CT Corporation

Service of Process Transmittal

03/25/2022
CT Log Number 541294229

TO: Dawne Petersen
PayPal, Inc.
7700 Eastport Pkwy
La Vista, NE 68128-4397

RE: **Process Served in Texas**

FOR: PayPal Holdings, Inc. (Domestic State: DE)

ENCLOSED ARE COPIES OF LEGAL PROCESS RECEIVED BY THE STATUTORY AGENT OF THE ABOVE COMPANY AS FOLLOWS:

TITLE OF ACTION:	FINTIV, INC. vs. PAYPAL HOLDINGS, INC.
DOCUMENT(S) SERVED:	Summons, Complaint, Cover Sheet, Attachment(s)
COURT/AGENCY:	Western District of Texas - United States District Court - Waco Division, TX Case # 622CV00288
NATURE OF ACTION:	Intellectual Property Litigation - Patent infringement
ON WHOM PROCESS WAS SERVED:	C T Corporation System, Dallas, TX
DATE AND HOUR OF SERVICE:	By Certified Mail on 03/25/2022 postmarked on 03/22/2022
JURISDICTION SERVED :	Texas
APPEARANCE OR ANSWER DUE:	Within 21 days after service (not continuing the day of receipt)
ATTORNEY(S) / SENDER(S):	Raymond W Mort III The Mort Law Firm, PLLC 100 Congress Ave, Suite 2000 Austin, TX 78701 512-865-7950
ACTION ITEMS:	CT has retained the current log, Retain Date: 03/25/2022, Expected Purge Date: 03/30/2022 Image SOP Email Notification, PayPal SOP Litigation Team CTCorpservice@paypal.com
REGISTERED AGENT ADDRESS:	C T Corporation System 1999 Bryan Street Suite 900 Dallas, TX 75201 877-564-7529 MajorAccountTeam2@wolterskluwer.com

The information contained in this Transmittal is provided by CT for quick reference only. It does not constitute a legal opinion, and should not otherwise be relied on, as to the nature of action, the amount of damages, the answer date, or any other information contained in the included documents. The recipient(s) of this form is responsible for reviewing and interpreting the included documents and taking appropriate action, including consulting with its legal and other advisors as necessary. CT disclaims all liability for the information contained in this form, including for any omissions or inaccuracies that may be contained therein.

The Mort Law Firm, PLLC
100 CONGRESS AVE STE 2000
AUSTIN TX 78701-2745

USPS CERTIFIED MAIL

9402 6118 9876 5841 2160 66

PayPal Holdings, Inc.
c/o CT Corporation System
1999 BRYAN ST STE 900
DALLAS TX 75201-3140

US POSTAGE AND FEES PAID
PRIORITY MAIL
Mar 22 2022
Mailed from ZIP 78701
1 lb PM Zone 3

11923275
CommercialBasePrice

stamps endicia

062S0012913542

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS

FINTIV, INC.,
Plaintiff

V. Civil Action No. **6:22-CV-00288**

PAYPAL HOLDINGS, INC.,
Defendant

SUMMONS IN A CIVIL ACTION

TO: **PayPal Holdings, Inc.**
c/o C T Corporation System
1999 Bryan St, STE 900
Dallas, TX 75201

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) -- or 60 days if you are the United States or a United States Agency, or an office or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) -- you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Raymond W Mort III
The Mort Law Firm, PLLC
100 Congress Ave, Suite 2000
Austin, TX 78701

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

JEANNETTE J. CLACK
CLERK OF COURT

s/LEIGH ANNE DIAZ
DEPUTY CLERK

ISSUED ON 2022-03-17 14:13:41

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

FINTIV, INC.,	§	
	§	**Civil Action No.: 6:22-cv-00288**
Plaintiff,	§	
	§	
v.	§	**JURY TRIAL DEMANDED**
	§	
PAYPAL HOLDINGS, INC.	§	
	§	
Defendant.	§	

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Fintiv, Inc. ("Fintiv"), by and through its attorneys, for its Original Complaint for Patent Infringement against Defendant PayPal Holdings, Inc. ("PayPal"), hereby alleges the following:

I. NATURE OF THE ACTION

1. PayPal, a $112 billion company, for years has been unlawfully using property owned by Fintiv — mobile wallet patents invented by Fintiv, a small technology company — and making enormous profits from its use of those extremely valuable patents. PayPal has not only been knowingly and unlawfully using Fintiv's patents without Fintiv's permission, but it has flatly refused to pay Fintiv for its use of those patents. Accordingly, Fintiv brings this patent infringement action to put an end to PayPal's unauthorized and infringing use of Fintiv's patented inventions and to recover the damages Fintiv has suffered as a result of PayPal's egregious misconduct.

2. Fintiv is the owner of all rights, titles, and interests in and to United States Patent Nos. 8,538,845 ("the '845 Patent"), 9,892,386 (the "'386 Patent"), and 11,120,413 ("the '413 Patent"), 9,208,488 (the "'488 Patent"), and the 10,438,196 (the "'196 Patent") (collectively the

"Patents-in-Suit"). The '845 Patent, '386 Patent, and '413 Patent are titled "Monetary Transaction System." The '488 Patent and '196 Patent are titled "Using a Mobile Warrant Infrastructure to Support Multiple Mobile Wallet Providers." True and correct copies of the Patents-in-Suit are attached hereto as Exhibits.

3. PayPal makes, provides, sells, offers for sale, uses, and/or distributes products and services which directly infringe the Patents-in-Suit. Further, PayPal indirectly infringes the Patents-in-Suit by inducing and/or contributing to infringement by others, including PayPal users.

4. Fintiv seeks monetary damages, injunctive relief, and pre- and post–judgment interest for PayPal's past and continuing infringement of the Patents-in-Suit.

II. PARTIES

5. Plaintiff Fintiv, Inc. is a Delaware corporation having a principal place of business at 801 Barton Springs, Austin, Texas 78704.

6. Fintiv is a financial technology company that provides mobile commerce, payment solutions, and digital currency globally.

7. Fintiv's cloud-based technology delivers payments, mobile loyalty solutions, and digital currency to companies in retail, financial services, consumer packaged goods, and telecom that serve both banked and unbanked consumers worldwide via the mobile phone. Fintiv also offers mobile wallet solutions that are capable of a variety of transactions, including mobile payments, digital currency, money transfer, remittance, bill payment, point-of-sale integration, loyalty rewards, and cloud payments.

8. Fintiv, through its wholly-owned operating subsidiary, Cloud Payments LLC ("Cloud Payments"), processes merchant and consumer payments and loyalty. Cloud Payments uses sophisticated and proprietary technologies and techniques to optimize online, point of sale,

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 5 of 381

and mobile payments. Cloud Payments' optimized payment processing service delivers a lower cost and higher value, offers a suite of digital engagement tools enabling marketing automation using payment data, and employs data monetization to generate net-new revenue for customers. It is available through app store through the app titled "Fundz."

9. Defendant PayPal Holdings, Inc. is a corporation organized and existing under the laws of Delaware and has a regular and established place of business at 7700 W Palmer Lane, Building D, Austin, Texas 78729 (the "Austin Office"). Upon information and belief, Defendant has over 150 employees at this location, including engineers, developers, and business analysts. PayPal consistently advertises jobs for its Austin Office, and hosts meetings at the Austin Office. For example, PayPal currently is advertising numerous technical and business roles involving the technology disclosed in the asserted Patents, including specifically positions related to mobile wallets, mobile payments including engineering, software development, marketing, sales, and related positions.

- https://jobsearch.paypal-corp.com/en-US/job/branded-experiences-quality-engineer/J3Q3006WVSS8T769XVH
- https://jobsearch.paypal-corp.com/en-US/job/branded-experiences-backend-engineer/J3M69M66890YLKYXGX5
- https://jobsearch.paypal-corp.com/en-US/job/branded-experiences-ios-engineer/J3V4TJ6S2WF7LFMYC7K
- https://jobsearch.paypal-corp.com/en-US/job/staff-software-engineer/J3T1Q16N10753B123TQ
- https://jobsearch.paypal-corp.com/en-US/job/director-payment-optimization-bd/J3V6DN5WBDG4TZG898Z

- https://jobsearch.paypal-corp.com/en-US/job/str-product-insights-market-research/J3R8F366SP695212H44
- https://jobsearch.paypal-corp.com/en-US/job/mobile-software-engineer-android/J3W2M8757N3NRY06Z67
- https://jobsearch.paypal-corp.com/en-US/job/sr-sales-engineer/J3P8635X03KDV1WFH32

10. PayPal is a financial technology company that operates an online payments system, serves as an electronic alternative to traditional paper methods such as checks and money orders, and processes payments.

III. JURISDICTION AND VENUE

11. This is an action for patent infringement, which arises under the Patent Laws of the United States, in particular, 35 U.S.C. §§ 271, 281, 282, 284, and 285. The Court has jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331 and 1338(a).

12. This Court has personal jurisdiction over Defendant because it has committed acts giving rise to this action within Texas and within this judicial district. Defendant also regularly does business or solicits business in this District and in Texas, engages in other persistent courses of conduct and derives substantial revenue from products and/or services provided in this District and in Texas, and has purposefully established substantial, systematic, and continuous contacts within this District and should reasonably expect to be sued in a court in this District. For example, Defendant has offices and employees in this District, including the Austin Office, and has a Texas registered agent for service. Given these contacts, the Court's exercise of jurisdiction over Defendant will not offend traditional notions of fair play and substantial justice.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 7 of 381

13. Venue in the Western District of Texas is proper pursuant to 28 U.S.C. §§ 1391(b), (c) and 1400(b) because Defendant has an established place of business in this District at 7700 W Palmer Lane, Building D, Austin, Texas 78729, has committed acts within this judicial district giving rise to this action, and continues to conduct business in this judicial district, including one or more acts of making, selling, using, importing and/or offering for sale infringing products and services to Defendant's customers in this District.

IV. THE PATENTS-IN-SUIT

The '845 Patent

14. The '845 Patent is titled "Monetary Transaction System." The provisional applications of the '845 Patent were filed on June 3, 2011 and August 10, 2011. The non-provisional application of the '845 Patent was filed on May 30, 2012. The '845 Patent issued on September 17, 2013. A true and correct copy of the '845 Patent is attached hereto as **Exhibit A** and incorporated herein by reference.

15. The '845 Patent is fully described and explained in the attached Exemplary '845 Patent Infringement Chart. A true and correct copy of the Exemplary '845 Patent Infringement Chart is attached hereto as **Exhibit B**.

16. Fintiv owns all substantial and material rights to and interests in the '845 Patent, including the right to recover damages for all past and future infringement thereof.

17. The '845 Patent is valid and enforceable.

The '386 Patent

18. The '386 Patent is titled "Monetary Transaction System." The non-provisional application of the '386 Patent was filed on July 1, 2016, which is a continuation of provisional applications filed on June 3, 2011 and August 10, 2011, and claims priority to the same. The '386

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 8 of 381

Patent issued on February 13, 2018. A true and correct copy of the '386 Patent is attached hereto as **Exhibit C** and incorporated herein by reference.

19. The '386 Patent is fully described and explained in the attached Exemplary '386 Patent Infringement Chart. A true and correct copy of the Exemplary '386 Patent Infringement Chart is attached hereto as **Exhibit D**.

20. Fintiv owns all substantial and material rights to and interests in the '386 Patent, including the right to recover damages for all past and future infringement thereof.

21. The '386 Patent is valid and enforceable.

The '413 Patent

22. The '413 Patent is titled "Monetary Transaction System." The non-provisional application of the '413 Patent was filed on September 12, 2019, which is a continuation of provisional applications filed on June 3, 2011 and August 10, 2011, and claims priority to the same. The '413 Patent issued on September 14, 2021. A true and correct copy of the '413 Patent is attached hereto as **Exhibit E** and incorporated herein by reference.

23. The '413 Patent is fully described and explained in the attached Exemplary '413 Patent Infringement Chart. A true and correct copy of the Exemplary '413 Patent Infringement Chart is attached hereto as **Exhibit F**.

24. Fintiv owns all substantial and material rights to and interests in the '413 Patent, including the right to recover damages for all past and future infringement thereof.

25. The '413 Patent is valid and enforceable.

The '488 Patent

26. The '488 Patent is titled "Using a Mobile Wallet Infrastructure to Support Multiple Mobile Wallet Providers." The non-provisional application of the '488 Patent was filed on

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 9 of 381

November 19, 2012, which is a continuation of provisional applications filed on November 21, 2011 and claims priority to the same. The '488 Patent was issued on December 8, 2015. A true and correct copy of the '488 Patent is attached hereto as **Exhibit G** and incorporated herein by reference.

27. The '488 Patent is fully described and explained in the attached Exemplary '488 Patent Infringement Chart. A true and correct copy of the Exemplary '488 Patent Infringement Chart is attached hereto as **Exhibit H**.

28. Fintiv owns all substantial and material rights to and interests in the '488 Patent, including the right to recover damages for all past and future infringement thereof.

29. The '488 Patent is valid and enforceable.

The '196 Patent

30. The '196 Patent is titled "Using a Mobile Wallet Infrastructure to Support Multiple Mobile Wallet Providers." The non-provisional application of the '196 Patent was filed on October 30, 2015, which is a continuation of provisional applications filed on November 21, 2011 and claims priority to the same. The '196 Patent was issued on October 8, 2019. A true and correct copy of the '196 Patent is attached hereto as **Exhibit I** and incorporated herein by reference.

31. The '196 Patent is fully described and explained in the attached Exemplary '196 Patent Infringement Chart. A true and correct copy of the Exemplary '196 Patent Infringement Chart is attached hereto as **Exhibit J**.

