

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,

Petitioner,

v.

PROXENSE, LLC,

Patent Owner

Case No. IPR2024-01328

U.S. Patent No. 9,298,905

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	Relief Requested.....	1
II.	The '905 Patent.....	1
A.	Overview	1
III.	Claim Construction.....	3
IV.	Level of Ordinary Skill.....	4
V.	Ground 1: Claims 1, 3-7, 9-10, and 12-18 Are Obvious Over Ludtke.....	5
A.	Overview of Prior Art Ludtke	5
B.	Claims.....	8
1.	Independent claim 1	8
a.	[1preamble]: “A method comprising:”	8
b.	[1a]: “persistently storing biometric data of a legitimate user and an ID code on an integrated device”	8
c.	[1b]: “responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;”	11
d.	[1c]: “comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;”	12
e.	[1d]: “responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and”	12
f.	[1e]: “responsive to receiving an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction.”	20
2.	Claim 3: “The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code.”.....	22

3.	Claim 4: “The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.”	23
4.	Claim 5: “The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.”	23
5.	Claim 6: “The method of claim 1, wherein completing the financial transaction includes accessing an application”:	25
6.	Claim 7: “The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.”	27
7.	Independent Claim 9	28
a.	[9preamble]: “An integrated device comprising:”	28
b.	[9a]: “a persistent storage media that persistently stores biometric data of a user and an ID code”	28
c.	[9b]: “a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and”	28
d.	[9c]: “a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based n the comparison of the ID code and allowing the user to complete a financial transaction.”	30
8.	Claim 10: “The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network.”	31
9.	Claim 12: “The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.”	31

10.	Independent claim 13	32
a.	[13preamble]: “A system, comprising:”	32
b.	[13a]: “an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the ID code;”	33
c.	[13b]: “an authentication circuit that receives the [I]D code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and”	33
d.	[13c]: “the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes.”	35
11.	Claim 14: “The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code.”	35
12.	Claim 15: “The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.”	38
13.	Claim 16: “The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.”	39
14.	Claim 17: “The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.”	39
15.	Claim 18: “The system of claim 11, wherein completing the financial transaction includes accessing an application.”	39

VI.	Ground 2: Claims 2 and 11 are Obvious Over Ludtke and Kon.	39
A.	Kon	39
B.	Claims.....	44
1.	Claim 2: “The method of claim 1, further comprising: registering an age verification for the user in association with the ID code.”.....	44
2.	Claim 11: “The integrated device of claim 7, wherein an age verification is registered in association with the ID code.”	49
VII.	Discretionary Denial Is Not Warranted.....	49
A.	Discretionary Denial Is Not Warranted Under <i>Fintiv</i>	49
B.	Discretionary Denial Is Not Warranted Under <i>General Plastics</i>	50
C.	Discretionary Denial is Not Warranted under § 325(d).	51
VIII.	Mandatory Notices.....	54
A.	Real Parties-in-Interest Under 37 C.F.R. § 42.8(b)(1).....	54
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2).....	54
C.	Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	55
D.	Service Information Under 37 C.F.R. § 42.8(b)(4).....	55
IX.	Standing	55
X.	Conclusion	56

LIST OF EXHIBITS

Exhibit	Description
Ex. 1001	U.S. Patent No. 9,298,905 to Giobbi (“the ’905 patent”)
Ex. 1002	File History of U.S. Patent No. 9,298,905
Ex. 1003	Declaration of Stephen Gray (Decl.)
Ex. 1004	Curriculum Vitae of Stephen Gray
Ex. 1005	U.S. Patent No. 7,188,110 to Ludtke et al. (“Ludtke”)
Ex. 1006	U.S. Patent Application Publication No. 2002/0046336 to Kon et al. (“Kon”)
Ex. 1007	<i>Samsung Electronics America, Inc. v. Proxense, LLC</i> , IPR2021-01447, Paper 12 (PTAB Feb. 28, 2022)
Ex. 1008	<i>Proxense, LLC v. Google LLC</i> , Case No. 6:23-cv-00320, Dkt. No. 31, Scheduling Order (W.D. Tex Aug. 18, 2023)
Ex. 1009	<i>Proxense, LLC v. Samsung Electronics Co., Ltd.</i> , Case No. 6-21-cv-00210, Dkt. No. 43, Claim Construction Order (W.D. Tex. Jan. 18, 2022)
Ex. 1010	<i>Proxense, LLC v. Samsung Electronics Co., Ltd.</i> , Case No. 6-21-cv-00210, Dkt. No. 149, Memorandum in Support of Claim Construction Order (W.D. Tex. Dec. 28, 2022)
Ex. 1011	Request for Reexamination, No. 90/015,053 (June 8, 2022)
Ex. 1012	U.S. Patent Application Publication No. 2003/0023882 to Udom (“Udom”)
Ex. 1013	U.S. Patent Application Publication No. 2002/0019811 to Lapsley et Al. (“Lapsley”)
Ex. 1014	<i>Proxense, LLC v. Google LLC</i> , Case No. 6:23-cv-00320, Dkt. No. 1, Complaint (W.D. Tex. May 2, 2023)

Ex. 1015	<i>Proxense, LLC v. Google LLC, Case No. 6:23-cv-00320, Preliminary Infringement Contentions (W.D. Tex. July 24, 2023)</i>
Ex. 1016	<i>U.S. Patent Application Publication No. 2002/0049806 to Gatz et al. (“Gatz”)</i>
Ex. 1017	<i>Proxense, LLC v. Google LLC, Case No. 6:23-cv-00320, Dkt. No. 45, Proxense’s Responsive Claim Construction Brief (W.D. Tex. Dec. 1, 2023)</i>
Ex. 1018	<i>Proxense, LLC v. Google LLC, Case No. 6:23-cv-00320, Dkt. No. 45, Proxense’s Expert Transcript (W.D. Tex. Dec. 18, 2023).</i>
Ex. 1019	<i>Decision on Petition, Ex Parte Reexamination, No. 90/015,053 (January 3, 2023)</i>
Ex. 1020	<i>Order Granting Request for Ex Parte Reexamination, Ex Parte Reexamination No. 90/015,053 (Aug. 2, 2022)</i>
Ex. 1021	<i>Proxense, LLC v. Google LLC, Case No. 6:23-cv-00320, Dkt. No. 50, Proxense’s Sur-Reply Claim Construction Brief (W.D. Tex. Jan. 5, 2023)</i>
Ex. 1022	<i>U.S. District Courts—National Judicial Caseload Profile, available at https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distcomparison0930.2023.pdf (retrieved Jan. 15, 2024).</i>
Ex. 1023	Microsoft Stipulation dated August 20, 2024

I. Relief Requested

Microsoft Corporation (“Microsoft” or “Petitioner”) requests *inter partes* review of claims 1-7 and 9-18 of U.S. Patent No. 9,298,905 (“the ’905 patent”) based on the following grounds (Decl., 71-72):

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

II. The ’905 Patent

A. Overview

The ’905 patent was filed on October 23, 2014 and claims priority to provisional applications filed on December 20, 2004 and February 14, 2005. Ex. 1001, cover. The ’905 patent generally relates to “authentication responsive to biometric verification of a user being authenticated.” Ex. 1001, 1:21-24.

Figure 6 illustrates a process for “verifying a subject” using a biometric key. Ex. 1001, 7:63-65. As shown in Figure 6, the integrated device receives biometric scan data, such as a fingerprint scan, from the user (step 620). Ex. 1001, FIG. 6. If the scan data matches “previously-stored biometric data,” (step 630), the user is “verified,” at which point a “code” is sent to a trusted key authority (steps 640, 650). Ex. 1001, 7:67-8:2.

