

Appeal No. 25-1484

United States Court of Appeals
for the
Federal Circuit

In re: Blaze Mobile, Inc.
Appellant

Appeal From The United States Patent and Trademark Office in
Ex Parte Reexamination Control No. 90/019,134

OPENING BRIEF OF APPELLANT BLAZE MOBILE, INC.

Dr. Gregory J. Gonsalves
Law Office of Dr. Gregory J. Gonsalves
2216 Beacon Lane
Falls Church, Virginia 22043
571.419.7252
gregoryjosephgonsalves@gmail.com

Counsel for Appellant
BLAZE MOBILE, INC.

Exemplary Patent Claim At Issue For U.S. Patent No. 10,825,007

The claim includes the corrections from the certificate of corrections dated June 13, 2023, July 18, 2023, and November 14, 2023.¹

2. A transaction server for processing a transaction, comprising:

a transaction server interface configured to: receive a payment method that corresponds to an identification code associated with a user from a remote management server, wherein prior to receiving the payment method that corresponds to the identification code associated with the user from the remote management server,

the remote management server sends a list of products to a non-browser based application generated screen generated by a non-browser based application with a graphical user interface that is downloaded and installed on a mobile device for display with a mobile device display of the mobile device, wherein the non-browser based application only generates a non-browser based application generated screen, the non-browser based application generated screen corresponding to a specific screen or area of the non-browser based application, the mobile device including the mobile device display, a mobile device processor, a mobile device wireless radio transceiver configured to support voice and data interactions through a first wireless communication channel, and a mobile device wireless fidelity (Wi-Fi) transceiver;

receives, from the non-browser based application generated screen, an identification of one or more products selected from the list of products,

¹ See Appx133-142 for a listing of all the claims including their corrections.

wherein the non-browser based application generated screen receives the identification of the one or more products selected from the list of products through user input via the mobile device display;

receives a transaction purchase request including information relating to the identification of the one or more products from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the transaction purchase request from the user via the mobile device display of the mobile device;

receives user input login information including an identification code associated with a user from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the user input login information via a mobile device display of the mobile device;

upon receipt of the user input login information, authenticating, at the remote management server, a user associated with the user input login information;

transmits the payment method that corresponds to the identification code associated with the user to the transaction server;

and send a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed and further wherein after receiving the transaction verification, the remote management server downloads the one or more products to the mobile device;

a transaction server processor that processes the transaction using the payment method.

Certificate Of Interest

Pursuant to Federal Circuit Rule 47.4, counsel for Appellant BLAZE MOBILE, INC. certifies as follows:

1. The full name of every party represented by me is:

BLAZE MOBILE, INC.

2. The name of the real party in interest represented by me is:

Not applicable

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party represented by me are:

Not applicable

4. The names of all law firms and the partners or associates that appeared for the party now represented by me in the trial court or agency or are expected to appear in this court (and who have not or will not enter an appearance in this case) are:

Carmichael IP, PLLC:

Stephen T. Schreiner

Glazer Weil, LLP:

Stephen Underwood

5. The title and number of any case known to counsel to be pending in this or any other court or agency that will directly affect or be directly affected by this court's decision in the pending appeal are:

In re: Blaze Mobile Inc., Appeal From The United States Patent and Trademark Office in Ex Parte Reexamination Control No. 90/019,135 for U.S. Pat. No. 10,699,259.

Samsung Electronics Co., Ltd. v. Blaze Mobile, Inc. et al., N.D. Cal. Case No. 21-cv-02989.

Respectfully submitted,

/s/ Gregory J. Gonsalves
Dr. Gregory J. Gonsalves
Law Office Of Dr. Gregory J. Gonsalves
2216 Beacon Lane
Falls Church, VA 22043
571.419.7252
gregoryjosephgonsalves@gmail.com

*Counsel for Appellant
Blaze Mobile, Inc.*

Table of Contents

Patent Claims At Issue	ii
Certificate Of Interest.....	iv
Table Of Authorities	viii
Table Of Abbreviations.....	xii
Statement Of Related Cases.....	1
Statement Of Jurisdiction.....	1
I. Statement Of The Issues	2
II. Statement Of The Case And Facts.....	3
A. Procedural Background	3
B. The '007 Patent: Ms. Michelle Fisher Invents A New Type Of System For Remote Processing Of A Transaction Using a Mobile Device.....	4
C. The Board's Decision On Appeal.....	7
III. Summary Of The Argument	11
IV. Standard Of Review.....	21
V. Argument.....	24
A. The User Login Information/User Authentication Claim Limitations Would Not Have Been Obvious Under The Proper Claim Construction	24
1. The Broadest Reasonable Claim Construction Standard.....	24
2. The Board's Claim Construction Erroneously Conflates The User Login Information/User Authentication Claim Limitations With.....	25
3. Blaze Mobile's Construction Of The User Login Information/User Authentication Claim Limitations Is Supported By The Claim Language, The Specification, And The Prosecution File History.	31
4. The Board's Ruling That The Prior Art Would Not Have Taught The User Login Information/User Authentication Claim Limitations Is Not Supported By Substantial Evidence Under The Proper Claim Construction.....	35
B. The Claim Limitations Relating To Sending "the identification of one or more products" and "the transaction purchase request" To The Remote Management Server Would Not Have Been Obvious Under the Proper Claim Construction.....	40

1. Blaze Mobile’s Construction Of The Claim Limitations Related To Sending “the identification of one or more products” and “the transaction purchase request” To The Remote Management Server Is Supported By The Claim Language and The Specification.	41
2. The Board’s Ruling That The Prior Art Would Have Taught The Claim Limitations Related To Sending “the identification of one or more products” and “the transaction purchase request” Is Not Supported By Substantial Evidence Under The Proper Claim Construction.	44
C. The Claim Limitations Relating To The Remote Management Server and Transaction Server Limitations Would Not Have Been Obvious Under the Proper Claim Construction.	50
1. Blaze Mobile’s Construction Of The Claim Limitations Relating To The Remote Management Server and Transaction Server Limitations Is Supported By The Claim Language and The Specification.	51
2. The Board’s Ruling That The Prior Art Would Have Taught The Claim Limitations Relating To The Remote Management Server and Transaction Server Limitations Is Not Supported By Substantial Evidence Under The Proper Claim Construction.	55
3. The Board Failed To Show That A POSITA Would Have Been Motivated To Modify Khedouri With Goldthwaite.	59
VI. Conclusion	64

Table Of Authorities

Cases

<i>In re Abbott Diabetes Care, Inc.</i> 696 F.3d 1142 (Fed. Cir. 2012)	22
<i>Adidas AG v. Nike, Inc.</i> 963 F.3d 1355 (Fed. Cir. 2020).	60
<i>Applied Med. Res Corp. v. U.S. Surgical Corp.</i> 448 F.3d 1324 (Fed. Cir. 2006)	12, 17, 31, 49, 55
<i>Ariosa Diagnostics v. Verinata Health, Inc.</i> 805 F.3d 1359 (Fed. Cir. 2015)	22, 24
<i>Beckson Marine, Inc. v. NFM, Inc.</i> 292 F.3d 718 (Fed. Cir. 2002)	20, 59
<i>Burlington Truck Lines v. United States</i> 371 U.S. 156 (1962).....	24
<i>CAE Screenplates Inc. v. Heinrich Fiedler GmbH</i> 224 F.3d 1308 (Fed. Cir. 2000)	49
<i>In re Chapman</i> 595 F.3d 1330 (Fed. Cir. 2010).	22
<i>Chemours Co. FC v. Daikin Indus.</i> 4 F.4th 1370 (Fed. Cir. 2021)	63
<i>In re Fine</i> 837 F.2d 1071 (Fed. Cir. 1988)	64
<i>In re Gordon</i> 733 F.2d 900 (Fed. Cir. 1984)	64
<i>Haemonetics Corp. v. Baxter Healthcare Corp.</i> 607 F.3d 776 (Fed. Cir. 2010)	27

<i>Hill-Rom Servs., Inc. v Stryker Corp.</i> 755 F.3d 1367 (Fed. Cir 2014)	12, 32
<i>Kinetic Concepts, Inc. v. Smith & Nephew, Inc.,</i> 688 F.3d 1342 (Fed. Cir. 2012)	25
<i>K/S HIMPP v. Hear-Wear Technologies, LLC</i> 751 F.3d 1362 (Fed. Cir. 2014)	20, 39
<i>KSR International Co. v. Teleflex Inc.</i> 550 U.S. 398 (2007).....	24
<i>In re Man Mach. Interface Techs. LLC</i> 822 F.3d 1282 (Fed. Cir. 2016)	22
<i>Microsoft Corp. v. Proxyconn, Inc.</i> 789 F.3d 1292 (Fed. Cir. 2015)	35
<i>In re Morris</i> 27 F.3d 1048 (Fed. Cir. 1997)	26
<i>Motor Vehicle Mfrs. Ass’n v. State Farm Mut. Auto. Ins. Co.</i> 463 U.S. 29 (1983).....	23
<i>Mylan Pharms. Inc. v. Merck Sharp & Dohme Corp.</i> 50 F.4th 147 (Fed. Cir. 2022)	22
<i>In re NuVasive, Inc.</i> 842 F.3d 1376 (Fed. Cir. 2016)	24, 25
<i>Omega Eng’g, Inc. v. Raytek Corp.</i> 334 F.3d 1314 (Fed. Cir. 2003)	32, 41, 52
<i>Par Pharm., Inc. v. TWI Pharms., Inc.</i> 773 F.3d 1186 (Fed. Cir. 2014)	23
<i>Perkin-Elmer Corp. v. Westinghouse Elec. Corp.</i> 822 F.2d 1528 (Fed. Cir. 1987)	26

<i>Personal Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017)	24
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	12, 31
<i>Power Integrations, Inc. v. Lee</i> 797 F.3d 1318 (Fed. Cir. 2005)	24
<i>Rambus Inc. v. Rea</i> 731 F.3d 1248 (Fed. Cir. 2013)	22
<i>Rovalma, S.A. v. Bohler-Edelstahl GmbH</i> 856 F.3d 1019 (Fed. Cir. 2017)	24
<i>SEC v. Chenery Corp.</i> 318 U.S. 80 (1943)	23
<i>In re Smith Int'l, Inc.</i> 871 F.3d 1375 (Fed. Cir. 2017)	25, 26, 44
<i>In re Suitco Surface, Inc.</i> 603 F.3d 1255 (Fed. Cir. 2010)	26
<i>Trivascular, Inc. v. Samuels</i> 812 F.3d 1056 (Fed. Cir. 2016)	63
<i>In re Translogic Tech., Inc.</i> 504 F.3d 1249 (Fed. Cir. 2007)	25
<i>Unique Concepts, Inc. v. Brown</i> 939 F.2d 1538 (Fed. Cir. 1991)	26
<i>In re Vivint, Inc.</i> 14 F.4th 1342 (Fed. Cir. 2021)	23

Statutes

5 U.S.C. § 706(2).....	22
28 U.S.C. § 1295(a)(4)(A).....	2
35 U.S.C. § 6(b)	1
35 U.S.C. § 103.....	8
35 U.S.C. § 134.....	4
35 U.S.C. § 141.....	2
35 U.S.C. § 306.....	4

Patent Office Rules

37 C.F.R. § 41.37	4
37 C.F.R. § 41.41	4

Table Of Abbreviations

Parties

Appellant, Patent Owner, Blaze Mobile	BLAZE MOBILE, INC.
Appellee, US PTO	United States Patent & Trademark Office

Citations

Appx_____	Joint Appendix at page(s) _____
MPEP	Manual of Patent Examining Procedure

Terms

'007 Patent	United States Patent No. 10,825,007
'234 Pub	U.S. Pat. Pub. No. 2009/0124234
'192 Pub	U.S. Pat. Pub. No. 2008/0052192
AIA	America Invents Act
APA	Administrative Procedure Act
Khedouri	U.S. Pat. Pub. No. 2006/0008256
Coward	U.S. Pat. Pub. No. 2005/0202385
Dua	U.S. Pat. Pub. No. 2006/02558289
Goldthwaite	U.S. Pat. Pub. No. 2004/0230489
Harrison	U.S. Pat. Pub. No. 2006/0229998
Horenz	U.S. Pat. Pub. No. 2004/0267611
Goh	JP 2001-256195

Board, PTAB

Patent Trial and Appeal Board

POSITA

person of ordinary skill in the art

Statement Of Related Cases

Under Fed. Cir. R. 47.5(a), counsel for Appellant, BLAZE MOBILE, INC. (“BLAZE MOBILE”), certifies that no other appeal from the same proceeding in the United States Patent & Trademark Office is or was previously before this Court or any other appellate court, whether under the same or a similar title.

Under Fed. Cir. R. 47.5(b), counsel for BLAZE MOBILE states that the Court’s decision in this appeal may affect the following judicial and administrative matters:

In re: Blaze Mobile Inc., Appeal From The United States Patent and Trademark Office in Ex Parte Reexamination Control No. 90/019,135 for U.S. Pat. No. 10,699,259.

Samsung Electronics Co., Ltd. v. Blaze Mobile, Inc. et al., N.D. Cal. Case No. 21-cv-02989.

Statement Of Jurisdiction

Pursuant to 35 U.S.C. § 6(b), the Patent Trial and Appeal Board (the “Board”) issued its Decision on Appeal on August 1, 2024 (Appx10-52) and its Decision on Request for Rehearing on January 8, 2025 (Appx1-9) for U.S. Patent 10,825,007 (“the ’007 Patent”). Appx53-71. Patent Owner timely filed a Notice of Appeal on February 24, 2025. Appx4243-4298399. This Court has jurisdiction pursuant to 28 U.S.C. § 1295(a)(4)(A) and 35 U.S.C. § 141(b).

I. Statement Of The Issues

1. Whether the U.S. PTO erred in construing the claim limitations relating to “user input login information including an identification code associated with the user from the non-browser based application” and “authenticating, at the remote management server, a user associated with the user input login information.”
2. Whether the U.S. PTO erred in construing the claim limitations relating to the “identification of one or more products selected from the list of products” and the “transaction purchase request.”
3. Whether the U.S. PTO erred in construing the claim limitations relating to the “remote management server” and the “transaction server.”
4. Whether the PTAB erred in ruling that independent claims 1, 2, and 3 of the '007 patent would have been obvious over Khedouri and Goldthwaite.
5. Whether the PTAB erred in ruling that a person of ordinary skill in the art would have been motivated to combine the teachings of Khedouri’s network and Goldthwaite’s financial institution server when such a combination would render Khedouri’s network unsuitable for its intended purpose.

II. Statement Of The Case And Facts

A. Procedural Background

This appeal involves a patent owner by Blaze Mobile: U.S. Patent No. 10,825,007 (“the ’007 patent”). The ’007 patent was filed on April 15, 2014 as application no. 14 / 253,648 and claims a priority date through a chain of continuation applications of November 30, 2007. The ’007 patent issued on November 3, 2020.

Samsung Electronics Co., Ltd. filed a request for ex parte reexamination of the ’007 Patent on November 22, 2022. Appx291-294. The USPTO issued an order granting ex parte reexamination of the ’007 Patent on February 15, 2023. Appx3281-3309.

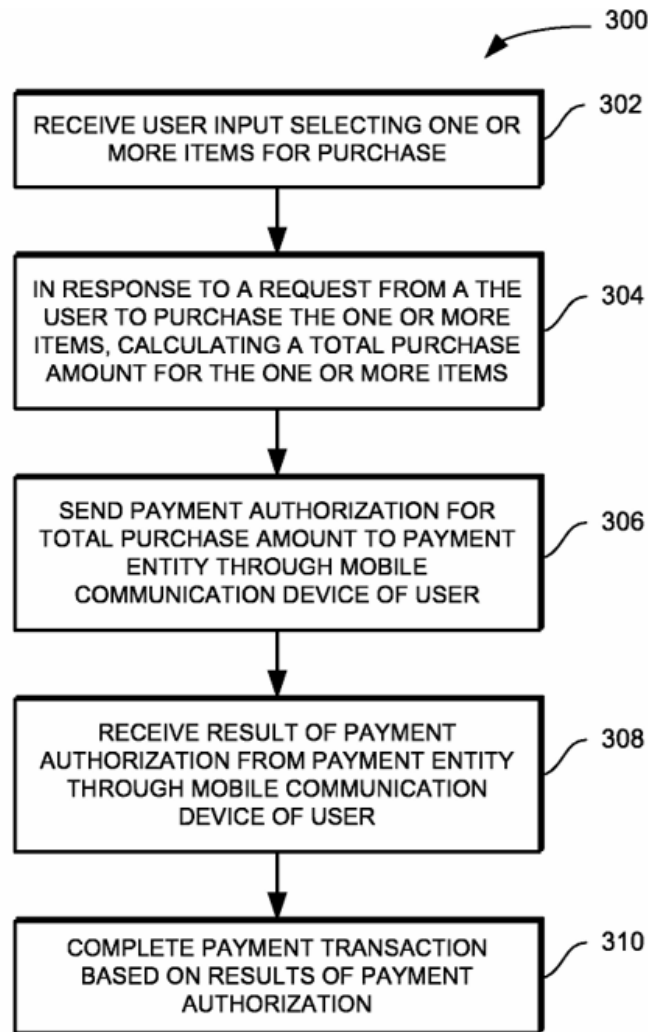
During the reexamination proceeding, the Examiner issued a Final Office Action on August 3, 2023, rejecting claims 1-36 of the ’007 Patent. Appx3447-3482. Patent Owner filed an appeal to the Patent Trial and Appeal Board, and then filed an Appeal Brief pursuant to 37 C.F.R. § 41.37 on December 22, 2023. Appx3641-3785. The Examiner issued an Answer on February 6, 2024 (Appx3968-4013), and Patent Owner filed a Reply Brief pursuant to 37 C.F.R. § 41.41 on March 7, 2024. Appx4016-4087.

On August 1, 2024, the Board issued its Decision on Appeal, affirming the Examiner’s rejections of claims 1-36 of the ’007 Patent. Appx10-52. Patent Owner

filed a Request for Rehearing on September 9, 2024 (Appx4132-4224) and the Board issued its Decision on Request for Rehearing on January 8, 2025, denying Patent Owner's rehearing request. Appx1-9. Patent Owner timely filed a Notice of Appeal on February 24, 2025. Appx4243-4298.

B. The '007 Patent: Ms. Michelle Fisher Invents A New Type Of System For Remote Processing Of A Transaction Using a Mobile Device.

Prior art systems for performing electronic transactions had various problems including fraudulent purchases, identify theft, and theft of sensitive information (*e.g.*, account numbers, pin numbers, identity information, identify theft). Appx63-64, 2:66- 3:5. To solve the problems associated with the prior art systems, Michelle Fisher created a new system for purchasing products comprising a mobile device with a non-browser based application, and a management server for processing a transaction in which there are two distinct steps for authenticating a user and authorizing a transaction. An exemplary method of one embodiment for conducting a payment transaction using a point of sale device is shown in FIG. 3, reproduced below.

**FIG. 3**

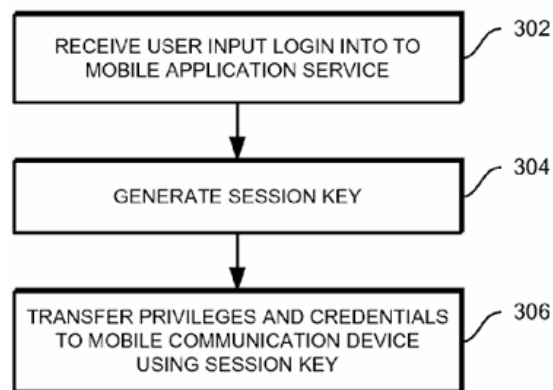
Appx60. In step 302, “[u]ser input is received selecting one or more items for purchase (e.g., at the point of sale device).” Appx65, 5:29-31. Next, in step 304, “a total purchase amount for the one or more items is calculated (e.g., by the point of sale device).” *Id.* at 5:36-38. Upon receiving a user request to make a purchase, payment is processed in accordance with a series of steps:

Payment **authorization** for the total purchase amount is sent to a payment entity through a mobile communication device of the user (step 306). A result of the payment **authorization** is received at the point of sale device from the payment entity via the mobile communication device (step 308). The payment transaction is completed based on the result of the payment authorization (step 310). Appx65, 5:44-51.²

“[T]he transaction being made at the point of sale device can be any type of transaction that involves the exchange or transfer of funds—e.g., the transaction can be a **payment transaction**, a **fund transfer**, or other type of transaction.” *Id.* at 5:31-35. “The point of sale device 104 can be a desktop computer, laptop computer, terminal, or **other device that is configured to receive user input selecting items for purchase or other transactions.**” Appx63, 2:53-55.

As explained in Patent Publication US20090124234 (“the ’234 Pub”, Appx4302-4307), corresponding to Ser. No. 11/939,821), which is incorporated by reference into the ’007 patent: “In one implementation, when a user subscribes to a mobile wallet the user is assigned credentials that include a unique WalletID, SiteKey, a user defined PIN, as well as tokens that specify access and privileges for the different services.” Appx4306, ¶ [0016]. FIG. 3 (reproduced below) of the ’234 Pub “illustrates one implementation of a method 300 for authenticating a user.” *Ibid.*

² All emphasis added unless otherwise noted.

**FIG. 3**

Appx4303. “The above example control[s] access to the Money Manager service and what privileges within the service a given user can perform. This will be used by the Client (mobile application) to enable/disable available features on the Client.” Appx4306, ¶ [0015]. As described in Patent Publication US20080052192 (“the ’192 Pub.”, Appx4308-4327), corresponding to Serial No. 11/933,351, which is incorporated by reference into the ’007 patent, “the mobile application 910 provides banking and money management service, which includes ... Fund Transfer - Inter Bank; Me-2-You (based on WalletID)”, and “Initiating/Triggering Banking Services” Appx4322-4323, ¶¶ [0036]-[0063].

C. The Board’s Decision On Appeal.

The Board affirmed the Examiner’s rejection of claims 1-36 as obvious under 35 U.S.C. § 103 over Khedouri in view of Goldthwaite and some additional

secondary references. Appx52. The Board concluded that the claim limitations “receives user input login information including the identification code associated with the user from the non-browser based application generated screen” and “upon receipt of the user input login information, authenticating, at the remote management server, a user associated with the user input login information” would have been obvious over Khedouri alone. Appx37-43. In reaching its obviousness conclusion, the Board did not rely on Khedouri’s deviceID or activation code. Appx38 (“We agree with Appellant that Khedouri at least suggests its device ID is provided by the device and therefore is not ‘user input’ as claimed”); Appx42 (“[W]e need not reach Khedouri’s Activation Code.”). Rather, the Board relied upon Khedouri’s disclosure of entering a PIN to “authorize charges.” Appx40, *quoting* Appx2746, ¶ [0094]. In reaching its obviousness conclusion, the Board disagreed with Blaze Mobile’s construction that distinguished authenticating a user with the user input login information from authorizing charges with a PIN and distinguished the claimed “identification code” from the PIN.” Appx30-34. Rather, the Board construed these user login information/user authentication claim limitations so broadly as to encompass Khedouri’s PIN information used to authorize charges. *Ibid.*

The Board concluded that the claim limitations of “receives, from the non-browser based application generated screen, an identification of one or more

products selected from the list of products; ...[and] receives a transaction purchase request including information relating to the identification of the one or more products from the non-browser based application generated screen” would have been obvious over Khedouri alone. Appx43-47. In reaching its obviousness conclusion, the Board disagreed with Blaze Mobile’s construction that these claim limitations require “the identification of one or more products” to have prices and be purchased and “the transaction purchase request” to be for the identified products. Appx34-35. The Board relied upon Khedouri’s disclosure of (i) free music samples, which do not have prices and cannot be purchased, and (ii) full music files, which are not both identified and requested to be purchased from the remote management server. Appx43-47.

The Board concluded that the claim limitations of a remote manager server that “receives user input login information including an identification code associated with a user,” “authenticat[es] ... a user associated with the user input login information,” and “transmits the payment method that corresponds to the identification code associated with the user to the transaction server,” and a transaction server configured to “receive a payment method that corresponds to an identification code associated with a user from a remote management server,” “send a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed,” and

“processes the transaction using the payment method” would have been obvious over the combination of Khedouri and Goldthwaite. Appx47-51. In particular, the Board concluded that the remote management server limitations would have been obvious over Khedouri’s disclosure of its network 315 authorizing payment with a PIN, and that the transaction server limitations would have been obvious over Goldthwaite’s disclosure of its financial institution server 112 issuing a payment card, processing a payment transaction and sending confirmation of the payment transaction. *Ibid.*

In reaching its obviousness conclusion, the Board disagreed with Blaze Mobile’s construction that these claim limitations require the remote management server to (i) receive “user input login information including an identification code associated with a user,” (ii) authenticate a “user associated with the user input login information,” and (iii) receive “a transaction verification” from a transaction server,” and a transaction server configured to (i) “receive a payment method that corresponds to an identification code associated with a user from a remote management server;” (ii) “send a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed;” and (iii) “processes the transaction using the payment method.” Appx25-27.

III. Summary Of The Argument

Reversal in this appeal of the Board's decision that claims 1-36 would have been obvious is justified because the Board's decision is based on erroneous claim constructions. Independent claim 2 recites "receives user input login information including an identification code associated with a user from the non-browser based application generated screen" and "authenticating, at the remote management server, a user associated with the user input login information." Appx66-67. The proper construction of these user login information/user authentication claim limitations requires (i) receiving at the mobile device user input login information including an identification code for the user *from a non-browser based application*, and (ii) *authenticating the user* associated with the user input login information (*i.e.*, confirm that the user is permitted access to a previously-established account).

Blaze Mobile's construction is consistent with the meaning as understood by a POSITA because "authentication" is "the process by which a user gains access to a website or application by logging in to it" using login information. Appx3422, ¶ 12. This construction is further supported by the definition of "login" as "[i]n a computer network, the authentication process in which a user supplies a login name and password" (Appx4328) and the definition of "authentication" as: "the process by which the system validates a user's login information. A user's name

and password are compared against an authorized list, and if the system detects a match, access is granted to the extent specified in the permission list for that user.”

Appx4330.

Nonetheless, the Board construed these user login information/user **authentication** claim limitations so broadly as to encompass information (*i.e.*, Khedouri’s PIN) used for the entirely different process of **authorizing** charges. Appx25-30. That is wrong because a POSITA would have understood that the claim limitation requiring information authenticating a user is different than Khedouri’s PIN authorizing charges. Appx3422, ¶ 12. Indeed, the specification of the ’007 patent including the patent applications incorporated therein distinguish authenticating a user to permit access to the user’s account from authorizing charges.” Appx4305, ¶ 4 (“The method can include use of biometrics to **authenticate the user** before **authorizing the transaction**”); Appx4325, ¶ 115 (“and then **authenticate, authorize**, and execute transfers of transaction information”).

The Board’s decision that Khedouri would have taught these user login information/user authentication claim limitations (Appx37-42) is not supported by substantial evidence under the proper claim construction because Khedouri makes no mention of them. The Board relied upon Khedouri’s teaching of “a PIN to authorize a purchase.” Appx39, *quoting* Appx2746, ¶ [0094] (“Billing follows the

above-described procedure and requires input at the minimum of a PIN code by the user to authorize charges on his or her credit card.”). But Khedouri’s PIN “*authorizing* charges” (Appx2746, ¶ [0094]) on a credit card is different than the information *authenticating* a user to permit access to the user’s account of claim 2. Indeed, the only authentication mentioned by Khedouri is for a device using a deviceID (Appx2740-2741, ¶¶ [0056] and [0058]). Khedouri’s deviceID cannot possibly be the claimed “user input login information” because it is associated with the *device, not the user* as required by claim 2, and is *not input by the user* from a non-browser application, as also required by claim 2. In addition, Khedouri’s PIN cannot be the claimed “identification code” because the claimed “PIN” and “identification code” must have different meanings under the proper claim construction. For these reasons alone, the Board’s obviousness decision of claim 2, as well as independent claims 1 and 3 and the claims dependent therefrom, should be reversed.

Independent claim 2 also recites:

receives, from the non-browser based application generated screen, an *identification of one or more products* selected from the list of products ... through user input via the mobile device display
receives a transaction purchase request including information relating to the identification of the one or more products from the non-browser based application generated screen ... from the user via the mobile device display of the mobile device;

Appx66-67. The proper construction of these claim limitations requires sending to the remote management server both (i) “the identification of one or more products” having prices and are purchased and (ii) “the transaction purchase request” of the identified products. This construction is consistent with the repeated disclosure in the specification of the ’007 patent that the “one or more products” are items having prices that are purchased, not merely free samples:

The method includes receiving input from a user *selecting an item for purchase* through the point of sale device; *calculating a total purchase amount for the item in response to a request from the user to purchase the item*; and sending payment authorization for the total *purchase amount* from the point of sale device to a payment entity, in which the payment authorization is sent to the payment entity.
Appx63, 1:43-50.

In response to a *request from the user to purchase the one or more items*, a *total purchase amount* for the one or more items is calculated (e.g., by the point of sale device) (step304). Appx65, 5:35-38.

“The user *request to purchase an item* can be received, e.g., by a user clicking on a ‘buy now’ icon that is displayed on a graphical user interface of the point of sale device.” Appx65, 5:41-44.

Nonetheless, the Board construed these claim limitations so broadly as to encompass Khedouri’s teachings of (i) free music samples, which do not have prices and cannot be purchased, and (ii) full music files, which are not both identified and requested to be purchased from the remote management server.
Appx43-47. More particularly, Khedouri’s “request” for an “audio or video clip”

cannot be an “identification” of the full audio or video file available for purchase for at least three separate and independent reasons. First, the clip is a different file from the full file. *See* Appx2748, ¶¶ [0108], [0110]. Second, when the request for the clip “is queued up” and “the device sends the request,” the user has not been “offered the opportunity to purchase the full file.” *Ibid*. Third, the clip is free, and therefore cannot be the claimed “one or more products,” which need to have prices and are purchased. *Ibid*.