32. Fintiv owns all substantial and material rights to and interests in the '196 Patent, including the right to recover damages for all past and future infringement thereof.

33. The '196 Patent is valid and enforceable.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 10 of 381

V. PAYPAL'S PRE-SUIT KNOWLEDGE OF FINTIV AND THE PATENTS-IN-SUIT

34. Prior to filing this complaint, Fintiv informed Defendant that it was using the Patents-in-Suit, offered to license its patents, including the Patents-in-Suit, to Defendant, and shared detailed information about its patents, including the Patents-in-Suit, with Defendant. Accordingly, Defendant had knowledge of Fintiv and the Patents-in-Suit prior to the filing of this complaint.

35. On or about March 15, 2016, the Global Strategic Partner of Business Development for PayPal at the time ("PayPal's Agent") emailed Fintiv requesting contact info or a teleconference with one of the founders of Fintiv (the "Fintiv's Founder"). PayPal's Agent held numerous roles at PayPal from August 2011 to November 2020, when he left to serve as Head of North America New Channel Sales at PayPal for Hyperwallet (where he remains today).

36. On or about March 16, 2016, Fintiv's Founder and PayPal's Agent had a phone call that lasted over an hour to discuss Fintiv's patented technology, a strategic partnership between the two companies, and PayPal's interest in acquiring Fintiv. On this call Fintiv, discussed the '845 and '488 Patents extensively.

37. In addition, during the call, PayPal asked about acquiring Fintiv. PayPal's Agent asked Fintiv's Founder if he and the management team would be available for a meeting with PayPal's Senior Vice President, Head of Corporate Development (M&A) ("PayPal's SVP") at the time. PayPal's Agent said that the meeting could be held within ten days at Fintiv headquarters in Austin. PayPal's Agent informed Fintiv's Founder that PayPal's SVP traveled regularly to PayPal's Austin offices. The meeting in Austin did not end up taking place.

38. On or about June 13, 2019, the Chairman of Advection Growth Capital LLC ("Advection"), acting on behalf of Fintiv, sent an email to PayPal's Director of Global Corporate Development ("PayPal's Director") specifically identifying the '845, '386, and '488 Patents and

explaining how these patents could be of benefit to Defendant under a section titled "PayPal Engagement Notes." PayPal's Director has been employed at PayPal since May 2015, and currently serves as PayPal's Senior Director of Global Corporate Development. This email also attached a 15-page PowerPoint presentation created by Fintiv that specifically discussed the '845, '386, and '488 Patents and the technology claimed by them to further illustrate the benefits of those patents to Defendant, and described Fintiv's lines of business, including Cloud Payments' payment processing and interchange optimization.

39. On or about August 1, 2019, Fintiv's President, one of Fintiv's directors ("Fintiv's Director"), and Advection, had a call with PayPal's Director, to further explore Defendant's licensing of the Patents-in-Suit due to their continued infringement of the patents.

40. On or about August 8, 2019, Fintiv's President, Fintiv's Director, and Advection met with Defendant at PayPal's headquarters in San Jose. PayPal's Director and its Investor of PayPal Ventures ("PayPal's Investor"), attended this one-hour meeting, during which Fintiv shared further details regarding the Patents-in-Suit for the purpose of entering into a license deal with Defendant. Fintiv further told PayPal's representatives of about the applications, amendments, and portfolio of an additional 80 pending patents it had and noted that PayPal would be infringing on said patents in addition to the issued patents they were already infringing upon. The Parties also talked about PayPal's continued interested in acquiring Fintiv.

41. After delaying over the course of a year, Defendant decided not to license the Patents-in-Suit or acquire Fintiv.

42. However, Defendant has continued to make, provide, sell, offer for sale, use, and/or distribute products and services which directly infringe the Patents-in-Suit. Further, Defendant has

continued to indirectly infringe the Patents-in-Suit by inducing and/or contributing to the infringement by others, including PayPal users and partners.

COUNT I: DIRECT INFRINGEMENT OF THE '845 PATENT

43. Fintiv incorporates paragraphs 1 through 42 herein by reference.

44. Defendant, without authorization or license from Fintiv, has been and is presently directly infringing, literally or under the doctrine of equivalents, at least claim 5 of the '845 Patent ("Exemplary '845 Patent Claims"), as infringement is defined by 35 U.S.C. § 271(a), including through making, using (including for testing purposes), selling, offering for sale, and/or distributing infringing products. Exemplary infringing products include at least PayPal's servers and Backend System that interacts with mobile devices (collectively, "Exemplary PayPal Products").

45. **Exhibit B** attached hereto includes charts comparing the Exemplary '845 Patent Claims to the Exemplary PayPal Products. As set forth in these charts, the Exemplary PayPal Products practice the technology claimed by the '845 Patent. Accordingly, the Exemplary PayPal Products incorporated in these charts satisfy all elements of the Exemplary '845 Patent Claims literally or under the doctrine of equivalents.

46. Defendant's acts of infringement have caused damage to Fintiv. Fintiv is entitled to recover damages in an amount to be determined at trial. Further, Defendant's infringement of Fintiv's rights under the '845 Patent will continue to damage Fintiv's business, causing irreparable harm for which there is no adequate remedy at law, unless enjoined by the Court.

47. Defendant is and has been aware of the '845 Patent since at least March 2016, well before this Complaint. Consequently, Defendant's infringement of the '845 Patent is willful and deliberate, entitling Fintiv to enhanced damages pursuant to 35 U.S.C. § 284.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 13 of 381

COUNT II: INDIRECT INFRINGEMENT OF THE '845 PATENT

48. Fintiv incorporates paragraphs 1 through 47 herein by reference.

49. As described above, Defendant is and has been aware of the '845 Patent since at least August 2016. And since that time, despite actual knowledge of the '845 Patent, Defendant has been and continues to indirectly infringe the '845 Patent.

50. Defendant has been indirectly infringing, and continues to indirectly infringe, at least claim 5 of the '845 Patent through its partners', merchants', customers', and end-users' direct infringement of at least claim 5 of the '845 Patent, through at least the use of the Exemplary PayPal Products without authorization of license from Fintiv.

51. Defendant is contributing to the infringement by others and/or inducing infringement by others by, among other things, providing instructions to its partners, merchants, customers, and end-users on how to download and use the PayPal application, including through its website www.PayPal.com and through instructions on third-party application providers, in a manner that infringes the Exemplary '845 Patent Claims.

52. Defendant has also contributed and/or induced, and continues to contribute and/or induce the infringement of at least claim 5 of the '845 Patent by contributing to and/or inducing its partners, merchants, customers, and end-users to use its products, such as Exemplary PayPal Products, in an infringing manner as described above, including encouraging and instructing its partners, merchants, customers, and end-users through software and documentation provided by Defendant.

53. For example, Defendant's website www.PayPal.com and its mobile application specifically instruct users how to use the PayPal front and backend systems in a manner that

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 14 of 381

infringes the patents. Moreover, third party application stores such as the Google Play store and the Apple App store provides instructions and information for end-users. On information and belief, this information is supplied by PayPal. In addition, PayPal provides instructions on its the PayPal mobile application that instructs users to interact with the PayPal front and backend systems in a manner that infringes the Patents.

54. Defendant has known that its infringing products, such as the Exemplary PayPal Products, cannot be used without infringing the technology claimed in the '845 Patent, as described in **Exhibit B**, and are not staple articles of commerce suitable for substantial non-infringing uses.

55. Fintiv has been damaged by Defendant's infringement of the '845 Patent and will continue to be damaged by such infringement. Fintiv is entitled to recover damages from Defendant to compensate it for Defendant's infringement, as alleged above, in an amount measured by no less than a reasonable royalty under 35 U.S.C. § 284, as well as enhanced damages pursuant to 35 U.S.C. § 284.

COUNT III: DIRECT INFRINGEMENT OF THE '386 PATENT

56. Fintiv incorporates paragraphs 1 through 55 herein by reference.

57. Defendant, without authorization or license from Fintiv, has been and is presently directly infringing, literally or under the doctrine of equivalents, at least claim 1 of the '386 Patent ("Exemplary '386 Patent Claims"), as infringement is defined by 35 U.S.C. § 271(a), including through making, using (including for testing purposes), selling, offering for sale, and/or distributing infringing products. Exemplary infringing products include at least PayPal's servers and Backend System that interacts with mobile devices (collectively, "Exemplary PayPal Products").

58. **Exhibit D** attached hereto includes charts comparing the Exemplary '386 Patent Claims to the Exemplary PayPal Products. As set forth in these charts, the Exemplary PayPal

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 15 of 381

Products practice the technology claimed by the '386 Patent. Accordingly, the Exemplary PayPal Products incorporated in these charts satisfy all elements of the Exemplary '386 Patent Claims literally or by the doctrine of equivalents.

59. Defendant's acts of infringement have caused damage to Fintiv. Fintiv is entitled to recover damages in an amount to be determined at trial. Further, Defendant's infringement of Fintiv's rights under the '386 Patent will continue to damage Fintiv's business, causing irreparable harm for which there is no adequate remedy at law, unless enjoined by the Court.

60. Defendant is and has been aware of the '386 Patent since at least August 2019, well before this Complaint. Consequently, Defendant's infringement of the '386 Patent is willful and deliberate, entitling Fintiv to enhanced damages pursuant to 35 U.S.C. § 284.

COUNT IV: INDIRECT INFRINGEMENT OF THE '386 PATENT

61. Fintiv incorporates paragraphs 1 through 60 herein by reference.

62. As described above, Defendant is and has been aware of the '386 Patent since at least August 2019. And since that time, despite actual knowledge of the '386 Patent, has been and continues to indirectly infringe the '386 Patent.

63. Defendant has been indirectly infringing, and continues to indirectly infringe, at least claim 1 of the '386 Patent through its partners', merchants', customers', and end-users' direct infringement of at least claim 1 of the '386 Patent, through at least the use of the Exemplary PayPal Products without authorization of license from Fintiv.

64. Defendant is contributing to the infringement by others and/or inducing infringement by others by, among other things, providing instructions to its partners, merchants, customers, and end-users on how to download and use the PayPal application, including through

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 16 of 381

its website www.PayPal.com and through instructions on third-party application providers, in a manner that infringes Exemplary '386 Patent Claims.

65. Defendant has also contributed and/or induced, and continues to contribute and/or induce the infringement of at least claim 1 of the '386 Patent by contributing to and/or inducing its partners, merchants, customers, and end-users to use its products, such as Exemplary PayPal Products, in an infringing manner as described above, including encouraging and instructing its partners, merchants, customers, and end-users through software and documentation provided by Defendant.

66. For example, Defendant's website www.PayPal.com and its mobile application specifically instruct users how to use the PayPal front and backend systems in a manner that infringes the patents. Moreover, third party application stores such as the Google Play store and the Apple App store provides instructions and information for end-users. On information and belief, this information is supplied by PayPal. In addition, PayPal provides instructions on its the PayPal mobile application that instructs users to interact with the PayPal front and backend systems in a manner that infringes the Patents. Defendant has known that its infringing products, such as the Exemplary PayPal Products, cannot be used without infringing the technology claimed in the '386 Patent, as described in **Exhibit D**, and are not staple articles of commerce suitable for substantial non-infringing uses.

67. Fintiv has been damaged by Defendant's infringement of the '386 Patent and will continue to be damaged by such infringement. Fintiv is entitled to recover damages from Defendant to compensate it for Defendant's infringement, as alleged above, in an amount measured by no less than a reasonable royalty under 35 U.S.C. § 284, as well as enhanced damages pursuant to 35 U.S.C. § 284.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 17 of 381

COUNT V: DIRECT INFRINGEMENT OF THE '413 PATENT

68. Fintiv incorporates paragraphs 1 through 67 herein by reference.

69. Defendant, without authorization or license from Fintiv, has been and is presently directly infringing, literally or under the doctrine of equivalents, at least claim 1 of the '413 Patent ("Exemplary '413 Patent Claims"), as infringement is defined by 35 U.S.C. § 271(a), including through making, using (including for testing purposes), selling, offering for sale, and/or distributing infringing products. Exemplary infringing products include at least PayPal's servers and Backend System that interacts with mobile devices (collectively, "Exemplary PayPal Products").

70. **Exhibit F** attached hereto includes charts comparing the Exemplary '413 Patent Claims to the Exemplary PayPal Products. As set forth in these charts, the Exemplary PayPal Products practice the technology claimed by the '413 Patent. Accordingly, the Exemplary PayPal Products incorporated in these charts satisfy all elements of the Exemplary '413 Patent Claims literally or by the doctrine of equivalents.

71. Defendant's acts of infringement have caused damage to Fintiv. Fintiv is entitled to recover damages in an amount to be determined at trial. Further, Defendant's infringement of Fintiv's rights under the '413 Patent will continue to damage Fintiv's business, causing irreparable harm for which there is no adequate remedy at law, unless enjoined by the Court.

72. Defendant is and has been aware of the non-provisional application that lead to the issuance of '413 Patent since at least August 2019, well before this Complaint. Consequently, Defendant's infringement of the '413 Patent is willful and deliberate, entitling Fintiv to enhanced damages pursuant to 35 U.S.C. § 284.

COUNT VI: INDIRECT INFRINGEMENT OF THE '413 PATENT

73. Fintiv incorporates paragraphs 1 through 72 herein by reference.

74. As described above, Defendant is and has been aware of the non-provisional application that led to the issuance of the '413 Patent since at least August 2019. And since that time, despite actual knowledge of the '413 Patent, has been and continues to indirectly infringe the '413 Patent.

75. Defendant has been indirectly infringing, and continues to indirectly infringe, at least claim 1 of the '413 Patent through its partners', merchants', customers', and end-users' direct infringement of at least claim 1 of the '413 Patent, through at least the use of the Exemplary PayPal Products without authorization of license from Fintiv.

