

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

AMENDMENT UNDER 37 C.F.R. § 1.111

Dear Commissioner:

This Amendment is being filed in response to the Office Action mailed July 29, 2025, regarding the above-identified proceedings.

This Amendment contains the following sections:

Amendments to the Claims, beginning on page 2; and

Remarks, beginning on page 10.

AMENDMENTS TO THE CLAIMS

Patent Owner respectfully requests the claims be amended as indicated below.

No new matter is added by way of the following amendments. An explanation of the Amendments and the support therefore is provided in the **Remarks** section of this Amendment.

1. (Cancelled)
2. (Cancelled)
3. (Cancelled)
4. (Cancelled)
5. (Cancelled)
6. (Cancelled)
7. (Cancelled)
8. (Cancelled)
9. (Cancelled)
10. (Cancelled)
11. (Cancelled)
12. (Cancelled)
13. (Cancelled)
14. (Cancelled)
15. (Cancelled)

16. (Cancelled)
17. (Cancelled)
18. (Cancelled)
19. (Cancelled)
20. (Cancelled)
21. (Cancelled)
22. (Cancelled)
23. (Cancelled)
24. (Cancelled)
25. (Cancelled)
26. (Cancelled)
27. (Cancelled)
28. (Cancelled)
29. (Cancelled)
30. (Cancelled)
31. (Cancelled)
32. (Cancelled)
33. (Cancelled)
34. (Cancelled)

35. (New) A method for verifying a user during authentication of an integrated device, comprising the steps of:

persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

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

responsive to a determination that the scan data matches the biometric data, wirelessly 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 possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and

responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message by an application from the agent allowing the user access to the application and complete a transaction of the user accessing the application, wherein principal parties to the transaction are the user and the application, and wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

36. (New) The method of claim 35, wherein the one or more codes and the other data values are transmitted to the agent over a network.
37. (New) The method of claim 35, further comprising:
registering an age verification for the user in the association with the device ID code.
38. (New) The method of claim 35, wherein the one or more codes and the other data values indicate that the biometric verification was successful.
39. (New) The method of claim 35, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.
40. (New) The method of claim 35, further comprising:
establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.

41. (New) The method of claim 35, further comprising:

receiving a request for the one or more codes and the other data values without a request for biometric verification; and

responsive to receiving the request for the one or more codes and the other data values without a request for biometric verification, sending the one or more codes and the other data values without requesting the scan data.

42. (New) An integrated device for verifying a user during authentication of the integrated device, comprising:

a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly 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 possessing a list of device ID codes

uniquely identifying legitimate integrated devices, wherein the one or more codes and the other data values includes the device ID code; and

responsive to the agent authenticating the one or more codes and the other data values, a radio frequency communicator, receives an access message by an application from the agent allowing the user access to the application and complete a transaction of the user accessing the application, wherein principal parties to the transaction are the user and the application, and wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

43. (New) The integrated device of claim 42, wherein the one or more codes and the other data values are transmitted to the agent over a network.
44. (New) The integrated device of claim 43, wherein an age verification is registered in association with the device ID code.
45. (New) The integrated device of claim 42, wherein the verifier comprises: an LED to be activated for requesting the biometric scan.
46. (New) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving one or more codes from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and the other

data values comprises the device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices;

requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the one or more codes and the other data values are-legitimate;

requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the one or more codes and the other data values are-legitimate;

receiving an access message by an application from the agent; and

in response to a positive access message, allowing the biometrically verified user access to the application and complete a transaction of the user accessing the application, wherein principal parties to the transaction are the user and the application, and wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file

47. (New) The method of claim 46, further comprising:

Registering a date of birth or age with the agent.

48. (New) The method of claim 46, further comprising:

establishing a secure communications channel with a biometric key, wherein the one or more codes and the other data values associated with the biometrically verified user is received from the biometric key.

49. (New) A system comprising:

a biometric key stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or more codes from the plurality of codes and other data values wherein the one or more codes and the other data values include the device ID code, and the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition; and

an authentication unit receives the plurality of codes and the other data values and 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

possessing a list of device ID codes uniquely identifying legitimate integrated devices, and responsive to the device ID code being authenticated, the authentication unit receiving an access message by an application from the agent allowing the user to access the application and complete a transaction of the user accessing the application, wherein principal parties to the transaction are the user and the application, and wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

50. (New) The system of claim 49, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data.
51. (New) The system of claim 49, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and the other data values.