Moreover, the sole request “to purchase the full file” (Appx2748, ¶ [0110]) cannot possibly satisfy each of the separate “identification” and “transaction purchase request” required by claim 2 of the ’007 patent. More particularly, Khedouri discloses that when “the user is offered the opportunity to purchase the full file,” the full file “may have already been delivered to the device, but its DRM [Digital Rights Management] may not be ‘unlocked’ because the ‘key’ for that file has not been provided yet.” *Ibid*. Rather than teach a separate “identification” prior to the “transaction purchase request,” as required by claim 2, Khedouri teaches that the full file has been downloaded without any “identification” in anticipation of the user purchasing the full file. Appx2742-2743, ¶ [0069] (“[T]he receiver may be able to obtain a copy of the file, but the digital rights management software local on the receiver’s player device will not permit the user to play the content.”). Clearly, Khedouri would not have taught or suggested to a POSITA both sending

to the remote management server both (i) “the identification of one or more products” having prices and are purchased and (ii) “the transaction purchase request” of the identified products. *See Applied Med. Res. Corp.*, 448 F.3d at 1333 n. 3 (“[T]he use of two terms in a claim requires that they connote different meanings.”). For these additional reasons, the Board’s obviousness decision of claim 2, as well as independent claims 1 and 3, which recite similar limitations, and the claims dependent therefrom, should be reversed.

Independent claim 2 also recites:

receives user input login information including an identification code associated with the user ...;

upon receipt of the user input login information, authenticating, at the remote management server, a user associated with the user input login information;

transmits the payment method that corresponds to the identification code associated with the user to the transaction server;

and send a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed ... ;

...

a transaction server processor that processes the transaction using the payment method.

Appx66-67. The proper construction of these claim limitations requires (1) a remote management server to (i) receive “user input login information including an

identification code associated with a user,” (ii) authenticate a “user associated with the user input login information,” and (iii) receive “a transaction verification” from a transaction server,” and (2) a transaction server configured to (i) “receive a payment method that corresponds to an identification code associated with a user from a remote management server;” (ii) “send a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed;” and (iii) “processes the transaction using the payment method.” This meaning is consistent with the disclosure in the specification of the ’007 patent of the remote management server *authenticating the user* and receiving transaction verification from a transaction server rather than merely entering a PIN to authorize charges on a credit card:

As such, the management server 180 can store user personal and credit and transaction information and history, including a code associated with the user. Appx4325, ¶ [0116].

[T]he data can be securely stored on the remote server using convention PCI guidelines. Hence, in the event the mobile communication device 102 is lost (or stolen), no confidential data can be recovered as no data is stored on the mobile communication device 102. Appx4306, ¶ [0013].

[S]oftware in transaction server 170 that will ... authenticate, authorize, and execute transfers of transaction information to the management server 180. In one implementation, the piggybacked payload is sent, instead of to the transaction server 170 to the management server 180. Appx4325, ¶[0115].

The transaction server 170 verifies the transaction, and forwards a transaction verification signal to the management server 180. The

management server 180 identifies the user corresponding to the transaction verification signal, and provides a first transaction response signal back to the mobile communication device 110. Appx4320, ¶ [0020]).

Nonetheless, the Board construed these claim limitations so broadly as to encompass Khedouri's teachings of a network element 315 that merely authorizes payment for a transaction. Appx48-49 ("The Examiner relied on Khedouri, not Goldthwaite, for teaching the claimed remote management server and authentication."). Khedouri's network 315, however, cannot possibly satisfy the claim limitations of the "remote management server" because it neither (i) receives "user input login information" nor (ii) authenticates a "user associated with the user input login information." Instead, Khedouri's network 315 merely authorizes payment with a PIN instead of a credit card number. Appx2741, ¶ [0057] ("[T]he user's card information can be stored on the network in the subscriber database (302, FIG. 3) in order that the user would not need to re-enter this information but would only need to enter a 4-digit security PIN code that is similarly stored and verified by the network.").

Moreover, the Board construed the "transaction server" claim limitations so broadly as to encompass Goldthwaite's financial institution/server 112 merely because it issues a payment card, processes a payment transaction and sends confirmation of the payment transaction. Appx48-49. The Board failed to even attempt to explain how Goldthwaite's financial institution/server 112 "processes

the transaction using the payment method,” which “corresponds to the [same] identification code associated with the user” that was used to authenticate the user, as required by claim 2. *See ibid.* The Board’s obviousness decision disregards important claim limitations. *Beckson Marine, Inc. v. NFM, Inc.*, 292 F.3d 718, 727 (Fed. Cir. 2002) (for claimed subject matter to be obvious either the prior art references must expressly reach each claim limitation exactly or else the record must disclose a reason for a person of ordinary skill in the art to modify the prior art teachings to obtain the claimed invention).

When claim limitations are wholly absent from the teachings of the prior art, documentary evidence is required to establish obviousness. *K/S HIMPP v. Hear-Wear Technologies, LLC*, 751 F.3d 1362, 1366 (Fed. Cir. 2014) (“an assessment of basic knowledge and common sense as a replacement for documentary evidence for core factual findings lacks substantial evidence support.”). The Board did not present the required documentary evidence to support its position that the claim limitations that are missing from the prior art, would have been obvious. The Board did not present any documentary evidence that it would have been obvious to modify a system that authorizes a device to complete a transaction with a credit card payment as in Khedouri to a system that authenticates a user with information input by the user with a non-browser application, as required by claim 2 of the ’007 patent. *See Appx37-42.*

The Board similarly failed to present documentary evidence that it would have been obvious to modify Khedouri's network 315 that merely inputs "a PIN code by the user to authorize charges on his or her credit card" (Appx2746, ¶ [0094]) to a system with a "remote management server" that (i) receives "user input login information" and (ii) authenticates a "user associated with the user input login information," and a "transaction server" that "processes the transaction using the payment method," which "corresponds to the [same] identification code associated with the user" that was used to authenticate the user, as required by claim 2. *See* Appx47-51. Indeed, Khedouri teaches that the content is sent without receiving a transaction verification. Appx2749, ¶ [0139] ("[w]hen the device connects to the network, the purchase is processed, and the content is sent"). Therefore, there would have been no need to modify any server in Khedouri to "download[] one or more products" only "after receiving the transaction verification," as required by claim 2. A POSITA would not have modified Khedouri in the manner suggested by the Board.

For these additional reasons, the Board's obviousness decision of claim 2, as well as independent claims 1 and 3, which recite similar limitations, and the claims dependent therefrom, should be reversed.

IV. Standard Of Review

This Court reviews decisions by the Board according to the standards of review set forth in the Administrative Procedure Act. *In re Chapman*, 595 F.3d 1330, 1336-37 (Fed. Cir. 2010). Accordingly, the Court reviews the Board’s legal conclusions de novo, and its factual findings for substantial evidence. *Id.*; see 5 U.S.C. § 706(2); see also *Rambus Inc. v. Rea*, 731 F.3d 1248, 1251 (Fed. Cir. 2013); *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1364 (Fed. Cir. 2015). The Court reviews the Board’s claim constructions de novo, as it relied only on intrinsic evidence. *Microsoft Corp. v. Proxyconn, Inc.*, 789 F.3d 1292, 1297 (Fed. Cir. 2015). The Board’s decision may be vacated and remanded to the Board to consider the patentability grounds under the proper construction. *In re Abbott Diabetes Care, Inc.*, 696 F.3d 1142, 1150 (Fed. Cir. 2012).

“Obviousness is a mixed question of law and fact, and we review the Board’s ultimate obviousness determination de novo and underlying fact-findings for substantial evidence.” *Mylan Pharms. Inc. v. Merck Sharp & Dohme Corp.*, 50 F.4th 147, 152 (Fed. Cir. 2022). Obviousness determinations that are based on an improper construction should be vacated. *In re Man Mach. Interface Techs. LLC*, 822 F.3d 1282, 1288-89 (Fed. Cir. 2016). “The presence or absence of a motivation to combine references in an obviousness determination is a pure question of fact. The presence or absence of a reasonable expectation of success is

also a question of fact. What a reference teaches and whether it teaches toward or away from the claimed invention are questions of fact.” *Par Pharm., Inc. v. TWI Pharms., Inc.*, 773 F.3d 1186, 1196-97 (Fed. Cir. 2014) (cleaned up).

“The ultimate question of whether the reexamination is based on a substantial new question of patentability remains a question of law.” *In re Vivint, Inc.*, 14 F.4th 1342, 1348 (Fed. Cir. 2021) (cleaned up).

Under the Administrative Procedure Act and longstanding precedent, an agency must provide “a satisfactory explanation for its action including a rational connection between the facts found and the choice made.” *Motor Vehicle Mfrs. Ass’n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983). The Board must address the “important aspect[s] of the problem” presented to it. *Id.* at 43. That requirement exists to facilitate judicial review and to ensure that agency decisions are not arbitrary and capricious. *SEC v. Chenery Corp.*, 318 U.S. 80, 94 (1943). The need for specific explanation applies with particular force to obviousness determinations, for both substantive and procedural reasons. To avoid hindsight, an obviousness “analysis should be made explicit,” and obviousness rulings “cannot be sustained by mere conclusory statements,” as opposed to “articulated reasoning with some rational underpinning.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007); *Rovalma, S.A. v. Bohler-Edelstahl GmbH*, 856 F.3d 1019, 1025 (Fed. Cir.

2017) (“The Supreme Court has recognized the importance of clarity with respect to obviousness determinations.”).

Importantly, this Court’s “review of [the Board’s] patentability determination is confined to the grounds on upon which the Board actually relied.” *Power Integrations, Inc. v. Lee*, 797 F.3d 1318, 1326 (Fed. Cir. 2015). The Court cannot “accept appellate counsel’s post hoc rationalizations for agency action” or “supply a reasoned justification for an agency action that the agency itself has not given.” *Id.* (quoting *Burlington Truck Lines v. United States*, 371 U.S. 156, 168 (1962) and citing *State Farm*, 463 U.S. at 43). This Court, thus, reverses or vacates Board decisions that ignore, assume away, or insufficiently explain important aspects of the obviousness analysis. *See, e.g., Personal Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 992 (Fed. Cir. 2017) (“We have repeatedly applied those requirements in reviewing the adequacy of the Board’s obviousness analysis. . . . Our review of the Board is rooted not just in the law of obviousness but in basic principles of administrative law.”); *Rovalma*, 856 F.3d at 1026; *In re NuVasive, Inc.*, 842 F.3d 1376, 1382 (Fed. Cir. 2016); *Ariosa*, 805 F.3d at 1364-67.

Even where this Court upholds a “motivation to combine” factual finding, the Court completes its review by assessing whether that same “motivation” is one that rationally would have led a POSITA to “achieve the claimed invention.” *In re*

NuVasive, 842 F.3d at 1381; *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1360 (Fed. Cir. 2012).

V. Argument

A. The User Login Information/User Authentication Claim Limitations Would Not Have Been Obvious Under The Proper Claim Construction

The Board’s Final Decision should be vacated because it is based on an incorrect claim construction of the claim limitations: “receives user input login information including an identification code associated with a user from the non-browser based application generated screen” and “authenticating, at the remote management server, a user associated with the user input login information” (*i.e.*, “the user login information/user authentication claim limitations”). Under the proper constructions, these claim limitations would not have been obvious to a POSITA.

1. The Broadest Reasonable Claim Construction Standard.

In construing claim terms in a reexamination, the Board must determine their meaning according to the broadest reasonable interpretation consistent with the specification. *In re Smith Int’l, Inc.*, 871 F.3d 1375, 1381 (Fed. Cir. 2017). Under the broadest reasonable construction standard, claim terms are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). Additionally, the “appropriate context” to read a

claim term includes both the specification and the claim language itself. *In re Suitco Surface, Inc.*, 603 F.3d 1255, 1260 (Fed. Cir. 2010).

“The correct inquiry in giving a claim term its broadest reasonable interpretation in light of the specification is not whether the specification proscribes or precludes some broad reading of the claim term adopted by the examiner.” *In re Smith Int’l, Inc.*, 871 F.3d at 1382-1383. “[I]t is not simply an interpretation that is not inconsistent with the specification. It is an interpretation that corresponds with what and how the inventor describes his invention in the specification, *i.e.*, an interpretation that is ‘consistent with the specification.’” *Ibid.* (quoting *In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997)). Significantly, “[a]ll the limitations of a claim must be considered meaningful.” *Unique Concepts, Inc. v. Brown*, 939 F.2d 1538, 1562 (Fed. Cir. 1991) (citing *Perkin-Elmer Corp. v. Westinghouse Elec. Corp.*, 822 F.2d 1528, 1532-33 (Fed. Cir. 1987)).

2. The Board’s Claim Construction Erroneously Conflates The User Login Information/User Authentication Claim Limitations With A PIN To Authorize Charges.

The Board construed these user login information/user authentication claim limitations so broadly as to encompass information used for the entirely different process in Khedouri of entering a PIN to “authorize charges” on a credit card. Appx38-39, *quoting* Appx2746, ¶ [0094]. That is wrong because a POSITA would

have understood that the claim limitation requiring information *authenticating* a user is different than information authorizing a charge. Appx3422, ¶ 12.

Indeed, the claims distinguish *authenticating a user* from *authorizing a transaction* (e.g., a charge) by separately claiming these different processes. For *authenticating a user*, claim 2 recites: “receives user input login information including an identification code associated with a user from the non-browser based application generated screen” and “authenticating, at the remote management server, a user associated with the user input login information.” Appx66-67. For *authorizing³ a transaction*, claim 2 recites a transaction server which “processes the transaction using the payment method,” which “corresponds to the [same] identification code associated with the user” that was used to authenticate the user, *Ibid.*

Therefore, the Board’s claim construction conflating *user authentication* with *transaction authorization* (i.e., “authorize charges”) contradicts the claim language, which expressly and separately recites both *user authentication* and

³ Authorization-The process of obtaining permission from the issuing bank to accept the card for payment. *Authorization entails assessing the card’s transaction risk and reserving the specified amount of credit on the cardholder’s account if approved.* If a merchant does not comply with Association rules regarding authorizations, payment to the merchant may be withheld or a subsequent charge-back may occur. Authorization processes vary between merchant types.

https://www.fdic.gov/regulations/examinations/credit_card/pdf_version/ch21.pdf

transaction authorization. Appx66-67. See *Haemonetics Corp. v. Baxter Healthcare Corp.*, 607 F.3d 776, 782 (Fed. Cir. 2010) (claims not to be construed to "contradict their plain language").

Likewise, the specification of the '007 patent distinguishes authenticating a user to permit access to the user's account from authorizing a service such as a transaction. Appx4305, ¶ 4 ("The method can include use of biometrics to **authenticate the user** before **authorizing the transaction**"). The '192 Pub. lists "authenticate" as a separate step than "authorize." Appx4325, ¶ [0115] ("software in transaction server ... will extract the piggybacked payload, associate the payload with the management server 180 if needed, and then authenticate, authorize, and execute transfers of transaction information to the management server 180.").

Disregarding this disclosure, the Board erroneously determined that "**the '007 patent itself discloses 'authentication' using a one-time code.**" Appx33, quoting Appx64, 4:42-60. The Board's determination, however, is flawed because it fails to consider much of the passage from the '007 Patent that it quoted to support its decision, as shown by the more complete reproduction of the passage below:

The merchant portal ... securely connects to the management server 408 In one implementation, the management server 408 **identifies the consumer through their cell phone number**, and verifies the consumer's authenticity by sending **a unique transaction code to the consumer mobile wallet on their cell phone**. The consumer then enters this **unique transaction code** onto the merchant's web portal. The merchant portal sends this transaction

number to the management server 408 for authentication. Upon authentication, the consumer's virtual wallet and payment methods (e.g., credit card, debit card, prepaid card, etc.) are securely retrieved from the management server 408 and are displayed to the consumer in a window on a website associated with the merchant portal. The consumer selects one of these payment methods to pay for their transaction ... ***After the consumer enters any necessary validation information to provide a multi-factor authentication*** and confirms the transaction, the online purchase is processed as normal by the merchant's online processor. The mobile wallet can retrieve transaction data, account balance from the management server 408. Appx64-65, 4:49-5:9.

The portions of the passage omitted by the Board indicate that the "unique transaction code" is used for ***device*** authentication, not ***user*** authentication because the "unique transaction code" is transmitted to a mobile device using the ***mobile phone number***, which is associated with the device. Indeed, this passage from the Specification clearly ***doesn't*** state that the ***user*** is authenticated with the "unique transaction code." Instead, the portions of the passage omitted by the Board state that "the management server 408...verifies the consumer's ***authenticity*** by sending a unique transaction code to the consumer mobile wallet on their cell phone." Appx64; *see also* Appx4647 (defining "authenticity" as "***not false or imitation : REAL, ACTUAL***"). In other words, the "unique transaction code" is used to verify that only the unique or real mobile device is being used in the transaction and not a rogue mobile device trying to impersonate the real mobile device. As would have been known by a POSITA, this type of verification prevents command spoofing, which is an attempt by an imitation device to impersonate the real mobile device

and send commands to compromise the security of the real mobile device. *See e.g.*, Appx4306, ¶ [0016] (preventing command spoofing with a session key: the “*session key is used to ensure the server can identify the client and ensure that the client has been previously authenticated*”). Furthermore, the portions of the passage omitted by the Board also indicate that multiple factors, rather than a single PIN for *authorization* at taught by Khedouri, are required to *authenticate a user*:

After the consumer enters any necessary validation information to provide a multi-factor authentication and confirms the transaction, the online purchase is processed as normal by the merchant’s online processor. Appx64, 4:5:4-8.

Thus, in every embodiment of the ’007 patent, a user enters user input login information for *user* authentication. This contrasts sharply with *device* authentication, which relies on a “unique transaction code” sent to a mobile phone number and entered by anyone in possession of the mobile device.

Likewise, the ’234 Pub discloses authorizing user access to a “Money Manager” service after authentication of a user by a remote management service: “The above example control[s] access to the Money Manager service and what privileges within the service a given user can perform. This will be used by the Client (mobile application) to enable/disable available features on the Client.” Appx4306, ¶ [0015]. This money management service is shown by FIG. 9 (reproduced below) of the ’192 Pub, which “illustrates a communication system

900 ... includ[ing] a mobile communication device 902, a management server 904, a user/profile database 906, and a money management database 908.” Appx4322, ¶ [0034].

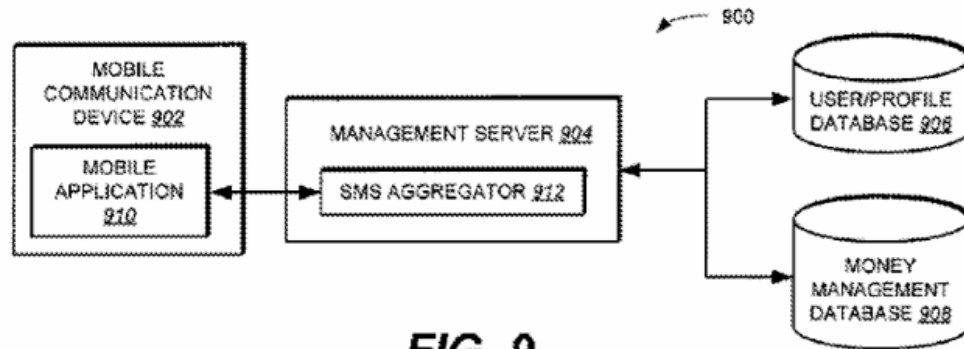


FIG. 9

Appx4318. More particularly, "[u]pon a **successful login**, the server will transfer credentials, **service access and privileges** (step 306), which are locally cached on the mobile communication device" (Appx4306, ¶ [0016]), thereby providing access after user authentication to services such as "Transactions, Payment."

Appx4305-4306, ¶¶ [0011], [0015].

Moreover, the specification indicates that the claimed "identification code associated with the user" is different than a personal identification number (PIN) because it separately refers to both terms:

The mobile application can include a **multi-factored** PIN-based **login** and **authentication**. Appx4305, ¶ [0012].

One potential benefit of having payment authorizations flow through the mobile communication device 102 is that sensitive user information (*e.g.* account numbers, **pin numbers**, and/or **identity information**) need

only be sent from the mobile communication device 102 directly to an issuer authorization. Appx63-64, 2:63-3:3.

Registration: User creates new MW Lite account with PIN (***PIN and user info*** can be stored in user/profile database 306). Appx4322, ¶ [0037].

In one implementation, when a user subscribes to a mobile wallet the user is assigned ***credentials*** that include a unique WalletID, SiteKey, ***a user-defined PIN***, as well as tokens that specify access and privileges for the different services. FIG. 3 illustrates one implementation of a method 300 for authenticating a user. User input is received (through a mobile communication device) logging into the mobile application service (step 302). In one implementation, when a user attempts to login with the client, the user is prompted to enter login ***credentials*** (e.g., mobile phone number, 1-time activation code, ***Wallet PIN***, etc.)... Upon a successful login, the server will transfer credentials, service access and privileges (step 306), which are locally cached on the mobile communication device. Appx4306, ¶ [0016].

The method can include use of biometrics to ***authenticate the user*** before ***authorizing the transaction***. Appx4305, ¶ 4

Clearly, the Board erred in construing the “identification code associated with the user” for authenticating the user of claim 2 to be a personal identification number (PIN) for authorizing a transaction.

3. Blaze Mobile’s Construction Of The User Login Information/User Authentication Claim Limitations Is Supported By The Claim Language, The Specification, And The Prosecution File History.

The proper construction of these user login information/user authentication claim limitations requires (i) receiving at the mobile device user input login information including an identification code for the user from a non-browser based application, and (ii) authenticating the user associated with the user input login

information (*i.e.*, confirm that the user is permitted access to a previously-established account).⁴ This construction is consistent with the meaning as understood by a POSITA because “authentication” is “the process by which a user gains access to a website or application by logging in to it” using login information. Appx3422, ¶ 12. This construction is further supported by the definition of “login” as “[i]n a computer network, the authentication process in which a user supplies a login name and password” (Appx4328) and the definition of “authentication” as: “the process by which the system validates a user’s login information. A user’s name and password are compared against an authorized list, and if the system detects a match, access is granted to the extent specified in the permission list for that user.” Appx4330. “Authentication” is also described in connection with “access control” as: “[i]n a network, a means of ensuring the systems security by demanding that users supply some means of identifying themselves, such as a login name and password.” Appx4331.

Blaze Mobile’s claim construction is also consistent with the specification. For example, the ’234 Pub discloses that the user login information is used to

⁴ The construction of this claim limitation must be consistent with the construction of a similar limitation in U.S. Patent 10,699,259 (“the ’259 patent”), the patent at issue in related appeal number 2025-1485. *Omega Eng’g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1334 (Fed. Cir. 2003) (“unless otherwise compelled ... the same claim term in the same patent or related patents carries the same construed meaning.”). The ’007 patent and ’259 patent have the same inventors and owner, and their specifications are nearly identical.

authenticate a user to permit access to a previously-established account: “[T]he session key is used to ensure the server can identify the client and ensure that *the client has been previously authenticated* ... Failure to validate the session key will ... force the user to *re-authenticate* (or re-login).” Appx4306, ¶ [0016]). The ’234 Pub explains that a user must first be authenticated using biometrics or multi-factored login before payment may be authorized in a subsequent, separate step using security and/or identification codes. Appx4305, ¶ [0004] (“The method can include use of biometrics to *authenticate the user before authorizing the transaction*”); Appx4305, ¶ [0012] (“The mobile application can include a *multi-factored PIN-based login and authentication*, and include session keys and have *command level authentication*. In one implementation, the mobile application running on the mobile communication device 102 can be remotely locked through a remote server.”).

Blaze’s claim construction is also consistent with the file history. *See e.g., Microsoft Corp.*, 789 F.3d at 1298 (holding that the PTO, in determining the broadest reasonable interpretation (BRI) of a claim term, should “consult the patent’s prosecution history in proceedings in which the patent has been brought back to the agency for a second review.”). During prosecution of the ’007 Patent, Blaze Mobile distinguished the claimed “user input login information including an identification code associated with a user” over the Rackley prior art reference:

[W]hile Rackley teaches that a one-time password is entered to initialize the mobile client in paragraph 266, Rackley positively recites that the PIN is stored on the client and that the user is authenticated locally in paragraph 280 and 336 relied upon by the Examiner.

...

In contrast, Applicant teaches that the ***user is authenticated at the server*** as reflected in amended claims which recite in part, “upon receipt of the user input login information, ***authenticating, at the remote management server***, a user associated with the user input login information;”

Rackley’s invention is different from an engineering, security, and reliability perspective. ***Because the PIN is stored on the mobile device, it is not as secure or reliable.***

Appx4144 (*emphasis in original*). That is, Blaze Mobile referenced the “user input login information including an identification code” which is “receive[d] ... from the non-browser based application generated screen” to distinguish the claims from Rackley’s disclosure of a PIN stored on a mobile device and clearly explained clearly that Rackley’s PIN is not the claimed “user input login information.”

Clearly, Blaze Mobile’s construction of the user login information/user authentication claim limitations to require (i) receiving at the mobile device user input login information including an identification code for the user from a non-browser based application, and (ii) authenticating the user associated with the user input login information (*i.e.*, confirm that the user is permitted access to a previously-established account) is supported by the plain meaning of the claim language, the specification, and the file history.

4. The Board’s Ruling That The Prior Art Would Not Have Taught The User Login Information/User Authentication Claim Limitations Is Not Supported By Substantial Evidence Under The Proper Claim Construction.

The Board exclusively relies on Khedouri’s discussion of a personal identification number (“PIN”) for credit card authorization in paragraphs [0057] and [0094] as allegedly meeting the user login information/user authentication claim limitations. Appx39-49.⁵ In particular, the Board relies upon Khedouri’s credit card authorization process wherein “the user’s card information can be stored on the network ... in order that the user would not need to re-enter this information but only need to enter a 4-digit security PIN code” and “[b]illing follows the above-described procedure and requires input at the minimum of a PIN code by the user to authorize charges on his or her credit card.” Appx39-49, *quoting* Appx2741, ¶ [0057] and Appx2746, ¶ [0094].

But as explained *supra* §§ V.A.2 and V.A.3, the proper construction of the user login information/user authentication claim limitations requires (i) receiving at the mobile device user input login information including an identification code for the user from a non-browser based application, and (ii) authenticating the user associated with the user input login information (*i.e.*, confirm that the user is

⁵ The Board “agree[s] with Appellant that Khedouri at least suggests its deviceID is provided by the device and therefore is not ‘user input’ as claimed” (Appx38) and did “not reach Khedouri’s Activation Code” as allegedly teaching the user login information/user authentication claim limitations. Appx42.

permitted access to a previously-established account). And Khedouri's mere disclosure of entering "a PIN code by the user to authorize charges" on a credit card (Appx2746, ¶ [0094]) is not nearly sufficient to satisfy these claim requirements.

Rather, Khedouri discloses how a user can purchase a subscription to become a subscriber (*e.g.*, unlimited music selections for one month) or purchase specific "a la carte" content items (*e.g.*, "Jessica" by the Allman Brothers). Appx2726, Appx2741, ¶ [0057]. In Khedouri, the user inputs credit card information such as the "digits of the credit card," "the type of card," and "the expiration date." *Ibid.* A POSITA would not have considered such credit card information to be the claimed user input login information for authenticating a user. Indeed, the input of the credit card information causes the network to "perform[] a credit card authorization process" to "charge[] his or her credit card appropriately." *Ibid.* Also, because the 4-digit security PIN code corresponds to the user's card information, Khedouri's network is simply verifying that the 4-digit security PIN code maps to the user's card information. *See* Appx2746, ¶ [0094]. If the mobile device is lost or stolen, anyone can make a purchase by guessing the 4-digit security PIN because the user is not identified, let alone authenticated as required by the proper construction of claim 2. Accordingly, Khedouri's PIN is not

used to login and authenticate a user as required by claim 2; it is instead used for a "credit card authorization process."

In Khedouri, the "user's card information can be stored on the network in the subscriber database" and rather than being input in its entirety next time, the user can enter a "4-digit security PIN code that is similarly stored and verified by the network." Appx2758, ¶ [0057]). Like the original credit card information, the 4-digit PIN does not meet the requirements for the proper construction of the user login information/user authentication claim limitations. Rather, it is simply a code to input for Khedouri's credit card authorization process.

Khedouri's paragraph [0094] similarly also fails to meet the requirements of the user login information/user authentication claim limitations. It instead describes the user interface in Figure 9 by which a user selects an artist (Allman Brothers) 901 causing a list of songs to be displayed ("Statesboro Blues" etc.). Appx2741, ¶ [0094]. After selecting a song (*e.g.*, "Jessica" from the "Legendary Hits" album of Figure 10), Figure 10 illustrates a user interface where the user is given the option to access the song/album for "Free" or instead, the user can select "buy song" (Appx2726) where the "[b]illing follows the above-describe procedure and requires input at the minimum of a PIN code by the user to authorize charges on his or her credit card." Appx2741, ¶ [0094]. Accordingly, Khedouri describes a

credit card authorization process, not the user login information/user authentication claim limitations.

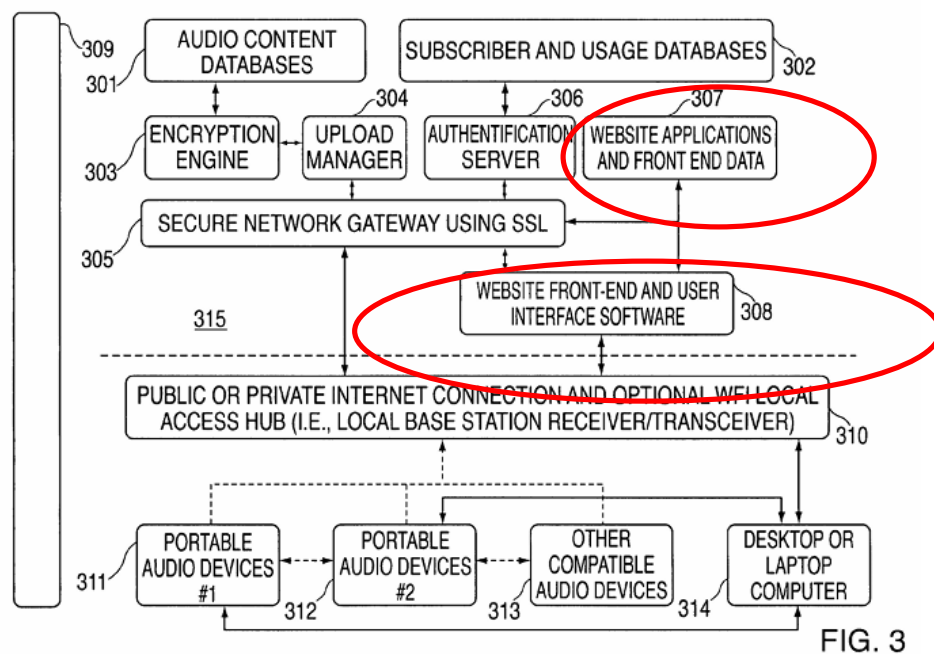
When claim limitations are wholly absent from the teachings of the prior art, documentary evidence is required to establish obviousness. *K/S HIMPP*, 751 F.3d at 1366. The Board did not present the required documentary evidence to support its position that the claim limitations that are missing from Khedouri, would have been obvious. The Board did not present any documentary evidence that it would have been obvious to modify a system that authorizes a device to complete a transaction with a credit card payment as in Khedouri to a system that authenticates a user to confirm that the user is permitted to access a previously-established account with information input by the user with a non-browser application, as required by claim 2 of the '007 patent. *See* Appx38-42.