76. Defendant is contributing to the infringement by others and/or inducing infringement by others by, among other things, providing instructions to its partners, merchants, customers, and end-users on how to download and use the PayPal application, including through its website www.PayPal.com and through instructions on third-party application providers, in a manner that infringes the Exemplary '413 Patent Claims.

77. Defendant has also contributed and/or induced, and continues to contribute and/or induce the infringement of at least claim 1 of the '413 Patent by contributing to and/or inducing its partners, merchants, customers, and end-users to use its products, such as Exemplary PayPal Products, in an infringing manner as described above, including encouraging and instructing its partners, merchants, customers, and end-users through software and documentation provided by Defendant.

78. For example, Defendant's website www.PayPal.com and its mobile application specifically instruct users how to use the PayPal Payment System including backend systems in a manner that infringes the patents. Moreover, third party application stores such as the Google Play store and the Apple App store provides instructions and information for end-users. On information

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 19 of 381

and belief, this information is supplied by PayPal. In addition, PayPal provides instructions on its the PayPal mobile application that instructs users to interact with the PayPal front and backend systems in a manner that infringes the Patents.

79. Defendant has known that its infringing products, such as the Exemplary PayPal Products, cannot be used without infringing the technology claimed in the '413 Patent, as described in **Exhibit F**, and are not staple articles of commerce suitable for substantial non-infringing uses.

80. Fintiv has been damaged by Defendant's infringement of the '413 Patent and will continue to be damaged by such infringement. Fintiv is entitled to recover damages from Defendant to compensate it for Defendant's infringement, as alleged above, in an amount measured by no less than a reasonable royalty under 35 U.S.C. § 284, as well as enhanced damages pursuant to 35 U.S.C. § 284.

COUNT VII: DIRECT INFRINGEMENT OF THE '488 PATENT

81. Fintiv incorporates paragraphs 1 through 80 herein by reference.

82. Defendant, without authorization or license from Fintiv, has been and is presently directly infringing, literally or under the doctrine of equivalents, at least claim 1 of the '488 Patent ("Exemplary '488 Patent Claims"), as infringement is defined by 35 U.S.C. § 271(a), including through making, using (including for testing purposes), selling, offering for sale, and/or distributing infringing products. Exemplary infringing products include at least PayPal's mobile payment system that facilitate the use of the PayPal Application and Backend System (collectively, "Exemplary PayPal Products").

83. **Exhibit H** attached hereto includes charts comparing the Exemplary '488 Patent Claims to the Exemplary PayPal Products. As set forth in these charts, the Exemplary PayPal Products practice the technology claimed by the '488 Patent. Accordingly, the Exemplary PayPal

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 20 of 381

Products incorporated in these charts satisfy all elements of the Exemplary '488 Patent Claims literally or by the doctrine of equivalents.

84. Defendant's acts of infringement have caused damage to Fintiv. Fintiv is entitled to recover damages in an amount to be determined at trial. Further, Defendant's infringement of Fintiv's rights under the '488 Patent will continue to damage Fintiv's business, causing irreparable harm for which there is no adequate remedy at law, unless enjoined by the Court.

85. Defendant is and has been aware of the '488 Patent since at least March 2016, well before this Complaint. Consequently, Defendant's infringement of the '488 Patent is willful and deliberate, entitling Fintiv to enhanced damages pursuant to 35 U.S.C. § 284.

COUNT VIII: INDIRECT INFRINGEMENT OF THE '488 PATENT

86. Fintiv incorporates paragraphs 1 through 85 herein by reference.

87. As described above, Defendant is and has been aware of the '488 Patent since at least March 2016. And since that time, despite actual knowledge of the '488 Patent, has been and continues to indirectly infringe the '488 Patent.

88. Defendant has been indirectly infringing, and continues to indirectly infringe, at least claim 1 of the '488 Patent through its partners', merchants', customers', and end-users', direct infringement of at least claim 1 of the '488 Patent, through at least the use of the Exemplary PayPal Products without authorization of license from Fintiv.

89. Defendant is contributing to the infringement by others and/or inducing infringement by others by, among other things, providing instructions to its partners, merchants, customers, and end-users on how to download and use the PayPal application, including through its website www.paypal.com and through instructions on third-party application providers, in a manner that infringes the Exemplary '488 Patent Claims.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 21 of 381

90. Defendant has also contributed and/or induced, and continues to contribute and/or induce the infringement of at least claim 1 of the '488 Patent by contributing to and/or inducing its partners, merchants, customers, and end-users to use its products, such as Exemplary PayPal Products, in an infringing manner as described above, including encouraging and instructing its partners, merchants, customers, and end-users through software and documentation provided by Defendant.

91. For example, Defendant's website www.PayPal.com and its mobile application specifically instruct users how to use the PayPal Payment System including backend systems in a manner that infringes the patents. Moreover, third party application stores such as the Google Play store and the Apple App store provides instructions and information for end-users. On information and belief, this information is supplied by PayPal. In addition, PayPal provides instructions on its the PayPal mobile application that instructs users to interact with the PayPal front and backend systems in a manner that infringes the Patents.

92. Defendant has known that its infringing products, such as the Exemplary PayPal Products, cannot be used without infringing the technology claimed in the '488 Patent, as described in **Exhibit H**, and are not staple articles of commerce suitable for substantial non-infringing uses.

93. Fintiv has been damaged by Defendant's infringement of the '488 Patent and will continue to be damaged by such infringement. Fintiv is entitled to recover damages from Defendant to compensate it for Defendant's infringement, as alleged above, in an amount measured by no less than a reasonable royalty under 35 U.S.C. § 284, as well as enhanced damages pursuant to 35 U.S.C. § 284.

COUNT IX: DIRECT INFRINGEMENT OF THE '196 PATENT

94. Fintiv incorporates paragraphs 1 through 93 herein by reference.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 22 of 381

95. Defendant, without authorization or license from Fintiv, has been and is presently directly infringing, literally or under the doctrine of equivalents, at least claim 1 of the '196 Patent ("Exemplary '196 Patent Claims"), as infringement is defined by 35 U.S.C. § 271(a), including through making, using (including for testing purposes), selling, offering for sale, and/or distributing infringing products. Exemplary infringing products include at least PayPal's mobile payment system that facilitate the use of the PayPal System (collectively, "Exemplary PayPal Products").

96. **Exhibit J** attached hereto includes charts comparing the Exemplary '196 Patent Claims to the Exemplary PayPal Products. As set forth in these charts, the Exemplary PayPal Products practice the technology claimed by the '196 Patent. Accordingly, the Exemplary PayPal Products incorporated in these charts satisfy all elements of the Exemplary '196 Patent Claims literally or by the doctrine of equivalents.

97. Defendant's acts of infringement have caused damage to Fintiv. Fintiv is entitled to recover damages in an amount to be determined at trial. Further, Defendant's infringement of Fintiv's rights under the '196 Patent will continue to damage Fintiv's business, causing irreparable harm for which there is no adequate remedy at law, unless enjoined by the Court.

98. Defendant is and has been aware of the '196 Patent since at least March 2016, well before this Complaint. Consequently, Defendant's infringement of the '196 Patent is willful and deliberate, entitling Fintiv to enhanced damages pursuant to 35 U.S.C. § 284.

COUNT X: INDIRECT INFRINGEMENT OF THE '196 PATENT

99. Fintiv incorporates paragraphs 1 through 98 herein by reference.

100. As described above, Defendant is and has been aware of the '196 Patent since at least March 2016. And since that time, despite actual knowledge of the '196 Patent, has been and continues to indirectly infringe the '196 Patent.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 23 of 381

101. Defendant has been indirectly infringing, and continues to indirectly infringe, at least claim 1 of the '196 Patent through its partners', merchants', customers', and end-users', direct infringement of at least claim 1 of the '196 Patent, through at least the use of the Exemplary PayPal Products without authorization of license from Fintiv.

102. Defendant is contributing to the infringement by others and/or inducing infringement by others by, among other things, providing instructions to its partners, merchants, customers, and end-users on how to download and use the PayPal application, including through its website www.paypal.com and through instructions on third-party application providers, in a manner that infringes the Exemplary '196 Patent Claims.

103. Defendant has also contributed and/or induced, and continues to contribute and/or induce the infringement of at least claim 1 of the '196 Patent by contributing to and/or inducing its partners, merchants, customers, and end-users to use its products, such as Exemplary PayPal Products, in an infringing manner as described above, including encouraging and instructing its partners, merchants, customers, and end-users through software and documentation provided by Defendant.

104. For example, Defendant's website www.PayPal.com and its mobile application specifically instruct users how to use the PayPal Payment System including backend systems in a manner that infringes the patents. Moreover, third party application stores such as the Google Play store and the Apple App store provides instructions and information for end-users. On information and belief, this information is supplied by PayPal. In addition, PayPal provides instructions on its the PayPal mobile application that instructs users to interact with the PayPal front and backend systems in a manner that infringes the Patents.

105. Defendant has known that its infringing products, such as the Exemplary PayPal Products, cannot be used without infringing the technology claimed in the '196 Patent, as described in **Exhibit J**, and are not staple articles of commerce suitable for substantial non-infringing uses.

106. Fintiv has been damaged by Defendant's infringement of the '196 Patent and will continue to be damaged by such infringement. Fintiv is entitled to recover damages from Defendant to compensate it for Defendant's infringement, as alleged above, in an amount measured by no less than a reasonable royalty under 35 U.S.C. § 284, as well as enhanced damages pursuant to 35 U.S.C. § 284.

VI. DEMAND FOR JURY TRIAL

107. Fintiv demands a trial by jury of any and all issues triable of right before a jury.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff Fintiv respectfully requests that the Court:

A. Enter a judgment that the Patents-in-Suit are valid and enforceable;

B. Enter a judgment that PayPal has directly infringed, contributorily infringed, and/or induced infringement of one or more claims of the Patents-in-Suit;

C. Enter a judgment awarding Fintiv all damages adequate to compensate it for PayPal's direct or contributory infringement of, or inducement to infringe, the Patents-in-Suit, including all pre-judgment and post-judgment interest at the maximum rate permitted by law;

D. Enter a judgment awarding Fintiv enhanced damages pursuant to 35 U.S.C. § 284, including for PayPal's willful infringement of the Patents-in-Suit;

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 25 of 381

E. Enter a judgment awarding Fintiv ongoing royalties for Defendant's continued direct infringement, contributory infringement, and/or induced infringement of the Patents-in-Suit;

F. Enter permanent injunctive relief preventing PayPal from further infringement, whether direct or contributory, and from further inducement of infringement of the Patents-in-Suit; or, in the alternative, enter a judgment awarding Fintiv ongoing royalties for PayPal's continued direct or indirect infringement of the Patents-in-Suit;

G. Declare this case exceptional pursuant to 35 U.S.C. § 285;

H. Enter an accounting of all damages not presented at trial; and

I. Award Fintiv its costs, disbursements, attorneys' fees, and such further and additional relief as is deemed appropriate by this Court.

Dated: March 17, 2022

RESPECTFULLY SUBMITTED,

By: */s/ Raymond W. Mort, III*

Raymond W. Mort, III
Texas State Bar No. 00791308
raymort@austinlaw.com
THE MORT LAW FIRM, PLLC
100 Congress Ave, Suite 2000
Austin, Texas 78701
Tel/Fax: (512) 865-7950

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 26 of 381

Jonathan K. Waldrop (CA Bar No. 297903)
(Admitted in this District)
jwaldrop@kasowitz.com
Darcy L. Jones (CA Bar No. 309474)
(Admitted in this District)
djones@kasowitz.com
Marcus A. Barber (CA Bar No. 307361)
(Admitted in this District)
mbarber@kasowitz.com
John W. Downing (CA Bar No. 252850)
(Admitted in this District)
jdowning@kasowitz.com
Heather S. Kim (CA Bar No. 277686)
(Admitted in this District)
hkim@kasowitz.com
ThucMinh Nguyen (CA Bar No. 304382)
(Admitted in this District)
tnguyen@kasowitz.com
KASOWITZ BENSON TORRES LLP
333 Twin Dolphin Drive, Suite 200
Redwood Shores, California 94065
Telephone: (650) 453-5170
Facsimile: (650) 453-5171

Paul G. Williams (Georgia Bar No. 764925)
(Admitted in this District)
pwilliams@kasowitz.com
KASOWITZ BENSON TORRES LLP
1230 Peachtree Street N.E., Suite 2445
Atlanta, Georgia 30309
Telephone: (404) 260-6080
Facsimile: (404) 260-6081

Attorneys for Plaintiff
FINTIV, INC.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 27 of 381

JS 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Fintiv, Inc.

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
The Mort Law Firm, PLLC
100 Congress Ave, Suite 2000, Austin, TX 78701
(512) 865-7950

DEFENDANTS

PayPal Holdings, Inc.

