UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/015,053	06/08/2022	9298905	2090-0002-REX	7424

142179 7590 03/04/2024
Hard IP LLC (General)
10 Notch Hill Drive
Livingston, NJ 07039

EXAMINER
CARLSON, JEFFREY D

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
03/04/2024	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

GOOGLE EXHIBIT 1024
GOOGLE v. PROXENSE
IPR2024-00234

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Marissa Ducca
Quinn Emanuel Urquhart & Sullivan
1300 I Street NW, Suite 900
Washington, DC 20005

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/015,053* .

PATENT UNDER REEXAMINATION *9298905* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

/JDC/

EX PARTE REEXAMINATION OFFICE ACTION

The present reexamination proceeding is being examined under the pre-AIA first to invent provisions.

This is a reexamination of US Patent 9,298,905. The Decision on Request mailed 8/2/2022 indicated that a substantial new question of patentability affecting patented claims 1–18 of the patent was raised by the request. The claims have not been amended. Patent Owner filed remarks on 1/12/2024. Accordingly, claims 1–18 are pending in this reexamination.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3–10 and 12–18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over US 7,188,110 (Ludtke) in view of US 2003/0196084 (Okereke).

1. A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device;

"The transaction device enhances security by authenticating the user of the card prior to usage . . . authentication may be achieved by . . . biometric solution (e.g., fingerprint recognition)." (Ludtke 4:62–5:1).

"The fingerprint data entry process . . . writes the fingerprint image data into write-once memory, or other memory that is protected from accidental modification" (Ludtke 19:35–39).

"The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID)" (Ludtke 3:32–35).

Further, see below regarding persistently storing an ID code on the integrated device.

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; comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

"At 3102 the user may start a device, such as a digital wallet (DW). 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" (Ludtke 39:48–54).

"a Fingerprint Identification Unit (FIU) 2806 . . . the user had pressed his finger against the FIU 2806" (Ludtke 39:23–27).

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

"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" (Ludtke at Abstract).

"If the fingerprint does match a stored one, then at 3108 the DW allows access to

functions of the DW" (Ludtke 39:56–59).

"The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID)" (Ludtke 3:32–35).

"The transaction device, e.g., the privacy card, is the identity that may be known to a vendor. The highly secured location, accessible through or part of a transaction processing clearing house (TPCH), provides the transaction processing clearing house the information necessary to authorize a transaction. For example, the transaction processing clearing house may access relevant account information to authorize transactions. However, the identity of the user is not revealed externally so that confidentiality of the user's identity is maintained" (Ludtke 3:38–47).

"a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125" (Ludtke 6:36–37).

Ludtke describes wireless communications capabilities for the transaction device and the TPCH:

"the transaction device may contain wireless data communication, data storage and communication protocols for selectively communicating with outside devices" (Ludtke 5:40–42).

"One embodiment of the TPCH 600 is illustrated by FIG. 6. 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 such as the digital wallet. A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc" (Ludtke 9:35–42).

Ludtke describes that the TPCH maintains previously registered ID codes:

"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" (Ludtke 6:49–55).

"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" (Ludtke 6:41–44).

"a transaction device which has a unique identifier (ID)" (Ludtke 3:34–35)

See also Goldberg Dec, ¶ 223.

Ludtke does not explicitly describe the "transaction device information" provided to the TPCH.

Okereke however describes "a system and method for allowing users of wireless and mobile devices to participate in Public Key Infrastructure [PKI]" and which "facilitates secure remote communications" (Okereke at Abstract). Okereke also states that "systems that perform electronic financial transactions or electronic commerce must protect against unauthorized access to confidential records and unauthorized modification of data" (Okereke ¶ 0003).

Okereke specifically teaches transmission of a device's unique identifier to a proxy as part of a scheme to authenticate the device:

"a unique identifier for the wireless product to be employed is passed as 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" (Okereke ¶ 0025).

"If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the desktop 140, which executes functionality to make a key exchange as at 225 . . . This key is used to encrypt information sent to the server" (Okereke ¶ 0025).

It would have been obvious to one of ordinary skill at the time of the

invention to have employed the techniques of Okereke with that of Ludtke in order to facilitate secure communications between the elements of Ludtke, including transmission of a transaction device's stored unique identifier (e.g., a serial number of the device). One of ordinary skill would have expected this to yield a predictable result of providing security through encryption with a private key, as well as the ability to ensure authentication of an authorized device using unique device identifying information such as a serial number or SIM.

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.

"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" (Ludtke 6:41–44).