Moreover, there is no mention in Khedouri of inputting a PIN for a “user from the non-browser based application,” as also required by claim 2. The Board relies on Khedouri’s disclosure that a device “can access and download information and content without a browser” (Appx39, *quoting* Appx2748, ¶ [0121]) and that “[u]sers may search for new content at any time, without being connected to the Internet or any external database, by searching the locally stored database on the device.” Appx39 (*emphasis omitted*), *quoting* Appx2746, ¶ [0093]. But none of these passages in Khedouri make any mention of inputting user input login

information from a non-browser based application, as required by claim 2. They instead relate to searching for new music content and downloading it.

Indeed, much of Khedouri's disclosure includes a web browser. Appx2748, ¶ [0122] ("Other devices use a **browser** to enable a user to purchase content."); see also Appx2739-2746, ¶¶ [0044]-[0045], [0078]-[0080], [0057], and [0094].

Khedouri's Figure 3 (reproduced with annotations below) includes a web browser to "access the network's Web site 308, the pages of which are generated dynamically based on *Web site software and related applications 307*. Content need not ever be delivered to the computer 314, and the *Web site front-end and user interface software 308* can merely enable the user to search, sort, organize, order content to be delivered to his or her portable device 311, 312, or for other account-related functions." Appx2744, ¶ [0079].



Khedouri discloses that the steps required to purchase music content require a web browser. First, the device automatically transmits the deviceID to network 315 for authentication (Appx2739-2747, ¶¶ [0044-0045], [0078-0080], and [0103-0104]) and then, a user enters a 4 digit Security PIN code into a web browser to *verify their credit card* so that “the user would not need to re-enter this information but would only need to *enter a 4-digit Security PIN code* that is similarly stored and *verified* by the network.” Appx2741, ¶ [0057]; *see also* Appx2746, ¶ [0094].

For these additional reasons, the user login information/user authentication claim limitations would not have been obvious.

B. The Claim Limitations Relating To Sending “the identification of one or more products” and “the transaction purchase request” To The Remote Management Server Would Not Have Been Obvious Under the Proper Claim Construction.

The Board’s Final Decision should be vacated because it is based on an incorrect claim construction of the claim limitations: “receives, from the non-browser based application generated screen, an identification of one or more products” and “receives a transaction purchase request including information relating to the identification of the one or more products from the non-browser based application generated screen.” Under the proper construction, these claim limitations would not have been obvious to a POSITA.

1. Blaze Mobile’s Construction Of The Claim Limitations Related To Sending “the identification of one or more products” and “the transaction purchase request” To The Remote Management Server Is Supported By The Claim Language and The Specification.

Independent claim 2 also recites:

receives, from the non-browser based application generated screen, an *identification of one or more products* selected from the list of products ... through user input via the mobile device display
receives a transaction purchase request including information relating to the identification of the one or more products from the non-browser based application generated screen ... from the user via the mobile device display of the mobile device;

Appx66-67. The proper construction of these claim limitations requires sending to the remote management server both (i) “the identification of one or more products” having prices that are purchased and (ii) “the transaction purchase request” of the identified products.⁶ This construction is consistent with the specification’s disclosure that the “one or more products” are items having prices that are purchased, not merely free samples:

“The method includes receiving input from a user *selecting an item for purchase* through the point of sale device; *calculating a total purchase amount for the item in response to a request from the user*

⁶ The construction of this claim limitation must be consistent with the construction of a similar limitation in the ’259 patent, the patent at issue in related appeal number 2025-1485. *Omega Eng’g*, 334 F.3d at 1334. The ’007 patent and ’259 patent have the same inventors and owner, and their specifications are nearly identical.

to purchase the item; and sending payment authorization for the total *purchase amount* from the point of sale device to a payment entity.” Appx63, 1:43-49.

“In response to a *request from the user to purchase the one or more items*, a *total purchase amount* for the one or more items is calculated (e.g., by the point of sale device) (step304).” Appx65, 5:35-38.

“The user *request to purchase an item* can be received, e.g., by a user clicking on a ‘buy now’ icon that is displayed on a graphical user interface of the point of sale device.” *Id.* at 5:41-44.

The Specification further explains that a user may select items for purchase:

[A] mobile application ... permits a user of the mobile communication device 102 to *conduct payment transactions*. Payment transactions can include, for example, using contactless payment technology *at a retail merchant point of sale* (e.g., through point of sale device 104), using mobile/internet commerce (e.g., *purchase tickets and products*, etc.), storage of payment information and other digital artifacts (e.g., receipts, tickets, coupons, etc.), storage of banking information (payment account numbers, security codes, PIN's, etc.), and accessing banking service (account balance, payment history, bill pay, fund transfer, etc.), and so on. The mobile communication device 102 can be a cellular phone ... The point of sale device 104 can be a ... device that is configured to *receive user input selecting items for purchase* or other transaction.

Appx63, 2:38-55.

In addition, the '192 Pub. describes a method for purchasing electronic tickets in which the claimed "one or more products" are represented as items having prices that are purchased:

In this manner, seat inventory (what's available and at what price) can be illustrated graphically ... a seat selection will *automatically cause a price to be calculated*. Any service fee can be included in the *ticket price*. Once user confirms purchase, reservation request is sent to ticket inventory system.

Appx4326, ¶ [0122]). That is, the specification provides consistent descriptions of the independent claims as requiring sending to the remote management server both (i) “the identification of one or more products” having prices that are purchased and (ii) “the transaction purchase request” of the identified products. *In re Smith Int’l, Inc.*, 871 F.3d at 1382-83 (The “correct inquiry in giving a claim term its broadest reasonable interpretation in light of the specification is not whether the specification proscribes or precludes some broad reading of the claim term . . . It is an interpretation that corresponds with what and how the inventor describes his invention in the specification, *i.e.*, an interpretation that is consistent with the specification.”). Indeed, this description throughout the specification is consistent with the claim language stating that “the transaction purchase request includes information relating to the identification of the one or more products.” Appx67, 9:4-6. In other words, the transaction purchase request sent to the remote management server is for the identified products that are sent to the remote server.

The Board erred in construing the identification of one or more products/transaction purchase claim limitations to encompass Khedouri’s teachings of (i) free music samples, which do not have prices and cannot be purchased, and (ii) full music files, which are not both identified and requested to be purchased from the remote management server. Appx44-46. The Board’s construction is wrong because Khedouri’s request for an audio or video clip cannot be an identification of the full audio or video file available for purchase for at least three

separate and independent reasons. First, the clip is a different file from the full file. Appx2748, ¶¶ [0108]-[0110]. Second, when the request for the clip “is queued up” and “the device sends the request,” the user has not been “offered the opportunity to purchase the full file.” *Ibid*. Third, the clip is free, and therefore cannot be the claimed “one or more products,” which need to have prices and to be purchased.

The Board’s construction of the identification of one or more products/transaction purchase request claim limitations is inconsistent with their plain meaning and the way those limitations are used “throughout the entire patent specification, in a manner consistent with only a single meaning.” *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996); *see also Scimed Life Sys. v. Adv. Cardiovascular*, 242 F.3d 1337, 1344 (Fed. Cir. 2001) (“[T]he written description can provide guidance as to the meaning of the claims, thereby dictating the manner in which the claims are to be construed, even if the guidance is not provided in explicit definitional format”).

2. The Board’s Ruling That The Prior Art Would Have Taught The Claim Limitations Related To Sending “the identification of one or more products” and “the transaction purchase request” Is Not Supported By Substantial Evidence Under The Proper Claim Construction.

The Board relies on Khedouri’s discussion of free sample video and audio clips and full video and audio files in paragraphs [0108] – [0110] as allegedly meeting the identification of one or more products/transaction purchase request claim limitations. Appx44-46.

But as explained *supra* in § V.B.1, the proper construction of these claim limitations requires sending to the remote management server both (i) “the identification of one or more products” having prices that are purchased and (ii) “the transaction purchase request” of the identified products. And neither the free clips nor the full files disclosed in Khedouri satisfy these claim requirements.

The first request in Khedouri’s process is not an identification of the full audio or video file that may be purchased. Appx2748, ¶ [0108]. It is instead only an identification of “an audio or video clip (which may have a duration of, for example, 30 seconds),” which is different than the full file. *Ibid.* The clips are free and therefore, don’t have prices and are not purchased. *Ibid.* The clips are instead merely “sample files” that are provided to the user for free, without the user making a purchase. Appx2748, ¶ [0109]. The user is not even “offered the opportunity” to make a purchase until after the “device receives the sample file.” *Id.* at ¶ [0110]). And the user has not been offered an opportunity to purchase the full file at the time the clip is requested. *Ibid.* Accordingly, a selection of any clip cannot possibly be an identification of one or more products having prices that are purchased, as required by the proper construction of the claims.

The only products that have prices and may be purchased are the full files. Appx2748, ¶ [0110]. But there is no mention in Khedouri of sending to the remote management server both (i) the identification of one or more full files and (ii) “the

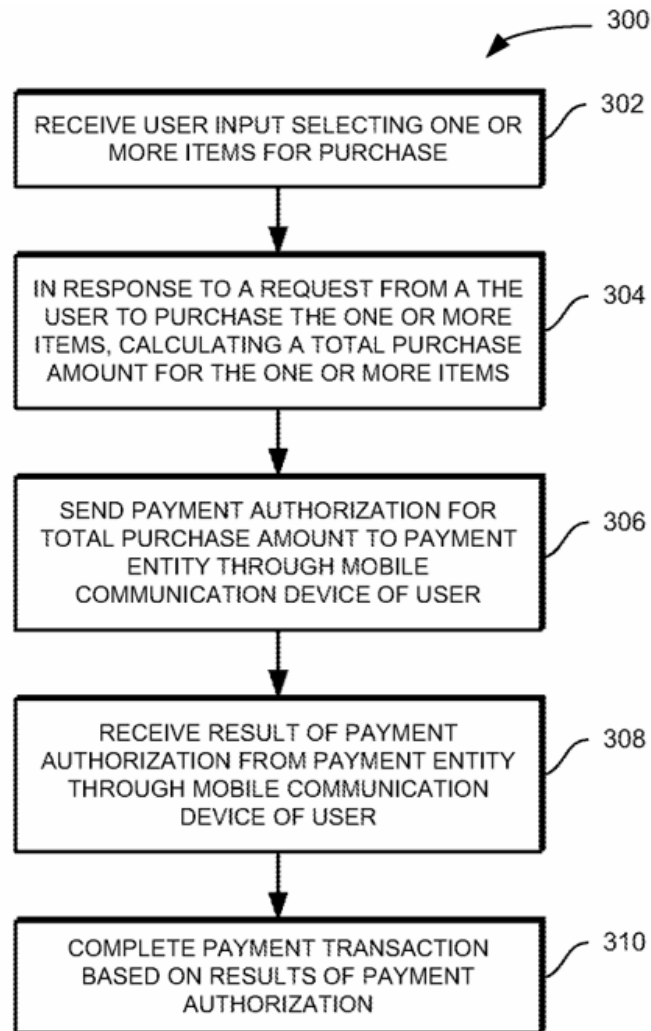
transaction purchase request” of any such identified full file. Instead, Khedouri discloses that when "the user is offered the opportunity to purchase the full file," the full file "may have already been delivered to the device, but its DRM may not be 'unlocked' because the 'key' for that file has not been provided yet." *Ibid.*; see also Appx2742-2743, ¶ [0069] (“[T]he receiver may be able to obtain a copy of the file, but the digital rights management software local on the receiver's player device will not permit the user to play the content.”); Appx2745, ¶ [0085] (“Once the file is obtained, 709 will only allow the user to access it if the digital rights management software on 709 permits it to do so.”)). In other words, a full file in Khedouri is not identified and does not need to be identified. Rather, the full file is downloaded without any identification of the full file, in anticipation of the possibility that the user will purchase the full file. In Khedouri, content "is delivered to the portable unit in encrypted form" and can only be played back if the "player device . . . contains a private key that is able to decode the encryption." Appx2741, ¶ [0058]. Khedouri's processing of the full files, therefore, cannot possibly satisfy the claim requirements of sending to the remote management server both (i) “the identification of one or more products” having prices that are purchased and (ii) “the transaction purchase request” of the identified products.

The Board relies on the “get song now” button 1003 of Khedouri's subscription service as allegedly meeting the identification of one or more

products/transaction purchase request claim limitations. Appx44-46. But this button does not meet the claim requirements of sending to the remote management server both (i) “the identification of one or more products” having prices that are purchased and (ii) “the transaction purchase request” of the identified products because there is no mention in Khedouri that a song associated with button 1003 has a price or is purchased. *See* Appx2748, ¶¶ [0108] – [0110]. Indeed, any song associated with button 1003 could not possibly have a price or be purchased because that button only appears for subscribers and the song is already available to subscribers without an additional purchase. *See ibid.*

The Board also relies on the “buy song now” button 1004 of Khedouri as allegedly meeting the identification of one or more products/transaction purchase request claim limitations. Appx44-46. The Board reasons that “when the user presses the ‘buy song’ button 1004, the portable device informs the sever both that a purchase is desired (i.e., ‘a transaction purchase request’) and what product is to be purchased (i.e., ‘an identification of one or more products selected’).” Appx46. But that argument has no merit because it is based on an erroneous claim construction. Claim 2 recites two distinct steps using different terms: (i) “receives, from the non-browser based application generated screen, an identification of one or more products” and (ii) “receives a transaction purchase request including information relating to the identification of the one or more products from the non-

browser based application generated screen” and therefore, the two steps are presumed to have different meanings. *Applied Med. Res. Corp.*, 448 F.3d at 1333 n.3 (“[T]he use of two terms in a claim requires that they connote different meanings ...”); *CAE Screenplates Inc. v. Heinrich Fiedler GmbH*, 224 F.3d 1308, 1317 (Fed. Cir. 2000) (“In the absence of evidence to the contrary, we must presume that the use of these different terms in the claims connotes different meanings.”). Indeed, the Specification confirms that sending the product identification and sending the transaction purchase request are two distinct steps by disclosing that the products are first selected for purchase in step 302 before a total purchase price for the identified products is calculated in step 304, and the transaction purchase request is sent as a payment authorization in step 306 as shown in FIG. 3, reproduced below.

**FIG. 3**

Appx60.

The Board also argues that the claimed “product’ can be viewed as a song” and that “[r]egardless of whether the user is seeking a free sample ... all of the choices relate to and identify the same song.” Appx45. But this argument also fails to meet the identification of one or more products/transaction purchase request claim limitations because they require the products that are identified to have

prices and be purchased. *See supra*, § B.1. In Khedouri, however, the only products that are identified are the free samples, which don't have prices and are not purchased, as explained above. In particular, Khedouri discloses that when "the user is offered the opportunity to purchase the full file," the full file "may have already been delivered to the device, but its DRM may not be 'unlocked' because the 'key' for that file has not been provided yet." Appx2748, ¶ [0110]; *see also* Appx2742-2743, ¶ [0069].

For these reasons, the Board's ruling that the prior art would have taught the claim limitations related to receiving "the identification of one or more products" and "the transaction purchase request" is not supported by substantial evidence under the proper claim construction.

C. The Claim Limitations Relating To The Remote Management Server and Transaction Server Limitations Would Not Have Been Obvious Under the Proper Claim Construction.

The Board's Final Decision should be vacated because it is based on an incorrect claim construction of the claim limitations: "receives user input login information including an identification code ... authenticating, at the remote management server, a user associated with the user input login information; transmits the payment method that corresponds to the identification code ... to the transaction server; and send a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has

processed ... ; [and] a transaction server ... processes the transaction using the payment method.” Appx66-67. Under the proper construction, these claim limitations would not have been obvious to a POSITA.

1. Blaze Mobile’s Construction Of The Claim Limitations Relating To The Remote Management Server and Transaction Server Limitations Is Supported By The Claim Language and The Specification.

Independent claim 2 recites:

receives user input login information including an identification code associated with the user ...;

upon receipt of the user input login information, authenticating, at the remote management server, a user associated with the user input login information;

transmits the payment method that corresponds to the identification code associated with the user to the transaction server;

and send a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed ... ;

...

a transaction server processor that processes the transaction using the payment method.

Appx66-67. The proper construction of these claim limitations requires (1) a remote management server to (i) receive “user input login information including an identification code associated with a user,” (ii) authenticate a “user associated with the user input login information,” and (iii) receive “a transaction verification” from

a transaction server,” and (2) a transaction server configured to (i) “receive a payment method that corresponds to an identification code associated with a user from a remote management server;” (ii) “send a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed;” and (iii) “processes the transaction using the payment method.”⁷

This construction is consistent with the repeated disclosure in the specification of the ’007 patent of the information that the remote management server receives and the information that it sends:

As such, the management server 180 can store user personal and credit and transactional information and history, including a code associated with the user, for a variety of different mobile communication devices, thereby allowing a system which can scale. Appx4325, ¶ [0116].

PIN and user info can be stored in user/profile database 306 at the management server. Appx4322, ¶ [0037].

The Specification also explains that the remote management server controls the mobile device as well as communication with the mobile device:

In one implementation, the mobile application running on the mobile communication device 102 can be remotely locked through a remote server (e.g., remote server 106). Appx4305, ¶ [0012].

⁷ The construction of this claim limitation must be consistent with the construction of a similar limitation in the ’259 patent, the patent at issue in related appeal number 2025-1485. *Omega Eng’g*, 334 F.3d at 1334. The ’007 patent and ’259 patent have the same inventors and owner, and their specifications are nearly identical.

Upon a successful login, the server will transfer credentials, service access and privileges (step 306), which are locally cached on the mobile communication device. The service access and privileges control the behavior of the client. Appx4306, ¶ [0016].

The method further includes transmitting data associated with the mobile application between the mobile communication device and the server, in which transmission of the data between the mobile communication device and the management server is monitored through the management server. Appx4305, ¶ [0003].

The Specification of the '007 patent also describes the advantages of receiving and storing the claimed "user input login information" and "payment information" at the remote management server:

In one implementation, authorizations for payment transactions that are made through the point of sale device 104 are sent from the point of sale device 104 to an issuer authorization (e.g., management server 106) through the mobile communication device 102 ... an issuer authorization is a payment entity that either approves or disapproves a payment transaction ... One potential benefit of having payment authorizations flow through the mobile communication device 102 is that sensitive user information (e.g. ***account numbers, pin numbers, and/or identity information***) need only be sent from the mobile communication device 102 directly to an issuer authorization. Such operation reduces the potential for identity theft and/or fraudulent purchases made through a point of sale device. Appx63-64, 2:56-3:6.

For example, the data can be securely stored on the remote server using conventional PCI guidelines. Hence, in the event the mobile communication device 102 is lost (or stolen), no confidential data can be recovered as no data is stored on the mobile communication device 102." Appx4306, ¶ [0013].

The Specification also describes the data communicated between the remote management server and the transaction server as well as the interaction between the two servers to both authenticate the user and authorize the transaction:

[S]oftware in transaction server 170 that will ... authenticate, authorize, and execute transfers of transaction information to the management server 180. In one implementation, the piggybacked payload is sent, instead of to the transaction server 170, to the management server 180. Appx4325, ¶ [0115].

The transaction server 170 verifies the transaction, and forwards a transaction verification signal to the management server 180. The management server 180 identifies the user corresponding to the transaction verification signal, and provides a first transaction response signal back to the mobile communication device. Appx4320, ¶ [0020].

Importantly, the claimed “payment method” (*e.g.*, credit card) is not the claimed “identification code associated with the user.” *See Applied Med. Res. Corp.*, 448 F.3d at 1333 n.3 (“[T]he use of two terms in a claim requires that they connote different meanings.”). Because the “an identification code associated with the user” and the “payment method corresponding to the identification code” are two different and separate terms, and because the claims expressly recite that the payment method “*corresponds to*” (*i.e.*, *not “is”*), the “payment method,” then the “an identification code associated with the user” must be something other than the “payment method.”

The Specification repeatedly and consistently confirms that the “identification code associated with the user” cannot be the same as the “payment

method" by explaining that unlike the "identification code associated with the user," which is input by the user at the mobile device, the "payment method" is not stored at the mobile device:

Hence, in the event the mobile communication device 102 is lost (or stolen), no confidential data can be recovered as ***no data is stored on the mobile communication device.***" Appx4306, ¶[0013].

Thus . . . sensitive information (*e.g.*, banking account numbers, credit card account numbers, expiry dates, and so on) are never stored on the mobile communication device. This reduces risk and exposure of the user's private information and data. *Ibid.*

Thus, the plain meaning of the claims and the Specification clearly show that the claimed "identification code associated with the user" and "payment method" are different.

2. The Board's Ruling That The Prior Art Would Have Taught The Claim Limitations Relating To The Remote Management Server and Transaction Server Limitations Is Not Supported By Substantial Evidence Under The Proper Claim Construction.

The Board "relied on Khedouri, not Goldthwaite, for teaching the claimed remote management server and authentication." Appx48. But under the proper construction shown *supra*, § V.C.1, the remote management server is required to (i) receive "user input login information including an identification code associated with a user," (ii) authenticate a "user associated with the user input login information," and (iii) receive "a transaction verification" from a transaction server." And as explained *supra*, §§ V.A.1, V.A.2 and V.A.3, the Board's reliance

on Khedouri's credit card authorization process using a PIN representing a credit card number is not nearly sufficient to satisfy these claim requirements because it is based on an improper construction of the claims that conflates user authentication from transaction authorization. The plain meaning of the user input login information/authentication claim limitations, the specification, and the file history clearly show that user authentication is different from credit card authorization for a transaction. *Supra*, §§ V.A.1, V.A.2. More particularly, the proper construction of the user login information/user authentication claim limitations requires (i) receiving at the mobile device user input login information including an identification code for the user from a non-browser based application, and (ii) authenticating the user associated with the user input login information (*i.e.*, confirm that the user is permitted access to a previously-established account). *Ibid*. And the mere disclosure of a credit card authorization process in Khedouri using a PIN representing a credit card number is not nearly sufficient to satisfy these claim requirements. *Supra*, § V.A.3. For this reason alone, the "remote management server" claim limitations would not have been obvious.

The Board relies on Goldthwaite's financial institution/server 112 to allegedly meet the "transaction server" limitations because it issues a payment card, processes a payment transaction and sends confirmation of the payment transaction. Appx50. But claim 2 requires that the "transaction server" to (i)

“receive a payment method that corresponds to an identification code associated with a user from a remote management server;” (ii) “send a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed;” and (iii) “processes the transaction using the payment method.” *Supra*, § V.C.1. And the Board failed to even attempt to explain how Goldthwaite’s financial institution/server 112 “processes the transaction using a payment method” which “corresponds to the [same] identification code associated with the user” that was used to authenticate the user, as required by claim 2. Appx66-67.

Moreover, Goldthwaite’s financial institution server 112 does not send a transaction verification to the remote management server; it instead transmits the confirmation (alleged by the PTO to be the claimed “transaction verification”) to the payment server 106. Appx2795, ¶ [0021]. And Goldthwaite’s payment server 106 cannot possibly be the claimed “remote management server.” Under the proper construction shown *supra*, § V.C.1, the remote management server is required to (i) receive “user input login information including an identification code associated with a user,” (ii) authenticate a “user associated with the user input login information,” and (iii) receive “a transaction verification” from a transaction server.” But Goldthwaite’s payment server 106 does not authenticate a user, let alone do so with “user input login information” or send “information

authenticating the user associated with the user input login information.”

Appx2795, ¶ [0021]. Instead, Goldthwaite’s payment server 106 receives an "authenticated card" from the authentication server 107 and "contacts the financial institution 112 that has issued the payment card and routes the payment card information and the order information." *Ibid.* Thus, Goldthwaite’s payment server 106 cannot be the claimed "remote management server." For this additional reason, Goldthwaite’s financial institution server 112 cannot be the claimed “transaction server,” given that it sends a confirmation (alleged by the PTO to be the claimed “transaction verification”) to the payment server 106, while claim 2 requires the “transaction server” to send a transaction verification to the remote management server.

In addition, Goldthwaite's authentication server 107 cannot be the claimed "remote management server," which is required by claim 2 to (i) receive “user input login information including an identification code associated with a user,” (ii) authenticate a “user associated with the user input login information,” and (iii) receive “a transaction verification” from a transaction server.” Rather, the payment server 106 receives a confirmation (alleged by the PTO to be the claimed “transaction verification”) from the financial institution server 112. Appx2795, ¶ [0021].

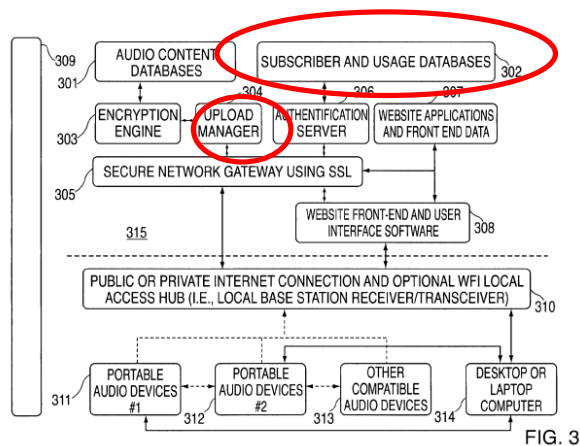
The Board's obviousness decision disregards important claim limitations. *Beckson Marine, Inc.*, 292 F.3d at 727 (for claimed subject matter to be obvious either the prior art references must expressly reach each claim limitation exactly or else the record must disclose a reason for a person of ordinary skill in the art to modify the prior art teachings to obtain the claimed invention).

3. The Board Failed To Show That A POSITA Would Have Been Motivated To Modify Khedouri With Goldthwaite.

The Board concluded that a POSITA would have been motivated to modify Khedouri with the teachings of Goldthwaite because "the benefits of using Goldthwaite's transaction confirmation would have been clear to a person of ordinary skill in the art at the time of the invention (e.g., confirming that the transaction was successful so that the rest of the purchase process can be completed." Appx51.

But the Board failed to consider that "[f]undamental differences between the references [which] are central to this motivation to combine inquiry." *Adidas AG v. Nike, Inc.*, 963 F.3d 1355, 1359 (Fed. Cir. 2020). For example, Khedouri is a closed system that has no need for such a payment confirmation: "The **network** performs a credit card authorization process and, if the user information is approved, subscribes the user and charges his or her credit card appropriately through a **standard electronic credit card billing procedure.**" Appx2741, ¶ [0057];

see also Appx2749, ¶ [0139] ("When the device connects to the network, the purchase is processed, and the content is sent. The user sees the charge on his next credit card bill."). That is, Khedouri's "**network 315**" is a closed self-sufficient system which performs a credit card authorization process. Khedouri makes no mention of utilizing an external or third party system to charge a credit card through a standard electronic credit card billing procedure. Rather, Khedouri's Network 315 is self-sufficient; "the user's card information can be stored on the network in the subscriber database (302, FIG. 3)" (Appx2741, ¶ [0057]), and content is downloaded from the Upload Manager 304 (Appx2744-2745, ¶¶ [0080], [0081]), as shown in FIG. 3, reproduced with annotations below.



Appx2719. Moreover, after a purchase in Khedouri, the server sends content to the mobile device:

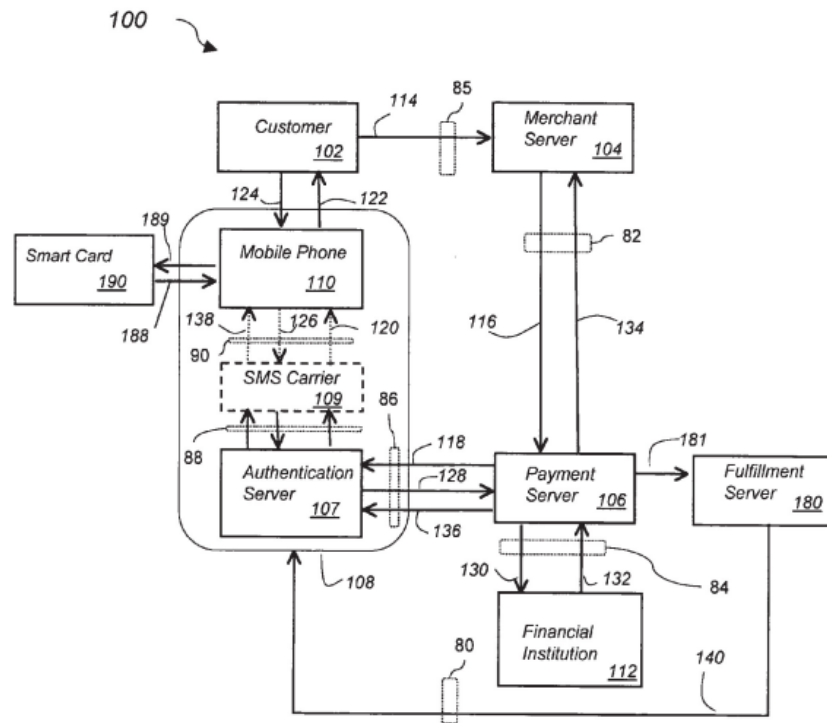
When the device connects to the network, the purchase is processed, and the content is sent. The user sees the charge on his next credit card bill. (Appx2749, ¶ [0139]).

The device also enables obtaining the content merely by "clicking" on a selection, initiating a download, pseudo-download, or streaming process directly to the portable device the next time the device is connected to the network ... securely download and stream music and other audio from the Internet-based database server. Appx2740, ¶¶ [0052], [0053].