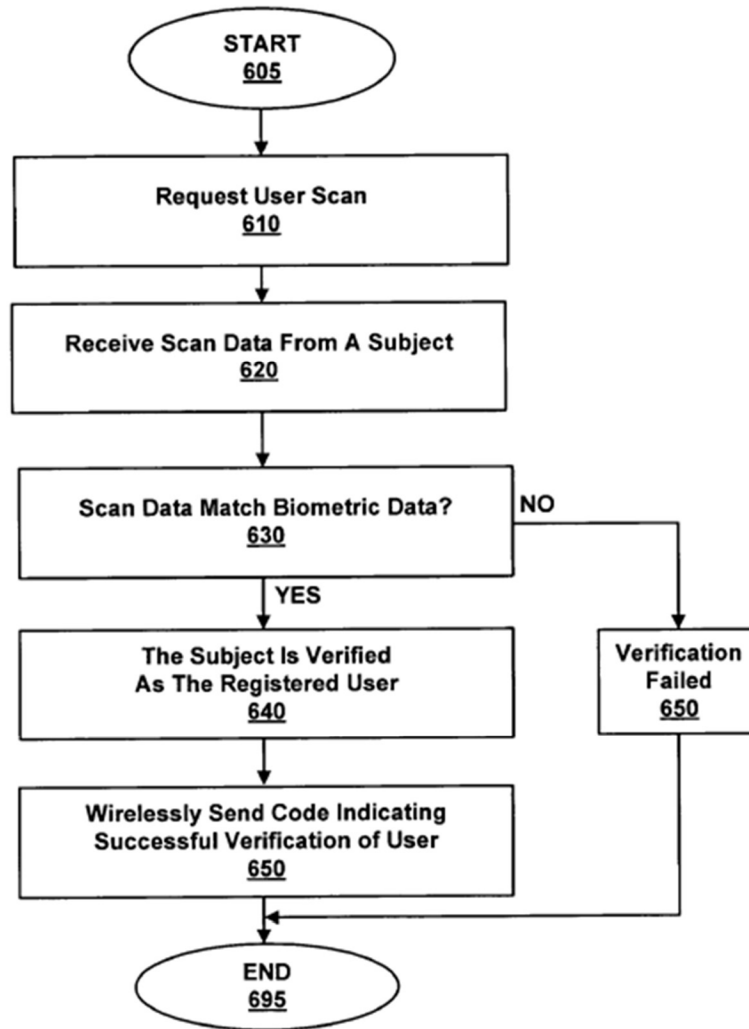


FIG. 6

Ex. 1001, FIG. 6.

Once the code is received, as illustrated in Figure 7, the trusted key authority determines whether the code is “authentic” (step 730). Ex. 1001, 8:12-18, FIG. 7. “If authentication is successful, the trusted key authority sends an access message to [an] application to allow user access and/or provide additional information from the profile” (step 740). Ex. 1001, 8:12-18. If authentication is not successful, authentication fails (step 750), and “the message to the application indicates that

the user should be denied access.” Ex. 1001, 8:18-20; Decl., 46-48.

700

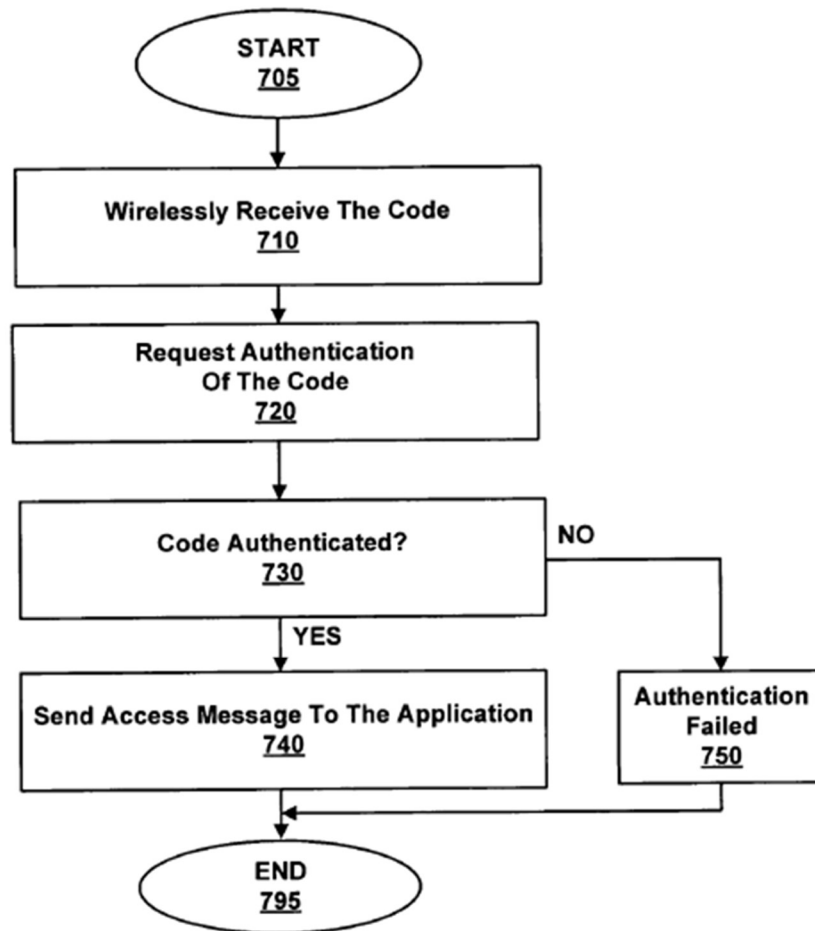


FIG. 7

Ex. 1001, FIG. 7.

III. Claim Construction

In a previous institution decision, the Board “interpreted” the term “third-party trusted authority,” as recited in the ’905 patent, “to mean a trusted authority that is an entity separate from the parties to a transaction.” Ex. 1007 at 14.

In the previous district court litigation, *Proxense, LLC v. Samsung*

Electronics Co., Ltd., Case No. 6:21-cv-00210, two terms from the '905 patent were construed by the court (Exs. 1009-1010):

- ID Code – “[a] unique code identifying a device”; and
- Access Message – “[a] signal or notification enabling or announcing access.”

Ex. 1009, 3; Ex. 1010, 15, 20; Decl., 49-53.

Because the prior art in this Petition discloses each of these prior constructions, and the plain and ordinary meaning of all terms, Petitioner submits that no claim terms need to be construed to resolve unpatentability in this Petition¹ (*Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019)).

IV. Level of Ordinary Skill

A person of ordinary skill in the art (“POSITA”) at the time of the purported invention would have had at least a bachelor’s degree in Computer or Electrical Engineering or an equivalent engineering discipline, and at least three years of experience in the field of encryption and security, or the equivalent. Decl., 31-32,

¹ Additional claim terms were construed in other proceedings relating the '905 patent, but the Board need not resolve those terms because the Grounds relied on in this petition render the challenged claims obvious under either the plain and ordinary or alternate construction.

54-56. Additional education could substitute for professional experience, and significant work experience could substitute for formal education. Decl., 55.

V. Ground 1: Claims 1, 3-7, 9-10, and 12-18 Are Obvious Over Ludtke.

A. Overview of Prior Art Ludtke

Ludtke, filed December 11, 2000, is prior art under at least 35 U.S.C. § 102(e). Ludtke, cover page. Ludtke discloses systems and methods of authorizing a user to conduct a transaction using a “biometric device” (also called a “transaction device”) such as a privacy card and/or digital wallet. Ludtke, Abstract, 3:32-36, 6:36-44. The transaction device includes a processor, memory, and fingerprint recognition technology. Ludtke, 5:60-64, FIG. 7A. Ludtke stores “authorized fingerprint recognition samples,” a device ID corresponding to the privacy card, and a public key infrastructure (“PKI”) key on the transaction device. Ludtke, 11:66-12:7, 14:19-21, 38:26-29.

When an authorized user attempts to use the transaction device, e.g., for a “shopping activity”, or other “service,” the user is “prompted to supply a fingerprint recognition sample,” as an initial security measure. Ludtke, 1:22-31, 1:37-38, 14:33-40, 18:45-50, 18:52-55. The sample is compared to stored fingerprints and if the sample is recognized, the user is authorized. Ludtke, 14:40-46.

In one embodiment, “the transaction device is used to trigger shopping

activity” such as a “web-based transaction using a transaction device such as a privacy card and/or digital wallet at a personal point of sale (“POS”) terminal” by “clicking on a ‘Buy’ or similar button in the web browser.” Ludtke, 28:26-40. The POS asks the transaction device to “validate the user” and the user is “prompted to supply a fingerprint recognition sample,” as an initial security measure. Ludtke, 1:22-31, 1:37-38, 14:33-42, 18:45-50, 18:52-55. The sample is compared to stored fingerprints and if the sample is recognized, the user is authorized. Ludtke, 14:41-46. Once the transaction device authorizes the user based on the matching biometric information, the personal POS terminal “opens a secure communications session to the TPCCH, requesting a transaction” and “provides the transaction record that it received from the web browser *and the unique ID of the transaction device.*” Ludtke, 29:5-12 (emphasis added); *see also* Ludtke, 27:12-13 (“Privacy card information is provided to TPCCH, step 1510.”), 34:25-27 (explaining that “necessary secure transaction communication with the TPCCH” includes “providing the transaction data *and its device ID.*” (emphasis added)). The TPCCH is a trusted third-party agent, separate from the transaction device, personal POS terminal, and the back-end transacting entity (e.g., vendor). Ludtke, 7:42-48, 9:26-42, FIG. 6.

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

into the digital wallet directly.” Ludtke, 28:41-45. Thus, Ludtke also discloses communicating the device ID directly from the transaction device to the TPCCH responsive to a “match” between the scanned biometric data (fingerprint) and stored data.