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.

"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" (Ludtke 27:13–16)

The transaction, as described in Ludtke, is a financial transaction because it is a purchase from a vendor by the user.

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

Ludtke and Okereke together disclose the transaction device receiving biometric information allowing access to the device and then subsequently communicating the ID code to the TPCH. 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 (Ludtke at 19:35–45), the sending of the ID code itself is an "indication that the biometric verification was successful". See also Dec at ¶ 226.

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 fingerprint data entry process . . . writes the fingerprint image data into write-once memory, or other memory that is protected from accidental modification" (Ludtke 19:35–39).

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. One of ordinary skill would have recognized that the transaction device disclosed in Ludtke, which includes a number of different alternatives, including a privacy card (at 20:43–50), and a

cellular telephone mechanism (17:3–10), would meet many of these limitations including "mobile phone," "tablet," and "key fob."

Further, Okereke states that its device may be provided in several mobile formats, including cell phone, laptop, etc.:

"The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication" (Okereke ¶ 0228).

It would have been obvious to one of ordinary skill at the time of the invention to have provided the transaction device of Ludtke in any convenient and mobile format, given the teachings of Okereke. Doing so would have provided convenience and functionality for the users of Ludtke and with predictable results.

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

Per the Goldberg Declaration, "[I]n Ludtke, access would be given applications of either computer software, a file (or both) . . . [i]n a number of embodiments, Ludtke describes the transaction device as including a "digital wallet" which a 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" (Dec ¶ 229). See also Ludtke at 5:1–5.

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.

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 (Ludtke at 5:1–5). Moreover, a POSITA would recognize that giving access to the digital wallet is providing access to a financial account. See Dec ¶ 230.

"An example of other financial data might include account balances that are dynamically updated as transactions are performed" (Ludtke 13:36–38).

"A sequence of events might then be: the user activates the biometric device that identifies him as an authorized user. He then selects the bank . . . The bank may then transmit the information to the user on, for example, the balances in each account" (Ludtke 36:46–61).

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 above for claims 1 and Ludtke 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" (Ludtke 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. See Dec ¶ 231. A POSITA would recognize that in this case, the ID code would be sent without biometric verification.

9. An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;

"The transaction device enhances security by authenticating the user of the card prior to usage . . . authentication may be achieved by . . . biometric solution (e.g., fingerprint recognition)." (Ludtke 4:62–5:1).

"The fingerprint data entry process . . . writes the fingerprint image data into write-once memory, or other memory that is protected from accidental modification" (Ludtke 19:35–39).

"The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID)" (Ludtke 3:32–35).

Further, see below regarding persistently storing an ID code on the integrated device.

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

"At 3102 the user may start a device, such as a digital wallet (DW). 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" (Ludtke 39:48–54).

"a Fingerprint Identification Unit (FIU) 2806 . . . the user had pressed his finger against the FIU 2806" (Ludtke 39:23–27).

The "validation module" can be the portion of the smartphone, including processors and instructions that receives the scan and verifies the biometric information. See Dec ¶ 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.

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

"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" (Ludtke at Abstract).

"If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW" (Ludtke 39:56–59).

"The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID)" (Ludtke 3:32–35).

"The transaction device, e.g., the privacy card, is the identity that may be known to a vendor. The highly secured location, accessible through or part of a transaction processing clearing house (TPCH), provides the transaction processing clearing house the information necessary to authorize a transaction. For example, the transaction processing clearing house may access relevant account information to authorize transactions. However, the identity of the user is not revealed externally so that confidentiality of the user's identity is maintained" (Ludtke 3:38–47).

"a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125" (Ludtke 6:36–37).

Ludtke describes wireless communications capabilities for the transaction device and the TPCH:

"the transaction device may contain wireless data communication, data storage and communication protocols for selectively communicating with outside devices" (Ludtke 5:40–42).

"One embodiment of the TPCH 600 is illustrated by FIG. 6. 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 such as the digital wallet. A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc" (Ludtke 9:35–42).

Ludtke describes that the TPCH maintains previously registered ID codes:

"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"

"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" (Ludtke 6:41–44).

"a transaction device which has a unique identifier (ID)" (Ludtke 3:34–35)

See also Goldberg Dec, ¶ 223.

Ludtke does not explicitly describe the "transaction device information" provided to the TPCH.

<u>Okereke</u> however describes "a system and method for allowing users of

wireless and mobile devices to participate in Public Key Infrastructure [PKI]" and which "facilitates secure remote communications" (Okereke at Abstract). Okereke also states that "systems that perform electronic financial transactions or electronic commerce must protect against unauthorized access to confidential records and unauthorized modification of data" (Okereke ¶ 0003).

