

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Ex Parte Reexamination of

U.S. Patent No. 8,352,730

Inventor: John J. Giobbi

Assignee: Proxense, LLC

Control No. 90/015,052

Issue Date: Jan. 8, 2013

Confirmation No. 9657

Art Unit: 3992

Examiner: Tarae, Catherine Michelle

Title: **BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION**

Mail Stop Ex Parte Reexam

Attn: Central Reexamination Unit
Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONES UNDER 37 C.F.R. § 1.111

Dear Commissioner:

This Response is being filed in response to the Office Action mailed September 12, 2024,
in regard to the above-identified proceedings.

This Response contains the following sections:

Notice of Prior or Concurrent Proceedings, beginning on page 2;

Interview Summary, beginning on page 3; and

Remarks, beginning on page 4.

NOTICE OF PRIOR OR CONCURRENT PROCEEDINGS

Pursuant to 37 C.F.R. § 1565, Patent Owner informs the Office of the following prior and concurrent proceedings in which the Patent at issue is or has been involved.

- *Proxense, LLC v. Samsung Electronics, Co., Ltd. et al.*, No. 6:21-CV-00210 (W.D. Tex. March 5, 2021)
- *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex. May 2, 2023)
- *Proxense, LLC v. Microsoft Corporation*, No. 6:23-CV-00319 (W.D. Tex. May 2, 2023)
- *Proxense, LLC v. LG Electronics, Inc. et al*, No. 6:24-cv-00302 (W.D. Tex. May 31, 2024)
- *Proxense, LLC v. Apple, Inc.*, No. 6:24-cv-00143 (W.D. Tex. March 18, 2024)
- *Samsung Electronics American, Inc. v. Proxense, LLC*, IPR2021-01444 (PTAB Aug. 26, 2021)
- *Google LLC v. Proxense, LLC*, IPR2024-00232 (PTAB Jan. 17, 2024)
- *Microsoft Corporation v. Proxense, LLC*, IPR2024-00775 (PTAB April 19, 2024)
- *Microsoft Corporation. v. Proxense, LLC*, IPR2024-01326 (PTAB Aug. 20, 2024)
- *Apple Inc. v. Proxense LLC*, IPR2024-013333 (PTAB Aug. 20, 2024)

INTERVIEW SUMMARY

Patent Owner thanks the Office for Interview held October 3, 20224.

The Interview was conducted on behalf of the Office by Reexamination Specialist C. Michelle Tarae, Examiner Jeffery D. Carlson, and Supervisory Patent Reexamination Specialist Andrew J. Fischer.

During the Interview, Patent Owner was represented by their counsel, James A. Zak and David Hecht.

During the Interview, the construction of “third-party trusted authority” was discussed with regards to the explicit language of the claims. In particular, Patent Owner noted the claims recite a transaction between a user and an application, and thus require the “third-party trusted authority” be a third with respect to a user and application.

Additionally, it was discussed why Ludtke (U.S. Patent No. 7,188,110) fails to disclose a “third-party trusted authority” because the Ludtke’s Transaction Privacy Clearing House (TPCH) is: 1) not an entity other than the principals involved in the transaction of accessing an application, but rather is the application being accessed; and 2) does not send access message allowing the user access to an application.

Finally, during the Interview Patent Owner noted that the structure for the “authentication unit” is fully recited (i.e., manifested) in claim 15.

At the end of the Interview, Reexamination Specialist Tarae stated the points and arguments raised by the Patent Owner would be considered if formally presented in a Response, which Patent Owner has done with the filing of this response.

REMARKS

Claim Interpretation

I. Third-Party Trusted Authority Required to be a third-party with Respect to User and an Application

The Rejections under 35 U.S.C § 103 are based on the premise that “Ludtke illustrate ‘Commerce General Architecture’ in which a consumer and vendor are the principals involved in a transaction. The transaction privacy clearing house (TPCH) is the one other than the principals involved in the transaction.” Office Action mailed September 12, 2024, page 30. The Office Action has thus construed the term “third-party trusted authority” as a third-party with respect to a user and merchant. However, express language of the independent claims 1, 8, 12, and 15 does not permit the recited “third-party trusted authority” to be a third-party with respect to a transaction between a merchant and user. Rather, the express language of the claims requires the “third-party trusted authority” to be third party with respect to a user and application being accessed.