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	☐ 625 Drug Related Seizure of Property 21 USC 881	☐ 422 Appeal 28 USC 158	☐ 375 False Claims Act
☐ 120 Marine	☐ 310 Airplane	☐ 365 Personal Injury - Product Liability	☐ 690 Other	☐ 423 Withdrawal 28 USC 157	☐ 376 Qui Tam (31 USC 3729(a))
☐ 130 Miller Act	☐ 315 Airplane Product Liability	☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	☐ 400 State Reapportionment
☐ 140 Negotiable Instrument	☐ 320 Assault, Libel & Slander	PERSONAL PROPERTY		☐ 820 Copyrights	☐ 410 Antitrust
☐ 150 Recovery of Overpayment & Enforcement of Judgment	☐ 330 Federal Employers' Liability	☐ 370 Other Fraud		☒ 830 Patent	☐ 430 Banks and Banking
☐ 151 Medicare Act	☐ 340 Marine	☐ 371 Truth in Lending		☐ 835 Patent - Abbreviated New Drug Application	☐ 450 Commerce
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	☐ 345 Marine Product Liability	☐ 380 Other Personal Property Damage		☐ 840 Trademark	☐ 460 Deportation
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 350 Motor Vehicle	☐ 385 Property Damage Product Liability	LABOR	SOCIAL SECURITY	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 160 Stockholders' Suits	☐ 355 Motor Vehicle Product Liability		☐ 710 Fair Labor Standards Act	☐ 861 HIA (1395ff)	☐ 480 Consumer Credit
☐ 190 Other Contract	☐ 360 Other Personal Injury		☐ 720 Labor/Management Relations	☐ 862 Black Lung (923)	☐ 490 Cable/Sat TV
☐ 195 Contract Product Liability	☐ 362 Personal Injury - Medical Malpractice		☐ 740 Railway Labor Act	☐ 863 DIWC/DIWW (405(g))	☐ 850 Securities/Commodities/ Exchange
☐ 196 Franchise			☐ 751 Family and Medical Leave Act	☐ 864 SSID Title XVI	☐ 890 Other Statutory Actions
			☐ 790 Other Labor Litigation	☐ 865 RSI (405(g))	☐ 891 Agricultural Acts
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	☐ 791 Employee Retirement Income Security Act		☐ 893 Environmental Matters
☐ 210 Land Condemnation	☐ 440 Other Civil Rights	Habeas Corpus:		FEDERAL TAX SUITS	☐ 895 Freedom of Information Act
☐ 220 Foreclosure	☐ 441 Voting	☐ 463 Alien Detainee	IMMIGRATION	☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 896 Arbitration
☐ 230 Rent Lease & Ejectment	☐ 442 Employment	☐ 510 Motions to Vacate Sentence	☐ 462 Naturalization Application	☐ 871 IRS—Third Party 26 USC 7609	☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 240 Torts to Land	☐ 443 Housing/ Accommodations	☐ 530 General	☐ 465 Other Immigration Actions		☐ 950 Constitutionality of State Statutes
☐ 245 Tort Product Liability	☐ 445 Amer. w/Disabilities - Employment	☐ 535 Death Penalty			
☐ 290 All Other Real Property	☐ 446 Amer. w/Disabilities - Other	Other:			
	☐ 448 Education	☐ 540 Mandamus & Other			
		☐ 550 Civil Rights			
		☐ 555 Prison Condition			
		☐ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
35 U.S.C. § 1 et seq.

Brief description of cause:
Patent Infringement

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
March 17, 2022

SIGNATURE OF ATTORNEY OF RECORD
/s/ Raymond W. Mort, III

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

Exhibit A
U.S. Patent No. 8,538,845

US008538845B2

(12) **United States Patent**
Liberty

(10) **Patent No.: US 8,538,845 B2**
(45) **Date of Patent: Sep. 17, 2013**

(54) **MONETARY TRANSACTION SYSTEM**

(75) Inventor: **Michael A. Liberty**, Windermere, FL (US)

(73) Assignee: **Mozido, LLC**, Dallas, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **13/484,199**

(22) Filed: **May 30, 2012**

(65) **Prior Publication Data**

US 2012/0310824 A1 Dec. 6, 2012

Related U.S. Application Data

(60) Provisional application No. 61/522,099, filed on Aug. 10, 2011, provisional application No. 61/493,064, filed on Jun. 3, 2011.

(51) **Int. Cl.**
G06Q 40/00 (2012.01)

(52) **U.S. Cl.**
USPC **705/35**; 705/40

(58) **Field of Classification Search**
USPC 705/40, 35
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,717,374	A	2/1998	Smith
5,828,739	A	10/1998	Nakanishi
5,991,749	A	11/1999	Morrill
6,185,545	B1	2/2001	Resnick
6,250,557	B1	6/2001	Forslund
6,415,156	B1	7/2002	Stadelmann
6,622,015	B1	9/2003	Himmel
6,697,839	B2	2/2004	Sini
6,714,797	B1	3/2004	Rautila
6,736,322	B2	5/2004	Gobburu
6,819,219	B1	11/2004	Bolle
6,840,448	B2	1/2005	Fukushima
6,873,974	B1	3/2005	Schutzer
6,957,342	B2	10/2005	Vatanen

(Continued)

FOREIGN PATENT DOCUMENTS

CA	2666616	4/2008
CN	101606400	12/2009

(Continued)

OTHER PUBLICATIONS

Sykes, Quintin; Daley, Tim; "Securing Mobile Banking"; Nov. 2010, Credit Union Management; ISSN: 0273-9267.*

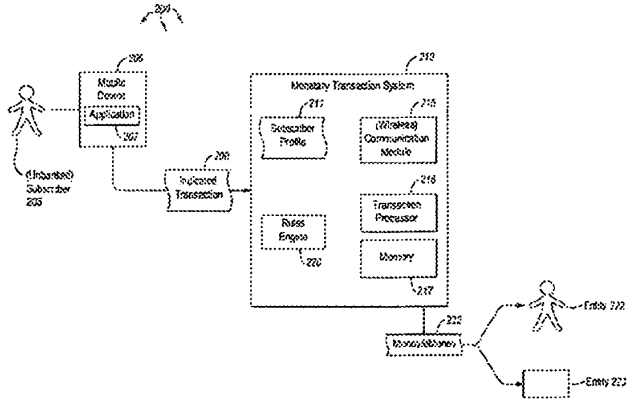
(Continued)

Primary Examiner — Edward Chang
(74) *Attorney, Agent, or Firm* — Workman Nydegger

(57) **ABSTRACT**

Embodiments are directed to monetary transaction system for conducting monetary transactions between transaction system subscribers and other entities. In one scenario, the monetary transaction system includes a mobile device that runs a monetary transaction system application. The monetary transaction system also includes a subscriber that has a profile with the system. The subscriber indicates a transaction that is to be performed with the monetary transaction system. The system further includes a monetary transaction system processor that performs the transactions specified by the subscriber including communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile. The monetary transaction system also includes at least one entity that is to be involved in the specified transaction, where the entity has a profile with the monetary transaction system. This entity may be a person, a retail store, an agent or other entity.

7 Claims, 21 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

7,024,174	B2	4/2006	Nagy	
7,054,430	B2	5/2006	Lynam	
7,069,001	B2	6/2006	Rupp	
7,089,208	B1	8/2006	Levchin	
7,099,850	B1	8/2006	Mann	
7,100,821	B2	9/2006	Rasti	
7,107,247	B2	9/2006	Kinoshita	
7,110,972	B1	9/2006	Handa	
7,221,939	B2	5/2007	Ylitalo	
7,240,836	B2	7/2007	Vrotsos	
7,248,855	B2	7/2007	Joyce	
7,255,264	B2	8/2007	De Leon	
7,275,685	B2	10/2007	Gray	
7,322,043	B2	1/2008	Letsinger	
7,325,132	B2	1/2008	Takayama	
7,347,361	B2	3/2008	Lovett	
7,349,871	B2	3/2008	Labrou	
7,353,382	B2	4/2008	Labrou	
7,363,261	B2	4/2008	Whitehead	
7,461,010	B2	12/2008	Kwan	
7,461,028	B2	12/2008	Wronski	
7,494,055	B2	2/2009	Fernandes	
7,512,098	B2	3/2009	Jiang	
7,527,194	B2	5/2009	Truitt	
7,562,818	B1	7/2009	Bierbaum	
7,606,560	B2	10/2009	Labrou	
7,657,489	B2	2/2010	Stambaugh	
7,677,973	B2	3/2010	Van Luchene	
7,699,218	B2	4/2010	Garcia	
7,708,194	B2	5/2010	Vawter	
7,729,963	B1	6/2010	Lego	
7,729,987	B1	6/2010	Wakim	
7,748,618	B2	7/2010	Vawter	
7,774,076	B2	8/2010	Skowronek	
7,774,231	B2	8/2010	Pond	
7,784,684	B2	8/2010	Labrou	
7,801,826	B2	9/2010	Labrou	
7,819,307	B2 *	10/2010	Lyons et al.	235/379
7,822,688	B2	10/2010	Labrou	
7,823,772	B2	11/2010	Vawter	
7,848,500	B2	12/2010	Lynam	
7,848,504	B2	12/2010	Lynam	
7,865,414	B2	1/2011	Fung	
7,865,431	B2	1/2011	Takayama	
7,877,605	B2	1/2011	Labrou	
7,886,962	B2	2/2011	Vawter	
7,890,424	B1	2/2011	Wakim	
7,937,302	B1	5/2011	Lego	
7,937,305	B1	5/2011	Lego	
7,958,052	B2	6/2011	Powell	
7,967,196	B1	6/2011	Bierbaum	
7,979,026	B2	7/2011	Hulvey	
7,988,060	B2	8/2011	Killian	
8,016,185	B2	9/2011	Modi	
8,019,365	B2	9/2011	Fisher	
8,041,338	B2	10/2011	Chen	
8,052,042	B2	11/2011	Kolinski-Schultz	
8,060,012	B2	11/2011	Sklovsky	
8,073,783	B2	12/2011	Felsted	
8,077,042	B2	12/2011	Peeters	
8,090,945	B2	1/2012	Singhal	
8,095,113	B2	1/2012	Kean	
8,116,734	B2	2/2012	Vawter	
8,116,773	B2	2/2012	Chitrapu	
8,121,945	B2	2/2012	Rackley	
8,145,568	B2	3/2012	Rackley	
8,160,959	B2	4/2012	Rackley	
8,170,485	B2	5/2012	Hulvey	
8,190,087	B2	5/2012	Fisher	
8,195,576	B1	6/2012	Grigg	
8,196,131	B1	6/2012	von Behren	
8,213,470	B2	7/2012	Gu	
8,229,354	B2	7/2012	Sklovsky	
8,239,325	B2	8/2012	Schwarz	
8,275,312	B2	9/2012	Fisher	
8,290,433	B2	10/2012	Fisher	
8,332,272	B2	12/2012	Fisher	
8,333,319	B2	12/2012	Roth	
8,352,323	B2	1/2013	Fisher	
8,355,670	B2	1/2013	White	
8,359,265	B2	1/2013	Van Rensburg	
8,360,329	B2	1/2013	Grigg	
8,374,916	B2	2/2013	White	
8,396,793	B2	3/2013	Hill	
2001/0011248	A1	8/2001	Himmel	
2001/0037264	A1	11/2001	Husemann	
2002/0042776	A1	4/2002	Woo	
2002/0052754	A1	5/2002	Joyce	
2002/0060246	A1	5/2002	Gobburu	
2002/0065774	A1	5/2002	Young	
2002/0069123	A1	6/2002	Soderlind	
2002/0131404	A1	9/2002	Mehta	
2002/0141586	A1	10/2002	Margalit	
2002/0152177	A1	10/2002	Wolf	
2002/0161708	A1	10/2002	Offer	
2003/0001010	A1	1/2003	Schmidt	
2003/0055735	A1	3/2003	Cameron	
2003/0071115	A1	4/2003	Horn	
2003/0154165	A1	8/2003	Horn	
2003/0195842	A1	10/2003	Reece	
2004/0181531	A1	9/2004	Becker	
2004/0205618	A1	10/2004	Sini	
2004/0235450	A1	11/2004	Rosenberg	
2004/0248554	A1	12/2004	Khan	
2005/0070265	A1	3/2005	Korpinen	
2005/0080697	A1	4/2005	Foss	
2005/0187873	A1 *	8/2005	Labrou et al.	705/40
2005/0199709	A1	9/2005	Linior	
2005/0222961	A1	10/2005	Staib	
2006/0116892	A1	6/2006	Grimes	
2006/0136901	A1	6/2006	Nichols	
2006/0165060	A1	7/2006	Dua	
2006/0179452	A1	8/2006	Amodeo	
2006/0200427	A1	9/2006	Morrison	
2006/0253335	A1	11/2006	Keena	
2006/0287004	A1	12/2006	Fuqua	
2007/0033285	A1	2/2007	Shiigi	
2007/0106564	A1	5/2007	Matotek	
2007/0123305	A1	5/2007	Chen	
2007/0125838	A1	6/2007	Law	
2007/0125840	A1	6/2007	Law	
2007/0162471	A1	7/2007	Samuelsson	
2007/0179885	A1	8/2007	Bird	
2007/0203850	A1	8/2007	Singh	
2007/0241189	A1	10/2007	Slavin	
2007/0244811	A1	10/2007	Tumminaro	
2007/0255620	A1	11/2007	Tumminaro	
2007/0255653	A1	11/2007	Tumminaro	
2008/0006685	A1	1/2008	Rackley	
2008/0010191	A1	1/2008	Rackley	
2008/0010196	A1	1/2008	Rackley	
2008/0010204	A1	1/2008	Rackley	
2008/0010215	A1	1/2008	Rackley	
2008/0011825	A1	1/2008	Giordano	
2008/0017704	A1	1/2008	VanDeburg	
2008/0040265	A1	2/2008	Rackley	
2008/0040285	A1	2/2008	Wankmueller	
2008/0052192	A1	2/2008	Fisher	
2008/0126145	A1	5/2008	Rackley	
2008/0126929	A1	5/2008	Bykov	
2008/0143487	A1	6/2008	Hulvey	
2008/0197190	A1	8/2008	Fujita	
2008/0204358	A1 *	8/2008	Sato et al.	345/2.2
2008/0208743	A1	8/2008	Arthur	
2008/0208744	A1	8/2008	Arthur	
2008/0208762	A1	8/2008	Arthur	
2008/0210751	A1	9/2008	Kim	
2008/0249927	A1	10/2008	Rethorn	
2008/0249928	A1	10/2008	Hill	
2008/0249930	A1	10/2008	Hill	
2008/0249933	A1	10/2008	Rethorn	
2008/0255947	A1	10/2008	Friedman	
2008/0275779	A1	11/2008	Lakshminarayanan	
2008/0281737	A1	11/2008	Fajardo	