Okereke specifically teaches transmission of a device's unique identifier to a proxy as part of a scheme to authenticate the device:

"a unique identifier for the wireless product to be employed is passed as 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" (Okereke ¶ 0025).

"If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the desktop 140, which executes functionality to make a key exchange as at 225 . . . This key is used to encrypt information sent to the server" (Okereke ¶ 0025).

It would have been <u>obvious</u> to one of ordinary skill at the time of the invention to have employed the techniques of Okereke with that of Ludtke in order to facilitate secure communications between the elements of Ludtke, including transmission of a transaction device's stored unique identifier (e.g., a serial number of the device). One of ordinary skill would have expected this to yield a predictable result of providing security through encryption with a private key, as well as the ability to ensure authentication of an authorized device using unique

device identifying information such as a serial number or SIM.

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.

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. See Dec ¶ 235.

"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" (Ludtke 6:41–44).

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.

"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" (Ludtke 27:13–16)

The transaction, as described in Ludtke, is a financial transaction because it is a purchase from a vendor by the user.

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

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." (Ludtke 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. See Dec ¶ 236.

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.

13. 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

"The transaction device enhances security by authenticating the user of the card prior to usage . . . authentication may be achieved by . . . biometric solution (e.g., fingerprint recognition)." (Ludtke 4:62–5:1).

"The fingerprint data entry process . . . writes the fingerprint image data into write-once memory, or other memory that is protected from accidental modification" (Ludtke 19:35–39).

"The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID)" (Ludtke 3:32–35).

Further, see below regarding persistently storing an ID code on the integrated device.

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 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.

"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" (Ludtke at Abstract).

"If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW" (Ludtke 39:56–59).

"The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID)" (Ludtke 3:32–35).

"The transaction device, e.g., the privacy card, is the identity that may be known to a vendor. The highly secured location, accessible through or part of a transaction processing clearing house (TPCH), provides the transaction processing clearing house the information necessary to authorize a transaction. For example, the transaction processing clearing house may access relevant account information to authorize transactions. However, the identity of the user is not revealed externally so that confidentiality of the user's identity is maintained" (Ludtke 3:38–47).

"a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125" (Ludtke 6:36–37).

Ludtke describes wireless communications capabilities for the transaction device and the TPCH:

"the transaction device may contain wireless data communication, data storage and communication protocols for selectively communicating with outside devices" (Ludtke 5:40–42).

"One embodiment of the TPCH 600 is illustrated by FIG. 6. 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 such as the digital wallet. A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc" (Ludtke 9:35–42).

Ludtke describes that the TPCH maintains previously registered ID codes:

"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"

"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" (Ludtke 6:41–44).

"a transaction device which has a unique identifier (ID)" (Ludtke 3:34–35)

See also Goldberg Dec, ¶ 223.

Ludtke does not explicitly describe the "transaction device information" provided to the TPCH.

Okereke however describes "a system and method for allowing users of wireless and mobile devices to participate in Public Key Infrastructure [PKI]" and which "facilitates secure remote communications" (Okereke at Abstract). Okereke also states that "systems that perform electronic financial transactions or electronic commerce must protect against unauthorized access to confidential records and unauthorized modification of data" (Okereke ¶ 0003).

Okereke specifically teaches transmission of a device's unique identifier to a proxy as part of a scheme to authenticate the device:

"a unique identifier for the wireless product to be employed is passed as 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" (Okereke ¶ 0025).

"If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the desktop 140, which executes functionality to make a key exchange as at 225 . . . This key is used to encrypt information sent to the server" (Okereke ¶ 0025).

It would have been obvious to one of ordinary skill at the time of the invention to have employed the techniques of Okereke with that of Ludtke in order to facilitate secure communications between the elements of Ludtke, including transmission of a transaction device's stored unique identifier (e.g. a serial number of the device). One of ordinary skill would have expected this to yield a predictable result of providing security through encryption with a private key, as well as the ability to ensure authentication of an authorized device using unique device identifying information such as a serial number or SIM.

"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" (Ludtke 6:41–44).

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.