REMARKS

Amendments to the Claims

By way of this Amendment, Patent Owner has cancelled claims 18-34, which renumbered original claims 1-17 as claims 18-34, and replaced them with claims 35-51, essentially renumbering claims 1-17 as claims 35-51.

In addition to renumbering independent claims 1, 8, 12, and 15 (previously renumbered as claims 18, 25, 29, and 32) as claims 35, 42, 46, and 49, the claims have been further amended consistent with the explicit language of claims 1, 8, 12, and 15 (previously renumbered claims 18, 25, 29, and 32) and their natural construction. Accordingly, the amendments to the claims are fully supported by the language of the original claims themselves.

Prior to the Amendment, Independent Claims 1, 8, 12, and 15 (previously renumbered as claims 18, 25, 29, and 32) each explicitly recited a user and an application, and no other party aside from a “third-party trusted authority.” Furthermore, each of the Independent Claims explicitly recited the underlying action of allowing the user access to the application. Finally, consistent with step 740 of Fig. 7 (“send access message to the application”) the claims recited “receiving an access message by an application from the agent allowing the user access to the application.” Thus, each of the independent claims recited a transaction in which the “third-party trusted authority” receives a request for authentication with a code,

determines whether the code is valid, authenticates the code, and transmits an access message, which allows a user access to an application. The Board noted in another proceeding involving the same patent that the very transaction recited in the claims is one in which the “third-party trusted authority” is a third-party with respect to the transaction of a user accessing an application, wherein the principal parties are a user being allowed access and an application being accessed.

[T]he trusted key authority of the preferred embodiments of the ’730 patent, which actively participates in *a transaction*, for example by receiving a request for authentication with a code, determining whether the code is valid, authenticating the code, and transmitting an access code to the requester, which allows a user access to an application. Ex. 1001, 7:10–22, **Fig. 7**. Although the trusted key authority in this example is not a principal party to the transaction (*here, those parties are the user and the application*), it is an active participant *in facilitating the transaction*.

Google LLC v. Proxense, LLC, IPR2024-00232, Paper 10, at 11.

The explicit language of claims 1, 8, 12, and 15 (previously renumbered as claims 18, 25, 29, and 32) thus without amendment recited a transaction of the user accessing the application, wherein the principal parties to the transaction are the user and the application. Accordingly, the amendments are fully supported by the language of the original claims themselves.

Claim Objections

Claims 18-34 are objected to for allegedly failing to comply with 37 C.F.R. § 1.530(f). By way of this Amendment, Patent Owner has cancelled claims 18-34 rendering this objection moot. Patent Owner thus respectfully requests the Examiner withdraw this objection.

Double Patenting

The Office Action asserts an improper obviousness-type double patenting rejection, explicitly forbidden by *Allergan USA. v. MSN Laboratories Private*, 111 F.4th 1358 (Fed. Cir. 2024). Accordingly, the rejection must be withdrawn.

Claims 18-34, which correspond to now pending claims 35-51, are rejected on the grounds of non-statutory double patenting for being allegedly unpatentable over claims 1-29 of U.S. Patent No. 8,886,954. However, the current patent is the first filed, first issued patent in its family, that includes U.S. Patent No. 8,886,954. This is readily apparent from:

- 1) the filing date of the present patent (December 20, 2005) compared with the subsequent and later filing date of U.S. Patent No. 8,886,954 (December 10, **2012**);
- 2) the issue date of the present patent (January 8, 2012) compared with the issue date of U.S. Patent No. 8,886,954 (November 11, **2014**);

- 3) the fact that the present patent claims priority only to provisional applications Nos. 60/637,358 and 60/652,765, whereas U.S. Patent No. 8,886,954 claims priority to the present patent in addition to the foregoing provisional applications; and
- 4) the terminal disclaimer filed in U.S. Patent No. 8,886,954 with respect to the present patent.

As the first filed, first issued patent in its family, the claims of the present patent cannot be invalidated by the later-filed, later-issued, earlier-expiring claims of U.S. Patent No. 8,886,954. *Allergan USA. v. MSN Laboratories Private*, 111 F.4th 1358, 1369 (Fed. Cir. 2024) (“As the first-filed, first-issued patent in its family, it is the patent that sets the maximum period of exclusivity for the claimed subject matter and any patentably indistinct variants. ***We therefore hold that a first-filed, first-issued, later-expiring claim cannot be invalidated by a later-filed, later-issued, earlier-expiring reference claim having a common priority date.***”) (emphasis added). Accordingly, the rejection is improper and in violation of binding precedent.