2009/0037326	A1	2/2009	Chitti
2009/0055322	A1	2/2009	Bykov
2009/0063312	A1	3/2009	Hurst
2009/0081989	A1	3/2009	Wuhrer
2009/0098854	A1	4/2009	Park
2009/0104888	A1	4/2009	Cox
2009/0106148	A1	4/2009	Prada
2009/0108015	A1	4/2009	Kreamer
2009/0119190	A1	5/2009	Realini
2009/0132362	A1	5/2009	Fisher
2009/0132392	A1	5/2009	Davis
2009/0138366	A1	5/2009	Bemmel
2009/0144161	A1	6/2009	Fisher
2009/0156190	A1	6/2009	Fisher
2009/0157546	A1	6/2009	Garcia
2009/0177578	A1	7/2009	Garcia
2009/0177581	A1	7/2009	Garcia
2009/0210308	A1	8/2009	Toomer
2009/0222353	A1	9/2009	Guest
2009/0222358	A1	9/2009	Bednarek
2009/0248537	A1	10/2009	Sarkeshik
2009/0254440	A1	10/2009	Pharris
2009/0254479	A1	10/2009	Pharris
2009/0265272	A1	10/2009	Dill
2009/0281904	A1	11/2009	Pharris
2009/0288012	A1	11/2009	Hertel
2009/0307132	A1	12/2009	Phillips
2010/0010964	A1	1/2010	Skowronek
2010/0023449	A1	1/2010	Skowronek
2010/0044430	A1	2/2010	Song
2010/0048226	A1	2/2010	Owen
2010/0049599	A1	2/2010	Owen
2010/0051685	A1	3/2010	Royyuru
2010/0057614	A1	3/2010	Rainey
2010/0057619	A1	3/2010	Weller
2010/0057624	A1	3/2010	Hurt
2010/0063895	A1	3/2010	Dominguez
2010/0088188	A1	4/2010	Kumar
2010/0125495	A1	5/2010	Smith
2010/0125510	A1	5/2010	Smith
2010/0197326	A1	8/2010	Ngo
2010/0223110	A1	9/2010	Slavin
2010/0235283	A1	9/2010	Gerson
2010/0248710	A1	9/2010	Sklovsky
2010/0250436	A1	9/2010	Loevenguth
2010/0260388	A1	10/2010	Garrett
2011/0057025	A1	3/2011	Denzer
2011/0087529	A1	4/2011	Angell
2011/0087610	A1	4/2011	Batada
2011/0105022	A1	5/2011	Vawter
2011/0113473	A1	5/2011	Corda
2011/0145049	A1	6/2011	Hertel
2011/0145149	A1*	6/2011	Valdes et al. 705/44
2011/0179113	A1	7/2011	Thomas
2011/0218911	A1	9/2011	Spodak
2011/0246284	A1	10/2011	Chaikin
2011/0250866	A1	10/2011	Fisher
2011/0251941	A1	10/2011	Dunwoody
2011/0258115	A1	10/2011	Mulhim
2011/0276417	A1	11/2011	Campbell
2011/0295750	A1	12/2011	Rammal
2011/0302016	A1	12/2011	Haddad
2011/0302406	A1	12/2011	Machani
2011/0313924	A1	12/2011	Carrell
2011/0320243	A1	12/2011	Khan
2011/0320293	A1	12/2011	Khan
2011/0320294	A1	12/2011	Votaw
2011/0320345	A1	12/2011	Taveau
2012/0011063	A1	1/2012	Killian
2012/0028612	A1	2/2012	Hurst
2012/0029990	A1	2/2012	Fisher
2012/0047070	A1	2/2012	Pharris
2012/0074232	A1	3/2012	Spodak
2012/0078735	A1	3/2012	Bauer
2012/0084203	A1	4/2012	Mehew
2012/0095855	A1	4/2012	Sterling
2012/0095856	A1	4/2012	Sanjeev
2012/0122447	A1	5/2012	Craft
2012/0123841	A1	5/2012	Taveau
2012/0123868	A1	5/2012	Brudnicki
2012/0123880	A1	5/2012	Craft
2012/0123935	A1	5/2012	Brudnicki
2012/0123937	A1	5/2012	Spodak
2012/0143752	A1	6/2012	Wong
2012/0150669	A1	6/2012	Langley
2012/0158589	A1	6/2012	Katzin
2012/0171992	A1	7/2012	Cheong
2012/0172026	A1	7/2012	Kwon
2012/0172089	A1	7/2012	Bae
2012/0174189	A1	7/2012	Lim
2012/0191557	A1	7/2012	Fisher
2012/0191612	A1	7/2012	Spodak
2012/0196586	A1	8/2012	Grigg
2012/0197691	A1	8/2012	Grigg
2012/0197740	A1	8/2012	Grigg
2012/0197743	A1	8/2012	Grigg
2012/0197745	A1	8/2012	Fisher
2012/0197787	A1	8/2012	Grigg
2012/0203632	A1	8/2012	Blum
2012/0209688	A1	8/2012	Lamothe
2012/0209749	A1	8/2012	Hammad
2012/0215701	A1	8/2012	Mehta
2012/0221421	A1	8/2012	Hammad
2012/0221475	A1	8/2012	Grigg
2012/0226610	A1	9/2012	Gill
2012/0229647	A1	9/2012	Calman
2012/0229657	A1	9/2012	Calman
2012/0231424	A1	9/2012	Calman
2012/0231425	A1	9/2012	Calman
2012/0232937	A1	9/2012	Calman
2012/0232977	A1	9/2012	Calman
2012/0245986	A1	9/2012	Regan
2012/0253852	A1	10/2012	Pourfallah
2012/0259686	A1	10/2012	Yurow
2012/0259698	A1	10/2012	Yurow
2012/0259732	A1	10/2012	Sasankan
2012/0265677	A1	10/2012	Rackley
2012/0265685	A1	10/2012	Brudnicki
2012/0271712	A1	10/2012	Katzin
2012/0284131	A1	11/2012	Soffer
2012/0286928	A1	11/2012	Mullen
2012/0290376	A1	11/2012	Dryer
2012/0290449	A1	11/2012	Mullen
2012/0293303	A1	11/2012	Khan
2012/0296708	A1	11/2012	Bachmann
2012/0296720	A1	11/2012	Pirillo
2012/0296722	A1	11/2012	Gosavi
2012/0296741	A1	11/2012	Dykes
2012/0297204	A1	11/2012	Buer
2012/0302204	A1	11/2012	Gupta
2012/0303425	A1	11/2012	Katzin
2012/0310720	A1	12/2012	Balsan
2012/0310760	A1	12/2012	Phillips
2012/0310824	A1	12/2012	Liberty
2012/0310826	A1	12/2012	Chatterjee
2012/0316950	A1	12/2012	LaPorte
2012/0316951	A1	12/2012	Fisher
2012/0316992	A1	12/2012	Oborne
2012/0317019	A1	12/2012	Carnes
2012/0323653	A1	12/2012	Fisher
2012/0323664	A1	12/2012	Klems
2012/0323670	A1	12/2012	Fisher
2012/0323777	A1	12/2012	Liberty
2012/0329394	A1	12/2012	Fisher
2012/0330737	A1	12/2012	Liberty
2012/0330792	A1	12/2012	Kashanian
2013/0012125	A1	1/2013	Fisher
2013/0012126	A1	1/2013	Fisher
2013/0012131	A1	1/2013	Fisher
2013/0013352	A1	1/2013	Fisher
2013/0013353	A1	1/2013	Fisher
2013/0013355	A1	1/2013	Fisher
2013/0013432	A1	1/2013	Fisher
2013/0013434	A1	1/2013	Fisher
2013/0013490	A1	1/2013	Keller
2013/0013498	A1	1/2013	Fisher
2013/0013499	A1	1/2013	Kalgi
2013/0013501	A1	1/2013	Rackley

2013/0017784	A1	1/2013	Fisher
2013/0018738	A1	1/2013	Faires
2013/0018740	A1	1/2013	Fisher
2013/0018742	A1	1/2013	Fisher
2013/0018793	A1	1/2013	Wong
2013/0023209	A1	1/2013	Fisher
2013/0023294	A1	1/2013	Singh
2013/0024220	A1	1/2013	Fisher
2013/0024221	A1	1/2013	Fisher
2013/0024223	A1	1/2013	Thomas
2013/0024280	A1	1/2013	Fisher
2013/0024364	A1	1/2013	Shrivastava et al.
2013/0024371	A1	1/2013	Hariramani
2013/0024372	A1	1/2013	Spodak
2013/0024377	A1	1/2013	Stong
2013/0029646	A1	1/2013	Chowdhury
2013/0030828	A1	1/2013	Pourfallah
2013/0030960	A1	1/2013	Kashanian
2013/0030997	A1	1/2013	Spodak
2013/0035035	A1	2/2013	Fisher
2013/0035036	A1	2/2013	Fisher
2013/0035037	A1	2/2013	Fisher
2013/0035068	A1	2/2013	Fisher
2013/0035069	A1	2/2013	Fisher
2013/0035070	A1	2/2013	Fisher
2013/0035071	A1	2/2013	Fisher
2013/0035072	A1	2/2013	Fisher
2013/0035087	A1	2/2013	Fisher
2013/0035967	A1	2/2013	Fisher
2013/0035968	A1	2/2013	Fisher
2013/0035969	A1	2/2013	Fisher
2013/0035970	A1	2/2013	Fisher
2013/0040568	A1	2/2013	Fisher
2013/0040569	A1	2/2013	Fisher
2013/0041699	A1	2/2013	Fisher
2013/0041700	A1	2/2013	Fisher
2013/0041701	A1	2/2013	Roth
2013/0041736	A1	2/2013	Coppinger
2013/0041743	A1	2/2013	Coppinger
2013/0041744	A1	2/2013	Coppinger
2013/0041745	A1	2/2013	Coppinger
2013/0041769	A1	2/2013	Fisher
2013/0046608	A1	2/2013	Coppinger
2013/0046634	A1	2/2013	Grigg
2013/0046645	A1	2/2013	Grigg
2013/0048723	A1	2/2013	King
2013/0052952	A1	2/2013	Fisher
2013/0054336	A1	2/2013	Graylin
2013/0054337	A1	2/2013	Brendell
2013/0054412	A1	2/2013	Brendell
2013/0054441	A1	2/2013	Kamdar
2013/0057392	A1	3/2013	Bullock
2013/0060618	A1	3/2013	Barton
2013/0073373	A1	3/2013	Fisher
2013/0073458	A1	3/2013	Sherwin
2013/0080228	A1	3/2013	Fisher
2013/0080229	A1	3/2013	Fisher
2013/0080230	A1	3/2013	Fisher
2013/0080231	A1	3/2013	Fisher
2013/0080232	A1	3/2013	Fisher
2013/0080233	A1	3/2013	Fisher
2013/0080240	A1	3/2013	Fisher
2013/0080241	A1	3/2013	Fisher
2013/0080329	A1	3/2013	Royyuru

FOREIGN PATENT DOCUMENTS

CN	102073958	5/2011
DE	10119808	9/2002
EP	1280115	1/2003
JP	2001-297198	10/2001
JP	2001-357164	12/2001
JP	2002-99716	4/2002
KR	10-2002-0065989	8/2002
KR	10-2003-0068603	8/2003
KR	10-2007-0092400	9/2007
WO	9834203	8/1998
WO	9913636	3/1999
WO	0171627	9/2001
WO	0197118	12/2001
WO	02071354	9/2002
WO	03012717	2/2003
WO	2004010393	1/2004
WO	2004023353	3/2004
WO	2004053640	6/2004
WO	2004088641	10/2004
WO	2005079254	9/2005
WO	2005086593	9/2005
WO	2007145500	12/2007
WO	2008008735	1/2008

OTHER PUBLICATIONS

Clarke, Irvine III, "Emerging Value Propositions for M-commerce"; Fall 2008; Journal of Business Strategies, ISSN: 0887-2058.*

Wei, June; Ozok, Ant, "Development of a web-based mobile airline ticketing model with usability features"; 2005; Industrial Management + Data Systems; v105n9; ISSN: 0263-5577.*

U.S. Appl. No. 13/680,824, filed Nov. 19, 2012, Liberty, Michael A.

Chen, Jiajun Jim et al, Short-Range Wireless Technologies with Mobile Payments Systems. Proceedings of the 6th International Conference on Electronic Commerce [Online] 2004, pp. 649-656.

Labrou, Yannis et al, Wireless Wallet. Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services [Online] 2004, pp. 1-10.

Motorola, Motorola M-Wallet Solution. [Online] 2006 http://www.motorola.com/networkoperators/pdfs/M-Wallet-Brochure.pdf (Accessed Oct. 4, 2012).

Valcourt, E. et al., "Investigating Mobile Payment," Wireless and Mobile Computing, Networking and Communications, 2005. (WiMob'2005), IEEE International Conference on Aug. 22-24, 2005, Aug. 2005, vol. 4, pp. 29-36.

Gao, Jerry, et al., "P2P-Paid: A Peer-to-Peer Wireless Payment System," Proceedings of the 2005 Second IEEE International Workshop on Mobile Commerce and Services (WMCS'05) Jul. 2005, 10 pages.

Edwin, et al., "Technobiography," Oct. 2004, 29 pages.