While the specification may detail such embodiments, it also details embodiments, such as shown in FIG. 7, in which the parties to the transaction are the user and the application. *See Google LLC, v. Proxense, LLC*, IPR2024-00232, Paper 10 at 11 (PTAB July 23, 2024) (“**Fig. 7.** Although the trusted key authority in this example is not a principal party to the transaction (*here, the parties are the user and the application*), it is an active participant in facilitating the transaction.”) (emphasis added). The claims are directed solely to such embodiments.

Claims 1 and 15 each recite “receiving an access message from *the agent* allowing *the user* access to *an application*.” Similarly, claim 8 recites “receives an access message from *the agent* allowing *the user* access to *an application*.” Likewise, claim 12 recites “receiving an access message from *the agent*; and in response to a positive access message, allowing *the biometrically verified user* access to *an application*.” The independent claims of the 730 Patent each recite three

participants: the user; the third-party trusted authority; and the application the user is allowed to access. The Office Action asserts the proper interpretation of a “third-party trusted authority” is “One other than the principals involved in a transaction” Office Action Mailed September 12, 2025, page 5. The PTAB, on multiple occasions, has similarly interpreted third-party trusted authority to mean “a trusted authority that is an entity separate from the parties to a transaction.” IPR2024-00232, Paper 10 at 12 (“Accordingly, we adopt the Samsung DDI’s construction without Patent Owner’s modifications. On the current record, a ‘third-party trusted authority’ is ‘a trusted authority that is an entity separate from the parties to a transaction.’”). The third-party trusted authority, therefore, is not a party or principal to the transaction. This only leaves the user and the application the user is allowed to access as the parties to the transactions. Thus, the claims explicitly require the parties to the transaction be the user and the application, and that the transaction is the user gaining access to the application. The “third-party trusted authority,” therefore, is required by the express language of the claims to be a third-party with respect to the user and the application being accessed.

Should there be any doubt, that a transaction in which the parties are a merchant and user is excluded by the explicit language of the claims, with referenced to Fig. 7 of the Patent, the PTAB observed “Although the trusted key authority in this example is not a principal party to the transaction (*here, the parties are the user and the application*), it is an active participant in facilitating the transaction.” IPR2024-00232, Paper 10 at 11 (PTAB July 23, 2024) (emphasis added). As shown by the below table, independent claims 1, 8, 12 and 15 directly map to FIG. 7.