In view of the foregoing, Patent Owner respectfully requests the rejection be withdrawn.

Claim Rejections – 35 U.S.C. § 102 - Burger

Claims 1, 2, 4-9, 11, 12, and 14-17 were rejected under pre-AIA 35 U.S.C. § 102(e) for allegedly being anticipated by Burger (U.S. Publication No. 2005/0050367). Claims 35, 36, 38-43, 45, 46, and 48-51 correspond directly to Claims 18, 19, 21-26, 28, 29, and 31-34 which correspond directly to claims 1, 2, 4-9, 11, 12, and 14-17. Accordingly, Patent Owner's remarks presented in the Response filed June 2, 2025, are directly applicable to claims 35, 36, 38-43, 46, and 48-51 and hereby incorporated by reference in their entirety.

In the Response filed June 2, 2025, Patent Owner detailed the flow process presented in Burger and demonstrated that Burger fails to disclose “receiving an access message by an application from the agent allowing the user access to the application” as required by the claims 35, 42, 46, and 49. As noted in the response filed June 2, 2025, prior to arriving at the subroutine 2006 of Routine 1922 executed by Network Server 114, the user has already been granted access to the file or hard drive of Pocket Vault 102 storing the Financial Media (*i.e.*, credit / debit card account) during the execution of authorized holder routine 722. Accordingly, the “encrypted approval message” transmitted at subroutine 2408 of Routine 1922 will not provide access to the application. Likewise, access to the Interface Station was previously provided when the operator inputted information regarding the proposed transaction at step 1702. Consequently, the “transaction approval message” that will

subsequently be provided to the Interface Station and Pocket Vault 102 will **not allow the user to access either**.

Additionally, after logging the transaction, “*the routine 1922 proceeds to a step 2408*, wherein an *encrypted approval message is transmitted* to the entity with which the transaction is being attempted (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107).” ¶ [0518] (emphasis added). At this point the process returns to step 1730 of the Interface Station routine shown in Fig. 17. After the process returns to the Interface Station, the Interface Station at step 1734 forwards the “transaction approval message” to Pocket Vault 102. This returns the process to step 1042 of Fig. 10. Simultaneously, the Interface Station continues with process 1414 of Routine 1400 by displaying the “transaction approval message” to the operator at step 1738 and then ends the process. Accordingly, after receiving the “transaction approval message” from Network Server 114, use of the Interface Station terminates. Thus, receipt of the “transaction approval message” ends use of the Interface Station. This is the exact opposite of allowing the user access, as required by independent claims 35, 42, 46, and 49. Consequently, the “transaction approval message” received from Network Server 114 is not an “access message” allowing the user access to the Interface Station as required by claims 35, 36, 38-43, 45, 46, and 48-51.

Likewise, after completing the Authorized Holder Routine 722, shown in Fig. 10, Pocket Vault 102 displays a shutdown screen at step 726 and then powers down at step 728. Powering down is the exact opposite of allowing access, as required by each of the independent claims. Accordingly, receipt of the “transaction approval message” from Network Server 114 terminates access and is thus not an “access message” as required by claims 35, 36, 38-43, 45, 46, and 48-51.

Independent claims 35, 42, 46, and 49 each explicitly recite responsive to authentication of a device ID code by the “third-party trusted authority” “receiving an access message by an application from the agent allowing the user access to the application.” Accordingly, the claims explicitly require that the “access message” allow the user access to the application. As the foregoing demonstrates, *receipt of the “transaction approval message” from Network Server 114 terminates the use of, rather than allows access to, Pocket Vault 102 and the Interface Station.* Burger’s “transaction approval message” is therefore the antithesis of the “access message” recited in each of the independent claims.

The two Examples cited in the Office Action fail to establish otherwise. The first Example fails to even cite any portion of Burger disclosing transmission of an access message from Network Server 114. Rather, the first example merely cites that “local software for each Pocket Vault 102 and pocket vault interface station 104 may be upgraded from time to time by automatic download from the network server

114.” But downloading software upgrades from a network server is the receipt of the application – not an access message. To conclude otherwise would be to improperly conflate separately recited elements in the claims, which separately recite “access message” and “application.” Furthermore, downloading from network server 114 means the network server is being accessed to transfer the upgrade to the pocket vault or interface station. Thus, it is an application on the network server that is being accessed and not an application on the pocket vault or interface station.