International Search Report for PCT/US2012/040131 Dated Jan. 29, 2013.

Written Opinion for PCT/US2012/040131 dated Jan. 29, 2013.

International Search Report for PCT/US2012/066013 dated Jan. 29, 2013.

Written Opinion for PCT/US2012/066013 dated Jan. 29, 2013.

* cited by examiner

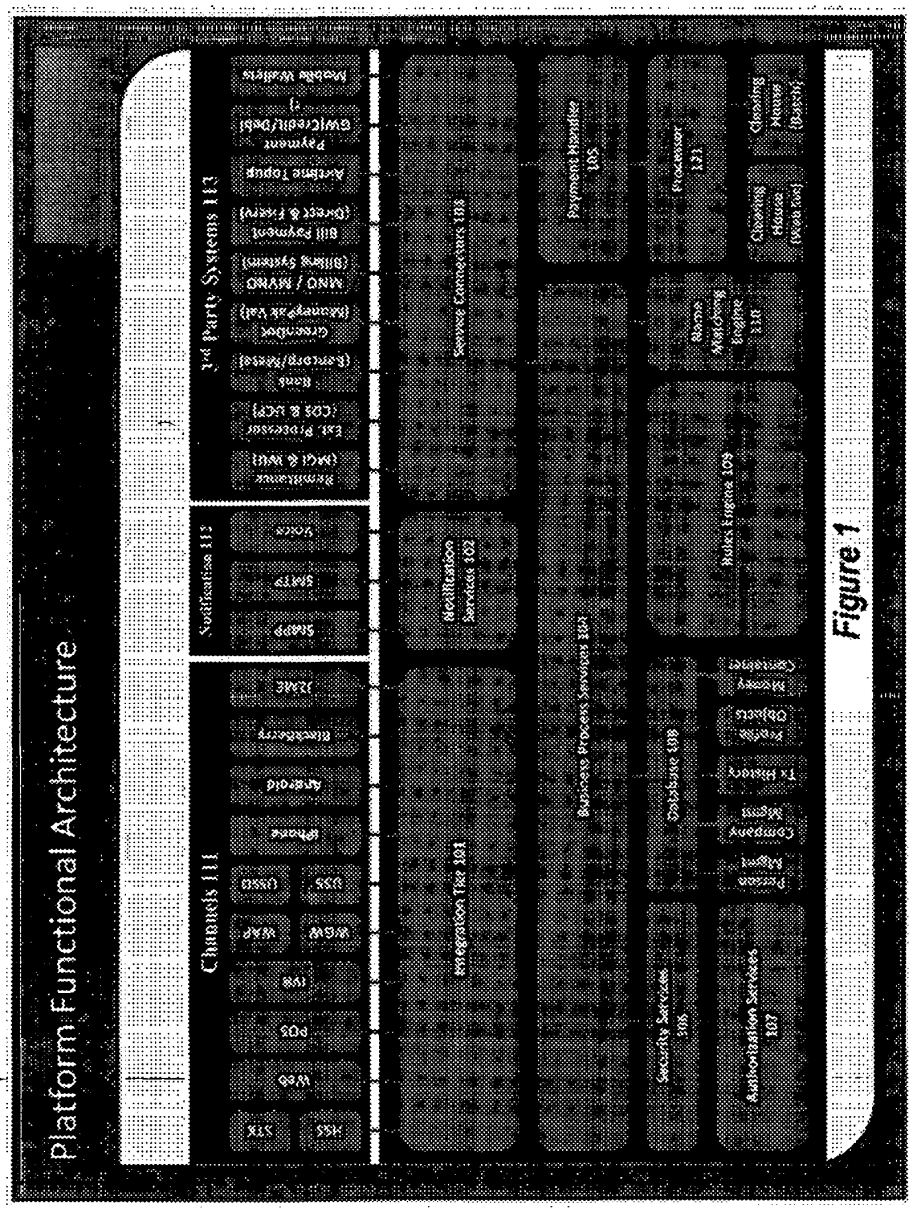

Platform Functional Architecture
Channels 111
J2ME
BlackBerry
Android
iPhone
USSD
SMS
WAP
WGW
IVR
POS
Web
STK
HSS
3rd Party Systems 113
Mobile Wallets
Payment Gw/Credit/Debit
Acertane Topup
Bill Payment (Direct & Fiserv)
MNO / MVNO (Billing Systems)
Groceries (Mastercard/Visa)
Banks (Barclays/Visa)
Ext. Processor (CDS & UCP)
Remittance (MGI & Intl)
Notifications 115
Voice
SMTP
SMPP
Integration Tier 101
Service Connectors 103
Notification Services 102
Payment Hubs 105
Processor 121
Closing House (Intra Bank)
Closing House (Inter Bank)
Rules Engine 109
Alerts Monitoring Engine 111
Business Process Services 104
Customer 108
Security Services 106
Authorization Services 107
Customer
Merchant
Products
Tx History
Company Mgmt
Payment Mgmt
Figure 1

FIG. 1

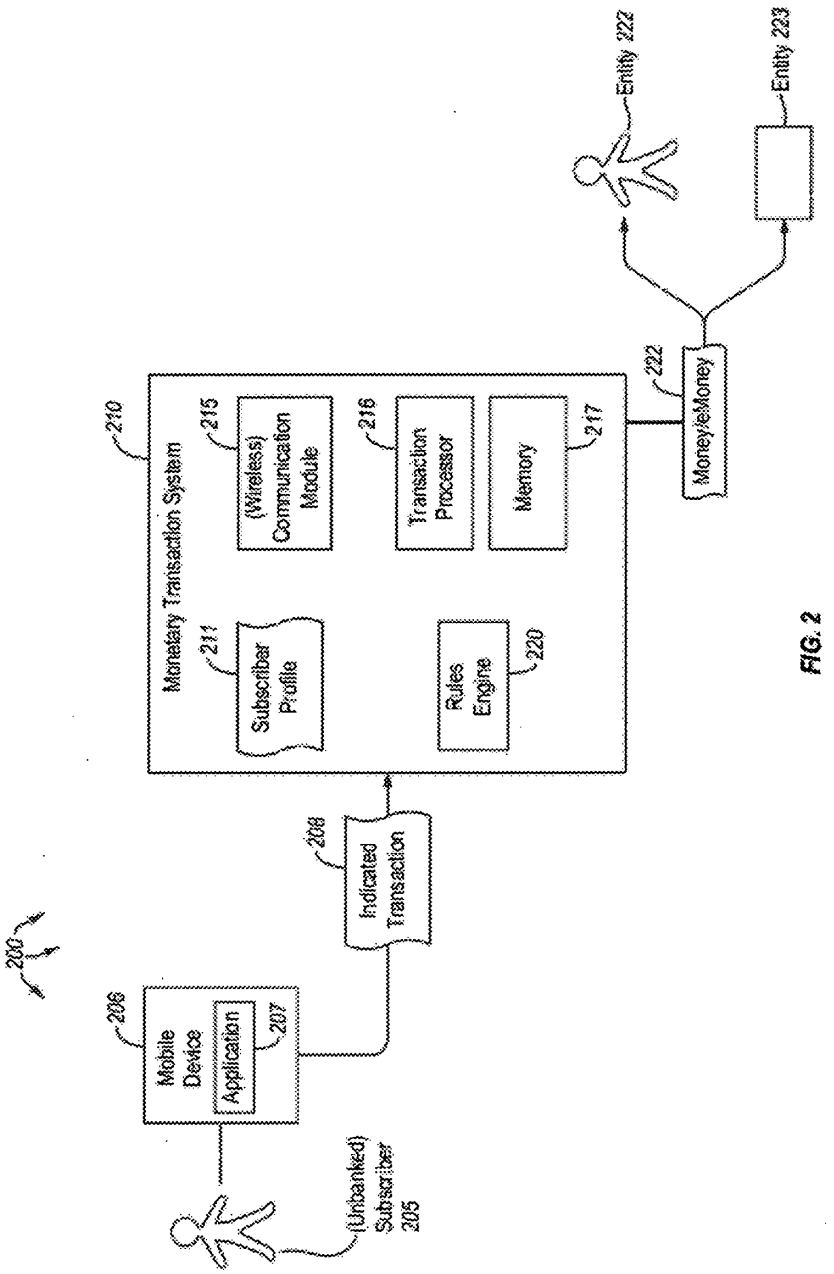


FIG. 2

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 35 of 381

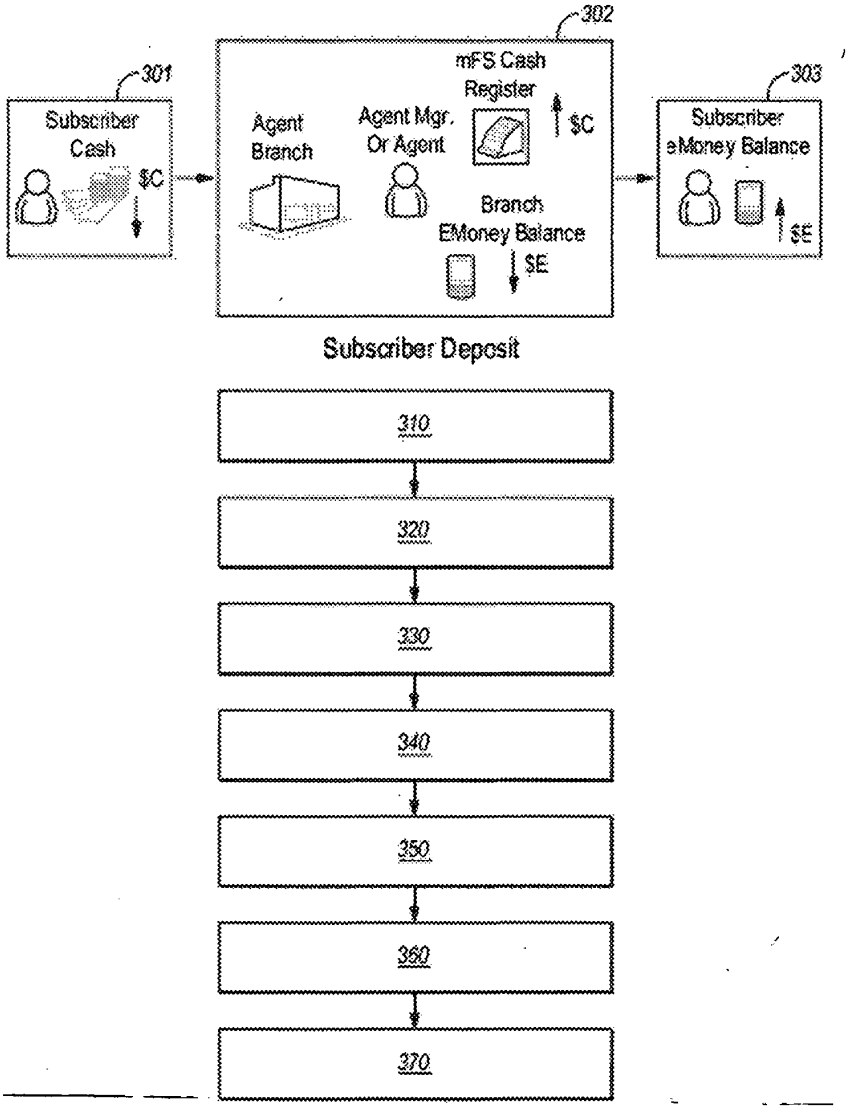
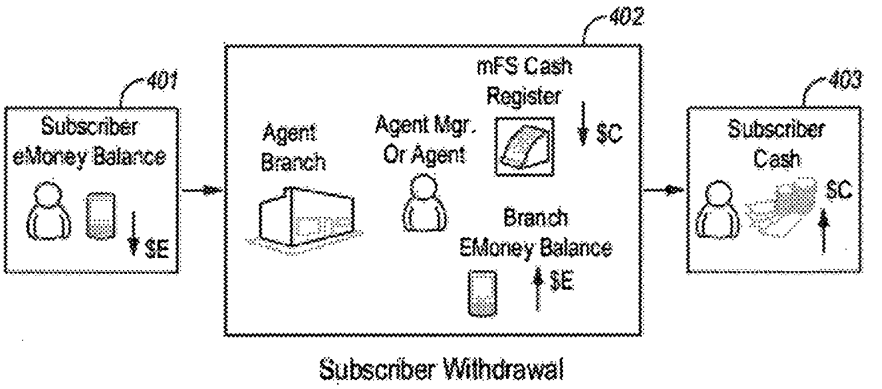

302
301
303
Subscriber Cash
$C
Agent Branch
Agent Mgr. Or Agent
mFS Cash Register
$C
Branch EMoney Balance
$E
Subscriber eMoney Balance
$E
Subscriber Deposit
310
320
330
340
350
360
370

FIG. 3


402
401
403
Subscriber eMoney Balance
$E
Agent Branch
Agent Mgr. Or Agent
mFS Cash Register
$C
Branch EMoney Balance
$E
Subscriber Cash
$C
Subscriber Withdrawal