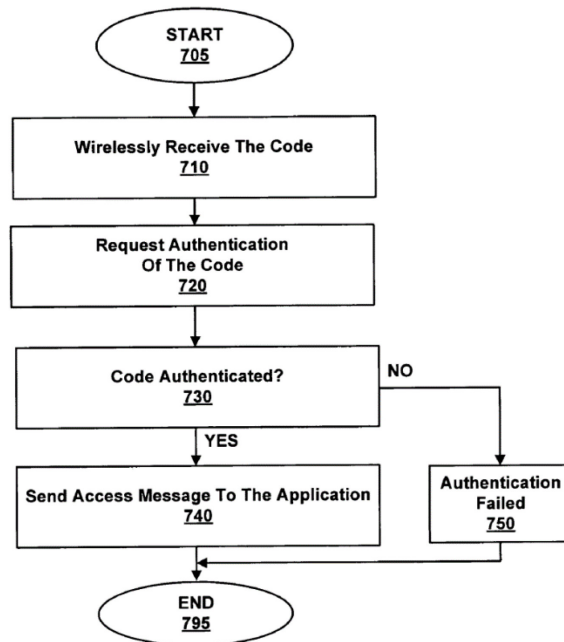


FIG. 7

FIG. 7	Claim 1	Claim 8	Claim 12	Claim 15
710 – Wirelessly Receive the Code	“persistently storing biometric data of the user and a plurality of codes and other data values ... in a tamper proof format written to a storage element” Code thus received from storage element	“a memory stores biometric data of a user and a plurality of codes and other data values ... a verification unit, in communication with the memory” Code thus received from memory	“receiving one or more codes from a plurality of codes and other data values”	“receives the plurality of codes and the other data values”
720 – Request Authentication of the Code	“sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority”	“sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority”	“requesting authentication of the one or more codes and the other data values by the agent” Note: in previous limitation is stated “an agent that is a third-party trusted authority”	“send the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third-party trusted authority”
730 – Code Authenticated? Yes / No	“responsive to authentication of the one or more codes ... receiving an access message from the agent”	“responsive to the agent authenticating the one or more codes ... receives an access message from the agent”	“receiving an access message from the agent; and in response to a positive access message”	“responsive to the device ID code being authenticated ... receiving an access message from the agent”
740 – Send Access Message to the Application	“an access message from the agent allowing the user access to an application”	“an access message from the agent allowing the user access to an application”	“in response to a positive access message, allowing the biometrically verified user access to an application,”	“an access message from the agent allowing the user to access an application”

As all the independent claims directly map to an embodiment in which the parties to the transaction are the user and the application, the claims of the patent expressly require the parties to the transaction be the user and the application, and that the transaction is the user gaining access to the application. The “third-party trusted authority,” therefore, is expressly required to be a third-party with respect to the user and the application being accessed.

By their express language, or when read considering the specification, the claims of the patent are explicitly limited to instances in which the third-party trusted authority is a third party with respect to a user and an application, and in which the transaction is accessing the application by the user. The claims, therefore, expressly require the third-party trusted authority be an entity of than the application being accessed.

II. 35 U.S.C. § 112, Sixth Paragraph, Does not Apply to Claims 8 and 15

In Claim 8: The Algorithm for a “Verification Unit” Is Fully Defined in the Claim

The Office Action asserts on page 7 that the term “verification unit” invokes 35 U.S.C. § 112, sixth paragraph, and the corresponding structure/algorithm is disclosed in column 4, lines 13-23, and FIG. 2. Patent Owner recognizes that term “unit” can be indicative of an intention to invoke § 112, sixth paragraph, but that is not the case here. The algorithm is fully manifested in the claim 8, as well as the other independent claims of the patent.

As an initial matter, Patent Owner believes the algorithm is presented in FIG. 6, which the 730 Patent describes as “illustrating a method for verifying a subject presenting the biometric key according to one embodiment of the present invention.” 730 Patent, 2:51-53; *see also* 6:65-67 (“FIG. 6 is a flow chart illustrating a method 600 for verifying a subject presenting the biometric key according to one embodiment of the present invention.”). The following discussion of FIG. 6 is provided in specification:

“FIG. 6 is a flow chart illustrating a method 600 for verifying a Subject presenting the biometric key according to one embodiment of the present invention. In response to an authentication request, a user scan is requested 610 (e.g., by a blinking LED). Once the Subject provides a fingerprint, Scan data is received 620. Scan data is compared for a match 630 to previously-stored biometric data. If there is no match, then verification fails 650.

If there is a match, the subject is verified 640 as the user. The code indicating a Successful verification is wirelessly sent 650 from the biometric key (e.g., by RF communication module 230).” 730 Patent, 6:65-7:9

Accordingly, the algorithm for a verification unit is presented in FIG. 6 and the accompanying discussion within the specification. As shown in the below tables, both FIG. 6 and the accompanying discussion are fully manifested in claim 8 and the other independent claims.