The second example is no better. Again, the Office Action relies on the transfer of information from the network server to the pocket vault. However, retrieving information from the network server means that the network server is being accessed and not the pocket vault nor interface station. Second, the example fails to cite any portion of Burger that details the transmission of the information from the interface station or pocket vault to the network server is conditioned upon the network server providing an access message. Rather, as detailed in the Response filed June 2, 2025, receipt of a “transaction approval message” from Network Server 114 terminates the use of, rather than allows access to, Pocket Vault 102 and the Interface Station. As the receipt of a message from the server terminates access, it cannot and does not allow information to be sent.

Disregarding the clear teachings of Burger, the Office Action cites IPR2024-00846, Paper 8, 19-25. However, the Board did not find that Burger disclosed receipt

of an access message allowing the user to access an application. Rather, the Board noted that:

Dr. Traynor testifies it would have been obvious that the pocket vault 102 would have received an access message from network server 114 in order for pocket vault 102 to grant access to the user and display credit card information. Ex. 103 ¶ 115.

IPR2024-00846, Paper 8, 20 (emphasis added).

Dr. Traynor testifies that it would have been obvious that the encrypted approval message from network server 114 could be sent to the pocket vault 102 in addition to or instead of interface stations 104c, 106, 107. Ex. 1003 ¶ 116.

Id. (emphasis added.).

Dr. Traynor testifies that it would have been obvious that, for pocket vault 102 to display an advertisement, it would have received an access message from network server 114 conditioned on network server 114 authenticating the pocket vault ID. Ex. 1003 ¶ 117.

IPR2024-00846, Paper 8, 23 (emphasis added).

Dr. Traynor testifies that it would have been obvious that network server 114 would send to pocket vault 102 a message allowing it to access the advertisement upon authenticating the pocket vault ID. Ex. 1003 ¶ 117.

IPR2024-00846, Paper 8, 25 (emphasis added).

Accordingly, the Institution Decision was not based on a finding that Burger discloses the access message required by the claims, but that Dr. Traynor testified such would be an obvious modification. As such, the Institution Decision cannot support the rejection nor refute Patent Owner's arguments.

Furthermore, the Examiner rightly rejected the testimony of Dr. Traynor and the rejection under 35 U.S.C. § 103 he advocated. As detailed in MPEP § 2141(III):

The key to supporting any rejection under **35 U.S.C. 103** is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in *KSR* noted that the analysis supporting a rejection under **35 U.S.C. 103** should be made explicit. The Court quoting *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006), stated that "*[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.*" *KSR*, 550 U.S. at 418, 82 USPQ2d at 1396.

In direct contradiction to the MPEP's demand for **articulated reasoning with some rational underpinning**, Dr. Traynor's testimony offers nothing more than mere conclusory statements.

It would have been obvious that an application in the Pocket Vault would have received an access message from controller 402 of the network server ("*receiving, at an application, an access message from the trusted authority*") to allow users access to the application after the

controller 402 and database 406 of the network server authenticated the Pocket Vault ID that was sent to the network server so that the Pocket Vault grants access to a user and displays sensitive information e.g., credit or debit card info) for conducting a transaction.

IPR2024-00846, Traynor Decl., Ex. 1003, ¶¶ 115 (emphasis in original).

Burger also discloses that, in some cases, the communications may be directly between the Pocket Vault and the network server, and thus, it would have been obvious that the encrypted approval message could be sent to the pocket Vault in addition to or instead of being sent to the interface stations. MSC-1005, ¶[101]. This may particularly be the case be displayed by the Pocket Vault or token coupled to the Pocket Vault.

IPR2024-00846, Traynor Decl., Ex. 1003, ¶¶ 116.

Again, it would have been obvious that for the Pocket Vault to be allowed to display the advertisements and home menu, the controller of the Pocket Vault would have received an access message from the network server ("***receiving, at an application, an access message from the trusted authority***") to "***allow[] the user access to an application***" after and conditioned on the network server successfully authenticating the Pocket Vault ID that was sent to the network server ("***the trusted authority successfully authenticated the one or more codes and other data values sent to the third party***").

IPR2024-00846, Traynor Decl., Ex. 1003, ¶¶ 117 (emphasis in original).