Additional new selections the user made are downloaded *automatically* in predetermined order. Appx2742, ¶ [0066].

Thus, the *content in Khedouri is sent without receiving a transaction verification*.

In sharp contrast, Goldthwaite consists of two systems: a payment transaction system including the Payment Server 106, Fulfillment Server 180, Merchant Server 104, and Financial Institution server 112, and a digital goods fulfillment system 108 which downloads content as shown in Figure 4A, reproduced below.



Appx2781.

In Goldthwaite, the Authentication Server 107 “transfers the digital goods” *after the authentication server receives a payment confirmation from the Fulfillment Server 180*. Appx2795, ¶ [0021]. Goldthwaite’s network 80 transmits the payment confirmation “from the fulfillment server 180 and the authentication server 107.” *Id.* at ¶¶ [0022].

Thus, Goldthwaite and Khedouri are fundamentally different because in Goldthwaite an authentication server receives a “*payment confirmation*” before content is sent while in Khedouri, there isn’t a requirement for the upload manager to receive a “payment confirmation” before sending content, let alone a separate

transaction processing system, a separate fulfillment system, and network to bridge the gap between the two systems, as in Goldthwaite.

The principle of operation and inventive concept of Khedouri consists of connecting a device to its single integrated network 315 and ***automatically*** sending content. Appx2749, ¶ [0139] (“[w]hen the device connects to the network, the purchase is processed, and the content is sent”). Combining Goldthwaite’s dual payment transaction and digital goods fulfillment systems requiring payment confirmation before sending content would change the principle of operation of Khedouri’s closed system, and therefore, there can be no motivation to combine Goldthwaite’s teachings with Khedouri in the manner suggested by the Board and the teachings of the references are not sufficient to render the claims *prima facie* obvious. *Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1068 (Fed. Cir. 2016) (finding no motivation to modify the prior art where doing so “would destroy the basic objective” of the prior art); *Chemours Co. FC v. Daikin Indus.*, 4 F.4th 1370, 1377 (Fed. Cir. 2021) (finding no motivation to modify the prior art “when doing so would necessarily involve altering the inventive concept.”); *see also In re Gordon*, 733 F.2d 900 (Fed. Cir. 1984) (there can be no motivation to make a proposed modification if it would render the prior art invention unsatisfactory for its intended purpose).

The Board impermissibly used the claimed invention of the ’007 patent “as

an instruction manual or ‘template’ to piece together the teachings of the prior art so that the claimed invention is rendered obvious.” *In re Fine*, 837 F.2d 1071, 1075 (Fed. Cir. 1988) ("One cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention.").

For these additional reasons, claim 2 of the '007 patent, along with independent claims 1 and 3, which recite similar limitations, and the claims dependent therefrom, would not have been obvious over the combination of Khedouri and Goldthwaite.

VI. Conclusion

For the reasons expressed above, the Court should reverse the Board’s Decision on Appeal that claims 1-36 of the '007 patent are unpatentable.

Respectfully submitted,

/s/ Gregory J. Gonsalves

Dr. Gregory J. Gonsalves
Law Office Of Dr. Gregory J. Gonsalves
2216 Beacon Lane
Falls Church, VA 22043
571.419.7252
gregoryjosephgonsalves@gmail.com

Counsel for Appellant
Blaze Mobile, Inc.
April 30, 2025

ADDENDUM

ADDENDUM TABLE OF CONTENTS

<u>Entry</u>	<u>Page “Appx”</u>
1.Decision on Request for Rehearing 2024-001870 Entered: January 8, 2025.....	1-9
2. Decision on Appeal 2024-001870 Entered: August 1, 2024	10-52
3. U.S. Patent No. 10,825,007	53-71



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.
90/019,134	11/22/2022	10825007	40031-158RX4	6127
12120	7590	01/08/2025		
Michelle Fisher 2930 Domingo Ave Suite 123 Berkeley, CA 94705			EXAMINER DESAI, RACHNA SINGH	
			ART UNIT 3992	PAPER NUMBER
			MAIL DATE 01/08/2025	DELIVERY MODE 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.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte MICHELLE FISHER
Patent Owner and Appellant

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2
Technology Center 3900

Before JOHN A. JEFFERY, HYUN J. JUNG, and MICHAEL J. ENGLE,
Administrative Patent Judges.

ENGLE, *Administrative Patent Judge.*

DECISION ON REQUEST FOR REHEARING

STATEMENT OF THE CASE

Appellant requests rehearing of our Decision on Appeal (“Decision”) dated August 1, 2024, affirming the Examiner’s rejections on obviousness for claims 1–36 of U.S. Patent No. 10,825,007 B2 (“’007 patent”).¹

Because we do not modify our affirmance of the Examiner’s rejections, the Request is denied.

¹ Appellant filed a document titled “HEARING REQUEST UNDER 37 CFR 41.52” on September 9, 2024. We refer to that document as the “Request.” On October 1, 2024, Appellant filed a document titled “NOTICE OF

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

ANALYSIS

In the Request, Appellant seeks rehearing based on (1) “relevant points the Board appears to have overlooked”; (2) “relevant points the Board appears to have misinterpreted”; (3) “relevant decisions by a Federal court”; and (4) an “undesignated new ground of rejection in the Board’s decision.” Request 1. In particular, Appellant argues that the Board triggered a new ground of rejection because it engaged in “claim construction” or “introduces new arguments” regarding obviousness. *Id.* at 3–4.

We are not persuaded by Appellant’s arguments. “It is well-established that the Board is free to affirm an examiner’s rejection so long as appellants have had a fair opportunity to react to the thrust of the rejection.” *In re Jung*, 637 F.3d 1356, 1365 (Fed. Cir. 2011) (quotation omitted). “A new ground of rejection, however, generally will not be found based on the Board further explaining the examiner’s rejection or the Board’s thoroughness in responding to an applicant’s argument.” *Honeywell Int’l Inc. v. Mexichem Amanco Holding S.A.*, 865 F.3d 1348, 1357 (Fed. Cir. 2017) (quotation omitted).

Here, Appellant fails to show how any aspect of the Decision changed the thrust of the rejections. In particular, it is not a new ground of rejection for the Decision to reject Appellant’s proposed claim constructions and agree with the Examiner that Appellant’s proposed claim constructions are, for example, duplicative of limitations elsewhere in the claim or unsupported by the record. Decision 13–27. Quite the opposite of being a new ground,

FILING OF REHEARING REQUEST UNDER 37 CFR 41.52” clarifying that the earlier Request was intended to be a rehearing request.

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

such claim construction issues were extensively addressed by the Examiner in the office actions, by Appellant in the initial brief, by the Examiner in the Answer, and by Appellant in reply. *See, e.g.*, Final Act. 22–30; Supp. Appeal Br. 22–48; Ans. 5–22; Reply Br. 4–34.²

Nor is it a new ground for the Decision to agree with the Examiner that specific aspects of the prior art teach specific claim limitations under the plain and ordinary meaning of those terms (i.e., because we did not adopt Appellant’s claim constructions). *See* Decision 27–41.

For example, independent claim 2, as corrected,³ recites “user input login information including the identification code associated with a user.” In our Decision, we were “not persuaded that the claimed ‘identification code’ excludes Khedouri’s ‘PIN code’ (i.e., a personal *identification* number *code*) or is otherwise limited to a username.” Decision 32. Appellant now requests to provide new claim constructions that exclude the “identification code” from being just a PIN (*e.g.*, Request 6) and instead require the “user input login information” to include *both* an ID *and* a PIN (*e.g.*, Request 25). However, the issue here—whether Khedouri’s PIN teaches or suggests the claimed “user input login information including the identification code associated with a user”—is not new.

² In this appeal, we refer to the Final Office Action (Aug. 25, 2023) (“Final Act.”); Supplemental Appeal Brief (Dec. 26, 2023) (“Supp. Appeal Br.”); Examiner’s Answer (Feb. 6, 2024) (“Ans.”); and Reply Brief (Mar. 7, 2024) (“Reply Br.”).

³ The issued claims have been corrected by three certificates of correction dated June 13, 2023; July 18, 2023; and November 14, 2023. Unless otherwise indicated, we refer to the claims as corrected.

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

In both the Final Office Action and the Answer, the Examiner expressly and repeatedly identified Khedouri's PIN as teaching or suggesting the claimed "user input login information including the identification code associated with a user":

Examiner finds that Khedouri's PIN is "user login information includes, but is not limited to an identification code associated with the user"

Ans. 10.

[W]hile Appellant attempts to boil the term "PIN" down to meaning merely a password, this is not in line with Khedouri's teachings which states that purpose of the PIN code is to allow a user to login using just the PIN alone which is associated with their subscriber database information. This is an identification code associated with a user.

Ans. 15.

Examiner finds that the "user input login information" is inclusive of a PIN.

Final Act. 24.

Moreover, regarding PO's argument that [Khedouri's] 4 digit PIN cannot be an identification code because of the number of unique values, Examiner notes there is no requirement in the claim that the identification code be unique.

Final Act. 25. Appellant even previously raised its argument that (1) the "user input login information" must include *both* an ID *and* a PIN and (2) the "identification code" must be a username, not a PIN or password, in both its briefs and the hearing. *E.g.*, Supp. Appeal Br. 64, 25; Reply Br. 14; Hearing Tr. 9:5–9 (mailed June 12, 2024) ("JUDGE ENGLE: . . . you're saying that login information essentially requires both a username and a password, and that the identification code corresponds to the username, not

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

the password? MS. FISHER: Yes, that’s correct.”). Thus, we are not persuaded by Appellant’s assertion that Khedouri’s PIN teaching the claimed “identification code” or “user input login information” is somehow new. The thrust of the rejection has not changed when we relied on exactly the same specific feature of Khedouri (i.e., the PIN) that the Examiner relied upon and clearly identified in the rejection.

In another example, for the claim phrase “upon receipt of the user input login information, authenticating, at the remote management server, a user associated with the user input login information,” Appellant’s Request now argues that “the Board’s claim construction . . . renders claim language meaningless” because the system must use “user input login information *as a basis for* authenticating the user.” Request 51 (some emphasis omitted). Yet we expressly considered and rejected this argument in our Decision, and doing so did not change the thrust of the rejection because—as explained in our Decision—the Examiner expressly set forth this interpretation:

We also agree with the Examiner that “the user input login information is not authenticating the user, but rather triggering the authentication, thus the phrase ‘upon receipt of the user input login information.’” Ans. 26. Moreover, Appellant’s proposed construction (“authenticating . . . a user . . . *with* user input login information”) essentially deletes the word “associated” from the claim (“authenticating . . . a user associated *with* the user input login information”), which improperly changes the meaning of the limitation. Put another way, the “authenticating” is triggered “*upon receipt* of the user input login information” and the user must be “*associated with* the user input login information,” but claim 2 does not necessarily require the authenticating itself be done “with” the user input login information, as Appellant’s construction requests.

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

Decision 22. The Board agreeing with the Examiner’s interpretation does not change the thrust of the rejection. *See also Ex parte Sami Chems. & Extracts, Ltd.*, 2009 WL 247849, at *5–6 (BPAI Feb. 2, 2009) (informative).

In other instances, Appellant’s arguments in the Request are largely unexplained. For example, in re-arguing proposed constructions for the terms (1) “one or more products”; (2) “remote management server”; and (3) “transaction server,” Appellant repeats the identical argument that “because the Board’s [sic] proposed claim construction is parsing the [sic] claim language without regard to the surrounding [sic] language in the claims, it is improper.” Request 67, 68. However, no further explanation of this argument is provided. Yet our Decision neither articulated a specific claim construction nor improperly “parsed” the claim language. Instead, as we explained in detail in our Decision, Appellant’s proposed constructions were “unnecessary” because “all of Appellant’s construction already appears elsewhere in claim 2” (e.g., “comes from a *different* limitation”). Decision 24–27.

“[T]he ultimate criterion of whether a rejection is considered ‘new’ in a decision by the board is whether appellants have had fair opportunity to react to the thrust of the rejection.” *In re Kronig*, 539 F.2d 1300, 1302 (CCPA 1976). Appellant fails to persuade us that any aspect of the Decision changes the thrust of the rejection when the Board agreed with the Examiner’s express explanations and interpretations in the Final Office Action and Answer. Rather, Appellant’s lengthy Request—which at 91 pages is even longer than either the Supplemental Appeal Brief (86 pages, excluding claims and exhibits) or Reply Brief (72 pages)—attempts

Appeal 2024-001870
 Reexamination Control 90/019,134
 Patent 10,825,007 B2

to reargue the same issues that were or should have been addressed in the original briefs. Nor are we persuaded that we “misapprehended or overlooked” any of Appellant’s arguments or evidence. The Decision explained in detail why Appellant’s arguments and evidence were not persuasive, and Appellant’s mere disagreement with the Board does not justify rehearing. Nor has Appellant identified any recent case law impacting our Decision. Accordingly, we are not persuaded by Appellant’s request for rehearing. *See* 37 C.F.R. § 41.52.

DECISION SUMMARY

The following table summarizes our decision on rehearing:

Claim(s) Rejected	35 U.S.C. §	Reference(s)/Basis	Denied	Granted
1–19, 22–26, 29–32, 35	103	Khedouri, Goldthwaite	1–19, 22–26, 29–32, 35	
20, 27	103	Khedouri, Goldthwaite, Goh	20, 27	
21, 28, 33, 34, 36	103	Khedouri, Goldthwaite, Hoerenz	21, 28, 33, 34, 36	
Overall Outcome			1–36	

Appeal 2024-001870
 Reexamination Control 90/019,134
 Patent 10,825,007 B2

The following table summarizes the outcome of the appeal after rehearing:

Claim(s) Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1–19, 22–26, 29–32, 35	103	Khedouri, Goldthwaite	1–19, 22–26, 29–32, 35	
20, 27	103	Khedouri, Goldthwaite, Goh	20, 27	
21, 28, 33, 34, 36	103	Khedouri, Goldthwaite, Hoerenz	21, 28, 33, 34, 36	
Overall Outcome			1–36	

DENIED

PATENT OWNER:
 MICHELLE FISHER
 2930 Domingo Ave
 SUITE123
 BERKELEY, CA 94705

THIRD PARTY REQUESTER:
 JAMES MARINA
 KIRKLAND & ELLIS LLP
 601 LEXINGTON AVENUE
 NEW YORK, NY 10022



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.
90/019,134	11/22/2022	10825007	40031-158RX4	6127
12120	7590	08/01/2024	EXAMINER	
Michelle Fisher			DESAI, RACHNA SINGH	
2930 Domingo Ave			ART UNIT	PAPER NUMBER
Suite 123				
Berkeley, CA 94705			3992	
			MAIL DATE	DELIVERY MODE
			08/01/2024	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.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte MICHELLE FISHER
Patent Owner and Appellant

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2
Technology Center 3900

Before JOHN A. JEFFERY, HYUN J. JUNG, and MICHAEL J. ENGLE,
Administrative Patent Judges.

ENGLE, *Administrative Patent Judge.*

DECISION ON APPEAL

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

STATEMENT OF THE CASE

Pursuant to 35 U.S.C. §§ 134(a) and 306, Appellant¹ appeals from the Examiner's rejection of claims 1–36 of U.S. Patent No. 10,825,007 B2 (“’007 patent”). A telephonic hearing was held on May 30, 2024. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

TECHNOLOGY

The application relates to “payment transactions” on “[m]obile communication devices—e.g., cellular phones, personal digital assistants, and the like.” ’007 patent, 1:25–27.

REPRESENTATIVE CLAIM

Appellant selects independent claim 2 as representative. *See, e.g.*, Supp. Appeal Br. 24 n.2. Independent claim 2 is reproduced below with (1) whitespace added; (2) labels added; (3) certain limitations at issue italicized; and (4) corrections after issuance either underlined (for added text) or crossed out (for deleted text):²

2. A transaction server for processing a transaction, comprising:

[(1)] a transaction server interface configured to:

[(A)] receive a payment method that corresponds to an identification code associated with a user from a remote

¹ According to Appellant, “[a]fter the ’007 patent was issued, the patent was assigned to Blaze Mobile, Inc.,” but “[i]n order to prosecute the appeal pro se, the patent has been assigned back to [the named inventor] Michelle Fisher.” Supp. Appeal Br. 4.

² The issued claims have been corrected by three certificates of correction dated June 13, 2023; July 18, 2023; and November 14, 2023. Unless otherwise indicated, we refer to the claims as corrected.

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

management server, wherein prior to receiving the payment method that corresponds to the identification code associated with the user from the remote management server,

[(i)] the remote management server

[(a)] sends a list of products to a non-browser based application generated screen generated by a non-browser based application with a graphical user interface that is downloaded and installed on a mobile device for display with a mobile device display of the mobile device, wherein the non-browser based application only generates a non-browser based application generated screen, the non-browser based application generated screen corresponding to a specific screen or area of the non-browser based application, the mobile device including the mobile device display, a mobile device processor, a mobile device wireless radio transceiver configured to support voice and data interactions through a first wireless communication channel, and a mobile device wireless fidelity (Wi-Fi) transceiver;

[(b)] *receives, ~~at~~ from the non-browser based application generated screen, an identification of one or more products selected from the list of products from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the identification of the one or more products selected from the list of products through user input via the mobile device display;*

[(c)] *receives a transaction purchase request including information relating to the identification of the one or more products from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the transaction purchase*

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

request from the user via the mobile device display of the mobile device;

[(d)] *receives user input login information including ~~an~~ the identification code associated with a user from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the user input login information via a mobile device display of the mobile device;*

[(e)] *upon receipt of the user input login information, authenticating, at the remote management server, a user associated with the user input login information; [and]*

[(f)] *transmits the payment method that corresponds to the identification code associated with the user to the transaction server;*

[(B)] *and send a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed and further wherein after receiving the transaction verification, the remote management server downloads the one or more products to the mobile device;*

[(2)] *a transaction server processor that processes the transaction using the payment method.*

RELATED PROCEEDINGS

Prior to issuance, the application for the '007 patent was before the Board in Appeal No. 2019-003843. The panel there reversed an obviousness rejection based on different prior art because “each of Rackley, Gautier, and Hotelling teach a browser-based application.” *See* Decision 8 (May 13, 2020).

Currently, the '007 patent is involved in district court proceedings captioned *Samsung Electronics Co. v. Blaze Mobile, Inc.*, No. 5:21-cv-02989

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

(N.D. Cal.). *See* Supp. Appeal Br. 85. That litigation is stayed pending the *ex parte* reexaminations of certain patents-in-suit, including the '007 patent. *See* Dkt. No. 132, Order Denying Motion to Lift Stay Without Prejudice (Dec. 15, 2023); Supp. Appeal Br. 4.

The '007 patent also has been involved in AIA proceedings captioned *Samsung Electronics, Co. v. Blaze Mobile, Inc.*, IPR2021-01530 (PTAB). The claims were challenged based on prior art not at issue here. *See* Paper 1, Petition 4–6 (Sept. 10, 2021). Institution was denied because “Petitioner does not argue with sufficient evidentiary support that Shore-I’s Immttec server teaches the recited ‘remote management server.’” *See* Paper 14, Decision on Institution 22, 31 (Mar. 16, 2022).

For related proceedings, Appellant also identifies Reexamination No. 90/019,135 for Appellant’s US 10,699,259 B2, which involves some of the same prior art and similar disputed claim limitations. *See* Supp. Appeal Br. 4. That reexamination is currently on appeal to the Board in Appeal No. 2024-002848.

INCORPORATIONS BY REFERENCE

The '007 patent incorporates by reference, in whole or in part, multiple other applications. Given that the briefs and this Decision refer to the disclosures in many of those incorporated-by-reference applications, we summarize them here with a citation to where the incorporation can be found in the '007 patent:

Appeal 2024-001870
 Reexamination Control 90/019,134
 Patent 10,825,007 B2

Application	Publication	Patent	Citation
11/467,441	US 2007/0156436 A1	Abandoned	1:25–35
11/933,321	US 2008/0051059 A1	US 8,275,312 B2	3:43–49
11/933,351	US 2008/0052192 A1	US 8,949,146 B2	1:25–35
11/939,821	US 2009/0124234 A1	US 8,290,433 B2	3:13–20
11/944,267	US 2009/0132362 A1	Pending	3:33–41, 5:11–16
11/948,903	US 2009/0144161 A1	US 8,352,323 B2	1:7–16
13/736,056	US 2013/0124290 A1	US 8,694,380 B2	1:7–16

PRIOR ART

The Examiner relies on the following references as prior art:

Name	Number	Date
Goh	JP 2001-256195 A	Sept. 21, 2001
Goldthwaite	US 2004/0230489 A1	Nov. 18, 2004
Hoerenz	US 2004/0267611 A1	Dec. 30, 2004
Khedouri	US 2006/0008256 A1	Jan. 12, 2006

REJECTIONS

The Examiner makes the following rejections under 35 U.S.C. § 103:

Claims	References	Final Act.
1–19, 22–26, 29–32, 35	Khedouri, Goldthwaite	4–19
20, 27	Khedouri, Goldthwaite, Goh	19–20
21, 28, 33, 34, 36	Khedouri, Goldthwaite, Hoerenz	20–21

ISSUES

1. Did the Examiner err in finding Khedouri teaches or suggests “receives user input login information including the identification code associated with a user from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the user input login information via a mobile device display of the mobile device” and “upon receipt of the user input login information,

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

authenticating, at the remote management server, a user associated with the user input login information,” as recited in claim 2?

2. Did the Examiner err in finding Khedouri teaches or suggests “receives, from the non-browser based application generated screen, an identification of one or more products selected from the list of products” and “receives a transaction purchase request including information relating to the identification of the one or more products from the non-browser based application generated screen,” as recited in claim 2?

3. Did the Examiner err in finding the combination of Khedouri and Goldthwaite teaches or suggests “send a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed,” as recited in claim 2?

ANALYSIS

Petitionable vs. Appealable Matters

The Federal Circuit’s predecessor has explained that “[t]here are a host of various kinds of decisions an examiner makes in the examination proceeding—mostly matters of a discretionary, procedural or nonsubstantive nature—which have not been and are not now appealable to the board or to this court when they are not directly connected with the merits of issues involving rejections of claims, but traditionally have been settled by petition.” *In re Hengehold*, 440 F.2d 1395, 1403 (CCPA 1971). “The line of demarcation between appealable matters for the Board and petitionable matters for the Director of the U.S. Patent and Trademark Office (Director) should be carefully observed.” Manual of Patent Examining Procedure § 1201 (9th ed. rev. 07.2022 Feb. 2023). In particular, “[t]he Board will not

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

ordinarily hear a question that should be decided by the Director on petition.” *Id.*

We carefully follow this line of demarcation between appealable matters and petitionable matters. To the extent Appellant contends the Examiner’s prior office actions did not follow proper *procedure* in responding to Appellant’s arguments (*see, e.g.*, Supp. Appeal Br. 22–23, 35–36, 41–42, 49–50, 69–70, 75–76), the Examiner correctly notes that such *procedural* concerns are petitionable to the Director, not appealable to the Board. Ans. 5, 16, 19, 22–23, 32, 37–38. Below, we address the appealable portions of Appellant’s arguments, including Appellant’s *substantive* arguments regarding proposed claim constructions and the prior art. *See also* 35 U.S.C. §§ 134(b), 6(b) (setting forth PTAB’s jurisdiction in appeals of reexaminations).

Overview of Khedouri

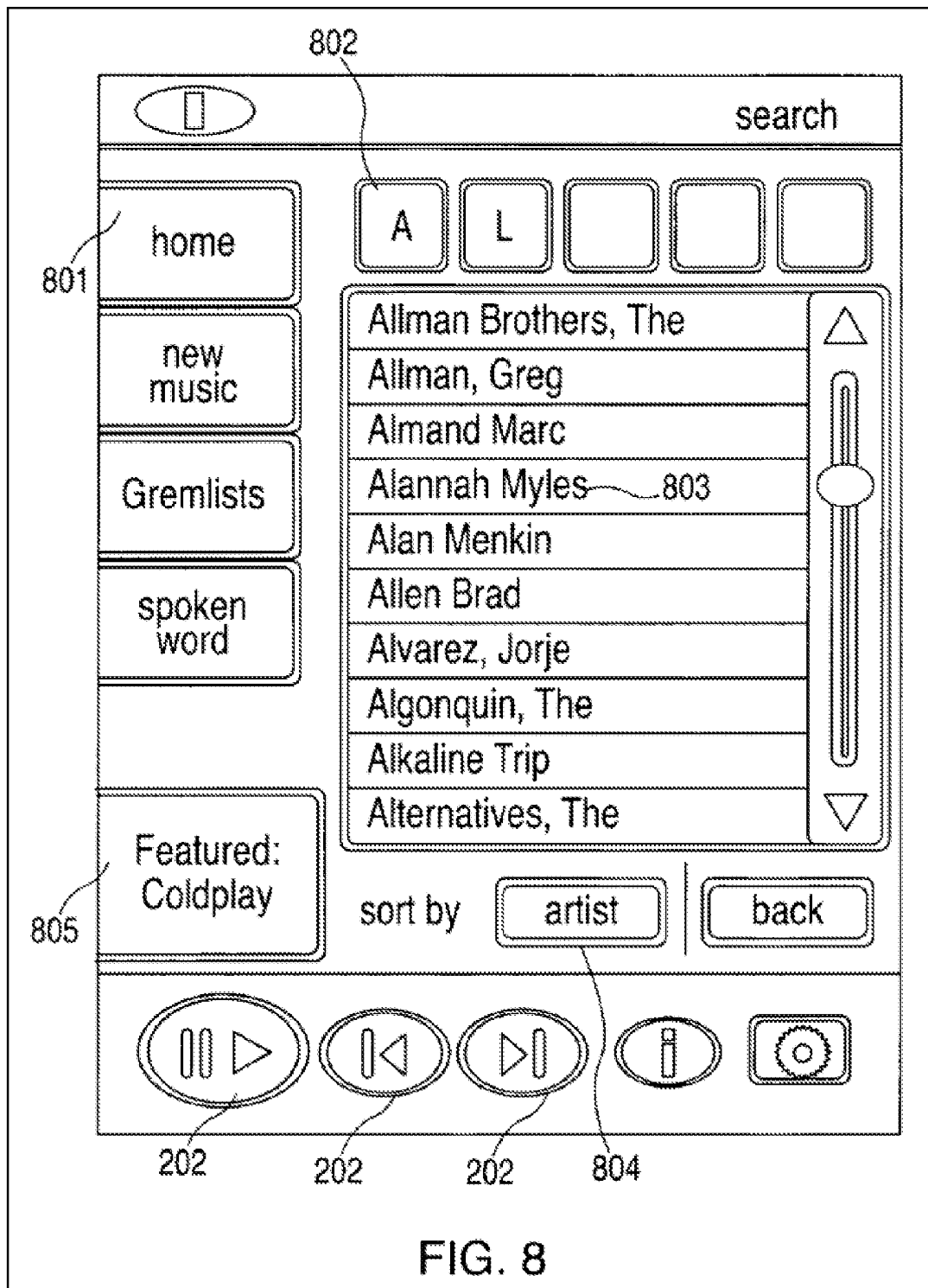
Given that the Examiner relies on Khedouri for teaching most of the elements of claim 2 (*see* Final Act. 4–13) and the briefs discuss multiple variations within Khedouri’s disclosures, we begin with an overview of the most relevant embodiments and aspects in Khedouri.

Khedouri relates to “portable digital media players” that “receive content either from a secure subscription-based or ‘a-la-carte’ content delivery service.” Khedouri ¶¶ 6, 3. “More specifically, the player . . . is able to function as a standalone device to . . . search and obtain new audio and/or video digital data files . . . wirelessly over the Internet, without the need to use an intervening device, such as a desktop or laptop computer” *Id.* ¶ 14.