Next, “[t]he TPCCH uses the unique ID of the transaction device to process the transaction. After validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCCH issues a transaction confirmation back to the personal POS terminal” that “reflects the transaction confirmation back to . . . the transaction device. The transaction device may display a transaction confirmation to the user and may additionally record the transaction in its local storage.” Ludtke, 29:12-24, FIG. 15.

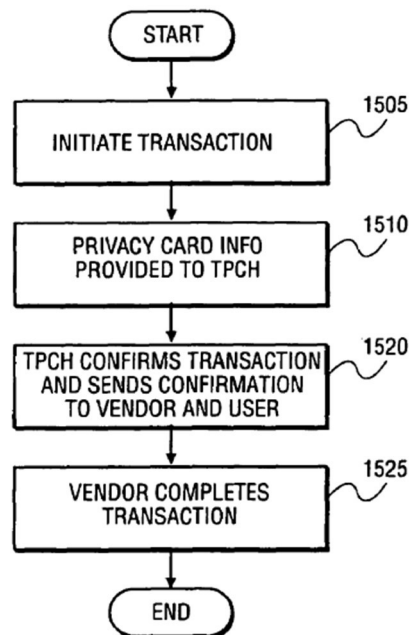


FIG. 15

Ludtke, FIG. 15.

Ludtke is analogous art to the '905 patent because it is directed to the same technical field: user authentication methods and systems. *Compare* Ex. 1001, 1:62-64, *with* Ludtke, 1:59-61. Decl., 33, 57-65.

B. Claims

1. Independent claim 1

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

To the extent limiting, Ludtke discloses [1preamble] because Ludtke discloses “[a] method of identifying an authorized user with a biometric device and enabling the authorized user to access private information” using a “transaction device” such as a privacy card and/or digital wallet (integrated device). Ludtke, Abstract, 3:32-36; Decl., 73-74.

Ludtke explains that “[t]he user connects to and performs transactions with [an] eCommerce system through a transaction device which has a unique identifier (ID)” such as “a privacy card is used” or “a digital wallet” (integrated devices). Ludtke, 3:32-36; Decl., 74.

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

Ludtke discloses [1a] because its privacy card and/or digital wallet (integrated device) stores “authorized fingerprint recognition samples” (biometric data of the legitimate user) in a “user identity/account information block 760” or

“write-once memory, or other memory that is protected from accidental modification” (persistent storage) (Ludtke, 13:27-29, 14:19-21, 19:9-14, 19:40, FIGS. 7B-7C) and a “unique transaction device ID value[]” (ID code) in its “permanent memory.” Ludtke, 30:20-23; Decl., 75-80.

The '905 defines “integrated device” as a device, such as a “mobile phone (e.g. a cellular phone or Smartphone), tablet, laptop, mp3 player, mobile gaming device, watch, key fob *or other mobile device*” “having an integrated biometric key.” Ex. 1001, 2:43-50, 4:10-16 (emphasis added). The '905 patent further describes a “biometric key” as including the elements illustrated in Figure 2, including a biometric module, a control module, and an RF module. Ex. 1001, FIG. 2, 4:42-5:64. Ludtke’s transaction devices (such as a digital wallet or privacy card) likewise includes a biometric key and constitute an integrated device consistent with this construction, as explained below. Decl., 76.

Ludtke further explains that its privacy card has a “user identity/account information block 760 [that] *stores data* about the user and accounts that are accessed by the card” including “the authorized fingerprint recognition samples.” Ludtke, 13:27-29, 14:19-21, 14:13-18 (emphasis added) (explaining that the privacy card embodied in Figure 7C “may include those functions set forth in FIG. 7b, referred to herein as first generation privacy card technology block 775 and

FeliCa² Technology block 774.”); Decl., 77.

Ludtke further explains that “[t]he fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). If confirmation succeeds, *“the device writes the fingerprint image data into write-once memory”* (persistent storage). Ludtke, 19:9-14, 19:29-40 (emphasis added); Decl., 78.

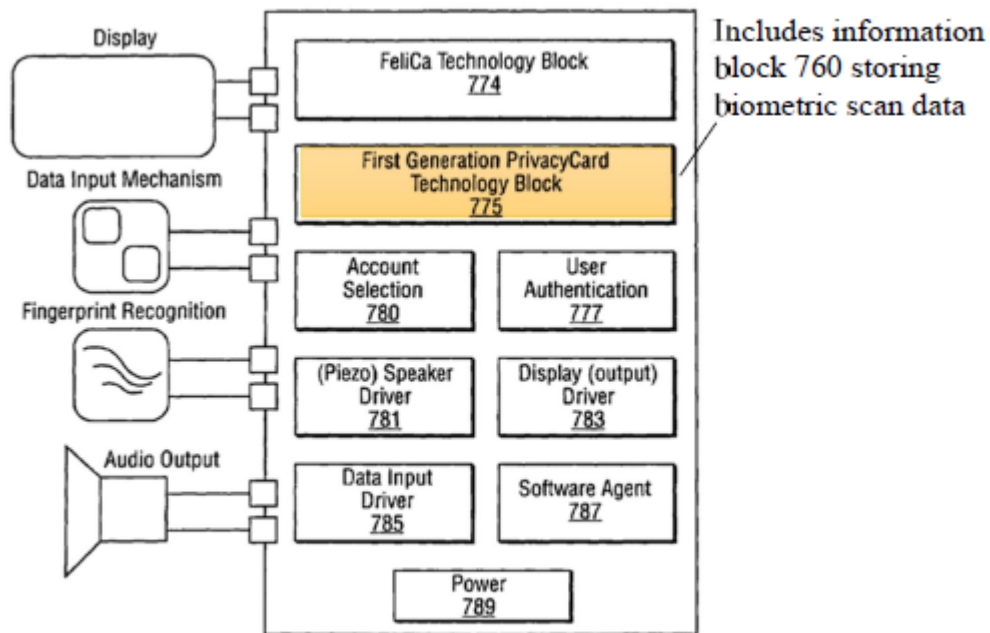


FIG. 7C

Ludtke, FIG. 7 (annotated).

Ludtke further discloses that the transaction device (integrated device) stores a “unique transaction device ID value[]” (device ID code) in its “permanent

² FeliCa is a “contactless (wireless) card execution platform.” Ludtke, 11:1-5.

memory” (persistent storage). Ludtke, 30:20-23; Decl., 79.

Ludtke’s stored device ID, like “globally unique silicon ID (GUID) 764[,] is used to identify the privacy card among other existing transaction cards,” and thus uniquely identifies the privacy card (integrated device). Ludtke, 13:39-41. The device ID is stored along with other codes and data values, e.g., magnetic stripe and bar codes, which allow the transaction device to interface with a POS terminal. Ludtke, 8:63-67, 9:18-25, 23:11-19; Decl., 80.

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

Ludtke discloses [1b] because Ludtke discloses “validating that the user interacting with the device is an authorized user” by prompting the user to “supply a fingerprint recognition sample” and receiving a fingerprint sample (scan data) from a “fingerprint recognition pad” (a biometric sensor) in response to the prompt (request for biometric verification). Ludtke, 14:33-42; Decl., 81-82.

In Ludtke, the privacy card user authentication³ block 777 “includes a biometric solution” such as a fingerprint recognition pad for “validating that the

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

user interacting with the device is an authorized user.” Ludtke, 14:33-40. In operation, “the user is prompted to supply a fingerprint recognition sample,” after which the “block captures the sample, and carries out a recognition algorithm against the authorized samples that are stored in the user identity block ... If a match is found, the user is authorized to access the data and functionality of the device.” Ludtke, 14:40-46; Decl., 82; *see also* Ludtke, 16:47-49 (explaining that the digital wallet also receives biometric scan data after prompting).

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

Ludtke discloses [1c] because, as explained for [1b], the transaction device uses a “recognition algorithm” to compare the fingerprint sample (scan data) “against the authorized samples that are stored in the user identity block” (biometric data) to determine “a match.” Ludtke, 14:40-46; Decl., 83.

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

Ludtke discloses or renders obvious [1d] because Ludtke discloses transferring (sending) the transaction device ID (ID code) to a “single trusted” and “highly secured” transaction processing clearing house (TPCH) (third-party trusted authority) for validation/confirmation using e.g. “wireless or cellular signals”

(wirelessly) once a fingerprint match is identified. Ludtke, 5:63-64, 7:46-48, 9:26-30, 9:35-42, 9:51-59, 28:50-29:12, 30:23-27; Decl., 84-97.