Dr. Traynor's testimony asserts that modifying Burger to receive an access message prior to access would have been obvious **without providing the articulated reasoning with some rational underpinning** required by the MPEP. Accordingly, Dr. Traynor is testifying that Burger fails to disclose all the elements of the claims and thus necessitates a modification. Dr. Traynor's testimony regarding the obviousness the modification, however, is nothing more than conclusory statements forbidden by MPEP § 2141(III). Correctly recognizing that Dr. Traynor's testimony could not justify nor support a rejection under 35 U.S.C. § 103, the Examiner rejected and did not assert the obvious rejection for which Dr. Traynor advocated.

Having rejected the advocated §103 rejection, the Office Action cannot reasonably rely on the testimony of Dr. Traynor, nor the Board's institution decision on §103, to support the §102 rejection, or refute Patent Owner's arguments that Burger fails to teach all the elements of the claims.

The Office Action also attempts to dismiss the Patent Owner's arguments by asserting the parties to the transaction could be "the user and vendors, advertisers, non-financial media issuers and financial media issuers. In the case where one of the parties is a vendor, advertiser, non-financial media issuer or financial media issuer, the user requires access to the application to conduct a transaction therewith." Such a construction, as detailed above in the *Amendments to the Claims* section, is in

direct contradiction to the explicit language of the claims and their natural construction.

Failing to disclose an access message as required by each of the independent claims, Burger does not anticipate claims 35, 36, 38-43, 45, 46, and 48-51. In view of the foregoing, Patent Owner respectfully requests the Examiner reconsider and withdraw the rejection.

Claim Rejections – 35 U.S.C. § 102 - Ludtke

Claims 32-34 were rejected under pre-AIA 35 U.S.C. § 102 (a,e) for allegedly being anticipated by U.S. Patent No. 7,188,11 to Ludtke et al. (Ludtke). This rejection is entirely improper.

Claims 32-34 correspond to original claims 15-17, which are now claims 39-51. The Final Office Action mailed March 3, 2025, stated that “the claims would be allowed if amended to recite: receiving an access message *by an application* from the agent allowing the user to access the application.” Final Office Action, page 31. Patent Owner has amended the claims as directed by the Office to overcome the rejection and the Office entered the amendments.

Yet, without citing any authority to do so, the Examiner has reinstated the rejection, which is arbitrary and capricious, and in violation of the Administrative Procedure Act (APA). Patent Owner acted in good faith reliance on the Office’s representation, including very likely sacrificing lawful patent rights. The Office has

responded by going back on its agreement without citing any authority to do so and based on an inaccurate recitation of the record. This is improper.

To justify this, the Office Action reference related proceedings. However, the related proceedings do not justify or factually support such act. The claims were amended as directed by the Examiner, that amendment was entered and in response to the amendment the rejection was withdrawn. However, for reasons unknown to the Patent Owner, the Board determined the opposite happened: “We treat the Examiner’s decision to withdraw the rejection involving Ludtke as a determination that that rejection is moot (and not an assessment of the merits), and ***her proposed amendment as withdrawn*** and, thus, of no relevance to this proceeding.” IPR2024-00233, Paper 35, 44 (emphasis added). Accordingly, the proceedings referenced by the Office Action were based on a misrepresentation of the record. Such findings cannot justify reinstatement of the rejections over Ludtke, and is again arbitrary and capricious, in violation of the APA.

In view of the foregoing, Patent Owner respectfully requests the Examiner reconsider and withdraw these rejections.

Claim Rejections – 35 U.S.C. § 103 - Burger

Claim 45 was rejected under pre-AIA 35 U.S.C. § 103 for allegedly being obvious over Burger.

Claims 37, 44, and 47 were rejected under pre-AIA 35 U.S.C. § 103 for allegedly being obvious over Burger in view of Robinson (U.S. Publication No. 2003/01777102)

Claims 37, 44, 45, and 47 correspond directly to claims 20, 27, 28, and 30. Accordingly, Patent Owner's remarks presented in the Response filed June 30, 2025, are directly applicable to claims 20, 27, 28, and 30.

Claims 37, 44, 45, and 47 are dependent upon one of independent claims 35, 42, and 46. As noted above, Burger fails to disclose an "access message" as required by claims 35, 42, and 46. The Office Action has not shown that Robinson discloses such an "access message". Consequently, the Office Action has not established claims 37, 44, 45, and 47 are *prima facie* obvious over Burger in view of Robinson.