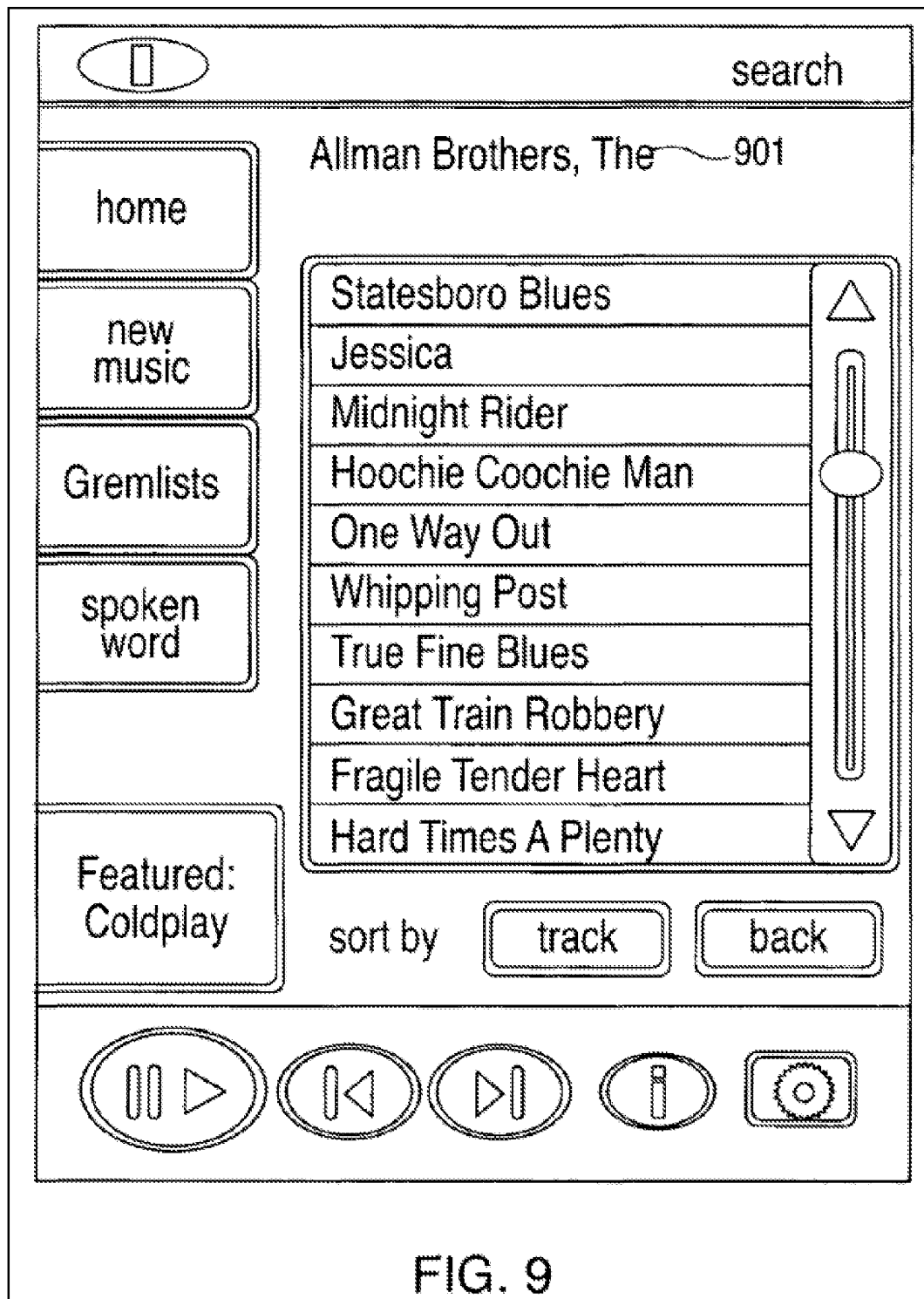
Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

For example, Khedouri teaches searching for and downloading songs. *See* Khedouri Figs. 8–10. However, in at least some embodiments, “[u]sers can search for new content at any time, *without being connected to the Internet* or any external database, by searching the *locally* stored database on the device.” *Id.* ¶ 93 (emphasis added); *see also id.* ¶¶ 52, 63, 126–34. “Once a media file, playlist or other file is identified and selected for download (901, FIG. 9), the selection is added to a ‘stack’ of tasks that are to occur at a next Internet connection” *Id.* ¶ 64; *see also id.* ¶¶ 52, 139. Examples of this searching and downloading process are shown in Figures 8–10, reproduced below:

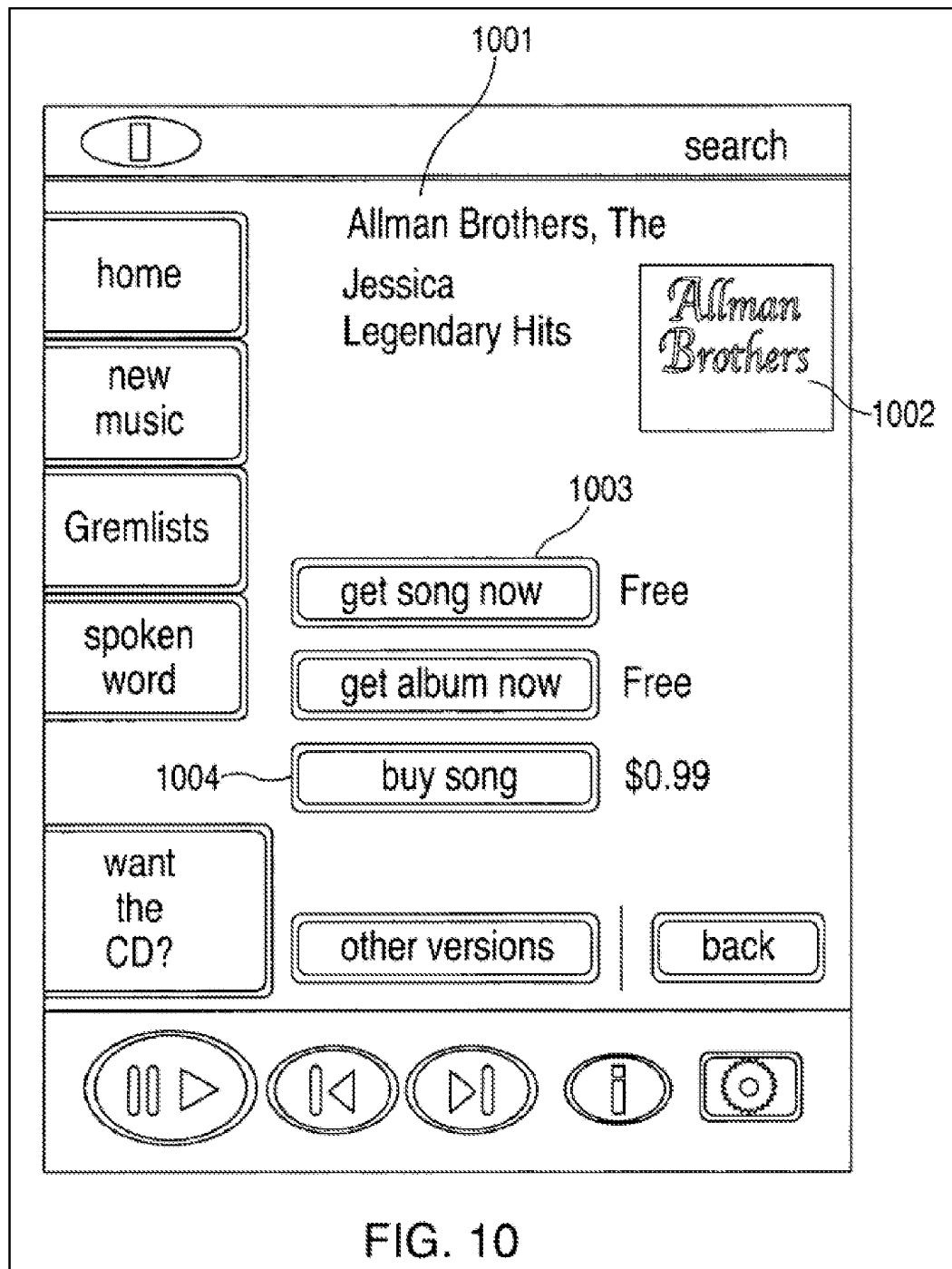
Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2



Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2



Appeal 2024-001870
 Reexamination Control 90/019,134
 Patent 10,825,007 B2



Figures 8–10 depict user interfaces in which “users can use the touch-screen to select an artist” (as shown in Figure 8); “after which, they are

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

presented with a listing of tracks by that artist, which may be scrolled through or searched” (as shown in Figure 9); and “[a]fter the user selects an item (by using the touch-screen . . .) the album, artist and title information are displayed . . . along with a graphic that represents the album cover art” and buttons to “get song now” or “get album now” for “subscribers” to “access the selection on demand” (as shown in Figure 10). Khedouri ¶ 94; *see also id.* ¶¶ 36, 37, 57, 63, 64, 93. “Alternatively, the user may purchase a track for a displayed price 1004, whether or not a current subscriber” (as also shown in Figure 10). *Id.* ¶ 94. “Billing . . . requires input at the minimum of a PIN code by the user to authorize charges on his or her credit card.” *Id.* For such billing, Khedouri discloses using “a standard electronic credit card billing procedure.” *Id.* ¶ 57.

Elsewhere, Khedouri also discloses that “one device can download an audio or video clip (which may have a duration of, for example, 30 seconds) from another, using for example direct download sharing.” Khedouri ¶ 108. “The device receives the sample file and can allow the user to render (i.e., play) it, enabling the user to sample the content,” after which “the user is offered the opportunity to purchase the full file.” *Id.* ¶ 110. Such a “sample file” is discussed in the context of a peer-to-peer embodiment. *Id.* ¶¶ 107–108.

Claim Construction

Appellant proposes constructions for five phrases:

- (1) “user input login information”;
- (2) “user authentication”;
- (3) “one or more products”;

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

(4) “remote management server”; and

(5) “transaction server.”

Supp. Appeal Br. 22–48. We address each of Appellant’s proposed constructions below.

“user input login information”

Appellant argues:

The proper construction of “*user input login information*” is that, “user login information includes, but is not limited to an identification code associated with the user is received from the *non-browser based application* generated screen, wherein the non-browser based application generated screen receives the user input login information via a mobile device display of the mobile device and is provided to the remote management server for *user authentication*.”

Supp. Appeal Br. 23.

The Examiner, however, determines that “[t]hese are features that are separate of the term ‘user input login information’” and instead *other* limitations in the claim “specif[y] where the information is received and how it is utilized.” Ans. 6.

First, we agree in part with the Examiner that much of Appellant’s construction is not necessary because it is specified by *other* limitations in the claim, not the term “user input login information.” Claim 2 recites “receives user input login information including the identification code associated with a user from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the user input login information via a mobile device display of the mobile device.” It is unnecessary and unhelpful to duplicate any of those limitations in the construction of “user input login information” itself. For example, the

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

requirement that the “user input login information” must be received “from the non-browser based application generated screen” comes not from any definition of the term “user input login information” but rather from the express language elsewhere in claim 2 (i.e., “receives user input login information . . . from the non-browser based application generated screen”). The same is true for the requirement in claim 2 that the login information is received “via a mobile device display of the mobile device.”

Second, to the extent Appellant argues that user input login information “includes, but is not limited to” an identification code (Supp. Appeal Br. 23), we agree with Appellant, but this construction is again unnecessary. Claim 2 recites “user input login information *including* the identification code.” It is well-settled that “[a]s a patent law term of art, ‘includes’ means ‘comprising’” and “[n]either includes, nor comprising, forecloses additional elements that need not satisfy the stated claim limitations.” *SanDisk Corp. v. Memorex Prods., Inc.*, 415 F.3d 1278, 1284 (Fed. Cir. 2005) (citation omitted). Put another way, the claimed “user input login information” *must* include at least an identification code and *optionally* may also include information other than the identification code. Yet this portion of the construction does not appear to be in dispute.

Third, in the Reply Brief, Appellant more specifically argues that the claimed “user input login information” requires *both* an ID *and* a PIN. *See* Reply Br. 14 (“By contrast, nothing in the specification suggests that the claims are [to] be misinterpreted to cover a system in which ‘WalletID and WalletPIN are not entered as the user input login information.’” (emphasis omitted)), 11 (“The ‘007 Patent (which incorporates by [reference] the ‘436

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

Pub) strives to provide ‘multi-factored PIN-based login and authentication’ which includes both the WalletID (‘identification code associated with the user’) and a Wallet PIN (‘password’)” (emphasis omitted); *see also* Hearing Tr. 9:5–9 (mailed June 12, 2024) (“JUDGE ENGLE: . . . you’re saying that login information essentially requires both a username and a password, and that the identification code corresponds to the username, not the password? MS. FISHER: Yes, that’s correct.”). Appellant appears to refer to this combination of both an ID and a PIN as “multi-factor” authentication and contends that “every embodiment . . . describes multifactor login and authentication.” *Id.* at 13. Appellant argues that compared to the prior art Khedouri, the invention of the ’007 patent is both “more secure” (because no identifier needs to be stored on the mobile device) and “more scalable” (because Khedouri’s identifier is for each *device* rather than each *user*). *Id.* at 23, 20 (emphasis omitted). Appellant notes that “claims 12, 13, 16, & 17 . . . recite in part, ‘ . . . no sensitive data is stored on the mobile device’ and . . . ‘the sensitive data comprises . . . information related to identification information,’” thereby suggesting that the ID must be input by the user when needed rather than saved locally on the mobile device. *Id.* at 19 (emphasis omitted).

However, the “sensitive data” claims are *dependent* claims. “[T]he presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1314–15 (Fed. Cir. 2005) (en banc). “This presumption is especially strong where the limitation in dispute is the only meaningful difference” between the two claims. *Hill-*

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

Rom Servs., Inc. v. Stryker Corp., 755 F.3d 1367, 1374 (Fed. Cir. 2014).

Thus, there is an un rebutted presumption that the *independent* claims are broader and permit sensitive information related to identification information to be stored on the mobile device. More generally, any alleged advantages of login and authentication being “multi-factored” (e.g., being “more secure” or “more scalable”) are not specified in the independent claims.

With respect to whether the “login information” or its “identification code” can be specific to one *device* rather than one *user*, we note that the ’007 patent incorporates by reference U.S. Patent App. No. 11/467,441, which published as US 2007/0156436 A1. *See* ’007 patent, 1:30–35. That publication discloses “a passive device 138', such as an RFID sticker or some other tag, that allows for a *user identification*,” and “[t]his passive device 138', with the *identification code* stored thereon, can thus be associated with a mobile device 110.” US 2007/0156436 A1, ¶ 38 (emphasis added); *see also id.* ¶ 6 (“can identify the identification code of the particular RFID and then subsequently charge the user”). Similarly, the ’007 patent incorporates by reference U.S. Patent App. No. 11/933,321, which issued as US 8,275,312 B2. *See* ’007 patent, 3:46–49. That patent likewise discloses “[t]he passive device 138 can be an RFID sticker or suitable tag that allows for *uniquely identifying a user*” and “[t]his passive device 138, with the *identification code* stored thereon, can thus be associated with a mobile communication device 110.” US 8,275,312 B2, 6:29–44 (emphasis added); *see also id.* at 1:42–45 (“the amount of the bus ticket can be forwarded to a server that can identify the *identification code* of

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

the particular RFID and then subsequently charge *the person* for the purchase of the bus ticket” (emphasis added)). Thus, although claim 2 certainly requires “login information including the identification code associated with a user,” the incorporated-by-reference disclosures suggest that an identification code *of a device* (e.g., RFID) can be “associated with a user.”

Appellant’s broader question is whether the claimed “login information” necessarily includes *both* a “WalletID” *and* a “WalletPIN.” *See, e.g.,* Reply Br. 14. We are not persuaded that it does. For example, another incorporated-by-reference application discloses that “[t]he method can include use of *biometrics* to authenticate the user before authorizing the transaction.” US 2009/0124234 A1, ¶ 4 (emphasis added); *see also* Supp. Appeal Br. 40 (citing same), 5 (noting incorporation by reference of U.S. App. No. 11/939,821); ’007 patent, 3:13–20 (incorporating by reference). Biometrics certainly could be used as an alternative to a PIN. For example, the prior art Goldthwaite expressly discloses biometrics as an alternative to a PIN or password: “In one example, the security code is a personal identification number (PIN). Other examples include a password, digital signature, and biometric identifier, i.e., retina scan, fingerprint, DNA scan, voice characteristics.” Goldthwaite ¶ 21. Similarly, Appellant’s related patent US 10,699,259 B2 includes dependent claims expressly stating “the user input login information includes biometric data” (claim 3) and “the user input login information includes a personal identification number (PIN)” (claim 4, as corrected on May 4, 2021), thereby suggesting that the “user input login information” of the independent claim need not include a PIN

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

but optionally could include biometrics instead. Indeed, a *single* biometric such as a fingerprint or retinal scan easily could replace *both* an ID *and* a PIN to authenticate a user or login. And although the '007 patent itself does not expressly define the term “login information,” the incorporated-by-reference disclosures suggest that the similar term “login credentials” is broad and not limited to a specific combination of a WalletID and WalletPIN. *E.g.*, US 2009/0124234 A1, ¶ 16 (“In one implementation, when a user attempts to login with the client, the user is prompted to enter login credentials (e.g., mobile phone number, 1-time activation code, Wallet PIN, etc.).”); *see also* Ans. 8 (“the user input description in paragraph [0016] specifically states a Wallet PIN can be a login credential on its own”). Thus, although “login information” can include the combination of a WalletID and a WalletPIN, we are not persuaded that the claimed “login information” always requires both a WalletID and a WalletPIN.

Though not phrased as such, Appellant might be arguing more generally that the claimed “user input login information” must include *all* information required to login, which in some systems could be both a username and a password. We are not persuaded that claim 2 requires this. As noted above, an incorporated-by-reference application is clear that a “Wallet PIN” is one example of a “login credential.” *See* US 2009/0124234 A1, ¶ 16 (“In one implementation, when a user attempts to login with the client, the user is prompted to enter login credentials (e.g., mobile phone number, 1-time activation code, Wallet PIN, etc.).”). Thus, a PIN is “login information.” So long as “login information including the identification code associated with a user” is “user input” from the non-browser based

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

application generated screen on a mobile device, nothing in claim 2 prohibits *also* receiving or using additional information related to login (e.g., automatically entering a locally-stored username but requiring manual input of a password or PIN).

Finally, Appellant proposes a construction that “the login information is used for authenticating the user” and more specifically that the login information “confirms the user is permitted access to a previously-established account.” Supp. Appeal Br. 23 (quotation and emphasis omitted). According to Appellant, “*Webster’s New World Computer Dictionary* defines ‘login’ as: ‘In a computer network, the **authentication process in which a user supplies a login name and password.**’” Supp. Appeal Br. 32–33 (citing <https://archive.org/details/webstersnewworld0000pfaf/page/224/mode/2up?q=login>). We agree with Appellant that the term “login information” means the “information” must be related to “login.” Yet for the reasons discussed above, we do not agree that the claimed “login information” always must include both a login name and a password. Nevertheless, we do agree with Appellant’s more general point that a “login” is an authentication process, in particular authenticating the user. For the relevance of that, however, we turn to what it means to authenticate a user.

“authenticating . . . a user”

Appellant argues:

The proper construction of “user authentication” is, “**authenticating**, at the remote management server, **a user logging into a mobile wallet service** with user input login information including an identification code associated with a

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

user received from a non-browser based application, wherein the non-browser based application generated screen receives the user input login information via a mobile device display of the mobile device and confirms that the *user is permitted access to a previously-established mobile wallet service account and is distinct from payment authorization.*”

Supp. Appeal Br. 37. Claim 2 does not expressly recite “user authentication,” so we treat Appellant’s argument as instead construing the claimed phrase “authenticating . . . a user.”

Appellant quotes a dictionary definition defining “authentication” as “In a network, a means of ensuring the systems security by demanding that users supply some means of identifying themselves, such as a login name and password.” Supp. Appeal Br. 40–41 (citing <https://archive.org/details/webstersnewworld0000pfaf/page/8/mode/2up?q=authentication>). Appellant further cites to expert testimony that “[t]he ‘ordinary and customary meaning’ of ‘authentication’ is ‘the process by which a user gains access to a website or application by logging in to it’.” *Id.* at 40 (emphasis omitted) (quoting Zatkovich Decl. ¶ 12 (June 19, 2023)).

Similar to above, much of Appellant’s proposed construction is unnecessary because it comes from the rest of the claim, not the definition of “authenticating . . . a user.” For example, claim 2 recites “upon receipt of the user input login information, authenticating, at the remote management server, a user associated with the user input login information.” These claimed features (e.g., “at the remote management server”) need not be repeated in the construction of “authenticating . . . a user.” Similarly, the origins of the “login information” found in previous limitations (e.g., “the non-browser based application generated screen receives the user input login

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

information via a mobile device display of the mobile device”) need not be repeated in the construction of “authenticating . . . a user.”

We also agree with the Examiner that “the user input login information is not authenticating the user, but rather triggering the authentication, thus the phrase ‘upon receipt of the user input login information.’” Ans. 26. Moreover, Appellant’s proposed construction (“authenticating . . . a user . . . *with* user input login information”) essentially deletes the word “associated” from the claim (“authenticating . . . a user associated *with* the user input login information”), which improperly changes the meaning of the limitation. Put another way, the “authenticating” is triggered “*upon receipt* of the user input login information” and the user must be “*associated with* the user input login information,” but claim 2 does not necessarily require the authenticating itself be done “with” the user input login information, as Appellant’s construction requests.

With respect to Appellant’s construction using the phrase “mobile wallet service,” claim 2 does not use this phrase and we are not persuaded that it is expressly required as written in the proposed construction. Nevertheless, the rest of claim 2 already captures much of this phrase in a more general context (e.g., transmitting “a transaction purchase request” and “payment method” for “products” selected on a “mobile device”).

Appellant’s construction also requires “authenticating” to confirm that the user is permitted access to “a previously-established . . . account.” Appellant’s construction seeks to distinguish “authenticating” an existing account from registering a new account or using a one-time code. *See* Supp. Appeal Br. 53–54 (discussing registration in prior art Khedouri), 57

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

(discussing a “unique transaction code” in the ’007 patent). Yet this argument is not persuasive because the ’007 patent itself discloses “authentication” using a one-time code:

When the consumer is ready to pay for their online product, they enter their cell phone number on the merchant portal. . . . In one implementation, the management server 408 identifies the consumer through their cell phone number, and verifies the consumer’s *authenticity* by sending a unique transaction code to the consumer mobile wallet on their cell phone. The consumer then enters this unique transaction code onto the merchant’s web portal. The merchant portal sends this transaction number to the management server 408 for *authentication*. Upon *authentication*, the consumer’s virtual wallet and payment methods (e.g., credit card, debit card, prepaid card, etc.) are securely retrieved. . . .

’007 patent, 4:42–60 (emphasis added). Appellant contends that “this embodiment is not claimed.” Supp. Appeal Br. 57. But even if *other* limitations elsewhere in the claim exclude this embodiment, the claim term “authenticating . . . a user” does not because the ’007 patent expressly discloses “authentication” of a user using a one-time “unique transaction code.”

Finally, Appellant’s construction proposes that authenticating “is distinct from payment authorization.” Supp. Appeal Br. 37 (emphasis omitted). According to Appellant, an incorporated-by-reference application “clearly lists authentication and authorization” as “distinct elements.” *Id.* at 40 (emphasis omitted) (citing US 2009/0124234 A1 ¶ 4 (“The method can include use of biometrics to *authenticate* the user *before authorizing the transaction*”) and “*Id.*, ¶ [0115]” (“and then *authenticate, authorize, and*

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

execute transfers of transaction information”³). Although we agree with Appellant insofar as authentication and authorization are not synonymous, these disclosures and the ’007 patent also make clear that authentication can be a precursor for payment authorization: “After the consumer enters any necessary *validation information* (e.g., *pin*) to provide a multi-factor *authentication* and confirms the transaction, the online purchase is processed as normal by the merchant’s online processor.” ’007 patent, 4:9–13 (emphasis added), 4:33–37. Thus, payment authorization is not necessarily wholly independent from authenticating.

Accordingly, we do not adopt Appellant’s proposed construction for “authenticating . . . a user.”

“one or more products”

Claim 2 recites (A) “sends a list of *products* to a non-browser based application generated screen”; (B) “receives, from the non-browser based application generated screen, an identification of one or more *products* selected from the list of *products* . . . through user input via the mobile device display”; (C) “receives a transaction purchase request including information relating to the identification of the one or more *products* from the non-browser based application generated screen”; and (D) “after receiving the transaction verification, the remote management server downloads the one or more *products* to the mobile device.”

³ There is no paragraph 115 in US 2009/0124234 A1. This instead appears to be a quotation from paragraph 115 of US 2008/0052192 A1.

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

Appellant argues that “the proper construction of ‘one or more products’ are ‘items that have prices and are purchased’.” Supp. Appeal Br. 43–44. According to Appellant, the claims and the rest of the Specification refer to products in relation to prices and purchase transactions, so the term should exclude free samples. *See id.* at 42–44, 71. However, Appellant’s citations to the ’007 patent and various applications incorporated by reference relate to the word “purchase,” not “products.” *See id.* at 44–45 (quoting, e.g., ’007 patent, 1:43–51 (“calculating a total *purchase* amount” (emphasis modified)), 5:41–44 (“The user request to *purchase* an item can be received, e.g., by a user clicking on a ‘buy now’ icon” (emphasis added)))).

Thus, Appellant’s construction for “one or more products” is again unnecessary because the “purchase” (and hence the price) instead comes from a *different* limitation (i.e., “a transaction *purchase* request”), not the meaning of “products.”

“remote management server”

Appellant argues that “[t]he proper construction of ‘remote managements’ is that the ‘remote management receives user input login information including, but not limited to an identification code associated with a user from the non-browser based application generated screen.’” Supp. Appeal Br. 45. But this construction is unnecessary because claim 2 already recites “the remote management server . . . receives user input login information including an identification code associated with a user from the non-browser based application generated screen.” *See* Ans. 21.

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

Similarly, Appellant argues “the proper construction of ‘remote managements’ is that the ‘remote management server conducts user authentication based on upon receipt of the user input login information including, but not limited to an identification code associated with a user from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the user input login information via a mobile device display of the mobile device.’” Supp. Appeal Br. 46. Yet this is again unnecessary because claim 2 already recites “upon receipt of the user input login information, authenticating, at the remote management server, a user associated with the user input login information” and “the non-browser based application generated screen receives the user input login information via a mobile device display of the mobile device.” *See* Ans. 21.

Finally, Appellant contends “the proper construction of ‘remote managements’ is that the ‘remote management server receives from a transaction server, a transaction verification which indicates that the transaction has processed.’” Supp. Appeal Br. 47. Yet this too is unnecessary because claim 2 recites “send a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed.” *See* Ans. 21.

Given that all of Appellant’s construction already appears elsewhere in claim 2, we are not persuaded that “remote management server” requires any further construction.

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

“transaction server”

Appellant argues: “The proper construction of ‘transaction server’ is that the ‘transaction server transmits a transaction verification to the remote management server.’” Supp. Appeal Br. 48. However, claim 2 already recites “A transaction server . . . comprising . . . a transaction server interface configured to: . . . send a transaction verification to the remote management server.” Accordingly, we are not persuaded that “transaction server” requires any further construction. *See* Ans. 22.

§ 103

Whether Khedouri teaches receiving “user input login information” from a “non-browser based application generated screen” and “authenticating”

Independent claim 2 recites the remote management server “receives *user input login information including the identification code* associated with a user from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the user input login information via a mobile device display of the mobile device” and “upon receipt of the user input login information, *authenticating*, at the remote management server, a user associated with the user input login information.”

The Examiner relies on Khedouri for teaching or suggesting these limitations. Final Act. 13 (“claim 2 is rejected under the same rationale provided above with respect to claim 1”), 9–11 (addressing claim 1).

Appellant argues various features of Khedouri (including its deviceID, PIN, and Activation Code) do not meet one or more of these limitations.

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

First, Appellant argues that Khedouri’s “automatic transmission of the deviceID does not correspond to the claimed ‘user input login information’ because the deviceID is not input by the user, as claimed.” Supp. Appeal Br. 64. We agree with Appellant that Khedouri at least suggests its deviceID is provided by the device and therefore is not “user input” as claimed. *See* Khedouri ¶¶ 137 (“The Code is then used with a series of hidden computations to create a secure ‘deviceID’ that is used to identify the device to the user account on an ongoing basis.”), 80 (“[T]he device 311 provides its unique ID or serial number, from laser-burned chip 118, in encrypted form to network 315. The network authenticates transmitted ID”).

Second, Appellant argues, “Instead of receiving the claimed ‘user input login information’ and performing the claimed[] ‘user authentication’, Khedouri’s non-browser based application *bypasses or navigates around the required login*” and “[b]ecause Khedouri states that the[] ‘deviceID that is used to identify the device to the user account on an ongoing basis,’ *the user does not need to enter their 4 digit security PIN* after registration and for an existing account.” Supp. Appeal Br. 51–52 (citing Khedouri ¶¶ 135–37, 139) (emphasis added). These appear to be based on a misreading of Khedouri. Khedouri’s discussion of “how to navigate around this introduction page” and “simulating the required communications to login and/or bypass this first page” is in the context of “[c]onnecting to paid access Wi-Fi points (e.g., T-Mobile at Starbucks)” that “generally direct IP communications to a readable HTML Web page” when using a device “not having a browser.” Khedouri ¶ 135. It is not discussing what happens when a user wishes to purchase or download a song. *Id.* Instead, Khedouri

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

expressly discloses requiring the user to input a PIN in order to make a purchase. *E.g.*, Khedouri ¶¶ 94 (“Billing follows the above-described procedure and requires input at the minimum of a PIN code by the user to authorize charges on his or her credit card.”), 57 (“The network performs a credit card authorization process [T]he user’s card information can be stored on the network . . . in order that the user would not need to re-enter this information but would only need to enter a 4-digit security PIN code”); Ans. 25 (citing Khedouri ¶¶ 94, 57). Thus, bypassing a page to login into a Starbucks Wi-Fi is not relevant to the Examiner’s rejection.

Appellant similarly attempts to argue that “because Khedouri distinguishes the ***non-browser based application embodiment*** for accessing content and authentication discussed in paragraphs [0123]-[0141], it is understood that the Khedouri’s prior disclosure is for a ***browser-based embodiment***.” Supp. Appeal Br. 60. However, we agree with the Examiner that although Khedouri discloses “[u]sers are permitted to use a computer if they wish . . . , in which case they can use a standard desktop or laptop computer 314 equipped with standard Internet browser software,” users “are *not* required to do so *at any time for any purpose*.” Khedouri ¶ 79 (emphasis added); Ans. 30. Instead, “[a]n important feature of the invention is that a device can access and download information and content *without a browser*.” Khedouri ¶ 121 (emphasis added). For example, “[u]sers can search for new content at any time, *without being connected to the Internet* or any external database, by searching the *locally stored database on the device*.” *Id.* ¶ 93 (emphasis added); *see also id.* ¶ 52 (“enabling users to search for new content *without being connected to the Internet*” (emphasis

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

added)). Thus, the bulk of Khedouri's teachings, including entering a PIN to authorize charges, applies to portable devices that lack an internet browser and are only intermittently connected to a network.

Third, Appellant argues that Khedouri's "4-digit security PIN" is "not being used to login and authenticate a user" but rather "for Khedouri's 'credit card authorization process' to 'charge his or her credit card appropriately.'" Supp. Appeal Br. 63 (quoting Khedouri ¶ 57).

We are not persuaded by Appellant's argument. Khedouri discloses a PIN to authorize a purchase: "Billing follows the above-described procedure and requires input at the minimum of a PIN code by the user to authorize charges on his or her credit card." Khedouri ¶ 94; Ans. 25–26 (citing same). In particular, Khedouri discloses a "credit card authorization process" that can be used for "payments the user is required to make": "the user's [credit] card information can be stored on the network in the subscriber database (302, FIG. 3) in order that the user would not need to re-enter this information but would only need to enter a 4-digit security PIN code that is similarly stored and verified by the network." Khedouri ¶ 57; Ans. 25 (citing same). Thus, Khedouri discloses a user entering a 4-digit security PIN to authorize a purchase.

An incorporated-by-reference application expressly states that a "PIN" is an example of "login credentials": "In one implementation, when a user attempts to login with the client, the user is prompted to enter *login credentials* (e.g., mobile phone number, 1-time activation code, *Wallet PIN*, etc.)." US 2009/0124234 A1, ¶ 16 (emphasis added). The '007 patent itself discloses that "validation information (e.g., pin)" is used to provide

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

“authentication” prior to processing a purchase: “After the consumer enters any necessary *validation information* (e.g., *pin*) to provide a multi-factor *authentication* and confirms the transaction, the online purchase is processed as normal by the merchant’s online processor.” ’007 patent, 4:9–13 (emphasis added), 4:33–37 (same). Based on these disclosures, Khedouri’s PIN is a login credential (i.e., “login information”) used for “authenticating.” *See also* Khedouri claim 8 (“the authentication system verifies the identity of the user to the content source”; “said content source releases the selected content to said user-operated device if said user-operated device is authenticated by said authentication system”); Ans. 26 (citing Khedouri claim 8).