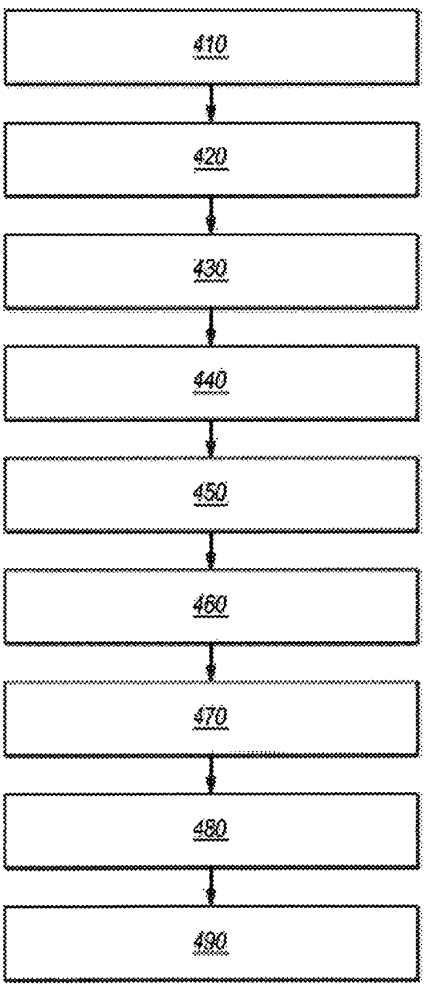
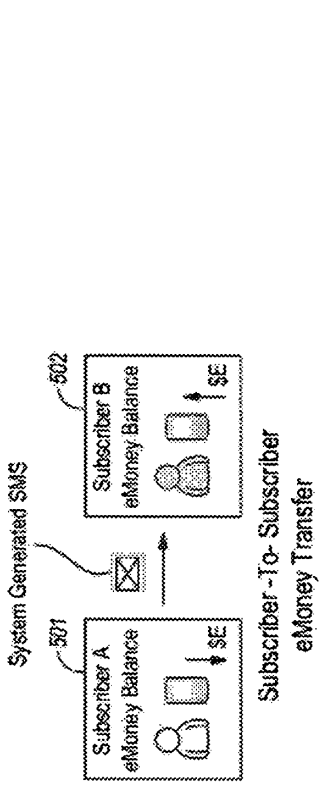
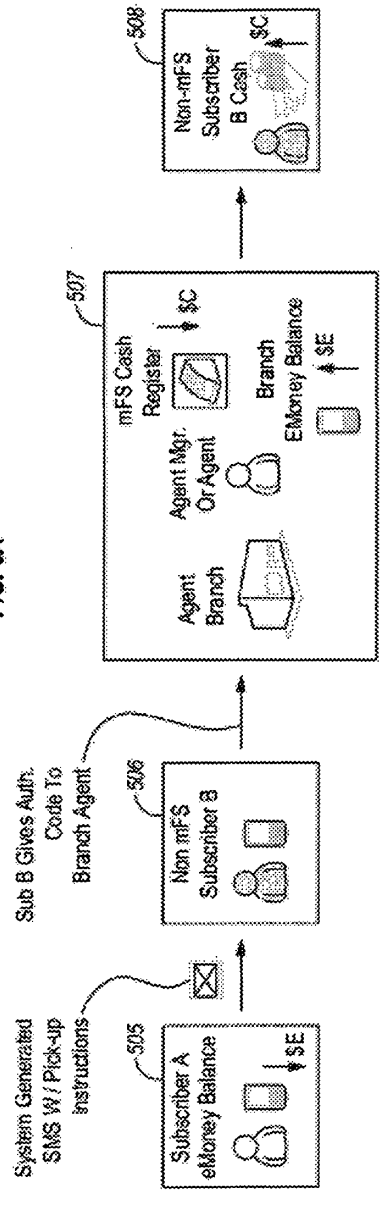

410
420
430
440
450
460
470
480
490

FIG. 4



Subscriber -To- Subscriber
eMoney Transfer

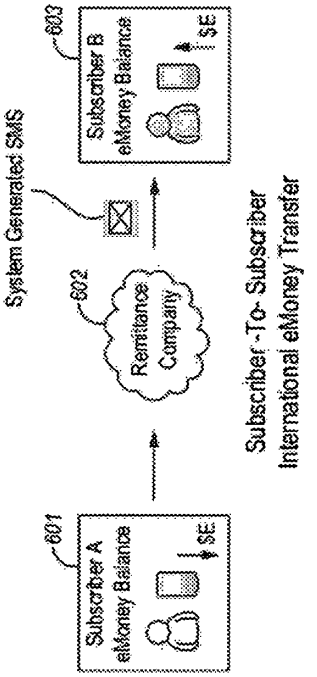
FIG. 5A



Subscriber -To- Non Subscriber
eMoney Transfer

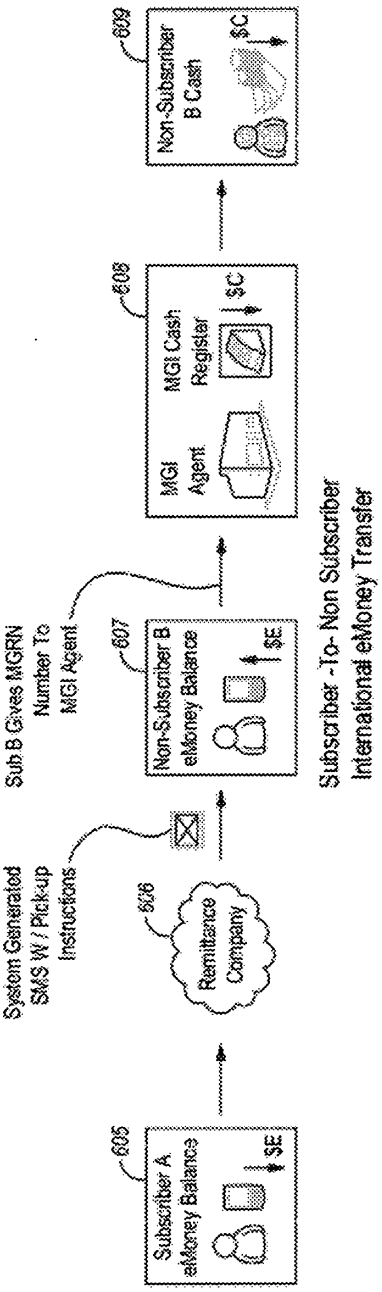
FIG. 5B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 38 of 381



Subscriber -To- Subscriber International eMoney Transfer

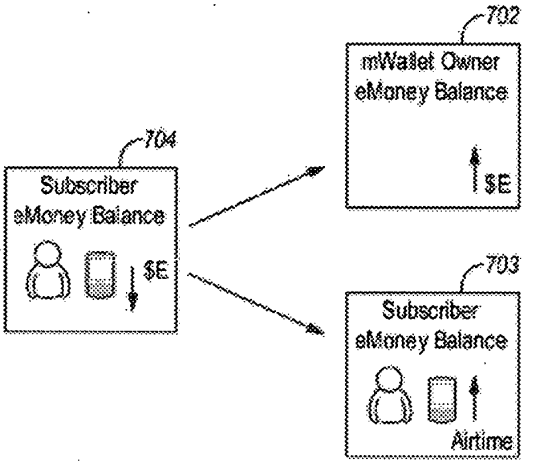
FIG. 6A



Subscriber -To- Non Subscriber International eMoney Transfer

FIG. 6B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 39 of 381



Subscriber Buys Airtime

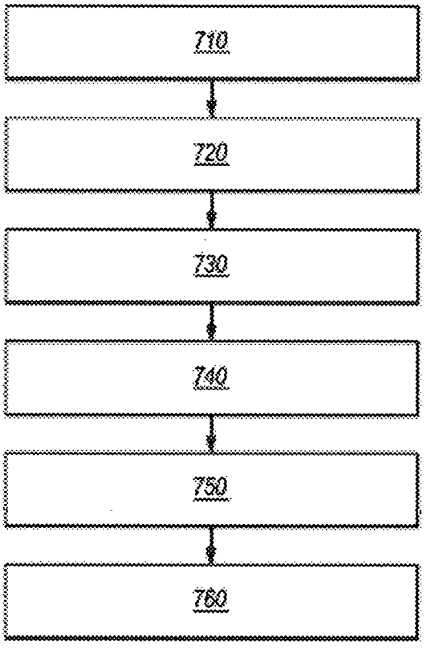
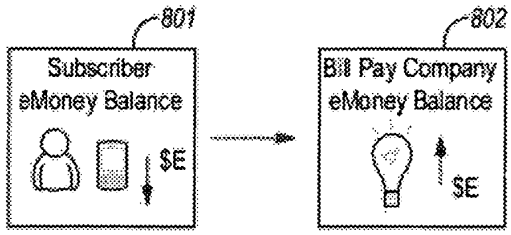


FIG. 7



Subscriber Pays Bill

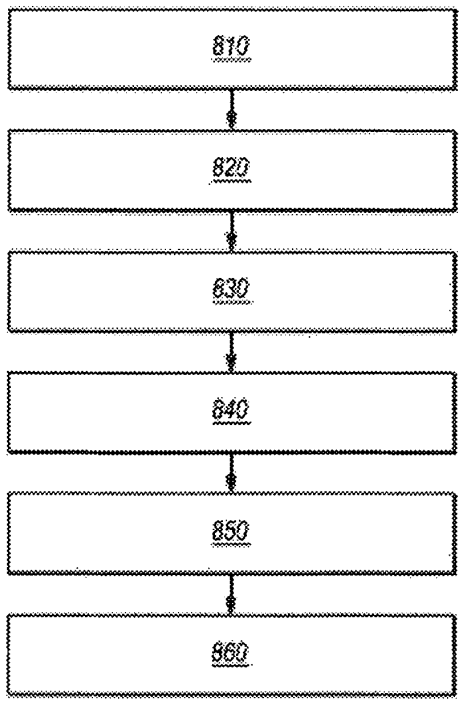
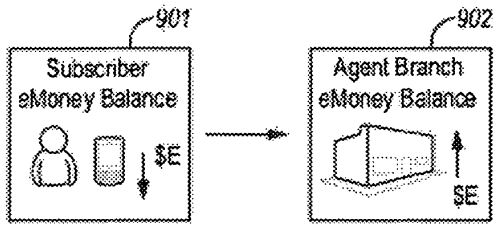


FIG. 8



Subscriber Makes Retail Purchase

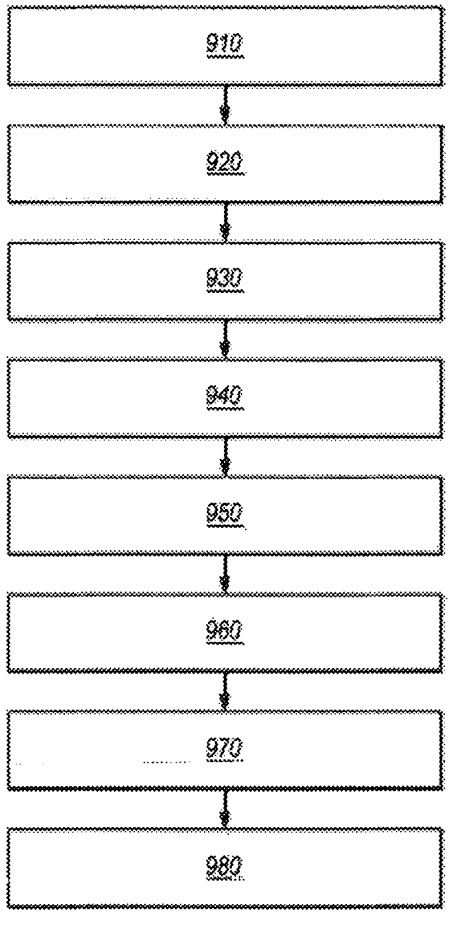
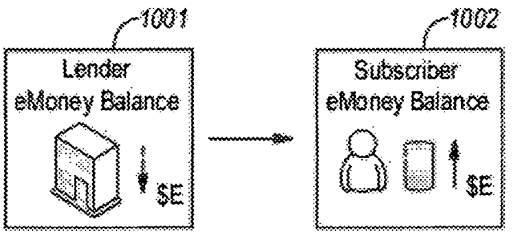
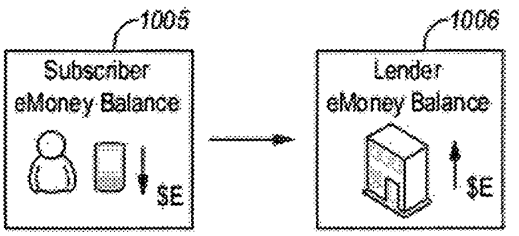