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

In one embodiment, “the transaction device is used to trigger shopping activity” such as a “web-based transaction using a transaction device such as a privacy card and/or digital wallet and a personal POS terminal,” “the user may tap on an on-screen icon being displayed by the transaction device, e.g., digital wallet; and the digital wallet transmits a signal,” which “causes” a “web browser” for purchasing desired content “to launch.” Ludtke, 28:15-18, 28:26-40. “Once a transaction has been triggered, the browser communicates with the personal POS terminal, requesting it to initiate a transaction” and “provides a transaction record, which includes all of the necessary data to support th[e] transaction, including a list of items being purchased, unit cost and quantity, the vendor who will provide the items, etc.” Ludtke, 28:13-18, 28:50-56; Decl., 86.

The POS asks the transaction device to “validate the user” and the user is “prompted to supply a fingerprint recognition sample,” as an initial security measure. Ludtke, 1:22-31, 1:37-38, 14:33-42, 18:45-50, 18:52-55, 28:57-62. The sample is compared to stored fingerprints and if the sample is recognized, the user

is authorized. Ludtke, 14:41-46. After the transaction device receives the fingerprint recognition sample “*to confirm [an] entire transaction and that the user is authorized,*” the personal POS terminal “opens a secure communications session to the TPCCH, requesting a transaction” and “provides the transaction record that it received from the web browser *and the unique ID of the transaction device.*” Ludtke, 28:50-29:12 (emphases added); Decl., 87; *see also* Ludtke, 27:12-13 (“Privacy card information is provided to TPCCH, step 1510.”), 34:25-27 (explaining that “necessary secure transaction communication with the TPCCH, providing the transaction data *and its device ID.*”) (emphasis added).

The “confirmation that the user is authorized” is based on the match between the scan data and stored data as explained for [1b] and [1c]. Ludtke, 14:40-46. *See also* Ludtke, 4:62-5:1 (“The transaction device enhances security by authenticating the user of the card *prior to usage* such that if a card is lost or stolen, it is useless in the hands of an unauthorized person ... [A]uthentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g., fingerprint recognition).”) (emphasis added); Decl., 88.

Ludtke also discloses an alternate embodiment in which the POS “functionality of providing secure communication and transactions with the Transaction Privacy Clearing House (TPCH),” described above, “can be integrated into the digital wallet directly.” Ludtke, 28:41-45. Thus, Ludtke also discloses

communicating the device ID directly from the transaction device to the TPCCH responsive to a “match” between the scan data and stored data. Decl., 89.

Second, Ludtke discloses sending the transaction device ID wirelessly. Decl., 90. Ludtke discloses that “the TPCCH is located at a secure location” and “embodied as a secure server.” Ludtke, 9:26-34. The TPCCH receives incoming communications, including the transaction ID, using an “incoming communications mechanism 605” using “wireless or cellular signals.” Ludtke, 9:35-42; Decl., 90.

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

As Ludtke explains with respect to Figure 6, the TPCCH is an entity separate from the parties to a transaction (third party) because it is distinct from the transaction device, the POS on which the user/transaction device is performing a transaction, and the “*external* retailers and vendors” that complete the transaction. Ludtke, 9:35-39 (emphasis added), FIG. 6. Indeed, as Ludtke explains, “The incoming communications mechanism 605 and outgoing communications mechanism 610 are the means of communicating with *external* retailers and vendors, as well as the transaction device.” Ludtke, 9:35-39 (emphasis added). That the vendors and transaction device are “external” to the TPCCH confirms that

the TPCCH is a third party, and not a party to the transaction itself. Decl., 92.

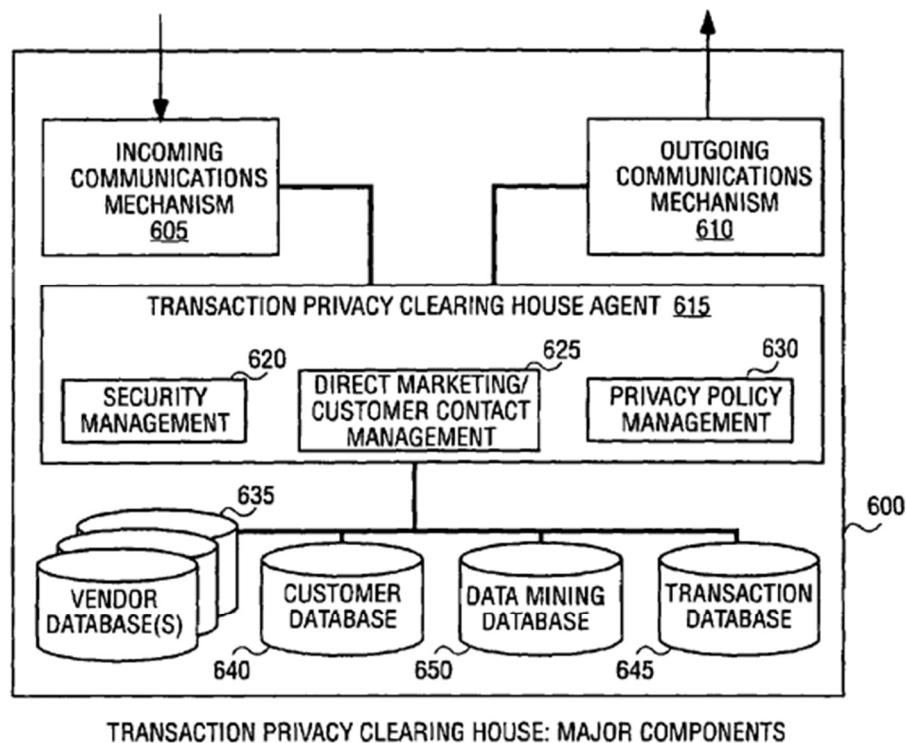


FIG. 6

Ludtke, FIG. 6.

This is consistent with Patent Owner's previous "agree[ment] that at a 'third-party trusted authority' is *an institution or entity that is outside of the multi-party system (user and application or vendor)* that is being authenticated" and the Board's construction that "third-party trusted authority" is a "trusted authority that is an entity separate from the parties to the transaction," and one that is "separate from the principal parties to a transaction." Ex. 1007, 13-15 (emphases added).

Indeed, the Board differentiated the prior art cited in the prior IPR2021-01447 because the purported third party authority was not a third party at all, stating “the DPC is the resource to be accessed, *but it is a party to the transaction, rather than a third party.*” Ex. 1007, 24; Decl., 93.

Here, to the extent Patent Owner raises any argument that the TPCCH of Ludtke is similar to the mapping in the prior IPR, Patent Owner is wrong, particularly because Ludtke expressly identifies the TPCCH as external to the parties to the transaction, capable only of communication with the parties, as explained above. That the TPCCH is capable in certain embodiments of settling funds does not make it a “party” to the transaction because it remains independent of the user, POS, and “external” vendors. Moreover, Ludtke expressly discloses that the TPCCH “may issue a funds settlement request to a third party financial institution on behalf of the user, causing the necessary funds to be transferred to the vendor from the user’s account” thus further confirming that the TPCCH is not the vendor/retailer, or even the user’s financial institution from which funds are withdrawn (not a principal party to the transaction, and therefore a third party). Ludtke, 29:43-46; Decl., 93.

Ludtke further discloses that the separation between the TPCCH, vendors, and the POS on which the user/transaction device is performing a transaction “ensures secure communications among the components internal to the TPCCH 600 and the

entities external to the TPOCH 600” and “ensures that only authorized entities are allowed access to data and that only authorized transaction devices can execute transactions against a user's account” thereby allowing the TPOCH to function “as the middleman of the distribution channel.” Ludtke, 7:44-48, 9:26-30, 9:43-59. Accordingly, the TPOCH is a third-party trusted authority. Decl., 92.

The TPOCH includes various databases for storing the transaction ID and linking the user to the transaction ID. Ludtke, 10:15-22, 10:40-45, 33:37-41. For example, the “customer database” “holds information regarding each customer of the TPOCH” and links the “actual user identity information” to “the digital aliases provided by the transaction device,” i.e., the transaction device ID. Ludtke, 10:15-19, 33:39-42 (“the transaction device acts as a digital alias for its user”). The “transaction database” maintains transaction records that include the transaction device ID. Ludtke, 10:19-22, 10:40-45, 33:37-41 (“Whenever the user carries out a transaction using the system, vendors receive only the transaction device ID *in the transaction record.*”) (emphasis added); Decl., 94.