Appellant also argues that “a ‘PIN’ is equivalent to a ‘password,’” not an “identification code associated with the user.” Supp. Appeal Br. 32 (emphasis omitted). Appellant appears to treat the claimed “identification code” as a username, not a password. *See id.* at 25–34 (e.g., “The user login information can include both the WalletID (‘identification code associated with the user’) and a Wallet PIN (‘password’)” (emphasis omitted)). Thus, in Appellant’s view, Khedouri’s PIN would not satisfy claim 2’s requirement of “user input login information including an *identification code* associated with a user.”

However, Appellant has not directed us to any definition or proposed construction of “identification code.” Using different words, the ’007 patent does refer to “sensitive user information (e.g., account numbers, pin numbers, and/or identity information)” (2:64–3:3), which distinguishes between “pin numbers” and “identity information” but also expressly

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

includes “pin numbers” as “user information.” In Reexamination No. 90/019,168 for Appellant’s US 9,652,771 B2, the Examiner construed “identification code” as “[s]imply a compound word meaning a set of symbols (as letters or numbers) used to identify something,” referring to dictionary definitions for “identification” and “code.” *See* App. No. 90/019,168, Notice of Intent to Issue Ex Parte Reexamination Certificate 6–7 (Jan. 2, 2024). Moreover, “PIN” stands for “personal *identification* number.” *E.g.*, Goldthwaite ¶ 21 (“the security code is a personal identification number (PIN)”). And Khedouri expressly refers to a “PIN *code*.” Khedouri ¶ 57 (emphasis added); *see also* Goldthwaite ¶ 21 (“the security *code* is a personal identification number (PIN)” (emphasis added)). Given the record before us, we are not persuaded that the claimed “identification code” excludes Khedouri’s “PIN code” (i.e., a personal *identification* number *code*) or is otherwise limited to a username.

Finally, Appellant argues that “in Khedouri, the credit card information and one-time Activation Code are used to **register** the user, not to log the user into an **existing** account.” Supp. Appeal Br. 53 (discussing Khedouri ¶ 137). Given our analysis of Khedouri’s PIN code above, we need not reach Khedouri’s Activation Code.

For the reasons above, we are not persuaded the Examiner erred in finding Khedouri’s purchase with a PIN code teaches or suggests “receives user input login information including the identification code associated with a user from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the user input login information via a mobile device display of the mobile device” and “upon

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

receipt of the user input login information, authenticating, at the remote management server, a user associated with the user input login information.”

Whether Khedouri teaches “products” and “transaction purchase request”

Independent claim 2 recites “receives, from the non-browser based application generated screen, an identification of one or more *products* selected from the list of products” and “receives a *transaction purchase request* including information relating to the identification of the one or more *products* from the non-browser based application generated screen.”

Appellant argues that “Khedouri sends two separate individual requests.” one for a sample of the content (e.g., a 30 second clip of a song) and “another for the ‘full file’” (e.g., the full song). Supp. Appeal Br. 71 (citing Khedouri ¶¶ 108–10).

The first request in this process is not an “identification” of the full audio or video file that might eventually be purchased, and thus is not an “identification” of “one or more products selected from the list of products,” as claimed. It is instead only an identification of “an audio or video clip (which may have a duration of, for example, 30 seconds).”

Supp. Appeal Br. 71 (quoting Khedouri ¶ 108). Appellant concedes that Khedouri’s full files are “products.” *See id.* However, Appellant argues that “[t]he clips are not products: they do not have prices and are not purchased. The clips are instead merely ‘sample file[s]’ that are provided to the user for free, without the user making a purchase.” *Id.*

We are not persuaded by Appellant’s arguments for three independent reasons. First, as the Examiner correctly points out, “Appellant appears to address embodiments that are not relied upon for the rejection of these

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

limitations.” Ans. 36. In particular, as Appellant appears to concede in the Reply Brief, Khedouri’s paragraphs discussing free samples “are directed to peer device sharing,” not Figure 10. *Id.* (citing Khedouri ¶¶ 107–109); *cf.* Khedouri ¶ 94 (discussing Figure 10 but not free samples); *see also* Reply Br. 60 (“Khedouri *elsewhere* describes” 30 second clips (emphasis added); “This disclosure is part of a discussion of peer-to-peer file sharing.”).

Notably, the song discussed as an example of a free sample (“Concerto in G”) is wholly unrelated to the song shown in Figure 10 (“Jessica” by “Allman Brothers, The”). Khedouri ¶ 108, Fig. 10. Figure 10 does depict two buttons 1003 with the word “Free” next to them (i.e., the buttons titled “get song now” and “get album now”), but Khedouri explains that those are for its subscription service to access content on demand: “By selecting ‘get song now’ or ‘get album now’ 1003, *subscribers* can access the selection *on demand*.” Khedouri ¶ 94 (emphasis added); *see also* Ans. 35 (quoting same). These subscriber buttons are contrasted with the purchase button: “Alternatively, the user may purchase a track for a displayed price 1004, *whether or not a current subscriber*” and “[t]hese song purchases permit *permanent ownership* of the track.” Khedouri ¶ 94 (emphasis added). Thus, Khedouri’s “get song now” button 1003 and “buy song” button 1004 both are for the full-length song, not a short clip or free sample, and instead merely distinguish subscriber access versus permanent ownership.

Khedouri’s subscriptions, like a la carte content, are purchased. Khedouri ¶ 57 (“To become a subscriber, or purchase a la carte content, a user is prompted by the device to enter credit card information”; “The network performs a credit card authorization process and, if the user

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

information is approved, subscribes the user and charges his or her credit card appropriately through a standard electronic credit card billing procedure.”). Although Appellant proposes construing “products” as “items that have prices and are purchased,” we determine that a streamed or downloaded song for a subscriber (e.g., from clicking the “get song now” button 1003 for “Jessica” by “Allman Brothers, The”) is still a “product” offered by Khedouri’s music service. We are not persuaded that the streamed or downloaded song must itself have an individual “price” or be “purchased” individually (rather than have access granted from a paid subscription) in order to qualify as a “product.”

Second, alternatively, the “product” can be viewed as the *song*, not the specific format or clip size of a particular file. *See also* Ans. 33 (“the broadest reasonable interpretation of this term [i.e., ‘products’] is inclusive of a clip which identifies a full portion of a file”). Regardless of whether the user is seeking a free sample, a subscriber’s selection on demand, or permanent ownership, all of the choices relate to and identify the same song (e.g., “Jessica” by “Allman Brothers, The”). By analogy, if a customer goes to an ice cream shop and wants strawberry ice cream, they could get a free sample by identifying the flavor (i.e., strawberry ice cream) and asking to try it, or they could get a full scoop by identifying the flavor (i.e., strawberry ice cream) and paying some money, but in both cases the identified product is the flavored ice cream (i.e., strawberry ice cream), not the quantity of that flavor.

Third, even if the claimed “product” did have to be the same clip or file rather than merely the same song, we agree with the Examiner that “the

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

identification of the product can be the selection of a clip representing the full product and the request to purchase the full clip can be the transaction purchase request.” Ans. 33. For example, in Figure 10 of Khedouri, when the user presses the “buy song” button 1004, the portable device informs the server both that a purchase is desired (i.e., “a transaction purchase request”) and what product is to be purchased (i.e., “an identification of one or more products selected”). See Khedouri ¶ 94. Given the significant overlap in how these two limitations are written (i.e., all of the italicized text in “*receives, from the non-browser based application generated screen, an identification of one or more products selected from the list of products*” and “*receives a transaction purchase request including information relating to the identification of the one or more products from the non-browser based application generated screen*”), if a “transaction purchase request” includes “an identification of one or more products selected from the list of products,” then *both* “receives” limitations are simultaneously satisfied. Nothing in claim 2 requires that these “receives” limitations be performed in two messages rather than one. Thus, Khedouri’s transaction purchase request identifying a specific product teaches or suggests these “receives” limitations.

Accordingly, we are not persuaded the Examiner erred in finding Khedouri teaches or suggests “receives, from the non-browser based application generated screen, an identification of one or more products selected from the list of products” and “receives a transaction purchase

Appeal 2024-001870
 Reexamination Control 90/019,134
 Patent 10,825,007 B2

request including information relating to the identification of the one or more products from the non-browser based application generated screen.”⁴

Whether the combination of Khedouri and Goldthwaite teaches a “transaction server” to “send a transaction verification to the remote management server”

Independent claim 2 recites a “transaction server” for processing a transaction, comprising a transaction server interface configured to “send a

⁴ In the event of further prosecution, the Examiner may wish to consider the obviousness of another alternative. According to Khedouri, “[t]he *portable* wireless communication player device 100 according to the present invention is constructed and arranged to operate as a standalone device that can *search* and obtain content *over the Internet*.” Khedouri ¶ 51 (emphasis added). If Khedouri’s portable device lacks a browser (¶ 121) and searching is done over the Internet (¶ 51) rather than via locally-stored databases (¶ 52), such as searching when the device is connected to a WiFi network or in its cradle hardwired to the Internet (per paragraph 64), then the selection of a song (e.g., selecting “Jessica” in Figure 9) may teach or suggest “receives, from the non-browser based application generated screen, an identification of one or more products selected from the list of products” and the selection to purchase that song (e.g., selecting “buy song” in Figure 10) may teach or suggest “receives a transaction purchase request including information relating to the identification of the one or more products from the non-browser based application generated screen.” Similar to browsers connected to the Internet, a non-browser searching over the Internet rather than searching local databases provides clear benefits: “Since users are searching in ‘real time’, they will always be seeing the latest, modified results” such that “customers (at the ‘point of purchase’—i.e., the time they decide to make the purchase) see the most current information” (e.g., “purchase price terms and information are always current”). *See id.* ¶¶ 122–23 (discussing benefits of browsers). “Without a browser the same features have to be provided.” *Id.* ¶ 125. Thus, Khedouri may teach or suggest a non-browser based application using the Internet to search while connected.

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed.”

Appellant argues “Goldthwaite’s financial institution server 112 is not the claimed ‘transaction server’” because “Goldthwaite’s financial institution server 112 transmits the confirmation (allegedly the ‘transaction verification’) to the *payment server 106*,” which is “*not the claimed ‘remote management server’*” because “Goldthwaite’s payment server 106 does not perform any authentication much less authenticate a user.” Supp. Appeal Br. 77. Appellant further contends that “Goldthwaite’s *authentication server 107* is not the claimed ‘remote management server’ either” because in Goldthwaite, “the user authenticates locally using the smart card on the mobile device.” *Id.* at 77–78 (some emphasis omitted).

Appellant further argues that “Khedouri’s network 315 does not receive a transaction verification from a transaction server.” Supp. Appeal Br. 79 (emphasis omitted).

The Examiner, however, explains that “[t]he rejections noted that to the extent[] Khedouri does not explicitly disclose **a transaction server**, Goldthwaite discloses a *transaction server*.” Ans. 39 (citing Goldthwaite ¶¶ 21, 22, 6–8, 25–29, Figs. 4, 4c). The Examiner relied on Khedouri, not Goldthwaite, for teaching the claimed remote management server and authentication. Ans. 38–39; Final Act. 5–6 (discussing similar limitations in claim 1), 13 (“claim 2 is rejected under the same rationale provided above with respect to claim 1”).

We therefore agree with the Examiner that Appellant is improperly attacking the references individually or requiring bodily incorporation. Ans.

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

40–41; *see, e.g., In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) (“Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references.”); *In re Keller*, 642 F.2d 413, 425 (CCPA 1981) (“The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art.”). “The argument that Khedouri’s network is not a remote management server because it does not receive a transaction verification from a transaction server fails to consider the combined teaching of Goldthwaite” Ans. 41. Khedouri discloses using “a standard electronic credit card billing procedure” after a user verifies a purchase request. Khedouri ¶ 57. Goldthwaite provides more details about what a standard electronic credit card billing procedure entails, including that “[t]he financial institution 112 processes the payment transaction and sends a confirmation of the payment transaction.” Goldthwaite ¶ 21. We see no error in this straightforward combination of Goldthwaite providing more details about what Khedouri says is a routine process.

Appellant further argues that the Examiner “fails to identify a reason” for combining Khedouri and Goldthwaite or relies on “impermissible hindsight.” Supp. Appeal Br. 83. According to Appellant, “the Office Action’s assertions are not reasons, but merely conclusionary statements.” *Id.* at 82 (emphasis omitted).

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

We are not persuaded by Appellant’s argument. As discussed above, Khedouri discloses using “a standard electronic credit card billing procedure” (Khedouri ¶ 57) and Goldthwaite merely provides the details for that standard procedure, including using a transaction server and providing a transaction verification (Goldthwaite ¶ 21). We agree with the Examiner that “a skilled artisan would recognize the financial institution utilizes a server for the transaction verification.” Ans. 43. “It would have been obvious to a skilled artisan at the time of the invention to incorporate Goldthwaite’s financial institution server within Khedouri’s system for purchasing digital content” *Id.* (emphasis omitted). “[B]oth references are drawn to making purchases in a financial system” and “Goldthwaite [merely] demonstrates that a transaction server for processing payment transactions and sending confirmation to a remote server of the payment transaction was known in the art at the time of the invention.” *Id.* at 43–44. Moreover, “the results would have been predictable because it was beneficial to receive [a] transaction verification from a transaction server in order to verify credit card transactions.” *Id.* (emphasis omitted).

The Supreme Court has explained that “[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). Moreover, a factfinder “need not seek out precise teachings directed to the specific subject matter of the challenged claim” and “can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.” *Id.* at 418. “Under the correct analysis, any need or problem known in the field of endeavor at the time of

Appeal 2024-001870
Reexamination Control 90/019,134
Patent 10,825,007 B2

invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.” *Id.* at 420. Here, we agree with the Examiner that Goldthwaite merely filling in the details of what Khedouri refers to as a “standard” electronic credit card billing procedure, namely Goldthwaite teaching that the transaction is performed on a server that provides a transaction verification when the transaction is complete, does no more than yield predictable results. Moreover, the benefits of using Goldthwaite’s transaction confirmation would have been clear to a person of ordinary skill in the art at the time of the invention (e.g., confirming that the transaction was successful so that the rest of the purchase process can be completed). Appellant fails to provide sufficient explanation why a person of ordinary skill in the art seeking to implement Khedouri’s “standard” billing procedure would not have looked to Goldthwaite to do so, as the Examiner suggests.

Accordingly, we sustain the Examiner’s rejection of claim 2, and claims 1 and 3–36, which Appellant argues are patentable for similar reasons. *See* Supp. Appeal Br. 85; 37 C.F.R. § 41.37(c)(1)(iv).

Appeal 2024-001870
 Reexamination Control 90/019,134
 Patent 10,825,007 B2

DECISION SUMMARY

The following table summarizes the outcome of each rejection:

Claim(s) Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1–19, 22–26, 29–32, 35	103	Khedouri, Goldthwaite	1–19, 22– 26, 29–32, 35	
20, 27	103	Khedouri, Goldthwaite, Goh	20, 27	
21, 28, 33, 34, 36	103	Khedouri, Goldthwaite, Hoerenz	21, 28, 33, 34, 36	
Overall Outcome			1–36	

TIME TO RESPOND

Requests for extensions of time in this *ex parte* reexamination proceeding are governed by 37 C.F.R. § 1.550(c). See 37 C.F.R. § 41.50(f).

AFFIRMED

PATENT OWNER/APPELLANT
 MICHELLE FISHER
 2930 DOMINGO AVE., STE. 123
 BERKELEY, CA 94705

THIRD PARTY REQUESTER
 JAMES MARINA
 KIRKLAND & ELLIS LLP
 601 LEXINGTON AVENUE
 NEW YORK, NY 10022



US010825007B2

(12) **United States Patent
Fisher**

(10) **Patent No.: US 10,825,007 B2**
(45) **Date of Patent: *Nov. 3, 2020**

(54) **REMOTE TRANSACTION PROCESSING OF
AT A TRANSACTION SERVER**

(71) Applicant: **Michelle Fisher**, Oakland, CA (US)

(72) Inventor: **Michelle Fisher**, Oakland, CA (US)

(73) Assignee: **Michelle Fisher**, Berkeley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 461 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/253,648**

(22) Filed: **Apr. 15, 2014**

(65) **Prior Publication Data**

US 2014/0324635 A1 Oct. 30, 2014

Related U.S. Application Data

(63) Continuation of application No. 13/736,056, filed on Jan. 7, 2013, now Pat. No. 8,694,380, which is a (Continued)

(51) **Int. Cl.**
G06Q 20/20 (2012.01)
H04W 4/21 (2018.01)
(Continued)

(52) **U.S. Cl.**
CPC **G06Q 20/20** (2013.01); **G06Q 20/00** (2013.01); **G06Q 20/108** (2013.01); **G06Q 20/16** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC G06Q 20/00-40; G06Q 20/102; G06Q 20/105; G06Q 30/0207; G06Q 10/00;

G06Q 20/32; G06Q 20/3223; G06Q 30/00-02; G06Q 20/3276; G06Q 40/00; G06Q 20/20; G06Q 30/0609; G06Q 20/04; G06Q 20/12; G06F 17/30; G06F 17/00; G06F 17/16; G06F 21/00; G06F 21/41; H04L 29/06; H04L 63/0428; H04N 7/14

(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,687 A * 7/1844 Hoe G06Q 20/32 235/375
5,852,775 A * 12/1998 Hidary H04L 12/1859 455/412.1

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO 2006095212 A1 * 9/2006 H04M 11/00
WO WO 2006095212 A1 9/2006

OTHER PUBLICATIONS

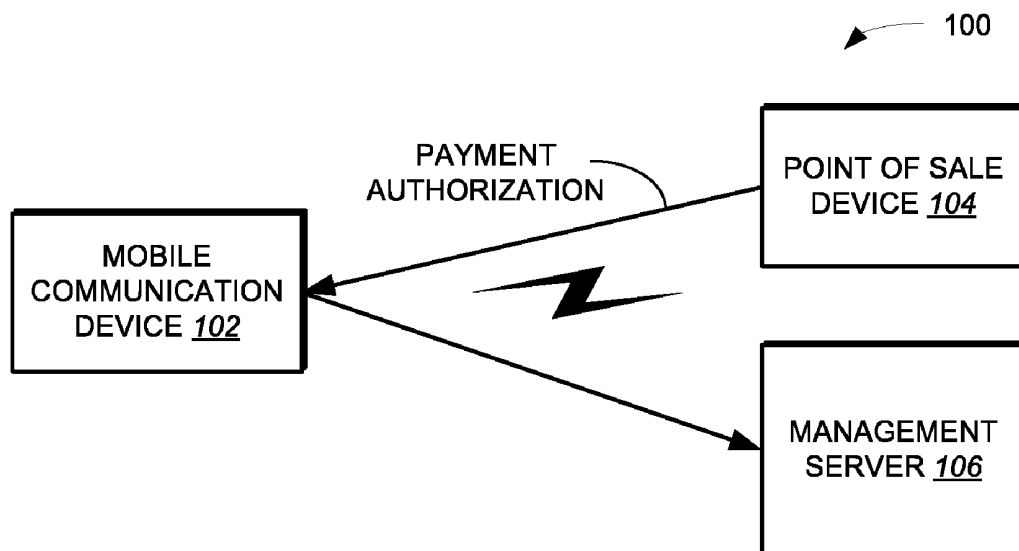
U.S. Appl. No. 11/933,337, Office Action dated May 27, 2010, 9 p.
(Continued)

Primary Examiner — Olusegun Goyea

(57) **ABSTRACT**

A method and system for receiving digital artifacts from a management server. The method includes sending a request for a digital artifact from a mobile application to the management server for display within a specific mobile application generated screen, receiving the digital artifact from the management server, and displaying the digital artifact with the specific mobile application generated screen.

36 Claims, 4 Drawing Sheets



US 10,825,007 B2

Page 2

Related U.S. Application Data

(56)

References Cited

continuation of application No. 11/948,903, filed on
Nov. 30, 2007, now Pat. No. 8,352,323.

U.S. PATENT DOCUMENTS

(51) Int. Cl.

G06Q 20/32 (2012.01)
G06Q 30/02 (2012.01)
G06Q 30/06 (2012.01)
G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
G06Q 20/36 (2012.01)
G06Q 20/16 (2012.01)
G06Q 20/00 (2012.01)
G06Q 20/10 (2012.01)
H04W 8/20 (2009.01)
H04M 1/725 (2006.01)
H04W 4/18 (2009.01)
H04B 5/00 (2006.01)
G06Q 40/00 (2012.01)
H04W 4/80 (2018.01)
H04W 4/029 (2018.01)
H04N 21/81 (2011.01)
G07F 7/10 (2006.01)
H04W 88/02 (2009.01)
H04W 4/02 (2018.01)

(52) U.S. Cl.

CPC **G06Q 20/202** (2013.01); **G06Q 20/204**
(2013.01); **G06Q 20/206** (2013.01); **G06Q**
20/32 (2013.01); **G06Q 20/322** (2013.01);
G06Q 20/325 (2013.01); **G06Q 20/3223**
(2013.01); **G06Q 20/3226** (2013.01); **G06Q**
20/3227 (2013.01); **G06Q 20/3255** (2013.01);
G06Q 20/3278 (2013.01); **G06Q 20/3674**
(2013.01); **G06Q 20/382** (2013.01); **G06Q**
20/3821 (2013.01); **G06Q 20/40** (2013.01);
G06Q 20/409 (2013.01); **G06Q 20/4012**
(2013.01); **G06Q 20/4014** (2013.01); **G06Q**
30/02 (2013.01); **G06Q 30/0222** (2013.01);
G06Q 30/0238 (2013.01); **G06Q 30/0251**
(2013.01); **G06Q 30/0253** (2013.01); **G06Q**
30/0255 (2013.01); **G06Q 30/0267** (2013.01);
G06Q 30/0268 (2013.01); **G06Q 30/06**
(2013.01); **G06Q 30/0613** (2013.01); **G06Q**
30/0635 (2013.01); **G06Q 40/10** (2013.01);
G06Q 40/12 (2013.12); **H04B 5/0025**
(2013.01); **H04M 1/72561** (2013.01); **H04W**
4/18 (2013.01); **H04W 4/21** (2018.02); **H04W**
8/205 (2013.01); **G06Q 20/10** (2013.01);
G06Q 20/105 (2013.01); **G06Q 40/00**
(2013.01); **G07F 7/1008** (2013.01); **H04N**
21/812 (2013.01); **H04W 4/02** (2013.01);
H04W 4/029 (2018.02); **H04W 4/80** (2018.02);
H04W 88/02 (2013.01)

(58) Field of Classification Search

USPC 705/7, 16, 18, 26.1, 30–34, 39–44, 70,
705/1.1, 14.67, 14.72, 24, 28, 35, 26.62,
705/65, 14.23, 26.8, 27.1, 26.81, 51, 46;
455/406, 407, 414.1, 411; 707/737, 754,
707/621, 622, 999.103, 999.107;
235/462.46; 380/201; 348/14.03;
713/153

See application file for complete search history.

5,887,266 A * 3/1999 Heinonen G06Q 20/04
455/406
5,915,243 A * 6/1999 Smolen G06Q 30/02
379/92.01
6,036,086 A * 3/2000 Sizer, II G06Q 20/32
235/375
6,038,367 A 3/2000 Abecassis
6,075,971 A * 6/2000 Williams H04N 21/25891
348/E7.063
6,101,483 A * 8/2000 Petrovich G06Q 20/202
705/21
6,115,601 A * 9/2000 Ferreira H04M 15/47
455/406
6,123,259 A * 9/2000 Ogasawara G06K 17/0022
235/380
6,128,655 A 10/2000 Fields
6,141,666 A 10/2000 Tobin
6,199,082 B1 3/2001 Ferrel
6,250,557 B1 * 6/2001 Forslund G06Q 20/3572
235/492
6,334,109 B1 * 12/2001 Kanevsky G06Q 30/02
705/14.67
6,394,341 B1 * 5/2002 Makipaa G06Q 20/02
235/379
6,415,156 B1 7/2002 Stadelmann
6,450,407 B1 * 9/2002 Freeman G06K 19/0723
235/376
6,487,540 B1 * 11/2002 Smith G06Q 20/209
705/21
6,535,132 B2 * 3/2003 Waters G09F 3/00
235/383
6,587,835 B1 * 7/2003 Treyz G06Q 20/12
705/14.64
6,605,120 B1 8/2003 Fields
6,647,257 B2 * 11/2003 Owensby H04M 3/42348
455/414.1
6,771,981 B1 8/2004 Zalewski
6,772,396 B1 8/2004 Cronin
6,775,539 B2 * 8/2004 Deshpande G06Q 30/02
455/414.4
6,886,017 B1 4/2005 Jackson
6,950,939 B2 9/2005 Tobin
6,975,856 B2 * 12/2005 Ogasawara G06Q 20/108
455/411
7,031,945 B1 4/2006 Donner
7,069,248 B2 6/2006 Huber
7,072,861 B1 * 7/2006 Yamanaka G06Q 20/04
705/17
7,092,905 B2 * 8/2006 Behrenbrinker G06Q 20/04
705/35
7,096,003 B2 8/2006 Joao
7,110,744 B2 9/2006 Freeny
7,110,792 B2 * 9/2006 Rosenberg G06Q 20/341
455/558
7,127,236 B2 10/2006 Khan
7,200,578 B2 * 4/2007 Paltenghe G06F 21/6209
705/1.1
7,289,810 B2 10/2007 Jagadeesan
7,308,254 B1 12/2007 Rissanen
7,357,312 B2 4/2008 Gangi
7,379,920 B2 5/2008 Leung
7,383,226 B2 * 6/2008 Kight G06Q 20/04
705/40
7,472,829 B2 1/2009 Brown
7,482,925 B2 1/2009 Hammad
7,487,912 B2 * 2/2009 Seifert G06Q 20/10
235/380
7,512,567 B2 * 3/2009 Bommel H04L 9/32
705/67
7,522,905 B2 4/2009 Hammad
7,555,284 B2 * 6/2009 Yan G06Q 20/045
455/411

US 10,825,007 B2

Page 3

(56)

References Cited

U.S. PATENT DOCUMENTS

7,680,824 B2 *	3/2010	Plastina	G06F 17/30026	2002/0060246 A1 *	5/2002	Gobburu	G06Q 20/04
			707/737				235/462.46
7,725,369 B2 *	5/2010	Shiftan	G06Q 20/04	2002/0063895 A1	5/2002	Agata	
			705/28	2002/0065774 A1 *	5/2002	Young	G06Q 20/327
							705/41
7,783,532 B2 *	8/2010	Hsu		2002/0077918 A1	6/2002	Lerner	
7,784,684 B2 *	8/2010	Labrou	G06Q 20/32	2002/0082879 A1	6/2002	Miller	
			235/375	2002/0087396 A1 *	7/2002	Shida	G06Q 30/02
7,792,756 B2 *	9/2010	Plastina	G06Q 30/02				705/14.33
			705/51	2002/0101993 A1 *	8/2002	Eskin	G01S 1/68
7,818,284 B1 *	10/2010	Walker	G06Q 20/387				380/270
			705/26.2	2002/0106081 A1 *	8/2002	Yang	H04N 21/25875
7,827,056 B2 *	11/2010	Walker	G06Q 10/101				380/201
			705/14.1	2002/0107756 A1	8/2002	Hammons	
7,870,077 B2 *	1/2011	Woo	G06Q 20/02	2002/0107791 A1 *	8/2002	Nobrega	G06Q 20/02
			235/379				705/39
7,979,519 B2 *	7/2011	Shigeta	H04L 67/2823	2002/0116269 A1 *	8/2002	Ishida	G06Q 30/02
			370/349				705/14.64
8,005,426 B2 *	8/2011	Huomo	G06Q 20/20	2002/0120589 A1 *	8/2002	Aoki	A63F 13/10
			235/441				705/400
8,019,362 B2 *	9/2011	Sweatman	H04W 4/12	2002/0160761 A1 *	10/2002	Wolfe	H04M 3/493
			455/455				455/414.1
8,073,424 B2 *	12/2011	Sun	G06Q 20/085	2002/0169664 A1 *	11/2002	Walker	G06Q 20/102
			455/406				705/14.36
8,086,534 B2 *	12/2011	Powell	G06Q 20/32	2002/0169984 A1	11/2002	Kumar	
			705/44	2002/0174444 A1 *	11/2002	Gatto	H04N 21/654
8,109,444 B2 *	2/2012	Jain	G06K 19/07739				725/133
			235/487	2002/0183046 A1 *	12/2002	Joyce	G06Q 20/06
8,121,945 B2	2/2012	Rackley					455/414.1
8,127,984 B2 *	3/2012	Zatloukal	G06K 7/0008	2003/0022655 A1 *	1/2003	Bogat	G06Q 20/04
			235/375				455/406
8,214,454 B1 *	7/2012	Barnes	G06F 17/30876	2003/0028426 A1 *	2/2003	Banerjee	G06Q 30/02
			709/217				705/14.37
8,396,758 B2 *	3/2013	Paradise	G06Q 30/0609	2003/0033272 A1 *	2/2003	Himmel	B42D 15/00
			705/26.62				705/14.36
8,429,030 B2 *	4/2013	Walker	G06Q 30/04	2003/0061113 A1 *	3/2003	Petrovich	G06Q 20/343
			705/26.7				705/26.43
8,429,031 B2 *	4/2013	Walker	G07G 1/12	2003/0065805 A1	4/2003	Barnes	
			705/26.7	2003/0066883 A1 *	4/2003	Yu	G06Q 20/327
8,429,048 B2 *	4/2013	Singh	G06Q 20/047				235/382
			705/35	2003/0074259 A1 *	4/2003	Slyman, Jr.	G06Q 30/0221
8,438,077 B2 *	5/2013	Walker	G07F 17/3248				705/14.22
			705/26.7	2003/0085286 A1 *	5/2003	Kelley	G06K 19/073
8,438,078 B2 *	5/2013	Walker	G06Q 30/0235				235/492
			705/26.7	2003/0087601 A1 *	5/2003	Agam	G06F 21/34
8,467,766 B2 *	6/2013	Rackley, III	G06Q 40/02				455/39
			455/406	2003/0093311 A1 *	5/2003	Knowlson	G06K 19/073
8,484,058 B2 *	7/2013	Benson	G06Q 10/02				235/492
			705/26.1	2003/0093695 A1	5/2003	Dutta	
8,489,067 B2 *	7/2013	Rackley, III	G06Q 20/325	2003/0105641 A1	6/2003	Lewis	
			455/406	2003/0132298 A1 *	7/2003	Swartz	G07G 3/00
8,510,220 B2 *	8/2013	Rackley, III	G06Q 40/00				235/472.02
			705/40	2003/0140004 A1	7/2003	O'Leary	
2001/0011250 A1 *	8/2001	Paltenghe	G06F 21/6263	2003/0159040 A1 *	8/2003	Hashimoto	G06F 21/35
			705/41				713/168
2001/0032333 A1 *	10/2001	Flickinger	G06Q 30/02	2003/0163359 A1 *	8/2003	Kanesaka	G06Q 30/0204
			725/39				705/7.33
2001/0044751 A1 *	11/2001	Pugliese, III	G06Q 30/0643	2003/0172028 A1	9/2003	Abell	
			705/14.1	2003/0225686 A1 *	12/2003	Mollett	G06Q 20/40145
2001/0049636 A1 *	12/2001	Hudda	G06Q 30/0601				705/38
			705/26.1	2004/0002897 A1 *	1/2004	Vishik	G06Q 30/0253
2001/0051915 A1 *	12/2001	Ueno	G06Q 20/04				705/14.51
			705/39	2004/0006497 A1	1/2004	Nestor	
2002/0026423 A1 *	2/2002	Maritzen	G06Q 20/02	2004/0030658 A1 *	2/2004	Cruz	G06Q 20/045
			705/56				705/65
2002/0046090 A1 *	4/2002	Stewart	G06Q 30/0261	2004/0034544 A1	2/2004	Fields	
			705/14.52	2004/0064407 A1 *	4/2004	Kight	G06Q 20/14
2002/0056091 A1 *	5/2002	Bala	H04L 69/329				705/40
			725/34	2004/0064408 A1 *	4/2004	Kight	G06Q 20/385
2002/0059100 A1	5/2002	Shore					705/40
2002/0059147 A1 *	5/2002	Ogasawara	G06Q 30/0641	2004/0064409 A1 *	4/2004	Kight	G06Q 40/04
			705/70				705/40
				2004/0064410 A1 *	4/2004	Kight	G06Q 20/102
							705/40
				2004/0073439 A1 *	4/2004	Shuster	G07C 9/00079
							705/5