6:65-7:9	Claim 1	Claim 8	Claim 12	Claim 15
“Once the Subject provides a fingerprint, Scan data is received 620.” 7:2-3	receiving scan data from a biometric Scan	receives scan data from a biometric scan	a biometrically verified user,	if scan data can be verified as being from the use
“scan data is compared for a match 630 to previously-stored biometric data.” 7:3-4	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data	for comparison against the biometric data		by comparing the scan data to the biometric data
“If there is a match, the subject is verified 640 as the user. The code indicating a successful verification is wirelessly sent 650 from the biometric key (e.g., by RF communication module 230).” 7:6-9	“sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority”	“sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority”	“requesting authentication of the one or more codes and the other data values by the agent” Note: in previous limitation is stated “an agent that is a third-party trusted authority”	“send the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third-party trusted authority”

FIG. 6	Claim 1	Claim 8	Claim 12	Claim 15
“Receive Scan Data From a Subject 620”	receiving scan data from a biometric Scan	receives scan data from a biometric scan	a biometrically verified user,	if scan data can be verified as being from the use
“Scan Data Match Biometric Data? 630” “Subject Is Verified As The Registered User 640”	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data	for comparison against the biometric data		by comparing the scan data to the biometric data
“Wirelessly Send Code Indicating Successful Verification of User 650”	“sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority”	“sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority”	“requesting authentication of the one or more codes and the other data values by the agent” Note: in previous limitation is stated “an agent that is a third-party trusted authority”	“send the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third-party trusted authority”

In Claim 15: The Algorithm for an “Authentication Unit” Is Fully Defined in the Claim

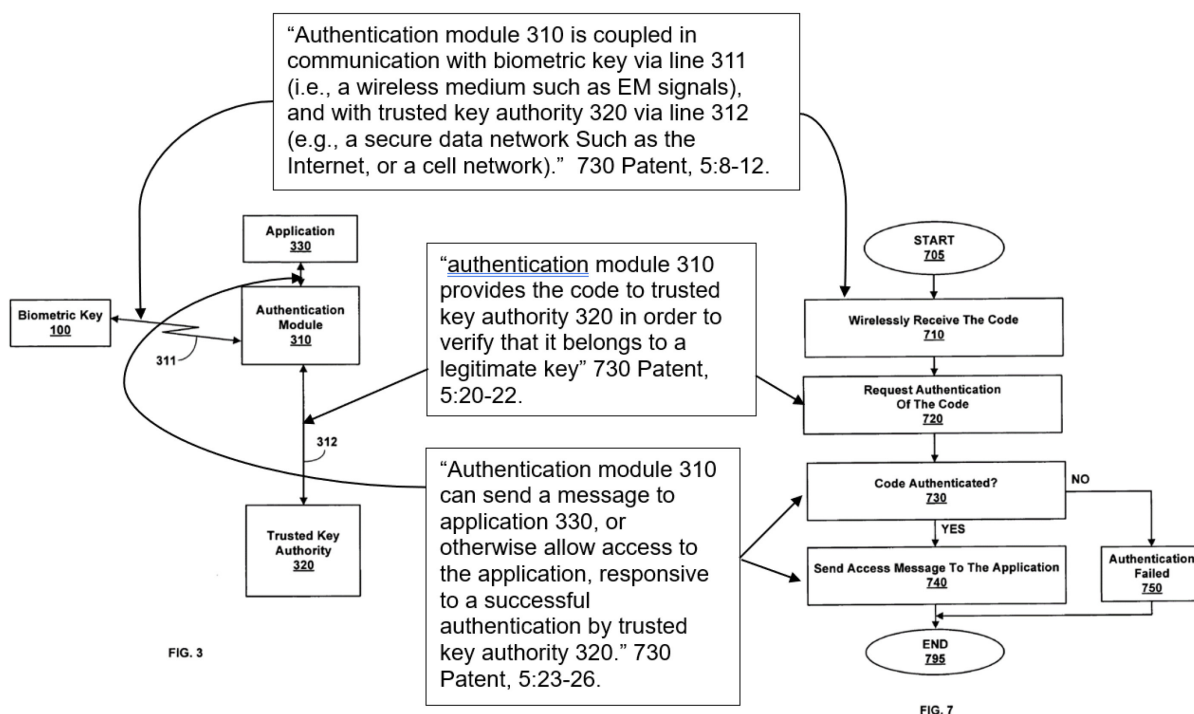
The Office Action asserts on pages 7-8 that the term “authentication unit” invokes 35 U.S.C. § 112, sixth paragraph, and the corresponding structure/algorithm is disclosed in column 5, lines 8-6, and FIG. 3. Patent Owner recognizes that term “unit” can be indicative of an intention to invoke § 112, sixth paragraph, but that is not the case here. The algorithm is fully manifested in the claim 15, as well as the other independent claims of the patent. As the below table shows, the language from the specification identified by the Office Action as corresponding to the “authentication unit” maps to each independent claim of the patent.