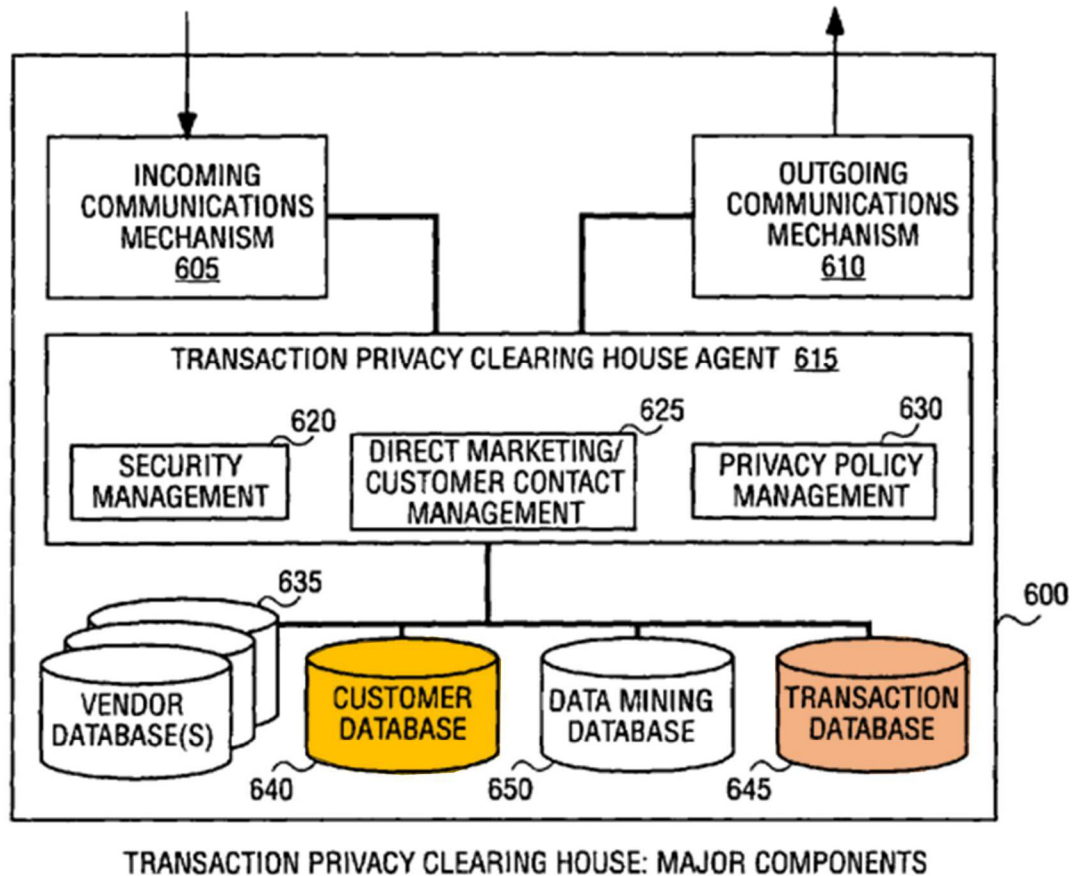


FIG. 6

Ludtke, FIG. 6 (annotated).

Ludtke further discloses that the TPCCH can “maintain a copy” of “unique transaction device ID values” so that “whenever a transaction arrives with one of these values, the TPCCH knows *which transaction device*, and hence which user, the transaction it associated with.” Ludtke 30:23-27 (emphasis added). Thus, Ludtke discloses storing device ID codes. Decl., 95.

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

To the extent this is disputed, a POSITA would have been motivated and found it obvious to configure the TPOCH to compare the received transaction device ID to the stored transaction device ID to ascertain which customer is requesting the transaction, whether “the transaction device is in good standing[,]” and whether the “selected account” associated with the transaction ID “has sufficient funds for the transaction.” Ludtke, 29:12-18, 30:23-27; Decl., 97.

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

Ludtke discloses [1e] because after the TPOCH authenticates the transaction device ID (ID code), the transaction device receives an indication of “approval of the transaction to be performed” (access message indicating that the third-party trusted authority successfully authenticated the ID code) from the TPOCH, which allows the user to complete a “purchase” or “shopping activity” (financial

transaction). Ludtke, 6:36-44, 28:26-31, 28:50-62, 29:5-23; Decl., 98-100.

As explained for [1d], the personal POS terminal “opens a secure communications session to the TPCCH, requesting a transaction” and “provides the transaction record that it received from the web browser *and the unique ID of the transaction device.*” Ludtke, 28:50-29:12. The TPCCH (third-party trusted authority) “*uses the unique ID of the transaction device to process the transaction*” to validate the transaction device and confirm that “the selected account has *sufficient funds* for the transaction.” Ludtke, 29:12-15 (emphases added). Once validated, the TPCCH “issues a transaction confirmation” (access message) “back to the personal POS terminal” where it is then reflected “*back to the web browser and the transaction device*” and displayed to the user. Ludtke, 29:15-23 (emphases added); Decl., 99.

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

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

Ludtke discloses claim 3. Decl., 101-104.

As explained for [1d], when the “personal POS terminal receives the transaction request, it communicates with the transaction device, *asking the transaction device to validate the user*, confirm that the user wants to make this transaction, and get the appropriate information for which account the user wants to use for payment.” Ludtke, 28:57-62 (emphasis added); Decl., 102.

Upon receiving the request, the transaction device “validat[es] that the user interacting with the device is an authorized user” by prompting the user to “supply a fingerprint recognition sample” and receiving a fingerprint sample (biometric scan) from the “fingerprint recognition pad” in response to the prompt to generate the scan data. Ludtke, 14:33-42; [1c], *supra*. The transaction device user authentication block “captures the sample, and carries out a recognition algorithm against the authorized samples that are stored in the user identity block.” Ludtke, 14:40-46. Then, “[i]f a match is found, the user is authorized to access the data and functionality of the device” and “validates that the user is authorized” to conduct their transaction at the POS terminal. Ludtke, 14:40-46, 29:5-6; Decl., 103; *see also* Ludtke, 16:47-50 (explaining that the digital wallet also receives biometric scan data after prompting).

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

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

Ludtke discloses claim 4 because its biometric data expressly includes a “fingerprint” as well as a “retinal scan, voice, DNA, hand profile, face recognition, etc.” Ludtke, 35:61-64; Decl., 105.

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

Ludtke discloses or renders obvious claim 5. Decl., 106-111.

Ludtke explains that the “transaction device is an interactive device with communications capabilities” that allows it to receive “messages via the TPCP in a

variety of ways, including wireless, Internet, a pager system, cellular, etc.” Ludtke, 33:46-49, 17:3-10. The transaction device is also configured to allow the user to “directly” “view and respond to messages” and further includes conventional computing circuitry, such as a processor, memory, and “instructions” for execution. Ludtke, 33:49-54, 11:66-12:7, 15:65-16:8, FIGS. 7A and 9A. Moreover, Ludtke expressly discloses the transaction device having “pager or cell phone functionality built-in.” Ludtke. 17:65-18:4; Decl., 107.

A POSITA reading Ludtke would have found the structural and functional configurations of the disclosed portable transaction device—especially its cellular and wireless adoptions to be at least suggestive of a tablet or mobile phone. Decl., 108 (citing Ludtke, 9:39-41 (explaining that transaction devices may operate on “cellular signals”), 26:56-57 (“The personal POS terminal may be configured to be mobile, such that the user may take it out of the home environment.”). Indeed, because the ’905 patent does not specify the precise nature of the mobile phone or tablet, a POSITA would have understood that a transaction device having “built in” “cell phone functionality” *is* a mobile phone Decl., 108.

To the extent this is disputed, a POSITA would have been motivated and found it obvious to implement the transaction device as a mobile phone to enable the user to safely conduct financial transactions (e.g., purchases) using a single device. Decl., 109. Furthermore, it was known in the art at the time of the

invention to implement biometric security features on a mobile device for financial transactions. Decl., 110 (citing Udom, Abstract, [0014], [0032]-[0033] (describing a “process of verifying an individual’s identity and authorizing that person to have access to a secure resource (e.g., a bank account . . .) [where] the software within the CPU 104 compares data from the sensor 106 that represents a scanned biometric characteristic, to either data or data templates stored for various individuals in memory 105” and “processor 104 might just as well be comprised of a cellular telephone.”); Lapsley, Abstract, [0024] (describing “biometric authorization of an electronic transaction between a consumer and a merchant us[ing] an electronic identicator and an access device” where “the access device may be a wireline telephone, a wireless telephone, a two-way pager, a personal digital assistant, or a personal computer.”)).

Thus, A POSITA would have reasonably expected implementing Ludtke’s transaction device as a mobile phone to succeed because Ludtke already contemplates using the transaction as a “cell phone” and such implementations were established in the art. Ludtke, 17:65-18:4; Decl., 111.

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

Ludtke discloses claim 6 because completing the purchase (financial transaction) includes accessing a financial account (application) by determining whether the user’s account has “sufficient funds” and transferring the appropriate

amount from the user's account to the vendor. Ludtke, 29:15-18, 29:29-36; Decl., 112-114; *see also* Ex. 1001, 6:20-26 (defining "application" as "resource that can be accessed by a verified and authenticated user" and identifying "a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.)" as one type of application.