US 10,825,007 B2

Page 4

(56)

References Cited

U.S. PATENT DOCUMENTS

2004/0073497 A1 *	4/2004	Hayes	G06Q 30/0601	2006/0031752 A1 *	2/2006	Surloff	G06F 3/0219
			705/26.1				715/205
2004/0078329 A1 *	4/2004	Kight	G06Q 20/108	2006/0044153 A1 *	3/2006	Dawidowsky	G06K 19/0723
			705/40				340/4.3
2004/0083167 A1 *	4/2004	Kight	G06Q 40/00	2006/0085840 A1 *	4/2006	Bruck	H04N 21/25816
			705/40				726/3
2004/0093271 A1 *	5/2004	Walker	G07F 5/24	2006/0089874 A1 *	4/2006	Newman	G06Q 30/02
			705/14.17				705/14.32
2004/0111320 A1 *	6/2004	Schlieffers	B62B 3/1424	2006/0089949 A1 *	4/2006	Robbin	G06Q 30/0641
			705/16	2006/0095339 A1 *	5/2006	Hayashi	G06Q 30/0601
2004/0122768 A1 *	6/2004	Creamer	G07F 7/0866				705/26.8
			705/41	2006/0100924 A1 *	5/2006	Tevanian, Jr.	G06Q 30/0222
2004/0127256 A1 *	7/2004	Goldthwaite	G06Q 20/02				705/14.23
			455/558	2006/0123052 A1 *	6/2006	Robbin	G06Q 30/00
2004/0143545 A1 *	7/2004	Kulakowski	G06Q 20/02	2006/0135156 A1 *	6/2006	Malu	
			705/39	2006/0143091 A1 *	6/2006	Yuan	G06Q 30/0601
2004/0168052 A1 *	8/2004	Clisham	H04W 12/001				705/26.1
			713/153	2006/0165060 A1 *	7/2006	Dua	G06Q 20/42
2004/0216108 A1 *	10/2004	Robbin	G06Q 20/2295				370/352
			718/100	2006/0170759 A1 *	8/2006	Roever	G07F 17/16
2004/0224638 A1 *	11/2004	Fadell	G06F 1/1632				348/14.03
			455/66.1	2006/0173701 A1 *	8/2006	Gurvey	G06Q 10/02
2004/0235450 A1 *	11/2004	Rosenberg	G06Q 20/085				705/67
			455/406	2006/0174314 A1 *	8/2006	Jacobs	H04N 21/41407
2004/0243479 A1 *	12/2004	Gross	H04N 21/4314				725/135
			705/26.25	2006/0180660 A1 *	8/2006	Gray	G06Q 20/24
2004/0243519 A1	12/2004	Perttila					235/380
2004/0254836 A1 *	12/2004	Emoke Barabas	G06Q 30/02	2006/0184398 A1 *	8/2006	Kasagi	G06Q 10/02
			705/14.35				705/309
2004/0267618 A1	12/2004	Judicibus		2006/0184431 A1 *	8/2006	Rosenberg	G06Q 30/06
2004/0267665 A1	12/2004	Nam					705/26.8
2005/0003810 A1	1/2005	Chu		2006/0191995 A1 *	8/2006	Stewart	G06Q 20/40
2005/0021478 A1 *	1/2005	Gautier	G06Q 20/123				235/379
			705/65	2006/0206709 A1 *	9/2006	Labrou	H04L 63/083
2005/0037735 A1 *	2/2005	Coutts					713/167
2005/0040230 A1 *	2/2005	Swartz	G06Q 20/343	2006/0212401 A1 *	9/2006	Ameerally	G06Q 30/02
			235/383				705/51
2005/0043994 A1 *	2/2005	Walker	G06Q 10/087	2006/0218092 A1 *	9/2006	Tedesco	G06Q 20/12
			705/14.19				705/40
2005/0050345 A1 *	3/2005	Dowdy	G06F 21/10	2006/0219780 A1 *	10/2006	Swartz	G07G 1/0054
			713/193				235/383
2005/0060536 A1 *	3/2005	Iga	G06Q 20/367	2006/0235864 A1 *	10/2006	Hotelling	G06Q 30/0601
			713/155	2006/0247976 A1 *	11/2006	Posokhow	G06Q 30/06
2005/0071780 A1 *	3/2005	Muller	G06F 16/954				705/26.81
			715/825	2006/0248113 A1 *	11/2006	Leffert	G06Q 40/04
2005/0076210 A1	4/2005	Thomas		2006/0248114 A1 *	11/2006	Anderson	G06Q 30/06
2005/0131837 A1 *	6/2005	Sanctis	G06Q 20/12	2006/0265637 A1 *	11/2006	Marriott	G06F 16/9535
			705/64				715/210
2005/0150945 A1 *	7/2005	Choi	G06Q 20/108	2006/0287920 A1 *	12/2006	Perkins	G06Q 30/02
			235/379				705/14.49
2005/0165646 A1 *	7/2005	Tedesco	G06Q 20/14	2006/0294025 A1 *	12/2006	Mengerink	G06Q 30/0239
			705/14.1				705/77
2005/0187873 A1 *	8/2005	Labrou	G07F 7/0886	2007/0004391 A1	1/2007	Maffei	
			705/40	2007/0011099 A1 *	1/2007	Sheehan	G06Q 20/32
2005/0203959 A1 *	9/2005	Muller	G06Q 20/1235				705/65
2005/0210387 A1 *	9/2005	Alagappan	H04L 67/14	2007/0012763 A1 *	1/2007	Van de Velde	G06Q 20/18
			715/700				235/380
2005/0215231 A1	9/2005	Bauchot		2007/0021969 A1 *	1/2007	Homeier-Beals	
2005/0222961 A1 *	10/2005	Staib	G06Q 20/327				G06Q 20/3227
			705/64				705/1.1
2005/0240484 A1 *	10/2005	Yan	G06Q 20/363	2007/0022058 A1 *	1/2007	Labrou	G07F 7/1008
			455/411				705/67
2005/0240494 A1 *	10/2005	Cue	G06F 16/4387	2007/0095892 A1	5/2007	Lyons	
			705/26.1	2007/0125838 A1 *	6/2007	Law	G06Q 20/32
2005/0278369 A1 *	12/2005	Tokita	H04N 5/23293				235/379
2005/0283444 A1 *	12/2005	Ekberg	G06Q 20/02	2007/0125840 A1 *	6/2007	Law	G06Q 20/10
			705/67				235/379
2006/0014518 A1 *	1/2006	Huh	H04M 15/06	2007/0138299 A1 *	6/2007	Mitra	G06Q 20/357
			455/406				235/492
2006/0015580 A1 *	1/2006	Gabriel	H04N 21/2389	2007/0131759 A1	7/2007	Cox	
			709/219	2007/0156436 A1 *	7/2007	Fisher	G06Q 20/401
							455/552.1
				2007/0175978 A1 *	8/2007	Stambaugh	G06Q 20/32
							235/379
				2007/0179883 A1 *	8/2007	Questembert	G07F 19/00
							705/39

US 10,825,007 B2

Page 5

(56)

References Cited

U.S. PATENT DOCUMENTS

2007/0210155 A1 *	9/2007	Swartz	G06Q 20/32 235/383	2008/0172285 A1 *	7/2008	Hurowitz	G06Q 30/0261 455/414.1
2007/0235519 A1	10/2007	Jang		2008/0172291 A1 *	7/2008	Hurowitz	G06Q 30/02 705/14.1
2007/0235539 A1 *	10/2007	Sevanto	G06K 7/10237 235/451	2008/0172292 A1 *	7/2008	Hurowitz	H04N 21/25841 705/14.14
2007/0255662 A1	11/2007	Tumminaro		2008/0177668 A1	7/2008	Delean	
2007/0270166 A1 *	11/2007	Hampel	H04L 51/20 455/456.3	2008/0207234 A1 *	8/2008	Arthur	G06Q 30/02 455/466
2007/0288966 A1 *	12/2007	Javid	H04N 21/4755 725/46	2008/0208681 A1	8/2008	Hammad	
2007/0293155 A1 *	12/2007	Liao	G06Q 20/3229 455/41.2	2008/0208743 A1 *	8/2008	Arthur	G06Q 20/105 705/41
2008/0004952 A1 *	1/2008	Koli	G06Q 30/0277 705/14.55	2008/0208744 A1 *	8/2008	Arthur	G06Q 20/105 705/41
2008/0006685 A1 *	1/2008	Rackley, III	G06Q 40/00 235/379	2008/0208762 A1 *	8/2008	Arthur	G06Q 20/20 705/79
2008/0010190 A1 *	1/2008	Rackley, III	G06Q 20/042 705/39	2008/0221997 A1 *	9/2008	Wolfe	G06Q 30/0261 705/14.26
2008/0010191 A1 *	1/2008	Rackley, III	G06Q 20/10 705/39	2008/0242274 A1 *	10/2008	Swanburg	G06Q 30/00 455/414.1
2008/0010192 A1 *	1/2008	Rackley, III	G06Q 20/3223 705/39	2008/0249938 A1 *	10/2008	Drake-Stoker ...	H04W 12/1006 705/44
2008/0010193 A1 *	1/2008	Rackley, III	G06Q 20/3221 705/39	2008/0255947 A1 *	10/2008	Friedman	G06Q 20/32 705/35
2008/0010196 A1 *	1/2008	Rackley, III	G06Q 20/102 705/40	2008/0262928 A1 *	10/2008	Michaelis	G06Q 30/0225 705/14.26
2008/0010204 A1 *	1/2008	Rackley, III	G06Q 20/042 705/45	2008/0274794 A1 *	11/2008	Mathieson	G06Q 30/02 463/25
2008/0010215 A1 *	1/2008	Rackley, III	G06Q 20/385 705/70	2008/0275779 A1 *	11/2008	Lakshminarayanan	G06Q 20/3227 705/39
2008/0011825 A1 *	1/2008	Giordano	G06Q 20/04 235/380	2008/0305774 A1	12/2008	Ramakrishna	
2008/0017704 A1 *	1/2008	VanDeburg	G06Q 20/32 235/380	2008/0319915 A1 *	12/2008	Russell	G06Q 30/0633 705/76
2008/0027795 A1 *	1/2008	Medlin	G06Q 30/0212 705/14.14	2009/0018913 A1 *	1/2009	Sarukkai	G06Q 30/0267 705/14.56
2008/0294556 A1	1/2008	Anderson		2009/0061884 A1 *	3/2009	Rajan	G06Q 30/02 455/445
2008/0040265 A1 *	2/2008	Rackley, III	G06Q 20/32 705/40	2009/0063312 A1 *	3/2009	Hurst	G06Q 20/206 705/30
2008/0045172 A1 *	2/2008	Narayanaswami	G06Q 30/02 455/187.1	2009/0076912 A1 *	3/2009	Rajan	G06Q 30/0273 705/14.64
2008/0046366 A1 *	2/2008	Bemmel	G06Q 20/20 705/44	2009/0098825 A1	4/2009	Huomo	
2008/0048022 A1 *	2/2008	Vawter	G06Q 20/388 235/380	2009/0106112 A1 *	4/2009	Dalmia	G06Q 20/04 705/14.17
2008/0051059 A1 *	2/2008	Fisher	H04M 1/7253 455/410	2009/0112747 A1 *	4/2009	Mullen	G06Q 20/04 705/35
2008/0051142 A1 *	2/2008	Calvet	H04W 88/02 455/558	2009/0124234 A1 *	5/2009	Fisher	G06Q 20/04 455/406
2008/0052192 A1 *	2/2008	Fisher	G06Q 20/32 705/5	2009/0132362 A1 *	5/2009	Fisher	G06Q 20/20 705/14.47
2008/0052233 A1 *	2/2008	Fisher	G06Q 20/102 705/40	2009/0143104 A1 *	6/2009	Loh	G06Q 20/352 455/558
2008/0059329 A1 *	3/2008	Luchene	G06Q 30/0609 705/26.35	2009/0144161 A1 *	6/2009	Fisher	G06Q 20/3227 705/16
2008/0126145 A1 *	5/2008	Rackley, III	G06Q 20/102 455/406	2009/0177587 A1 *	7/2009	Siegal	G06Q 30/06 705/67
2008/0133336 A1 *	6/2008	Altman	H04L 51/32 455/456.1	2009/0227281 A1 *	9/2009	Hammad	G06K 19/07309 455/550.1
2008/0139155 A1	6/2008	Boireau		2010/0057619 A1 *	3/2010	Weller	G06Q 20/382 705/67
2008/0140520 A1 *	6/2008	Hyder	G06Q 30/0207 705/14.1	2010/0063895 A1 *	3/2010	Dominguez	G06Q 20/425 705/26.1
2008/0148040 A1 *	6/2008	Machani	H04L 9/3226 713/150	2010/0082491 A1 *	4/2010	Rosenblatt	G06Q 10/02 705/65
2008/0167017 A1 *	7/2008	Wentker	H04L 12/66 455/414.1	2010/0145835 A1 *	6/2010	Davis	G06Q 20/10 705/30
2008/0167961 A1 *	7/2008	Wentker	G06Q 20/10 705/14.25	2010/0312694 A1 *	12/2010	Homeier-Beals	G06Q 20/10 705/39
2008/0167988 A1 *	7/2008	Sun	G06Q 20/26 705/39	2011/0055038 A1 *	3/2011	Mengerink	G06Q 20/085 705/26.1
2008/0172274 A1 *	7/2008	Hurowitz	G06Q 30/0267 455/433	2011/0320316 A1 *	12/2011	Randazza	G06Q 20/02 705/26.43
				2012/0030044 A1 *	2/2012	Hurst	G06Q 20/206 705/18

US 10,825,007 B2

Page 6

(56)

References Cited**U.S. PATENT DOCUMENTS**

2012/0150744 A1* 6/2012 Carlson G06Q 20/12
705/44
2012/0215573 A1* 8/2012 Sussman G06F 9/50
705/5
2012/0220314 A1* 8/2012 Altman G06Q 30/0207
455/456.3
2012/0265677 A1* 10/2012 Rackley, III G06Q 20/10
705/41
2013/0013501 A1* 1/2013 Rackley, III G06Q 20/32
705/41
2013/0054470 A1* 2/2013 Campos G06Q 20/40
705/67
2013/0212016 A1* 8/2013 Davis G06Q 20/3223
705/42

OTHER PUBLICATIONS

U.S. Appl. No. 11/933,351, Office Action dated Oct. 3, 2008, 5 p.

U.S. Appl. No. 11/933,367, Office Action dated May 27, 2010, 8 p.
U.S. Appl. No. 11/467,441, Office Action dated May 27, 2009, 17 p.
U.S. Appl. No. 12/592,581, Office Action dated Jun. 4, 2010, 20 p.
U.S. Appl. No. 11/933,351, Office Action dated Jul. 8, 2009, 7 p.
U.S. Appl. No. 11/939,821, Office Action dated Aug. 17, 2010, 11 p.
U.S. Appl. No. 11/933,351, Office Action dated Aug. 18, 2010, 16 p.
U.S. Appl. No. 11/933,321, Office Action dated May 27, 2010, 11 p.
Deena, M. Amato, "Mobile Rewards." Chain Store Age 82.5 (2006): 160, 161, 163. Hoover's Company Profiles; ProQuest Central. Web. Oct. 5, 2012.
"ViVOtech to Demonstrate Industry's First End-to-End Near Field Communication (NFC) Solution at the NRF Show." Business Wire: 1 Jan. 16, 2006. Business Dateline; Hoover's Company Profiles; ProQuest Central. Web. Oct. 5, 2012.

* cited by examiner

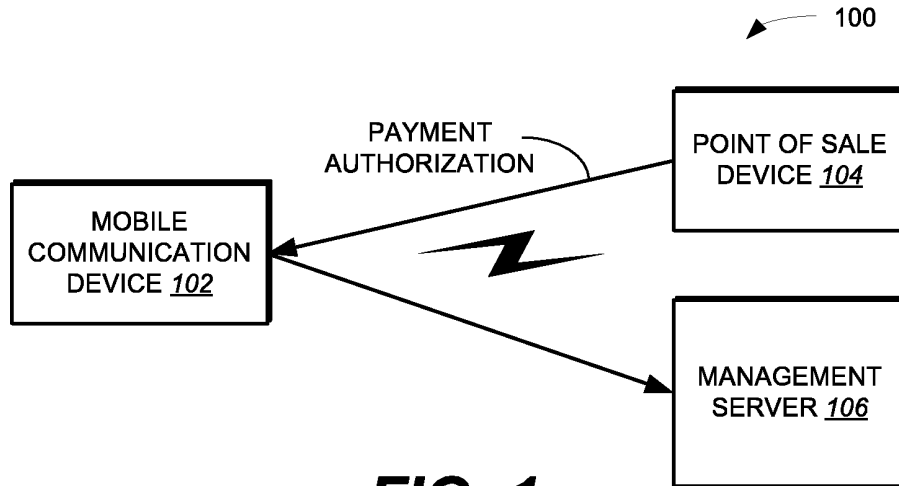


FIG. 1

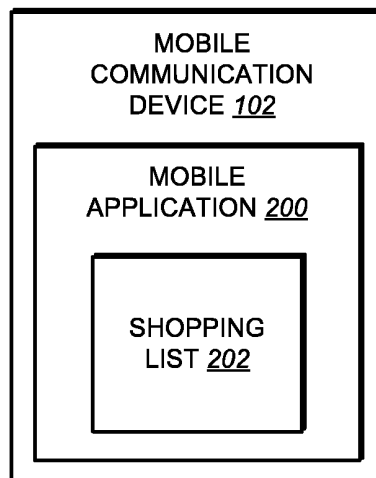
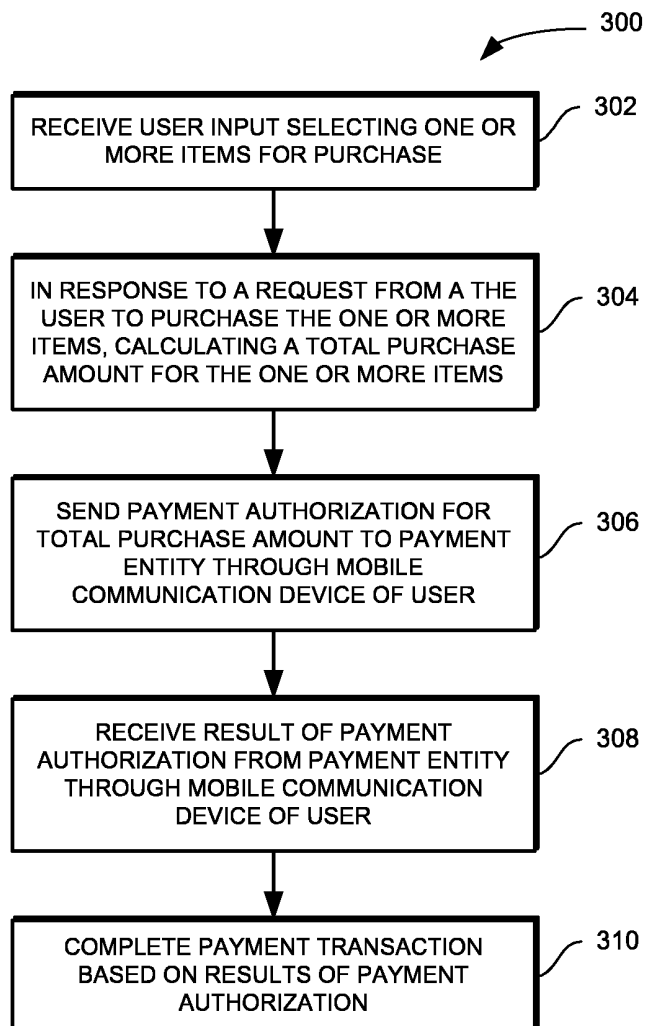
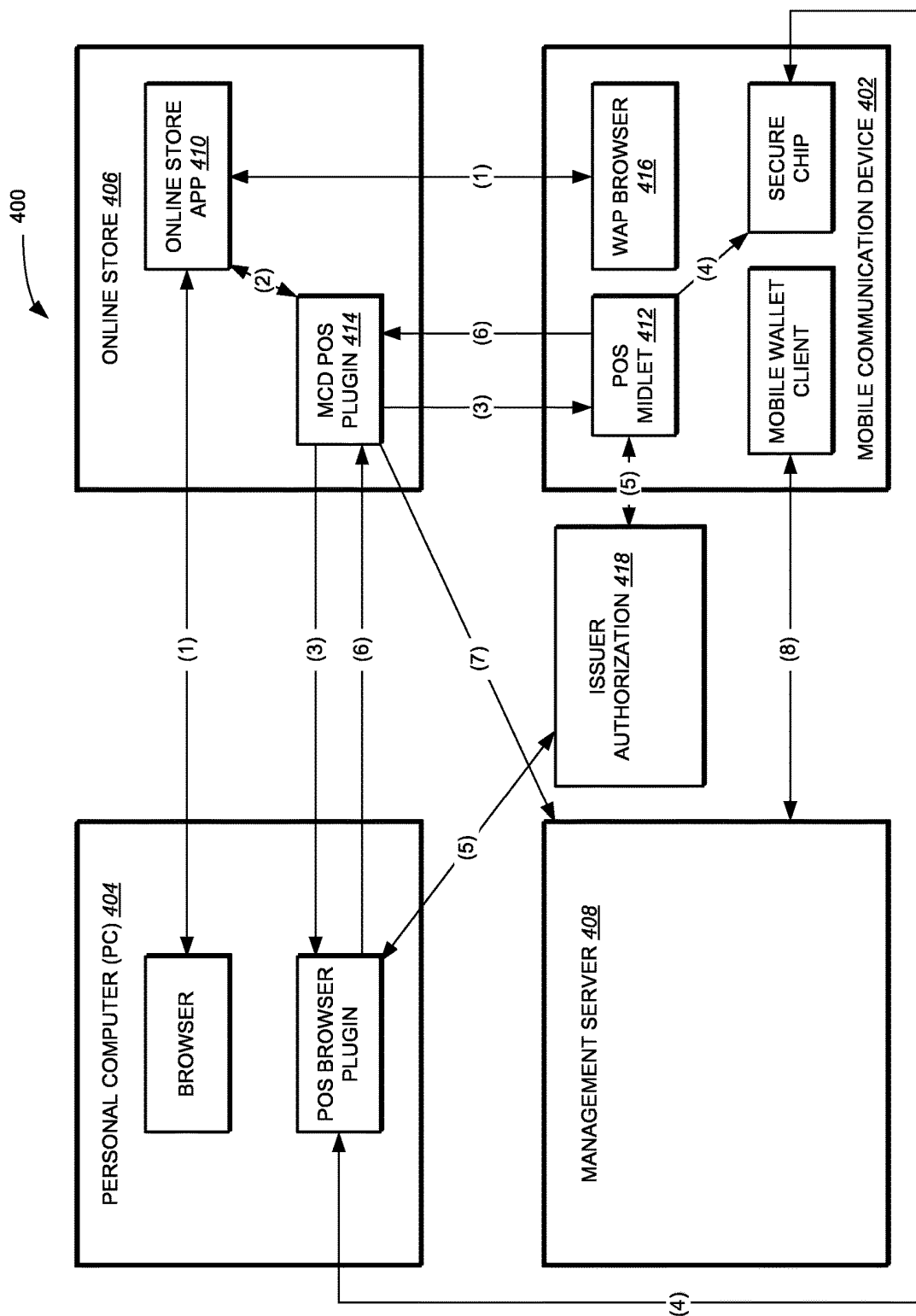
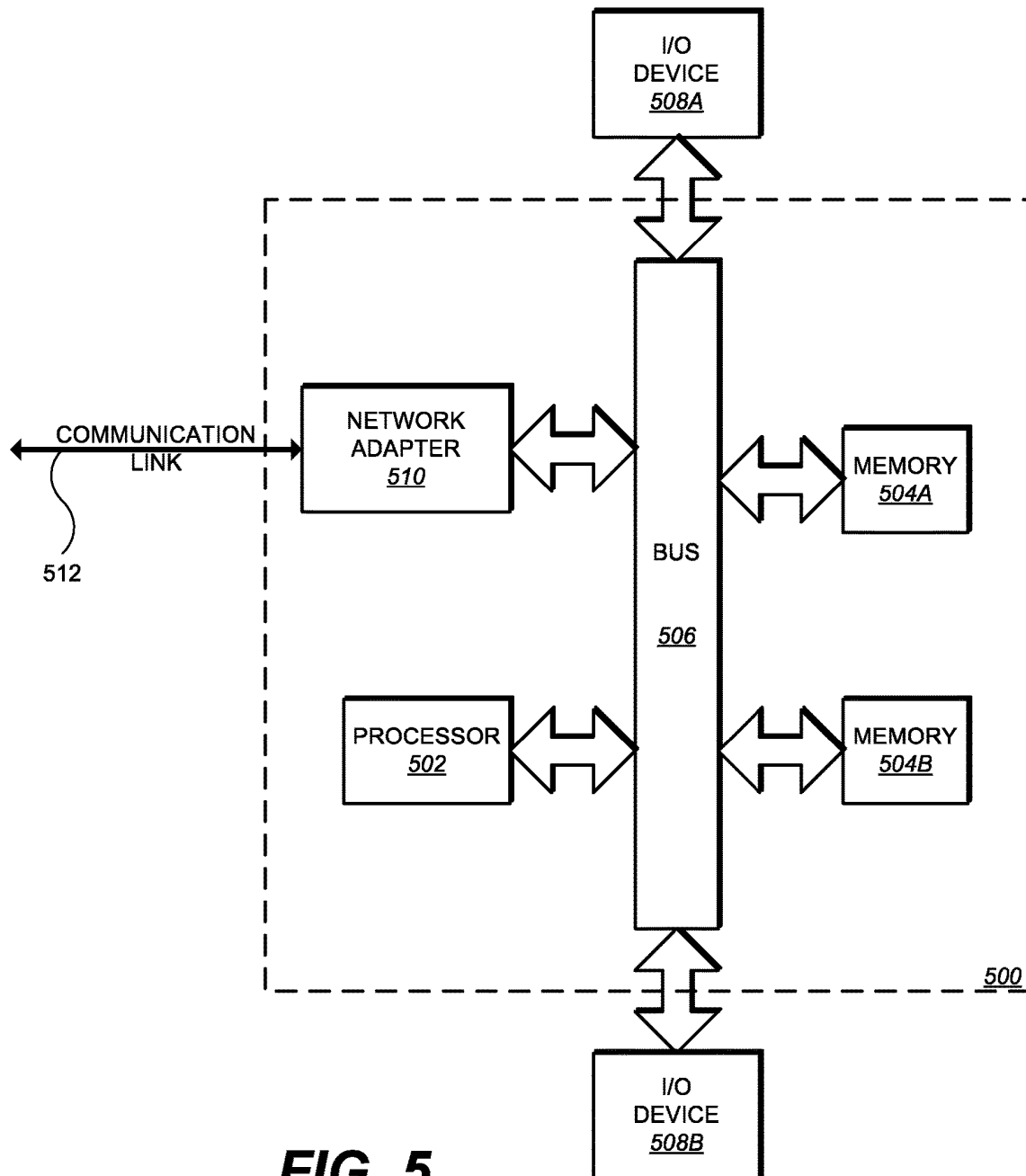


FIG. 2

**FIG. 3**

**FIG. 4**



US 10,825,007 B2

1

REMOTE TRANSACTION PROCESSING OF AT A TRANSACTION SERVER

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of application Ser. No. 13/736,056, filed Jan. 7, 2013, titled "REMOTE TRANSACTION PROCESSING USING A DEFAULT PAYMENT METHOD" which is a continuation and claims priority to application Ser. No. 11/948,903, filed Nov. 30, 2007, titled "METHOD AND SYSTEM FOR CONDUCTING AN ONLINE PAYMENT TRANSACTION USING A MOBILE COMMUNICATION DEVICE", now U.S. Pat. No. 8,352,323 issued on Jan. 8, 2011 both of which are incorporated by reference herein in their entirety.