5:8-26	Claim 1	Claim 8	Claim 12	Claim 15
“Authentication module 310 is coupled in communication with biometric key via line 311 (i.e., a wireless medium such as EM signals).” 5:8-10	“persistently storing biometric data of the user and a plurality of codes and other data values ... in a tamper proof format written to a storage element” Code received from communicatively coupled storage element	“a memory stores biometric data of a user and a plurality of codes and other data values ... a verification unit, in communication with the memory” Code received from communicatively coupled memory	“receiving one or more codes from a plurality of codes and other data values”	“receives the plurality of codes and the other data values”
“[A]uthentication module 310 provides the code to trusted key authority 320 in order to verify that it belongs to a legitimate key.” 5:20-22	“sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority”	“sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority”	“requesting authentication of the one or more codes and the other data values by the agent” Note: in previous limitation is stated “an agent that is a third-party trusted authority”	“send the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third-party trusted authority”
“[R]esponsive to a successful authentication by trusted key authority 320.” 5:25-26	“responsive to authentication of the one or more codes ... receiving an access message from the agent”	“responsive to the agent authenticating the one or more codes ... receives an access message from the agent”	“receiving an access message from the agent; and in response to a positive access message”	“responsive to the device ID code being authenticated ... receiving an access message from the agent”
“Authentication module 310 can send a message to application 330, or otherwise allow access to the application, responsive to a successful authentication by trusted key authority 320.” 5:23-26	“an access message from the agent allowing the user access to an application”	“an access message from the agent allowing the user access to an application”	“in response to a positive access message, allowing the biometrically verified user access to an application,”	“an access message from the agent allowing the user to access an application”

Every independent claim of the patent recites the function of authentication unit / module (310) sending a code to a trusted key authority (320) for verification and allowing access to an

application (330) in response to successful authentication of the code by the trusted key authority (320). Furthermore, each of the independent claims recite some form of biometric verification by a biometric key (100). Thus, all the independent claims correspond to the embodiment of FIG. 3, which depicts a system “for providing authentication information for a biometrically verified user” that includes an application (330) and a trusted key authority (320).

It is further noted that FIG. 7, which the PTAB observes present an embodiment in which the principal parties are the user and the application, maps to the “structure/algorithm in the specification” that the Office Action identifies as corresponding to the “authentication unit” of claim 15, as shown by the below figure.



As FIG. 7 maps to the portions of the specification the Office Action has identified as disclosing the algorithm for an “authentication unit, table presented above with regards to FIG. 7 further evidences the algorithm for the “authentication unit” is full manifested in the claim 15 and all the other independent claims.

Claim Rejection – 35 U.S.C. § 103

Claims 1, 2, 4-9, 11, 12, and 14-17 are rejected under 35 U.S.C. § 103 for allegedly being rendered obvious by Ludtke (U.S. Patent No. 7,188,110) in view of Okereke (U.S. Publication No. 2003/019608).

Claims 3, 10 and 13 are rejected under 35 U.S.C. § 103 for allegedly being rendered obvious by Ludtke (U.S. Patent No. 7,188,110) in view of Okereke (U.S. Publication No. 2003/019608) and Robinson (U.S. Publication No. 2003/0177102).