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

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

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

Ludtke discloses claim 7 because, as explained for claim 6, completing the purchase (financial transaction) includes determining whether the user’s account has “sufficient funds” and transferring the appropriate amount from the user’s account to the vendor (accessing a financial account). Ludtke, 29:15-18, 29:29-36; Decl., 115-116. *See also* Ludtke, 5:49-52 (“The transaction device may represent a single account such as a particular credit card, or it might represent multiple accounts such as a *credit card*, telephone card and *debit card*.” (emphasis added)).

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

funds. Decl., 116.

7. Independent Claim 9

a. [9preamble]: “An integrated device comprising:”

Ludtke discloses [9preamble] because, as explained for [1preamble] and [1ai], Ludtke discloses “a biometric device” (also called a transaction device), such as a privacy card and/or digital wallet, for “enabling the authorized user to access private information over a voice network.” Ludtke, Abstract, 3:32-36. Decl., 117.

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

Ludtke discloses [9a] for the same reasons explained for [1a]. Decl., 118.

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

Ludtke discloses or renders obvious [9b] for the same reasons explained for [1d]. Decl., 119-122.

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

that “*stores data* about the user and accounts that are accessed by the card” including “the authorized fingerprint recognition samples”) to “carr[y] out a recognition algorithm against the authorized samples that are stored in the user identity block.” Ludtke, 13:27-29, 14:19-21, 14:40-46 (emphasis added); [1a] and [1c], *supra*; *see also* Ludtke, 16:47-49 (explaining that the digital wallet also receives biometric scan data after prompting). Finally, “[i]f a match is found, the user is authorized to access the data and functionality of the device.” Ludtke, 14:45-46; Decl., 120.

Once the user/transaction device is verified (fingerprint match identified), the transaction device ID (ID code) is wirelessly sent to a “single trusted” and “highly secured” TPCCH (third-party trusted authority) using e.g., input/output logic that “enable[s] the privacy card to send and receive information” using “wireless or cellular signals,” or (in the case of a digital wallet) a “wireless transmission driver” that uses the same wireless technology. Ludtke, 5:63-64, 7:46-48, 9:26-30, 9:35-42, 9:51-59, 12:10-16, 17:3-4, 28:50-29:12, 30:23-27; Decl., 121. This is consistent with the ’905 patent which does not explain how a validation module communicates a code, but does explain that an RF module wirelessly sends a code to the trusted authority. Ex, 1001, 5:49-52, 8:2-4; Decl., 121.

The TPCCH uses the received transaction device ID to confirm/validate that the transaction device is in “good standing” by ensuring that the received device ID

matches an ID maintained in e.g. its customer database (comparing the received ID with stored IDs), as explained for [1d]. Decl., 122.

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

Ludtke discloses [9c] because the transaction device receives an “approval of the transaction to be performed” (access message) from the TPCCH via its “cellular” “wireless communication mechanism” (radio frequency communication module) after the code is authenticated (based on the comparison of the ID code). Ludtke, 5:63-64, 6:36-44, 9:39-42, 17:3-10, 29:5-23, 29:29-30, 31:11-52 33:46-49; Decl., 123-125.

As explained for [1e], the transaction device receives an indication of “approval of the transaction to be performed” (access code) from the TPCCH after the code is authenticated (based on the comparison of the ID code), and the approval allows the user access to the application to complete their purchase at the POS (financial transaction). Ludtke, 6:36-44, 28:26-31, 28:50-62, 29:5-23; Decl., 124. In one embodiment, the TPCCH “issues a transaction confirmation” (access message) “back to the personal POS terminal” where it is then reflected “*back to the web browser and the transaction device*” and displayed to the user. Ludtke,

29:15-23 (emphases added). Alternatively, where the communication functions of the POS are integrated into the transaction device, the confirmation may be delivered to the transaction device. Ludtke, 28:41-45; Decl., 124.

Ludtke further discloses that the transaction device uses a “wireless communication mechanism for input and output,” including for receiving “cellular signal” communication output from the TPOCH. Ludtke, 5:63-64, 9:39-42, 17:3-10, 33:46-49. Because the transaction device communicates using cellular technology, a POSITA would have understood that the mechanism performing the wireless communication is a radio frequency communication module. Decl., 125.

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

Ludtke discloses claim 10. Decl., 126-127.

As explained for [1e], the device ID and other codes are sent to the external TPOCH server over a wireless network connection using e.g. “wireless or cellular signals.” Ludtke, 9:35-42, 5:63-64 (“Furthermore, the privacy card may have a wireless communication mechanism for input and output.”) Decl., 127.

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

Ludtke discloses or renders obvious claim 12 for the same reasons explained for claim 5. Decl., 128.

below. Decl., 130.

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

Ludtke discloses [13a] for the same reasons explained for [1a] and [1d].

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

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

Ludtke discloses [13b] because the system includes a POS terminal (authentication circuit) that (1) receives the transaction device ID from the transaction device, (2) sends the transaction ID to the TPC (third-party trusted authority) for authentication, and (3) receives an approval (access message) from the TPC indicating that the ID was authenticated allowing the user to complete a purchase (financial transaction). Ludtke, 28:50-29:12; Decl., 132-134.

Ludtke describes an exemplary transaction performed utilizing the disclosed

system and illustrated in Figure 17, wherein “the transaction device is used to trigger” a “purchase” such as a “shopping activity” and a POS (authentication circuit) “initiates the transaction.” Ludtke, 28:11-18, 28:22-23, 28:26-31, 28:50-52. “When the personal POS terminal receives the transaction request, it communicates with the transaction device, asking the transaction device to validate the user, confirm that the user wants to make this transaction, and get the appropriate information for which account the user wants to use for payment.” Ludtke, 28:57-62. Then, the “POS terminal opens a secure communications session to the TPCCH” (third-party trusted authority) and “*provides the transaction record that it received from the web browser and the unique ID of the transaction device.*” Ludtke, 29:6-12 (emphasis added). Thus, Ludtke discloses receiving the device ID and providing the device ID to a third-party trusted authority. Decl., 133.

“The TPCCH uses the unique ID of the transaction device to process the transaction” and “[a]fter validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCCH issues a transaction confirmation” (access message indicating that the third-party trusted authority successfully authenticated the ID code) “back to the personal POS terminal” which allows the user to complete the purchase (financial transaction).

Ludtke, 29:12-23; [1e], *supra*; Decl., 134.

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

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

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

Ludtke discloses claim 14. Decl., 136-143.

As explained for [1b] and [13b], the transaction device (integrated device) receives a validation request from the POS terminal (authentication request from the authentication unit) and prompts the user to scan their fingerprint (requests a biometric scan) to validate the user. Ludtke, 14:33-41, 28:57-62; Decl., 137.

For example, when the “personal POS terminal receives the transaction request, it communicates with the transaction device, *asking the transaction device to validate the user*, confirm that the user wants to make this transaction, and get the appropriate information for which account the user wants to use for payment.” Ludtke, 28:57-62 (emphasis added); [1e], *supra*. Upon receiving the request, the transaction device “validat[es] that the user interacting with the device is an authorized user” by prompting the user to “supply a fingerprint recognition sample” and receiving a fingerprint sample (biometric scan) from the “fingerprint recognition pad” in response to the prompt to generate the scan data. Ludtke, 14:33-42; [1c], *supra*. More specifically, the transaction device user authentication block “captures the sample[] and carries out a recognition algorithm against the authorized samples that are stored in the user identity block.” Ludtke, 14:40-46; Decl., 138.

Then, “[i]f a match is found, the user is authorized to access the data and functionality of the device” and “validates that the user is authorized” to conduct their transaction at the POS terminal. Ludtke, 14:40-46; 29:5-6; Decl., 139; *see also* Ludtke, 16:47-49 (explaining that the digital wallet also receives biometric scan data after prompting).

A POSITA would have understood that the transaction device does not send the one or more codes if it cannot verify the scan data is from the user because the

biometric scan data “is used as a security mechanism that limits access to the card 705 to authorized users” and the user is only authorized/validated “[i]f a match is found” between the scan data and “stored” “authorized samples.” Ludtke, 12:23-25, 14:40-46; Decl., 140. Indeed, a transaction device that cannot be authenticated/validated as being from the user is “useless.” Ludtke, 4:62-5:1; *see also* Ludtke, 39:50-56 (“At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. *If a match does not occur, then at 3110 an error message is output* and the DW returns to checking to see if a fingerprint has been detected 3104.”) (emphasis added); Decl., 140.

To the extent this is disputed, a POSITA would have been motivated and found it obvious to configure the transaction device to not send the one or more codes and other data values if the transaction device (integrated device) cannot verify the scan data as being from the user, to prevent unauthorized use of the transaction device when “lost or stolen.” Ludtke, 4:62-5:1, 18:23-31; Decl., 141.