"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" (Ludtke 27:13–16)

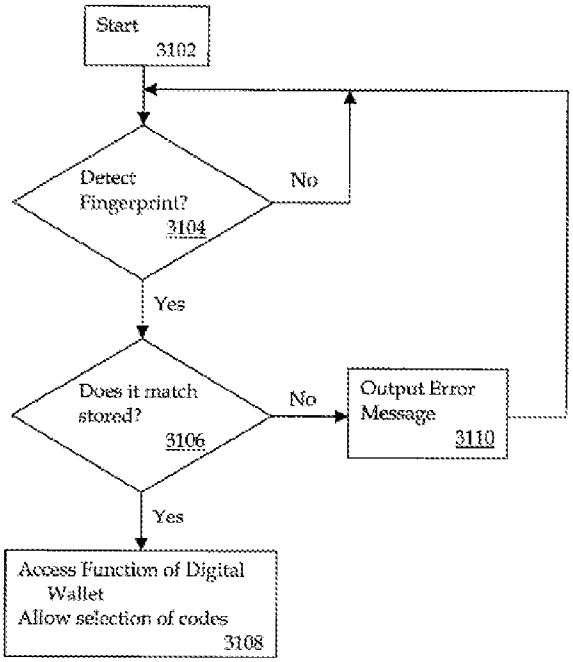
The transaction, as described in Ludtke, is a financial transaction because it is a purchase from a vendor by the user.

The integrated devices described above are hardware devices because they are held by the user. See Dec ¶ 238. The "authentication circuit" is the portion of the hardware device, including processors and instructions that receives the scan and verifies the biometric information. See Dec ¶ 238.

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 claims 1, 9 and 13.

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



[Ludtke FIG 31]

As can be seen in the flowchart, 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. See Ludtke 39:47–59 and Dec ¶ 240–241.

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.

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 fingerprint data entry process . . . writes the fingerprint image data into write-

once memory, or other memory that is protected from accidental modification" (Ludtke 19:35–39).

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.

See claim 7.

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

See claim 6.

Claims 2 and 11 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Ludtke and Okereke in view of US 2003/0177102 (Robinson).

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

Neither Ludtke nor Okereke describe age verification. Robinson however also teaches biometric-based user authorization and further teaches the use of age verification:

"biometric-based age verification for authorizing presenter access of age-restricted good or Services" (Robinson at Abstract).

"System presenters register at least one biometric identifier, at least one identification number, personal age-verifying data, and personal identity-verifying data. A presenter presents a biometric sample obtained from the presenter's person and the presenter's system ID number to conduct age verifications for purchase of or access to age-restricted goods or services" (Robinson at Abstract).

"Age verifying records hold presenter age verifying and identity Verifying information, Such as a presenter's age, date of birth, government ID number and State of issue, home address, or a telephone number; at least one biometric template; and at least one ID number (SID) that identifies the presenter within the System" (Robinson ¶ 0028).

See age verification steps (308, 408, 508, 608) using the stored information in FIGs 3–6 of Robinson.

It would have been obvious to one of ordinary skill at the time of the invention to have provided such age registration and verification with the user authentication and transactions of Ludtke in view of Okereke. Doing so would have provided the ability for the vendor transactions of Ludtke to be restricted to certain age users in the manner as taught by Robinson, for example.

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

See claim 2.

Response to Arguments

Patent Owner states:

"the above rejections are based upon an allegation raised in the Request that Ludtke's transaction privacy clearing house (TPCH) is a "third-party trusted authority" as required by claims 1-18. However, Ludtke's TPCH is the system being accessed by the payee and payor and is thus not a third-party trusted authority" (1/12/2024 Response p. 2).

"The PTAB found that "[t]he plain meaning of 'third-party trusted authority' suggests an entity or party separate from the principal parties to a transaction"" (1/12/2024 Response p. 2).

"However, just like the DPC at issue in IPR2021-01447, the TPCH of Ludtke is the system being accessed by the payee and payor" (1/12/2024 Response p. 3).

Examiner notes that the PTAB interpreted "third-party trusted authority" to mean "a trusted authority that is an entity separate from the parties to a transaction"[1].

The PTAB then looked at the specific facts to determine that the proposed combination of Scott and Lapsley fell short of the claimed third-party trusted authority. The PTAB determined that Scott's host facility 4 (accessed by the users) and Host Processing Unit 32 (the alleged third-party trusted authority) were both part of the same Host System 30 in concluding that Unit 32 was not an entity separate from the transaction parties[2]. The PTAB also determined that petitioner "has not explained sufficiently why Lapsley's DPC is a third-party trusted authority, what entities the DPC is a third-party relative to, or what application the user is being permitted to access in the asserted combination"[3].

