, *supra*. Ex. 1003 at ¶289.

See also Claim 5. Section X.C.5, *supra*. Ex. 1003 at ¶290.

12. Claim 13:

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.12.a, *supra*. Ex. 1003 at ¶291.

See also Claim 1, elements [1a], [1d], [1e]. Section X.A.1.a, d-e, *supra*. Ex. 1003 at ¶292.

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a

comparison of the ID code received and the legitimate codes included in the list of the legitimate codes."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.12.b, *supra*. Ex. 1003 at ¶293.

See also Claim 1, elements [1d], [1e]. Section X.A.1.d-e, *supra*. Ex. 1003 at ¶294.

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

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.13, *supra*. Ex. 1003 at ¶295.

See Claim 1, elements [1b], [1c]. Section X.A.1.b-c, *supra*. Ex. 1003 at ¶296.

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

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.14, *supra*. Ex. 1003 at ¶297.

See also claim 5, section X.C.5, *supra*. Ex. 1003 at ¶298.

15. **Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a**

facial recognition, a signature recognition, and a voice recognition."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.15, *supra*. Ex. 1003 at ¶299.

See also claim 4, Section X.C.4, *supra*. Ex. 1003 at ¶300.

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

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.16, *supra*. Ex. 1003 at ¶301.

See also claim 7, Section X.C.7, *supra*. Ex. 1003 at ¶302.

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

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.17, *supra*. Ex. 1003 at ¶303.

See also claim 6, Section X.A.6, *supra*. Ex. 1003 at ¶304.

D. SNQ 4: Ludtke in combination with Scott and Robinson Renders Claims 2 and 11 Obvious

1. The proposed combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 4 relies entirely on Ludtke and Scott for the same reasons as outlined in SNQ 3, but also relies on Robinson for the limitations in dependent claims 2 and

11. Both of these dependent claims involve registering an age verification. Where Ludtke and Scott do not explicitly disclose registering an age verification, Robinson discloses the age verification in claims 2 and 11. As explained below, a POSITA would be motivated to combine the age verification disclosed in Robinson with the system disclosed in Ludtke with the secret information and unique device ID disclosed in Scott. Ex. 1003 at ¶¶305-307.

(b) A POSITA Would have been Motivated to Combine Robinson with Ludtke and Scott

The scope and content of the prior art would have motivated a POSITA to combine Robinson with Ludtke and Scott. Ex. 1003 at ¶¶308-311. Like both Ludtke and Scott, Robinson discloses a way to improve security and to authenticate a user and device. Ex. 1007 at ¶¶27-29, 32, 66-67, Fig. 1.

All three of the references are therefore in the same field of endeavor, with Robinson specifically teaching improving security with an additional age-based authorization factor and to authenticate a user for age-restricted access or transactions initiated by a wireless device like Ludtke's transaction device. Ex. 1007 at ¶9-10; Ex. 1003 at ¶¶308-311. A POSITA would have recognized that the disclosure of Ludtke welcomes this modification with its stated aim to provide, for example, secure access to restricted areas. Ex. 1005 at 2:5-8, 10:24-28. Indeed, a POSITA would have recognized that the age verification disclosed in

Robinson would, for example, allow a way for the Ludtke system to ensure that the user is old enough to conduct a transaction, access a specific financial system or application, or to enter a restricted area. Ex. 1003 at ¶310.

A POSITA would also have had a reasonable expectation of success because age verification as disclosed in Robinson is a logical extension of the type of information that is exchanged. Ex. 1003 at ¶311. Robinson, like Ludtke and Scott, also discloses the use of biometric information to verify a user. Ex. 1007 at ¶39. It would be logical to modify the system of Ludtke and Scott to also include the age of the user who was verified with biometric information. Ex. 1003 at ¶¶308-311. The age would logically be registered at Ludtke's TPCH, where the age can also be kept confidential from third parties, consistent with Ludtke's goals. *Id.*

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

Ludtke in combination with Scott disclose all of the limitations of claim 1. *See* SNQ 3, Claim 1. Section X.C.2, *supra*. Ex. 1003 at ¶312.

However, neither Ludtke nor Scott expressly disclose "registering an age verification for the user" as recited in this limitation. Robinson discloses this limitation as described in SNQ 2. *See* Section X.B.2; *see also* Ex. 1003 at ¶313.

3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the device ID code.

Ludtke in combination with Scott disclose all of the limitations of claim 9. *See* SNQ 3, Claim 9. Section X.C.9, *supra*. Ex. 1003 at ¶314.

Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 11 for the same reasons as described in conjunction with claim 2. Section X.D.2, *supra*. Ex. 1003 at ¶315.

XI. REAL PARTIES OF INTEREST

Requestor certifies that Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd. are the real parties-in-interest.

XII. CONCLUSION

For at least the reasons cited herein, the prior art references cited in this Request present substantial new questions of patentability with respect to the Challenged Claims of the '905 patent. Accordingly, the Office should declare a reexamination of these claims and reject them on at least the SNQs detailed in this Request.

DATED: June 8, 2022

Respectfully submitted,

By *__/s/ Marissa Ducca*

QUINN EMANUEL URQUHART & SULLIVAN, LLP

Marissa Ducca
Quinn Emanuel Urquhart & Sullivan, LLP
1300 I Street NW, Suite 900
Washington, DC 20005
Email: marissaducca@quinnemanuel.com
Phone: (202) 538-8000
Fax: (202) 538-8100

James M. Glass (Reg. No. 46,729)
Quinn Emanuel Urquhart & Sullivan, LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Email : jimglass@quinnemanuel.com
Phone: 212-849-7142
Fax: 212-849-7100

Attorneys for Third-Party Requestor Samsung Electronics America, Inc.