A POSITA would also have been motivated to not send the one or more codes and other data values if the transaction device (integrated device) cannot verify the scan data as being from the user for network efficiency reasons. Decl., 142. Because there would be no reason to send a message when the data is not

verified, foregoing the potentially unnecessary message would conserve processing resources of the device and transmission resources of the network. Decl., 142.

Such a modification would have been within the purview of one skilled in the art, and would have only required the use of known conventional components in accordance with their known use—for example, configuring Ludtke’s authorization block to output an “error” or “authentication failure” message upon failing to detect a fingerprint match, as was well known in the art. *See e.g.*, Ludtke, 39:50-56; Kon, [0007]-[0010] (describing “a conventional process of identifying a person using biometric information” wherein a comparator transmits an “authentication failure message” “[i]f it is determined that the input data does not match with the registered information.”); Decl., 143. Accordingly, a POSITA would have been motivated to make such a modification and had a reasonable expectation of success in doing so. Decl., 143.

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

Ludtke discloses or renders obvious claim 15 for the same reasons explained for claim 5. Decl., 144.

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

Ludtke discloses claim 16 for the same reasons explained for claim 4. Decl.,
145.

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

Ludtke discloses claim 17 for the same reasons explained for claim 7. Decl.,
146.

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

Ludtke discloses claim 18 for the same reasons explained for claim 6.
Decl.,147.

VI. Ground 2: Claims 2 and 11 are Obvious Over Ludtke and Kon.

A. Kon

Kon, filed August 31, 2001 and published April 18, 2002, is prior art under 35 U.S.C. § 102(b). Kon, cover page.

Kon discloses systems and methods for authenticating a user transaction “in response to a request from a user device.” Kon, [0174]. Like Ludtke, Kon uses the user’s biometric information, which includes “fingerprint information, retina

pattern information, iris pattern information, voice print information, and handwriting information” and “the ID of a user device” (device ID) to authorize a user and their corresponding device to conduct a transaction. Kon, [0060], [0173], [0178], [0194] (explaining that a public key certificate (“PKC”) includes the ID of the user device), [0226]-[0229] (explaining that a person identification certificate (“IDC”) includes the PKC).

The information may be stored in an IDC, illustrated in Figure 5. Kon, FIG. 5, [0194] (explaining that the PKC “**Subject**” field includes the ID of the user device), [0217] [0026]-[0229] (explaining that the IDC includes “**Subject Template Info**” where “data representing biometric information such as a fingerprint of the user is stored,” and “**Subject PKC Info**” containing the PKC information).

FIG. 5

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

Kon, FIG. 5 (annotated, excerpted).

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

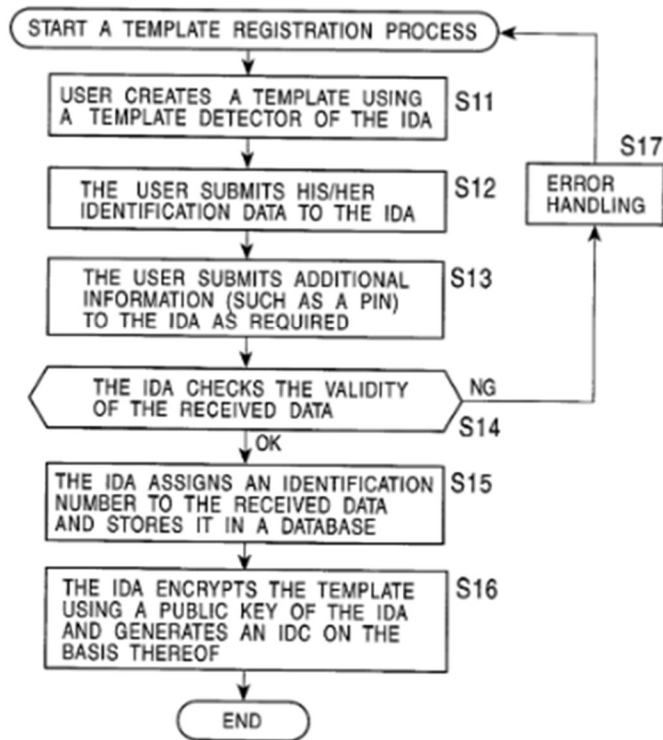
supplies services is described” (emphasis added)), [0234] (“[A]n arbitrary attribute of [a] user, such as an *age*, sex, address, [or] telephone number, is encrypted *as required to identify the user.*” (emphases added)), [0241] (“The person identification certificate (IDC) described above includes information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

FIG. 5

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

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

FIG. 9



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

Kon is analogous art to the '905 patent because it is directed to the same technical field: user authentication methods and systems. *Compare* Ex. 1001, 1:62-64, *with* Kon, [0020], [0034]. Decl., 66-70.

B. Claims

- 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 Kon renders obvious claim 2. Decl., 148-154.

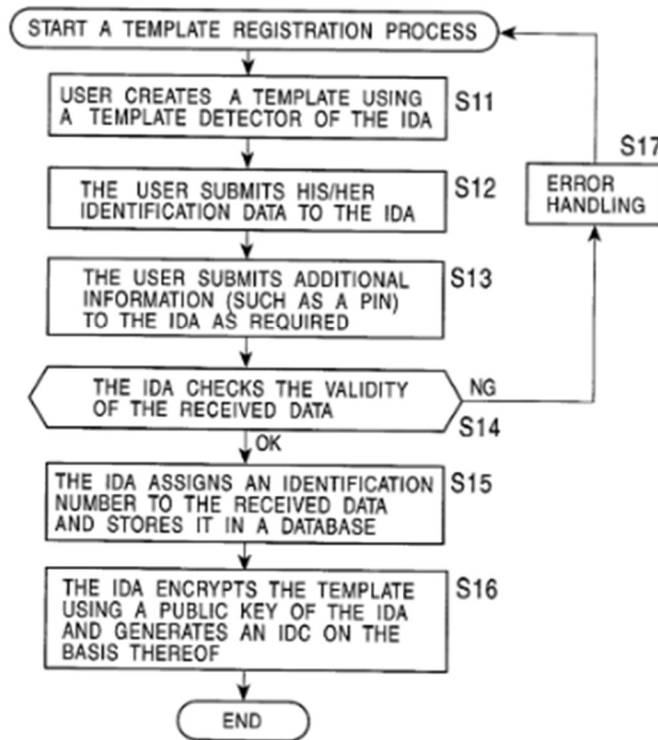
Kon discloses registering and storing a user's personal information, including the user's age, in association with the user device's device ID—the user's device ID is stored in a “Subject” field and the user's age is stored in a “Directory Attribute” field of a registered IDC certificate. Kon, [0194] (“Subject is a field in which the name of a subject or a user is described . . . , for example, *the ID of a user device* or the ID ”) (emphasis added), [0234] (“[A]n arbitrary attribute of a[] user, such as an age, sex, address, [or] telephone number, is encrypted as required to identify the user.”), [0265] (“FIG. 9 illustrates a flow in terms of registration of a template and creation of an IDC. Registration of a template is performed on the basis of information (sampling information) acquired using an apparatus capable of acquiring personal information in one of the various forms described earlier.”), FIGS. 5, 9; Decl., 150.

FIG. 5

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

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

FIG. 9



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

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

license, and a card.” (emphasis added)). Thus, Kon discloses registering the user’s age verification in association with the user’s device ID. Decl., 151.

The user’s age, like the biometric information, provides another data point for identifying the user (Kon, [0241]); thus, a POSITA would have understood the benefit of using age as an identifying data point for authentication. Decl., 152. Indeed, a POSITA would have considered age to be an especially useful identifier where, for example, a service or transaction implicates an age minimum (e.g., purchasing alcohol, cigarettes, or other age-restricted shopping content). Decl., 152-153 (citing Ex. 1016, [0005] (“As particular types of information or images contained in this uncontrolled information collection may not be suitable for certain users, it may be desirable to selectively restrict access to WWW resources.”), [0078] (noting that if an account is designated to a child, it may be restricted from accessing “age-restricted shopping content” or require verification “that the associated account can access such shopping content”), [0082] (describing the need to control access to certain services, and explaining that age may be used to restrict user access); FIG. 14 (showing a user interface for accessing age-restricted shopping content))).

Accordingly, a POSITA would have been motivated and found it obvious to register the user’s age in association with the device ID of Ludtke to facilitate age prohibitive transactions. Decl., 154 (citing Ex. 1016).