The combination of Ludtke and Okereke in this action differs from the arrangements considered by the PTAB previously. The rejection above asserts

[1] IPR2021-01447, Decision Denying Institution, 2/28/2022, p. 14.
[2] *Id.*, p. 22.
[3] *Id.*, p. 24.

three parties – the buyer/user, the vendor and the transaction privacy clearinghouse (TPCH). The transaction privacy clearinghouse (TPCH) meets the claim construction for a "third-party trusted authority" provided by the PTAB, namely by being "a trusted authority that is an entity separate from the parties to a transaction".

Ludtke describes the transaction privacy clearinghouse (TPCH) as an interface between the buyer/user party and the vendor party, as an element that communicates with "external" vendors as well as the user's transaction device, and provides a "middleman" and "intermediary" to shield certain user information from the plurality of vendors:

"a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125" (Ludtke 6:37–38).

"One embodiment of the TPCH 600 is illustrated by FIG. 6. 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 such as the digital wallet" (Ludtke 9:35–39).

"The eCommerce system acts as a financial transaction middleman, stripping off user identity information from transactions" (Ludtke 4:44–45).

"One embodiment of a system that utilizes a point of sale (POS) terminal is shown in FIG. 2. In this embodiment, the privacy card 205 interfaces with the POS terminal 210 and the POS terminal 210 communicates with the TPCH 215. The TPCH 215 interfaces with the financial processing system 220, the vendor 225 and the distribution system 230. The POS terminal may be an existing (referred to herein as a legacy POS terminal) or a newly configured POS terminal located in a retail environment" (Ludtke 8:25–33).

"When vendors need to contact the user who performed a transaction, they use the TPCH as an intermediary, requesting that it send the message to the transaction device with a given ID" (Ludtke 33:42–45).

Patent Owner states:

"The TPCH, which transfer funds into the vendor's account, is the same system being accessed by the user to pay the merchant - and therefore cannot be the claimed "third-party trusted authority"" (1/12/2024 Response p. 5).

Examiner disagrees. The TPCH of Ludtke itself further interfaces with a financial processing system 140 to perform associated financial transactions:

"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" (Ludtke 6:49–55).

Conclusion

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a), to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the patent throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the patent throughout the course of this reexamination

proceeding. The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

THIS ACTION IS MADE FINAL.

A shortened statutory period for response to this action is set to expire TWO MONTHS from the mailing date of this action.

Extensions of time under 37 CFR 1.136(a) do not apply in reexamination proceedings. The provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Further, in 35 U.S.C. 305 and in 37 CFR 1.550(a), it is required that reexamination proceedings "will be conducted with special dispatch within the Office."

Extensions of time in reexamination proceedings are provided for in 37 CFR 1.550(c). A request for extension of time must specify the requested period of extension and it must be accompanied by the petition fee set forth in 37 CFR 1.17(g). Any request for an extension in a third party requested ex parte reexamination must be filed on or before the day on which action by the patent owner is due, and the mere filing of a request will not effect any extension of time. A request for an extension of time in a third party requested ex parte reexamination will be granted only for sufficient cause, and for a reasonable time specified. Any

request for extension in a patent owner requested ex parte reexamination (including reexamination ordered under 35 U.S.C. 257) for up to two months from the time period set in the Office action must be filed no later than two months from the expiration of the time period set in the Office action. A request for an extension in a patent owner requested ex parte reexamination for more than two months from the time period set in the Office action must be filed on or before the day on which action by the patent owner is due, and the mere filing of a request for an extension for more than two months will not effect the extension. The time for taking action in a patent owner requested ex parte reexamination will not be extended for more than two months from the time period set in the Office action in the absence of sufficient cause or for more than a reasonable time.

The filing of a timely first response to this final rejection will be construed as including a request to extend the shortened statutory period for an additional two months. In no event, however, will the statutory period for response expire later than SIX MONTHS from the mailing date of the final action. See MPEP § 2265.

All correspondence relating to this ex parte reexamination proceeding should be directed:

By Mail to: Mail Stop *Ex Parte* Reexam
Central Reexamination Unit
Commissioner for Patents

United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Information regarding the status of reexamination proceedings may be obtained from Patent Center. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Any inquiry concerning this communication should be directed to **the Central Reexamination Unit** at telephone number **517-272-7705.**

/JEFFREY D CARLSON/
Primary Examiner, Art Unit 3992

Conferees:

/C. Michelle Tarae/
Reexamination Specialist, Art Unit 3992
/MICHAEL FUELLING/
Supervisory Patent Examiner, Art Unit 3992