FIELD OF INVENTION

The present invention relates to data communications and wireless devices.

BACKGROUND OF THE INVENTION

Mobile communication devices—e.g., cellular phones, personal digital assistants, and the like—are increasingly being used to conduct payment transactions as described in U.S. patent application Ser. No. 11/933,351, entitled "Method and System For Scheduling A Banking Transaction Through A Mobile Communication Device", and U.S. patent application Ser. No. 11/467,441, entitled "Method and Apparatus For Completing A Transaction Using A Wireless Mobile Communication Channel and Another Communication Channel, both of which are incorporated herein by reference. Such payment transactions can include, for example, purchasing goods and/or services, bill payments, and transferring funds between bank accounts.

BRIEF SUMMARY OF THE INVENTION

In general, this specification describes a method and system for conducting an online payment transaction through a point of sale device. The method includes receiving input from a user selecting an item for purchase through the point of sale device; calculating a total purchase amount for the item in response to a request from the user to purchase the item; and sending payment authorization for the total purchase amount from the point of sale device to a payment entity, in which the payment authorization is sent to the payment entity via a mobile communication device of the user. The method further includes receiving a result of the payment authorization from the payment entity through the mobile communication device; and completing the payment transaction based on the result of the payment authorization.

Particular implementations can include one or more of the following features. The point of sale device can be a desktop computer, a laptop computer, or a terminal. The mobile communication device can be a cellular phone, a wireless personal digital assistant (PDA), or a laptop computer. The cellular phone can be an NFC-enabled phone. Sending payment authorization for the total purchase amount from the point of sale device to a payment entity can include sending the payment authorization securely to the payment entity. The payment entity can be a person, a computer system, or a bank. The method can further include maintaining a shopping list on the mobile communication device

2

of the user, in which the shopping list includes a listing of one or more items to be purchased by the user. The payment authorization can be an authorization for payment with a credit card, a debit card, or a prepaid card.

The details of one or more implementations are set forth in the accompanying drawings and the description below. Other features and advantages will be apparent from the description and drawings, and from the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a block diagram of a communication system including a wireless mobile communication device and a management server in accordance with one implementation.

FIG. 2 illustrates one implementation of the wireless mobile communication device of FIG. 1.

FIG. 3 is a method for conducting a payment transaction using a point of sale device in accordance with one implementation.

FIG. 4 illustrates a block diagram of a communication system including a wireless mobile communication device and an online store in accordance with one implementation.

FIG. 5 is a block diagram of a data processing system suitable for storing and/or executing program code in accordance with one implementation.

Like reference symbols in the various drawings indicate like elements.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates one implementation of a communication system 100. The communication system 100 includes a hand-held, wireless mobile communication device 102 a point-of-sale device 104 and a management server 106. In one implementation, the mobile communication device 102 includes a mobile application (discussed in greater detail below) that permits a user of the mobile communication device 102 to conduct payment transactions. Payment transactions can include, for example, using contactless payment technology at a retail merchant point of sale (e.g., through point of sale device 104), using mobile/internet commerce (e.g., purchase tickets and products, etc.), storage of payment information and other digital artifacts (e.g., receipts, tickets, coupons, etc.), storage of banking information (payment account numbers, security codes, PIN's, etc.), and accessing banking service (account balance, payment history, bill pay, fund transfer, etc.), and so on. The mobile communication device 102 can be a cellular phone, a wireless personal digital assistant (PDA), a laptop computer, or other wireless communication device. The point of sale device 104 can be a desktop computer, laptop computer, terminal, or other device that is configured to receive user input selecting items for purchase or other transaction.

In one implementation, authorizations for payment transactions that are made through the point of sale device 104 are sent from the point of sale device 104 to an issuer authorization (e.g., management server 106) through the mobile communication device 102 (as shown in FIG. 1). In one implementation, an issuer authorization, is a payment entity that either approves or disapproves a payment transaction. An issuer authorization can be, e.g., a person, computer system, bank (or other third party). One potential benefit of having payment authorizations flow through the mobile communication device 102 is that sensitive user information (e.g. account numbers, pin numbers, and/or

US 10,825,007 B2

3

identity information) need only be sent from the mobile communication device **102** directly to an issuer authorization. Such operation reduces the potential for identity theft and/or fraudulent purchases made through a point of sale device. For example, (in one implementation) payment authorizations cannot be sent to an issuer authorization if the mobile communication device **102** is turned off.

FIG. 2 illustrates one implementation of the mobile communication device **102**. The mobile communication device **102** includes a mobile application **200** that (in one implementation) is provided to the mobile communication device **102** through a remote server (e.g., management server **106**). In one implementation, the mobile application is a Mobile Wallet application available from Mobile Candy Dish, Inc., of Alameda, Calif. In one implementation, the mobile application is a hosted service, as described in U.S. patent application Ser. No. 11/939,821, entitled "Method and System For Securing Transactions Made Through a Mobile Communication Device", which is incorporated herein by reference. In one implementation, the mobile application **200** is configured to send requests to the management server for artifacts based on user input, e.g., received through a keypad (not shown) of the mobile communication device **102**. Requests to the management server **106** can also be automated, via proximity-based services, e.g., consumer tapping (or in close proximity) an LBS/contactless/RFID enabled phone against a smart poster (RFID/Bluetooth/LBS enabled, etc.), kiosk, or other device.

In one implementation, the mobile application **200** running on the mobile communication device **102** is configured to receive artifacts (e.g., advertisements, receipts, tickets, coupons, media, content, and so on) from the management server **106**. In one implementation, the management server **106** sends artifacts to the mobile application based on user profile information and/or a transaction history (or payment trends) associated with a user of the mobile communication device **102** as described in U.S. patent application Ser. No. 11/944,267, entitled "Method and System For Delivering Information To a Mobile Communication Device Based On Consumer Transactions", which is incorporated herein by reference.

In one implementation, the mobile communication device **102** is an NFC-enabled phone. The mobile communication device **102** can be NFC-enabled, for example, through an embedded chip or a sticker that is affixed to the cellular phone, as described in U.S. application Ser. No. 11/933,321, entitled "Method and System For Adapting a Wireless Mobile Communication Device For Wireless Transactions", which is incorporated herein by reference. In one implementation, the NFC chip (or sticker) on the cellular phone can be used in conjunction with a merchant's point of sale device as described in greater detail below.

For example, with reference to FIG. 4, in one implementation, the NFC chip (or sticker) on the cellular phone can communicate with NFC chips that are installed on the front of PC's (TV's, Kiosks, or any other device) and serve as scanners/readers. In this implementation a mobile candy dish applet (e.g., MCD POS plugin **414**) is installed on the consumer's computer (e.g., PC **404**) which interfaces with the NFC chip on the PC. When a consumer (or user) is logging online and they are ready to pay for their products, the consumer opens his mobile wallet and selects one of the payment methods (e.g., credit card, debit card, prepaid card, etc.) from their mobile wallet. If a default card has been selected already, this step is not necessary. The consumer then waves their phone over the NFC reader present on the PC **404**. The consumer's payment credentials are transferred

4

from the phone to the merchant website (e.g., online store application **410**) using a communication protocol between the chip in the phone and the chip in the PC, which can be radio frequency for example. If the consumer has coupons in their mobile wallet the consumer can either elect to manually apply the coupon, save the coupon for a future use (against a larger purchase for example), or have the coupon automatically applied during the transaction and the transaction amount is updated. After the consumer enters any necessary validation information (e.g., pin) to provide a multi-factor authentication and confirms the transaction, the online purchase is processed as normal by the merchant's online processor. The mobile wallet can retrieve transaction data, account balance from the management server **408**.

In one implementation, the mobile communication device **102** is a non NFC-enabled phone. In this implementation, the consumer connects his phone to the PC **404** via some non radio frequency method (e.g., IR, Bluetooth, USB cable, etc.). When a consumer is shopping online and they are ready to pay for their products, the consumer opens his mobile wallet and selects one of the payment methods (e.g., credit card, debit card, prepaid card, etc.) from their mobile wallet. If a default card has been selected already, this step is not necessary. The consumer then pushes, e.g., a "Buy now" button and the consumer's payment credentials are transferred from the phone to the merchant website (e.g., online store application **410**) using the protocol between the phone and the PC **404** which can be radio frequency, for example. If the consumer has coupons in their mobile wallet the consumer can either elect to manually apply the coupon, save the coupon for a future use, or have the coupon automatically applied during the transaction and the transaction amount is updated. After the consumer enters any necessary validation information (e.g., pin) to provide multi-factor authentication and confirms the transaction, the online purchase is processed as normal by the merchant's online processor. The mobile wallet can retrieve transaction data and account balance from the management server **408**.

In one implementation, the management server **408** and merchant portal (e.g., online store **408**) are maintained by trusted parties and use an encrypted tunnel to transfer financial data. When the consumer is ready to pay for their online product, they enter their cell phone number on the merchant portal. The merchant portal (which has an MCD applet (e.g., MCD POS plugin **414**) installed on its server) securely connects to the management server **408** (that in one implementation is maintained by Mobile Candy Dish (MCD)). In one implementation, the management server **408** identifies the consumer through their cell phone number, and verifies the consumer's authenticity by sending a unique transaction code to the consumer mobile wallet on their cell phone. The consumer then enters this unique transaction code onto the merchant's web portal. The merchant portal sends this transaction number to the management server **408** for authentication. Upon authentication, the consumer's virtual wallet and payment methods (e.g., credit card, debit card, prepaid card, etc.) are securely retrieved, from the management server **408** and are displayed to the consumer in a window on a website associated with the merchant portal. The consumer selects one of these payment methods to pay for their transaction. If a default card has been selected already, this step is not necessary. If the consumer has coupons in their mobile wallet the consumer can either elect to manually apply the coupon, save the coupon for a future use, or have the coupon automatically applied during the transaction and the transaction amount is updated. After the consumer enters any necessary validation information to

US 10,825,007 B2

5

provide a multi-factor authentication and confirms the transaction, the online purchase is processed as normal by the merchant's online processor. The mobile wallet can retrieve transaction data, account balance from the management server **408**.

Referring to FIG. 2, in one implementation, the mobile application **200** maintains a shopping list **202** for a consumer. Accordingly, consumers have the ability to store their shopping list in their mobile wallet and add, delete, or change items on their shopping list either in offline or online mode. In one implementation, consumers are sent coupons based on items on their shopping list, preferences, previous shopping history, proximity to the physical retail store, or a combination of these parameters, as discussed in application Ser. No. 11/944,267, which is incorporated by reference above. If the consumer has coupons in their mobile wallet the consumer can either elect to manually apply the coupon, save the coupon for a future use, or have the coupon automatically applied during the transaction and the transaction amount is updated. When a consumer wants to order the items on their shopping list via an online merchant (in contrast to a physical retail store), the consumer can logon to the merchant portal and electronically transmit their shopping list to the merchant portal either by waving their phone over NFC enabled PC's or some other connection such as IR, bluetooth, USB, or the like.

FIG. 3 illustrates a method **300** for conducting a payment transaction using a point of sale device (e.g., point of sale device **104**). User input is received selecting one or more items for purchase (e.g., at the point of sale device) (step **302**). In general, the transaction being made at the point of sale device can be any type of transaction that involves the exchange or transfer of fluids—e.g., the transaction can be a payment transaction, a fund transfer, or other type of transaction. In response to a request from the user to purchase the one or more items, a total purchase amount for the one or more items is calculated (e.g., by the point of sale device) (step **304**). If the user has coupons in their mobile wallet the user can either manually apply the coupon or have the coupon automatically applied during the transaction and the transaction amount is updated. The user request to purchase an item can be received, e.g., by a user clicking on a “buy now” icon that is displayed on a graphical user interface of the point of sale device. Payment authorization for the total purchase amount is sent to a payment entity through a mobile communication device of the user (step **306**). A result of the payment authorization is received at the point of sale device from the payment entity via the mobile communication device (step **308**). The payment transaction is completed based on the result of the payment authorization (step **310**). If the payment transaction was authorized by the payment entity, then the sale of the items through the point of sale device is completed. Otherwise, if the payment transaction was not authorized by the payment entity, then the point of sale device terminates the payment transaction.

FIG. 4 illustrates an example payment transaction being made in a communication system **400** in accordance with one implementation. The communication system **400** includes a mobile communication device **402**, a personal computer (PC) **404**, an online store **406**, and a core (or datastore) **408**. As indicated by interaction (1), a user (or customer), using a phone (e.g., mobile communication device **402** or personal computer **404**), browses an online store website (online store application **410**) and finds an item that the customer wishes to purchase. This could also be a purchase made through a midlet application (POS midlet **412**) residing on the mobile communication device **402**. The

6

user then goes to, e.g., a checkout of the online store **406** make a purchase. If the user has coupons in their mobile wallet the user can either manually apply the coupon or have the coupon automatically applied during the transaction and the transaction amount is updated. When it comes time to authorize the purchase, (in one implementation) the user is given an option to purchase with the mobile communication device **402**. In one implementation, the mobile communication device **402** is an NFC-equipped phone (or NFC phone).

In interaction (2), when the user chooses to purchase with the mobile communication device **402**, the online store application **410** sends the transaction information for authorization to the POS vendor plugin (e.g., MCD POS plugin **414**). In one implementation, the POS vendor plugin is installed in the merchant's online store and enables the merchant to accept MCD Blaze payments as an alternative form of payment, similar to accepting credit cards for payment. As shown by interaction (3), the POS vendor plugin formats, encrypts, and cryptographically signs the purchase authorization request which is sent via a secure SSL link (e.g., HTTPS, Bluetooth, IR, USB, or other suitable protocol) established by the browser/web application **416** back to the mobile communication device **402**. As with the first scenario, all communications is over secure channels. (It may be required that the mobile wallet application be opened prior to beginning a phone online purchase.) The POS midlet **412** is a component of the mobile wallet application that executes PayPass or other payment authorization protocol between itself and the SE payment applications on the mobile communication device **402** (interaction (4)). The results of the request are sent back to the POS vendor plugin.

As shown by interaction (5), the POS midlet **412** then forwards the properly formatted authorization request to a payment entity (e.g., issuer authorization **418**) for authorization. The results of the request are then sent back to the POS component of the mobile wallet. Through interaction (6), the POS midlet **412** then forwards the results back to the MCD POS plugin **414** to complete the purchase. The MCD POS plugin **414** then forwards the purchase transaction information to the management server **408** for later customer viewing (interaction (7)). As indicated by interaction (8), users (or customers) will then be able to query the management server **408** and immediately obtain purchase information, either by phone or PC.

One or more of method steps described above can be performed by one or more programmable processors executing a computer program to perform functions by operating on input data and generating output. Generally, the invention can take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment containing both hardware and software elements. In one implementation, the invention is implemented in software, which includes but is not limited to firmware, resident software, microcode, etc. Furthermore, the invention can take the form of a computer program product accessible from a computer-usable or computer-readable medium providing program code for use by or in connection with a computer or any instruction execution system. For the purposes of this description, a computer-usable or computer readable medium can be any apparatus that can contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device. The medium can be an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device) or a propagation medium. Examples

US 10,825,007 B2

7

of a computer-readable medium include a semiconductor or solid state memory, magnetic tape, a removable computer diskette, a random access memory (RAM), a read-only memory (ROM), a rigid magnetic disk and an optical disk. Current examples of optical disks include compact disk read only memory (CD-ROM), compact disk read/write (CD-R/W) and DVD.

FIG. 5 illustrates a data processing system 500 suitable for storing and/or executing program code. Data processing system 500 includes a processor 502 coupled to memory elements 504A-B through a system bus 506. In other implementations, data processing system 500 may include more than one processor and each processor may be coupled directly or indirectly to one or more memory elements through a system bus. Memory elements 504A-B can include local memory employed during actual execution of the program code, bulk storage, and cache memories that provide temporary storage of at least some program code in order to reduce the number of times the code must be retrieved from bulk storage during execution. As shown, input/output or I/O devices 508A-B (including, but not limited to, keyboards, displays, pointing devices, etc.) are coupled to data processing system 500. I/O devices 508A-B may be coupled to data processing system 500 directly or indirectly through intervening I/O controllers (not shown).

In one implementation, a network adapter 510 is coupled to data processing system 500 to enable data processing system 500 to become coupled to other data processing systems or remote printers or storage devices through communication link 512. Communication link 512 can be a private or public network. Modems, cable modems, and Ethernet cards are just a few of the currently available types of network adapters.

Although the present invention has been particularly described with reference to implementations discussed above, various changes, modifications and substitutes are can be made. Accordingly, it will be appreciated that in numerous instances some features of the invention can be employed without a corresponding use of other features. Further, variations can be made in the number and arrangement of components illustrated in the figures discussed above.

What is claimed is:

1. A method for processing a transaction, comprising:

receiving, at a transaction server, a payment method that corresponds to an identification code associated with a user from a remote management server, wherein

prior to receiving the payment method that corresponds to the identification code associated with the user from the remote management server, the remote management server

sends a list of products to a non-browser based application generated screen generated by a non-browser based application with a graphical user interface that is downloaded and installed on a mobile device for display with a mobile device display of the mobile device, wherein the non-browser based application only generates a non-browser based application generated screen, the non-browser based application generated screen corresponding to a specific screen or area of the non-browser based application, the mobile device including the mobile device display, a mobile device processor, a mobile device wireless radio transceiver configured to support voice and data interactions through a first wireless communication channel, and a mobile device wireless fidelity (Wi-Fi) transceiver,

8

receives, at the non-browser based application generated screen, an identification of one or more products selected from the list of products from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the identification of the one or more products selected from the list of products through user input via the mobile device display;

receives a transaction purchase request from a user from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the transaction purchase request via the mobile device display of the mobile device

receives user input login information including an identification code associated with the user from the non-browser based application generated screen, wherein the non-browser based application generated screen stored on the mobile device receives the user input login information via a mobile device display of the mobile device;

upon receipt of the user input login information, authenticating, at the remote management server, the user associated with the user input login information; and

transmits the payment method that corresponds to the identification code associated with the user to the transaction server;

processing, at the transaction server, the transaction using the payment method; and

sending, from the transaction server, a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed and further wherein after receiving the transaction verification, the remote management server downloads the one or more products to the mobile device.

2. A transaction server for processing a transaction, comprising:

a transaction server interface configured to:

receive a payment method that corresponds to an identification code associated with a user from a remote management server, wherein

prior to receiving the payment method that corresponds to the identification code associated with the user from the remote management server, the remote management server

sends a list of products to a non-browser based application generated screen generated by a non-browser based application with a graphical user interface that is downloaded and installed on a mobile device for display with a mobile device display of the mobile device, wherein the non-browser based application only generates a non-browser based application generated screen, the non-browser based application generated screen corresponding to a specific screen or area of the non-browser based application, the mobile device including the mobile device display, a mobile device processor, a mobile device wireless radio transceiver configured to support voice and data interactions through a first wireless communication channel, and a mobile device wireless fidelity (Wi-Fi) transceiver;

receives, at the non-browser based application generated screen, an identification of one or more products selected from the list of products from the non-browser based application generated screen, wherein the non-browser based application generated screen receives

US 10,825,007 B2

9

the identification of the one or more products selected from the list of products through user input via the mobile device display;

receives a transaction purchase request including information relating to the identification of the one or more products from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the transaction purchase request from the user via the mobile device display of the mobile device;

receives user input login information including an identification code associated with a user from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the user input login information via a mobile device display of the mobile device;

upon receipt of the user input login information, authenticating, at the remote management server, a user associated with the user input login information;

transmits the payment method that corresponds to the identification code associated with the user to the transaction server; and

send a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed and further wherein after receiving the transaction verification, the remote management server downloads the one or more products to the mobile device;

a transaction server processor that processes the transaction using the payment method.

3. A non-transitory computer readable medium for processing a transaction, comprising:

computer code for receiving, at a transaction server, a payment method that corresponds to an identification code associated with a user from a remote management server from a remote management server, wherein prior to receiving the payment method that corresponds to the identification code associated with the user from the remote management server, the remote management server

sends a list of products to a non-browser based application generated screen generated by a non-browser based application with a graphical user interface that is downloaded and installed on a mobile device for display with a mobile device display of the mobile device, wherein the non-browser based application only generates a non-browser based application generated screen, the non-browser based application generated screen corresponding to a specific screen or area of the non-browser based application, the mobile device including the mobile device display, a mobile device processor, a mobile device wireless radio transceiver configured to support voice and data interactions through a first wireless communication channel, and a mobile device wireless fidelity (Wi-Fi) transceiver;

receives, at the non-browser based application generated screen, an identification of one or more products selected from the list of products from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the identification of the one or more products selected from the list of products through user input via the mobile device display;

receives a transaction purchase request including information relating to the identification of the one or more products from the non-browser based applica-

10

tion generated screen, wherein the non-browser based application generated screen receives the transaction purchase request from a the user via the mobile device display of the mobile device;

receives user input login information including an identification code associated with the user from the non-browser based application generated screen, wherein the non-browser based application generated screen stored on the mobile device receives the user input login information via a mobile device display of the mobile device;

upon receipt of the user input login information, authenticating, at the remote management server, a user associated with the user input login information; and

transmits the payment method that corresponds to the identification code associated with the user to the transaction server;

computer code for processing, at the transaction server, the transaction using the payment method; and

computer code for sending, from the transaction server, a transaction verification to the remote management server, wherein the transaction verification indicates that the transaction has processed and further wherein after receiving the transaction verification, the remote management server downloads the one or more products to the mobile device.

4. The method of claim 1, wherein the payment method is a default payment method.

5. The method of claim 1, wherein the payment method is a user selected payment method.

6. The transaction server of claim 2, where the payment method includes credit card information.

7. The transaction server of claim 2, wherein the payment method is a default payment method.

8. The transaction server of claim 2, wherein the payment method is a user selected payment method.

9. The transaction server of claim 2, where the payment method includes credit card information.

10. The method of claim 1, further wherein the non-browser based application can be used when the mobile device is not connected to a wireless network.

11. The method of claim 10, further wherein the non-browser based application monitors for access to the wireless network and automatically reconnects to the wireless network when the wireless network is available.

12. The method of claim 1, further wherein no sensitive data is stored on the mobile device.

13. The method of claim 12, wherein the sensitive data comprises at least one of information related to the payment method, information related to the user input login information, information related to identification information, and information related to an expiration dates associated with the payment method.

14. The transaction server of claim 2, further wherein the non-browser based application can be used when the mobile device is not connected to a wireless network.

15. The transaction server of claim 14, further wherein the non-browser based application monitors for access to the wireless network and automatically reconnects to the wireless network when the wireless network is available.

16. The transaction server of claim 2, further wherein no sensitive data is stored on the mobile device.

17. The transaction server of claim 16, wherein the sensitive data comprises at least one of information related to the payment method information related to the user input login information, information related to identification infor-

US 10,825,007 B2

11

mation, and information related to an expiration dates associated with the payment method.

18. The method of claim 1, further wherein after the transaction has processed, the remote management server sends a digital artifact to the mobile device.

19. The method of claim 18, further wherein the digital artifact is cached on the mobile device and accessible by the non-browser based application when there is no network connection.

20. The method of claim 18, further wherein the, non-browser based application generates an alert if it has not received the digital artifact from the remote management server within a certain period of time.

21. The method of claim 18, wherein the remote management server sends the digital artifact to the non-browser based application generated screen based on the geographical location of the mobile device.

22. The method of claim 1, further wherein the non-browser based application generated screen receives input to zoom into an image associated with a product to be purchased which results in an updated image of the product to be purchased being displayed, wherein the non-browser based application receives the input to zoom into the image associated with the product to be purchased via the mobile device display of the mobile device.

23. The method of claim 1, further wherein the graphical user interface enables the interaction between the non-browser based application and the mobile device through a graphical icon, wherein the non-browser based application receives the interaction via the mobile device display of the mobile device.

24. The method of claim 18, further wherein the non-browser based application is configured to use a structured format and further wherein the structured format means the non-browser based application can store and display a digital artifact in an organized and easily retrievable fashion.

25. The transaction server of claim 2, further wherein after the transaction has processed, the remote management server sends a digital artifact to the mobile device.

26. The transaction server of claim 25, further wherein the digital artifact is cached on the mobile device and accessible by the non-browser based application when there is no network connection.

12

27. The transaction server of claim 25, further wherein the, non-browser based application generates an alert if it has not received the digital artifact from the remote management server within a certain period of time.

28. The transaction server of claim 25, wherein the remote management server sends the digital artifact to the non-browser based application generated screen based on the geographical location of the mobile device.

29. The transaction server of claim 2, further wherein the non-browser based application generated screen receives input to zoom into an image associated with a product to be purchased which results in an updated image of the product to be purchased being displayed, wherein the non-browser based application receives the input to zoom into the image associated with the product to be purchased via the mobile device display of the mobile device.

30. The transaction server of claim 2, further wherein the graphical user interface enables the interaction between the non-browser based application and the mobile device through a graphical icon, wherein the non-browser based application receives the interaction via the mobile device display of the mobile device.

31. The transaction server of claim 25, further wherein the non-browser based application is configured to use a structured format and further wherein the structured format means the non-browser based application can store and display a digital artifact in an organized and easily retrievable fashion.

32. The method of claim 18, wherein the digital artifact is media, content, ticket, a receipt, advertisement or coupon.

33. The method of claim 32, wherein the advertisement or coupon is based on one or more targeting parameters.

34. The method of claim 33, wherein the one or more targeting parameters comprise personal information and transaction related information.

35. The transaction server of claim 25, wherein the digital artifact is media, content, ticket, a receipt, an advertisement or coupon.

36. The transaction server of claim 35, wherein the advertisement or coupon is based on one or more targeting parameters.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 10,825,007 B2
APPLICATION NO. : 14/253648
DATED : November 3, 2020
INVENTOR(S) : Michele Fisher

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

Claim 1 in Column 8, Line 1-4 should read:

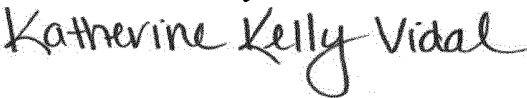
“receives, from the non-browser based application generated screen, an identification of one or more products selected from the list of products, wherein the non-browser based application generated screen receives the identification of the one or more products selected from the list of products through user input via the mobile device display;”

Claim 2 in Column 8, Line 63-66 should read:

“receives, from the non-browser based application generated screen, an identification of one or more products selected from the list of products, wherein the non-browser based application generated screen receives the identification of the one or more products selected from the list of products through user input via the mobile device display;”

Claim 3 in Column 9, Line 57-60 should read:

“receives, from the non-browser based application generated screen, an identification of one or more products selected from the list of products, wherein the non-browser based application generated screen receives the identification of the one or more products selected from the list of products through user input via the mobile device display;”

Signed and Sealed this
Thirteenth Day of June, 2023

Katherine Kelly Vidal
Director of the United States Patent and Trademark Office

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 10,825,007 B2
APPLICATION NO. : 14/253648
DATED : November 3, 2020
INVENTOR(S) : Michelle Fisher

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

Claim 1 should be amended which is in Column 8, Lines 15-16 as shown below:

“receives user input login information including the identification code associated with the user from the non-browser based application generated screen, wherein the non-browser based application generated screen stored on the mobile device receives the user input login information via a mobile device display of the mobile device;”

Claim 2 should be amended which is in Column 9, Lines 10-11 as shown below:

“receives user input login information including the identification code associated with a user from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the user input login information via a mobile device display of the mobile device;”

Claim 3 should be amended which is in Column 10, Lines 5-6 as shown below:

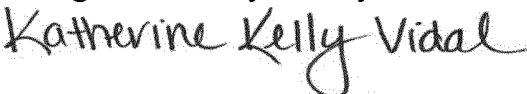
“receives user input login information including the identification code associated with the user from the non-browser based application generated screen, wherein the non-browser based application generated screen stored on the mobile device receives the user input login information via a mobile device display of the mobile device;”

Claim 6 should be amended which is in Column 10, Lines 32-33 as shown below:

“The method of claim 1, wherein the payment method includes credit card information.”

Claim 9 should be amended which is in Column 10, Lines 38-39 as shown below:

“The transaction server of claim 2, wherein the payment method includes credit card information.”

Signed and Sealed this
Eighteenth Day of July, 2023


Katherine Kelly Vidal
Director of the United States Patent and Trademark Office

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 10,825,007 B2
APPLICATION NO. : 14/253648
DATED : November 3, 2020
INVENTOR(S) : Michelle Fisher

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

Claim 1 should be amended which is in Column 8, Line 9-14 as shown below:

“receives a transaction purchase request including information relating to the identification of the one or more products from a user from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the transaction purchase request via the mobile device display of the mobile device;”

Signed and Sealed this
Fourteenth Day of November, 2023



Katherine Kelly Vidal
Director of the United States Patent and Trademark Office

Certificate of Compliance

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B) or Federal Rule of Appellate Procedure 28.1(e).
 - ✓ The brief contains 13,805 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure, or
 - ☐ The brief uses a monospaced typeface and contains N/A lines of text, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).
2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) or Federal Rule of Appellate Procedure 28.1(e) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6).
 - ✓ The brief has been prepared in a proportionally spaced typeface using **Microsoft® Word for Windows in 14-point Times New Roman**, or
 - ☐ The brief has been prepared in a monospaced typeface using N/A with N/A.

/s/ Gregory J. Gonsalves
Dr. Gregory J. Gonsalves

Counsel for Appellant
Blaze Mobile, Inc.

April 30, 2025

Certificate of Service

I hereby certify that on this 30th day of April, 2025, I electronically filed the foregoing document with the Clerk of the United States Court of Appeals for the Federal Circuit using the CM/ECF System, which will send notice of such filing to all registered CM/ECF users.

Dated: May 5, 2025.

/s/ Gregory J. Gonsalves
Dr. Gregory J. Gonsalves

Law Firm:	Law Office of Dr. Gregory J. Gonsalves
Address:	2216 Beacon Lane
City, State, ZIP:	Falls Church, VA 22043
Telephone:	571.419.7252
E-mail Address:	gregoryjosephgonsalves@gmail.com