Patent Owner respectfully requests the Examiner reconsiders and withdraws these rejections.

Claim Rejections – 35 U.S.C. § 103 - Ludtke

Claims 18, 19, 21-26, 28, 29, and 31 were rejected under 35 U.S.C. § 103 for allegedly being obviously over U.S. Pub. No. 2003/0196084 to Okereke et al. (Okereke). Patent asserts this rejection is entirely improper.

Claims 18, 19, 21-26, 28, 29, and 31 correspond to original claims 1, 2, 4-9, 11, 12 and 14, which are now claims 35, 37, 38-43, 45, 46, and 48. The Final Office Action mailed March 3, 2025, stated that "the claims would be allowed if amended

to recite: receiving an access message *by an application* from the agent allowing the user to access the application.” Final Office Action, page 31. Patent Owner has amended the claims as directed by the Office to overcome the rejection and the Office entered the amendments.

Yet, the Examiner has reinstated the rejection, which again, is a violation of the Administrative Procedure Act (APA), as set forth above.

In view of the foregoing, Patent Owner respectfully requests the Examiner reconsider and withdraw these rejections.

Estoppel

The Office Action asserts the claims are not patentably distinct from the original claims, but these vary proceedings demonstrate the opposite. The Final Office Action mailed March 3, 2025, stated that “the claims would be allowed if amended to recite: receiving an access message *by an application* from the agent allowing the user to access the application.” Final Office Action, page 31. Patent Owner has amended the claims as directed by the Office to overcome the rejection and the amendments were entered. Accordingly, the claims as now presented include amendments the Office determined would distinguish the claims over Ludtke and are thus patentably distinct from the original claims.

Furthermore, the claims were not finally refused. While the Board granted Patent Owner's request for adverse judgment, that request was based on concessions made when the Patent Owner authorized entry of the Examiner's amendment.

Patent Owner, Proxense LLC ("Proxense"), ***requests adverse judgement in IPR2024-00775 based on the concessions of unpatentability made when Patent Owner authorized entry of the Examiner's amendment in EPR 90/015,052.*** Under 37 C.F.R. § 42.73(b), "a party may request judgement against itself at any time during a proceeding." Pursuant to 42.73(b)(3) a party may request adverse judgment by a "concession of unpatentability." ***Patent Owner has conceded the unpatentability of the claims at issue in this proceeding by authorizing entry of the Examiner's amendment in EPR 90/015,052.*** As such, Patent Owner requests adverse judgment pursuant to 42.73(b)(3)."

IPR2024-00755, Paper 14, 1 (emphasis added). Accordingly, the Patent Owner requested adverse judgment because, by authorizing entry of the Examiner's amendment, the Patent Owner conceded the unpatentability of the original claims over Ludtke.

In granting adverse judgment, the Board specifically acknowledged the concession of unpatentability made over Ludtke.

Patent Owner 'requests adverse judgement in IPR2024-00775 ***based on the concessions of unpatentability made when Patent Owner authorized entry of the Examiner's amendment in EPR 90/015,052.***'

Paper 14, 1. “Patent Owner has *conceded the unpatentability of the claims at issue in this proceeding by authorizing entry of the Examiner’s amendment in EPR 90/015,052*. As such, Patent Owner requests adverse judgment pursuant to 42.73(b)(3).’ *Id.*

IPR2024-00755, Paper 15, 2 (emphasis added). Accordingly, the Board found that the Patent Owner conceded the unpatentability of the original claims over Ludtke.

Patent Owner made no concession regarding the patentability of the original claims over Burger. Likewise, the Board made no finding regarding the patentability of the original claims over Burger. Rather, the patentability over Burger became a moot point as the Patent Owner conceded the original claims were unpatentable over Ludtke and the amended claims were not before the Board. As such, the Board was incapable of making any determination regarding the amended claims.

Finally, it would be nonsensical for the Board to lift the stay in these proceedings to permit entry of the Examiner’s Amendment if the Board had determined the amended claims were unpatentable over Burger.

Therefore, the Board made no determinations regarding the patentability of the original claims or amended claims over Burger.

CONCLUSION

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

September 29, 2025

Respectfully submitted by:

/Peter J. Park/

Peter J. Park

Attorney for Patent Owner

Proxense, LLC

Reg. No. 71,267

Hecht Partners LLP

125 Park Ave. 25th Floor

New York, NY 10017

E: jzak@hechtpartners.com

P: (651) 357-8517