Patent Owner respectfully traverses the rejections to they extent they are maintained in view of the following remarks.

I. Ludtke’s Transaction Privacy Clearing House (TPCH) is Not a Third-Party Trusted Authority

Independent claims 1, 8, 12, and 15 each recite the recite a “third-party trusted authority,” The Office Action mailed September 12, 2024, equates the recited “third-party trusted authority with Ludtke’s Transaction Privacy Clearing House (TPCH). To qualify as a “third-party trusted authority” Ludtke’s Transaction Privacy Clearing House (TPCH) must:

- 1) Send an access message allowing the user access to an application; and
- 2) Be an entity other than the principals involved in the transaction of accessing the application – i.e., not be the application being accessed.

Ludtke’s TPCH fails both requirements.

The Transaction Privacy Clearing House (TPCH) Is the Application Being Accessed

Ludtke's transaction privacy clearinghouse (TPCH) is being accessed to perform the accepted function of a clearing house. A clearing house is "An office where banks exchange checks and drafts and *settle accounts*." American Heritage Dictionary Entry: clearinghouse (ahdictionary.com), <https://ahdictionary.com/word/search.html?q=clearinghouse> (emphasis added). Likewise, the Cambridge English Dictionary defines a clearing house as "a central office used by banks to collect and send out money and checks." CLEARING HOUSE definition | Cambridge English Dictionary, <https://dictionary.cambridge.org/us/dictionary/english/clearing-house>. Similarly, Merriam-Webster defines a clearinghouse as "an establishment maintained by banks for *settling mutual claims and accounts*." Clearinghouse Definition & Meaning - Merriam-Webster, <https://www.merriam-webster.com/dictionary/clearinghouse> (emphasis added). Accordingly, a clearinghouse's accepted function is to perform settlement by transferring money. In accordance with the accepted function of a clearing house, Ludtke states, "The TPCH *settles* funds, *transferring* the appropriate amount into the vendor's account." Ludtke, 27:66-67. Furthermore, Ludtke states, "The *settlement* of funds involves *the transfer* of the appropriate financial credit into the vendor's account." Ludtke, 29:35-36. Ludtke further notes, that the core functionality of the TPCH is "financial settlement and allocation of payments to internal and external accounts". Specifically, Ludtke states, "The TPCH *agent 615* handles system management and policy control, and *forms the core functionality of the TPCH 600*... Among the *responsibilities handled by the agent include* internal system management functions such as data mining, *financial settlement and allocation of payments to internal and external accounts*, and registration of new users joining the system." Ludtke, 9:43-51 (emphasis added). Accordingly, the TPCH is accessed by the user to perform the accepted function of a clearing house by

transferring money from the user's account to the vendor's accounts and is therefore the application being accessed.

Ludtke teaches that settlement is carried out by the TPOCH issuing transaction authorizations to a financial processing system (FP) 140. Specifically, Ludtke discloses:

“In one embodiment, the *financial processing system (FP) 140 performs tasks of transferring* funds between the user's account and the vendor's account for each transaction... The *TPCH 110 issues transaction authorizations* to the FP140 function on an anonymous basis on behalf of the user over a highly secure channel.”

Ludtke, 6:65-7:6. By “issu[ing] transactions authorizations to the FP 140 function” the TPOCH is directing FP 140 to perform the transfer indicated in the authorization. Of course, before the TPOCH can direct FP 140 to perform the transfer, it needs to collect certain information to be able to formulate a transaction authorization indicating how much to transfer, from what account, and into which account. Ludtke states that this information is provided to the TPOCH by a POS terminal.

“The POS terminal may collect the necessary information from the transaction device, e.g., the digital wallet, combine it with the purchase data, and send it to the TPOCH. *The TPOCH may then authorize the transaction*, store data relevant to the transaction in its records and trigger a financial transfer to the vendor's account. The POS terminal may then receive verification that the transaction is complete, and transfer the wireless receipt to the transaction device.”

Ludtke, 23:50-57 (emphasis added).