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

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

VII. Discretionary Denial Is Not Warranted

A. Discretionary Denial Is Not Warranted Under *Fintiv*

In *Apple Inc. v. Fintiv, Inc.*, the Board enumerated six factors to determine whether a petition should be discretionarily denied institution under §314(a). IPR2020-00019, Paper 11 at 2-3 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv*”). In June 2022, the USPTO issued updated discretionary denial guidance in view of the *Fintiv* factors and expressly noted that ***the PTAB will not discretionarily deny institution if Petitioner presents a Sotera stipulation.*** Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (USPTO June 21, 2022) (“Director’s Guidance”), 3, 7-8. Here, Petitioner has eliminated any risk of duplicated effort by voluntarily presenting a *Sotera* stipulation to Patent Owner. Ex-1023; *Sotera Wireless, Inc. v. Masimo Corp.*, Case IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020). For at least this reason, the Board should not discretionarily deny this petition.

B. Discretionary Denial Is Not Warranted Under *General Plastic*

The *General Plastic* factors weigh in favor of institution. *Gen. Plastic Indus. Co. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 (PTAB Sept. 6, 2017).

IPR2021-01447 (“the Samsung IPR”) does not preclude institution because Petitioner was not a party to the Samsung IPR and does not have a “significant relationship” with Samsung. This IPR relies on Grounds that were not presented in the Samsung IPR and was diligently prepared by Petitioner after Patent Owner filed a complaint in the Western District of Texas accusing Petitioner of infringing the ’905 patent in May 2023.

Factor 1 favors institution. Petitioner was not a party to the Samsung IPR and Petitioner does not have a “significant relationship” with Samsung.

Factors 2 and 5 have limited relevance or favor institution. Petitioner was not a party to the Samsung IPR, and was not aware of Patent Owner’s infringement allegations at the time of the Samsung IPR, which was filed on August 26, 2021, nearly two years before Patent Owner filed its complaint against Petitioner. IPR2021-01447, Paper 1. Petitioner had no reason to perform any prior art searches when the Samsung IPR was filed and did not perform any prior art searches at that time. Nor did Petitioner have reason to challenge the ’905 patent until Patent Owner alleged infringement in the district court.

Factor 3 favors institution. This Petition raises grounds relying on prior art that was not relied on in the Samsung IPR. There is no evidence of road mapping, and the mere fact that the preliminary patent owner response and decision denying institution of the Samsung IPR issued more than one year before the filing of this petition, is insufficient to establish otherwise.

Factor 4 favors institution. Petitioner conducted prior art searching and diligently prepared to file the instant petition shortly after receiving Patent Owner's allegations of infringement in the district court.

Factors 6-7 favor institution. The merits of this petition are strong, asserting obviousness grounds based on art not considered during prosecution and not previously presented to the Board. There is significant value for the Board to consider the invalidity grounds in this petition "to improve patent quality and restore confidence in the presumption of validity that comes with issued patents." *Code200, UAB v. Bright Data, Ltd.*, IPR2022-00861, Paper 18, 5 (PTAB Aug. 23, 2022) (citations omitted). Furthermore, because the Samsung petition was not instituted, a decision granting institution of this IPR would not hinder the Board's ability to issue a final determination not later than one year after granting such a decision.

C. Discretionary Denial is Not Warranted under § 325(d).

Neither Ludtke nor Kon were considered by the Examiner during

prosecution or in the earlier-filed IPR. *See generally* Ex. 1002; Section VII.B, *supra*. Ludtke is currently cited in an *ex parte* reexamination request challenging the '905 patent, but in combination with various references that are not relied on in the instant petition:

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.

Ex. 1011, 39.

Although pending, the claims of the '905 patent have not been finally rejected in the *ex parte* reexamination, nor has an intent to issue a reexamination certificate issued.

Moreover, Patent Owner's Petition to the Director Under 1.181(a)(2) to Exercise Her Discretion Under § 325(d) and its respective request for rehearing on the same, were denied on January 3, 2024, confirming that grounds based on Ludtke do not warrant denial under § 325(d) and further confirming that Ludtke

raised substantial new questions of patentability that, in the public interest of issuing valid patents, should be considered. Ex. 1019, 1020. That same reasoning applies even more so here, where, unlike in the pending *ex parte* reexamination, Petitioner relies on Ludtke differently, in a single reference obviousness challenge and in combination with new references. Ludtke alone presents a new and meritorious challenge to the independent claims and all but two dependent claims of the '905 patent, and Ludtke in combination with new reference Kon raises a meritorious challenge to the additional dependent claims. There is, therefore, no basis for denial under § 325(d).

Additionally, Petitioner submits that the evidence and facts presented in the Petition warrant reconsideration of the prior art. Petitioner presents testimony from Mr. Gray, not reexamination expert Dr. Andrew Wolfe. Mr. Gray's declaration relates to grounds not previously presented in the reexamination and is not based on the opinions of Dr. Wolfe. If this proceeding is instituted, Mr. Gray, unlike Dr. Wolfe, will be subject to cross-examination—allowing the Board further opportunity to reach an accurate conclusion on the validity of the challenged claims over the prior art.

Petitioner further interprets the Ludtke reference in a new light that is materially different than the one articulated in the reexamination request. For example, the Petition asserts that Ludtke alone discloses or suggests all limitations

of the challenged independent claims of the '905 patent; whereas the reexamination request states that "Ludtke discloses all of the limitations in claims 1, 3-10, and 12-18 except the 'unique Device ID'... .," Ex. 1011, 40. The Requester relies on secondary references for these limitations, and in doing so overlooks Ludtke's express disclosure, teaching, and suggestion of these claim elements, as explained in this Petition. *See e.g.*, Section V.B.1.b.

Finally, as 35 U.S.C. § 325(d) is discretionary, regardless of the *Advanced Bionics* factors, discretionary denial of this Petition in view of the pending *ex parte* reexamination is improper because Petitioner here has been accused of infringing the '905 patent and should be entitled to challenge the claims asserted against it.

VIII. Mandatory Notices

A. Real Parties-in-Interest Under 37 C.F.R. § 42.8(b)(1)

Microsoft Corporation is the real party-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

To the best of Petitioner's knowledge, the '905 patent is/was involved in the following district court litigations/proceedings:

Name	Number	Court	Filed
<i>Proxense, LLC v. Samsung Electronics Co., Ltd. et al</i>	6-21-cv-00210	WDTX	Mar. 5, 2021
<i>Samsung Electronics America, Inc. v. Proxense, LLC</i>	IPR2021-01447	PTAB	Aug. 26, 2021

<i>Proxense, LLC v. Microsoft Corp.</i>	6:23-cv-00319	WDTX	May 2, 2023
<i>Proxense, LLC v. Google LLC</i>	6:23-cv-00320	WDTX	May 2, 2023
<i>Google LLC v. Proxense, LLC</i>	IPR2024-00234	PTAB	Jan. 17, 2024
<i>Proxense, LLC v. Apple, Inc</i>	6-24-cv-00143	WDTX	Mar. 18, 2024
<i>Microsoft Corporation v. Proxense, LLC</i>	IPR2024-00776	PTAB	Apr. 26, 2024
<i>Proxense, LLC v. LG Electronics, Inc. et al</i>	6-24-cv-00302	WDTX	May 31, 2024

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR42342-0138IP2@fr.com	Roberto J. Devoto, Reg. No. 55,108 Usman Khan, Reg. No. 70,439 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 PTABInbound@fr.com

D. Service Information Under 37 C.F.R. § 42.8(b)(4)

Please address all correspondence and service to the address listed above.

Petitioner consents to electronic service by email at IPR42342-0138IP2@fr.com

(referencing No. 42342-0138IP2 and cc'ing PTABIn-bound@fr.com, axf-ptab@fr.com, devoto@fr.com and khan@fr.com).

IX. Standing

Petitioner certifies that the '905 patent is available for IPR, and Petitioner is

not barred or estopped from requesting IPR on the grounds identified in this
Petition.

X. Conclusion

Petitioner has established a reasonable likelihood of prevailing for the
challenged claims and requests the Board institute IPR and cancel each challenged
claim as unpatentable.

Respectfully submitted,

Dated August 20, 2024

/ Roberto J. Devoto /

W. Karl Renner, Reg. No. 41,265

Roberto J. Devoto, Reg. No. 55,108

Usman Khan, Reg. No. 70,439

Fish & Richardson P.C.

60 South Sixth Street, Suite 3200

Minneapolis, MN 55402

T: 202-783-5070

F: 877-769-7945

(Control No. IPR2024-01328)

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 9,667 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated August 20, 2024

/ Roberto J. Devoto /
W. Karl Renner, Reg. No. 41,265
Roberto J. Devoto, Reg. No. 55,108
Usman Khan, Reg. No. 70,439
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on August 20, 2024, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

Patent Law Works/Proxense
Greg Sueoka
4516 South 700 East, Suite 290
Salt Lake City, UT 84107

/Diana Bradley/
Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667