The TPOCH is thus receiving data from the POS and using that data to formulate a transaction authorization directing the FP to make requested transfer from the user's account to the vendor's account. Thus, Ludtke's transaction privacy clearing house is *the application being accessed by the user* to settle the transaction by causing the appropriate amount to be transferred from the user's account to the vendor's account.

Ludtke discloses four ways in which the TPCCH performs settlement when accessed by the user. The simplest settlement method disclosed by Ludtke is one in which “the account is managed completely by the TPCCH, and thus the funds transfer is handled completely inside of the TPCCH.” Ludtke, 29:37-39. With this method of settlement, the TPCCH simply directs the transfer of funds from an account held by the TPCCH to the vendor’s account.

In the next settlement method disclosed, “the TPCCH 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, 6:51-55 (emphasis added). In this method the TPCCH issues credit to the user based on the availability of funds in an account registered with the TPCCH, and then directs the transfer of funds from an account held by the TPCCH to the vendor’s account. At some point in time, the user would have to reimburse the TPCCH.

The third settlement process disclosed is one in which “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.” Ludtke, 29:43-46. Here, the TPCCH is accessed to provide access to the user’s account. In this instance, however, the transaction authorization issued by the TPCCH would direct the transfer of funds from an account of the user to the vendor’s account.

The final settlement process disclosed by Ludtke is one in which the TPCCH directly charges an account registered with the TPCCH. “[T]he FP140 is contacted by the TPCCH requesting a generic credit approval of a particular account... The TPCCH 110 can request the credit using a dummy charge ID that can be listed in the monthly credit statement sent to the user, so that the user can reconcile his credit statement.” Ludtke, 7:12-20; *accord* Ludtke, 29:46-51 (“In yet another

alternative embodiment, the TPOCH may act as a proxy for the user, whereby the TPOCH takes the funds from the user's account as managed by a third party financial institution, and then issues a funds transfer from the TPOCH account to the vendor's account.”). In this process, the TPOCH provides access to a registered account to issue the “dummy charge,” collecting funds from the user's account, and transferring funds to the vendor. Accordingly, the transaction authorization issued by the TPOCH directs the transfer of funds from an account held by the TPOCH to the vendor's account.

In all the foregoing settlement methods, the TPOCH is performing the established function of a clearing house, thereby making the TPOCH *the application being accessed by the user* to settle the transaction by causing the appropriate amount to be transferred from the user's account to the vendor's account.

The Transaction Privacy Clearing House (TPCH) Does Not Send an Access Message Allowing the User to Access an Application

Independent claims 1, 8, 12, and 15 each recite in response to authentication of a device ID code by the thirding party trusted authority, receiving an access message from the third-party trusted authority allowing the user access to an application. Ludtke fails to disclose its transaction privacy clearing house (TPCH) sends such a message in response to authenticating a device ID code.

The Office Action fails to identify an access message. The Office Action does identify various functions on the digital wallet as the “applications”. However, Ludtke does not detail the TPOCH sends an access message allowing the user to access functionality of the digital wallet after the TPOCH successfully authenticates device ID codes sent to the TPOCH.

Assuming, solely for the sake of discussion, the Office Actions was intended to identify the confirmation returned from the TPCCH to the point-of-sale device (POS) as the access message, the conformation sent from the TPCCH to the POS does not enable an application.

The confirmation sent from the TPCCH to the POS does not allow access to the POS because the POS is the used to access the TPCCH. As described in Ludtke, “the POS terminal may collect the necessary information from the transaction device, e.g., digital wallet, combine it with the purchase data, and send it to the TPCCH. The TPCCH may then authorize the transaction, store data relevant to the transaction in its records and trigger a financial transfer to the vendor’s account.” Ludtke, 23:50-55; see also id., 21:51-57 (“In one embodiment, a POS terminal is the link between the digital wallet or privacy card and the transaction privacy clearinghouse (TPCH) of the eCommerce system. The main purpose of the POS terminal is to establish a secure transaction connection between the transaction device and the TPCCH and to transfer transaction data to the TPCCH for completion of the transaction.”). A similar process for web transactions is shown in Figure 17 of Ludtke. However, instead of receiving data from the digital wallet via a magnetic stripe on a privacy card, the POS “communicates with the transaction device, asking the transaction device to validate the user, confirm the user wants to make this transaction, and get the appropriate information for which account the user to use for payment.” Ludtke, 28:58-62. This is shown by step 6 in Figure 17:

“When information on the user’s side of the transaction has been set up to perform a transaction, the personal POS terminal opens a secure communication session to the TPCCH, requesting a transaction. The personal POS terminal provides the transaction record that it received from the web browser and the unique ID of the transaction device. The TPCCH uses the unique ID of the transaction device to process the transaction.”

Ludtke, 29:6-14.

Accordingly, for both web and retail transactions, the primary purpose of Ludtke's POS terminal is to establish a secure connection with the TPCCH and to transfer transaction data to the TPCCH. Consequently, the user must have been allowed access to the POS prior to the receipt of the confirmation received back from the TPCCH.

Likewise, the confirmation received from the TPCCH does not allow access to a website. When making a web transaction, "The user triggers the purchase, usually by clicking on a 'Buy' or similar button in the web browser." Ludtke, 28:34-35. "Once a transaction has been triggered, the browser communicates with the personal POS terminal, requesting it to initiate a transaction." Ludtke, 28:50-52. Then, as detailed above, the POS establishes a secure connection with the TPCCH and transfers transaction data to the TPCCH. Accordingly, to initiate a transaction, the user must have been allowed access to the website prior to the receipt of the confirmation from the TPCCH.

The confirmation message also does not enable the transaction device / digital wallet of Ludtke. While the transaction device may receive receipts after each transaction, access to the files storing the receipts is not allowed by the receipt of the confirmation. Rather, "The user then has the data readily available for use on demand, whether it is for a business expense report or for personal record keeping." Ludtke, 10:37-39. Accordingly, the user always has access to files storing electronic receipts.

II. Okereke and Robinson Do Not Disclose a "Third-Party Trusted Authority"

The Office Action does not point to the teachings of Okereke or Robinson for as disclosing a third-party trusted authority. Accordingly, neither Okereke nor Robinson, alone or in combination, disclose or suggest a third-party trusted authority.

III. The Combination of Ludtke, Okereke and Robinson Do Not Render Claims 1-17 Obvious under 35 U.S.C. § 103

For the reasons stated above, neither Ludtke, Okereke, nor Robinson, alone or in combination, disclose or suggest a third-party trusted authority. The combination Ludtke, Okereke, nor Robinson, therefore, fails to disclose all the elements of claims 1-17, and thus fail to render claims 1-17 obvious under 35 U.S.C. § 103. In view of the foregoing, Patent Owner respectfully requests the Examiner reconsider and withdraw these rejections.

Claim Rejections – 35 U.S.C. § 102

Claims 15-17 are rejected under 35 U.S.C. § 102(a, e) for being allegedly anticipated by Ludtke (U.S. Patent No. 7,188,110). For the reasons stated above, Ludtke fails to disclose a “third-party trusted authority” as recited in claim 15, from which claims 16 and 17 depend. Accordingly, Ludtke fails to disclose all the elements of claims 15-17 and thus does not anticipate claims 15-17 under 35 U.S.C. § 102(a, e). In view of the foregoing, Patent Owner respectfully requests the Examiner reconsider and withdraw this rejection.

CONCLUSION

In view of the foregoing remarks, withdrawal of all rejections and termination of these proceedings is respectfully requested.

October 9, 2024

Respectfully submitted by:

/James A. Zak, Esq./

Attorney for Patent Owner
Proxense, LLC
Reg. No. 60,190

Hecht Partners LLP
125 Park Ave. 25th Floor
New York, NY 10017
E: jzak@hechtpartners.com
P: (651) 357-8517