FIG. 9



Subscriber Requests Micro-Loan

FIG. 10A



Subscriber Repays Micro-Loan

FIG. 10B

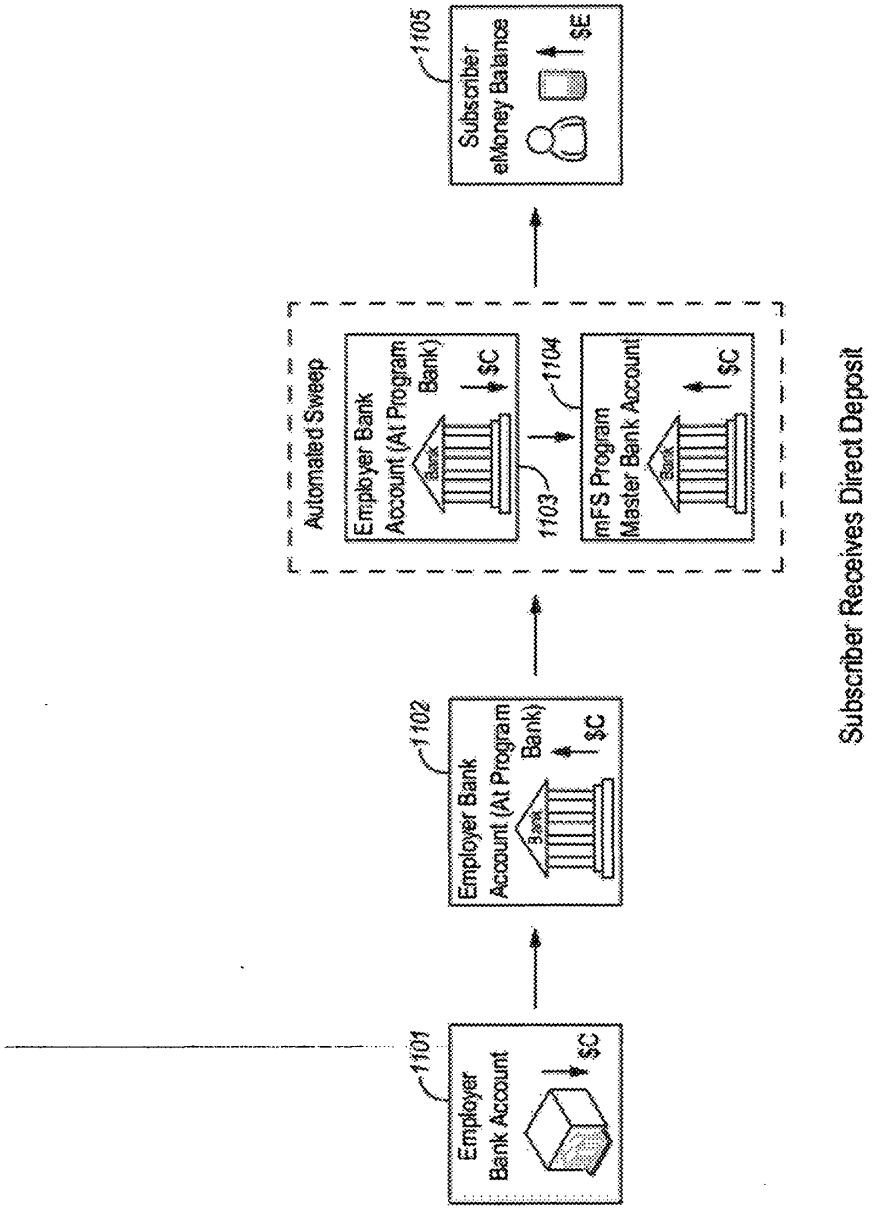
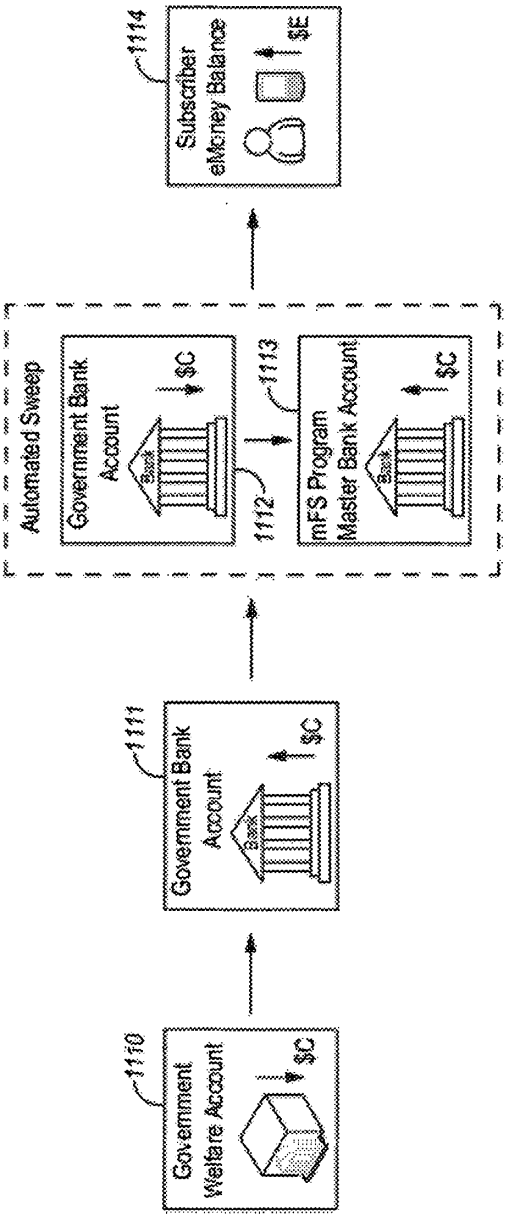


FIG. 11A

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 44 of 381



Subscriber Receives Government Welfare Payment

FIG. 11B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 45 of 381

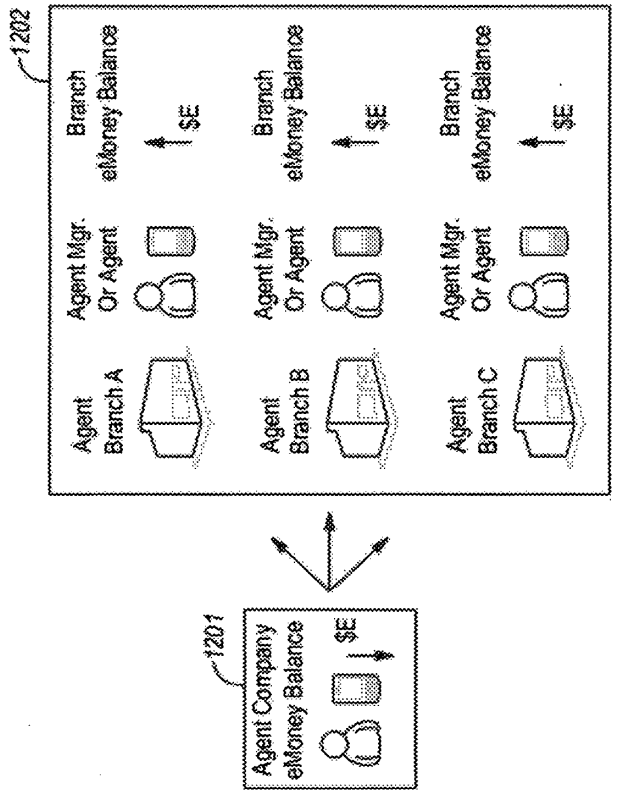


FIG. 12A

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 46 of 381

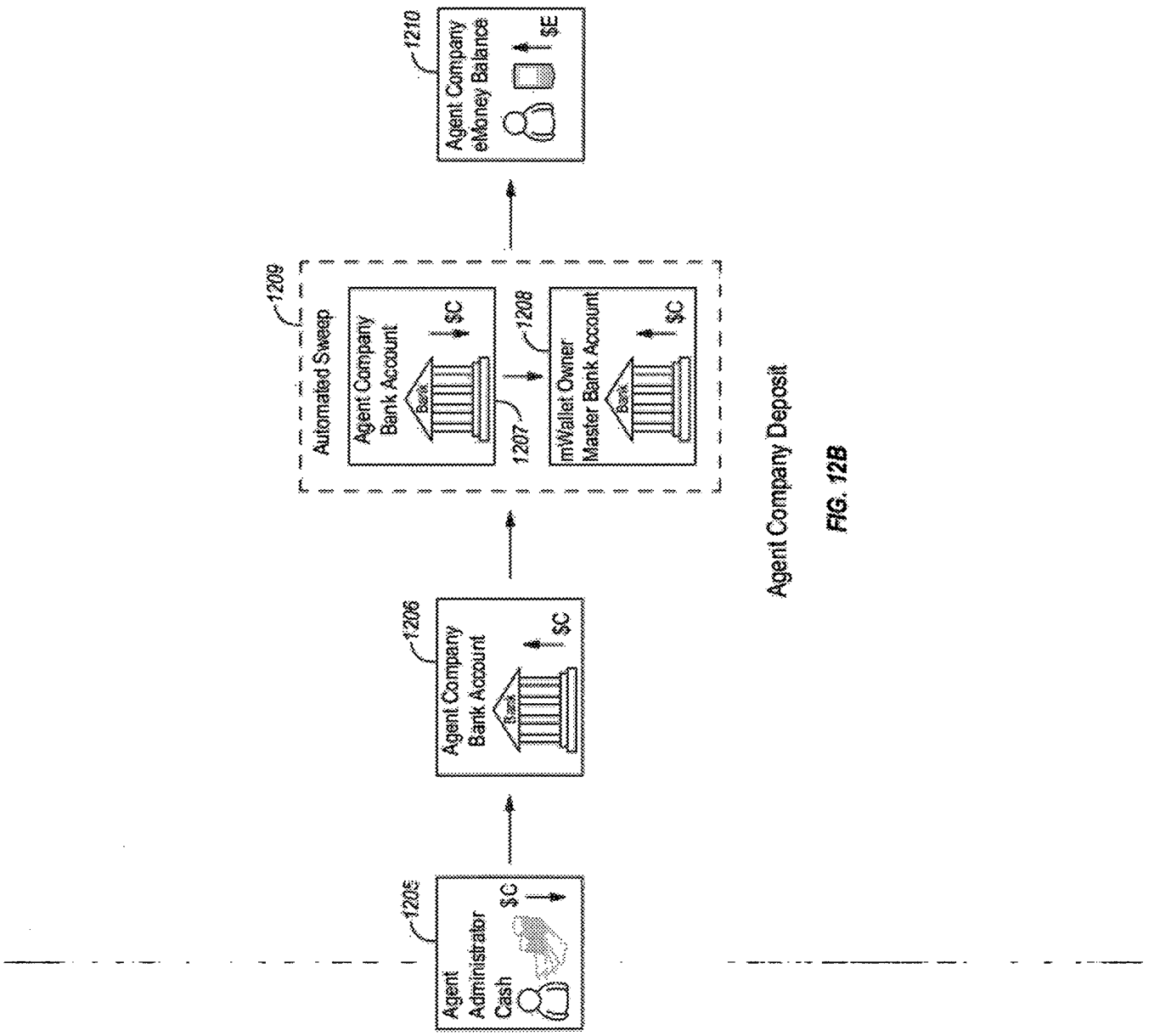
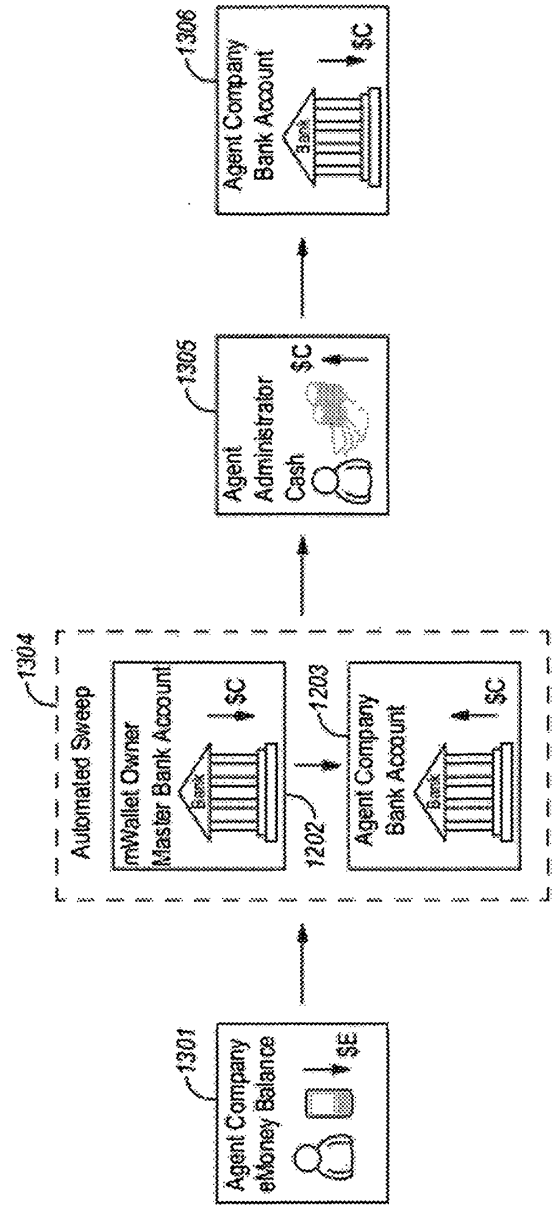


FIG. 12B

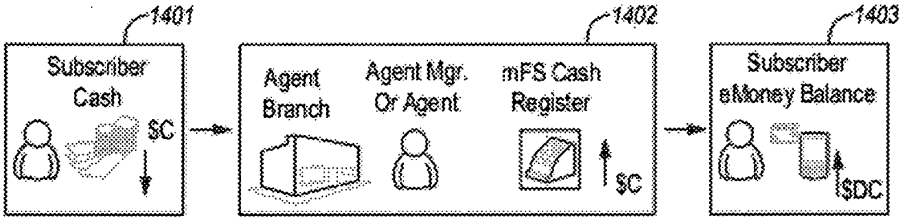
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 47 of 381



Agent Company Withdrawal

FIG. 13

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 48 of 381



Subscriber Deposit At Agent Branch

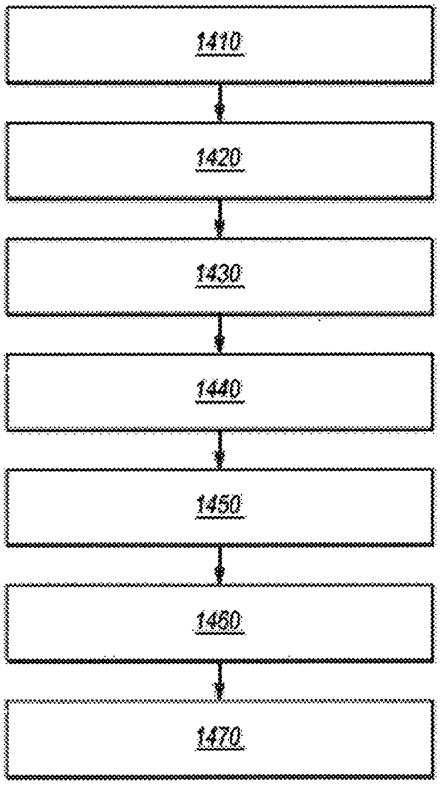


FIG. 14

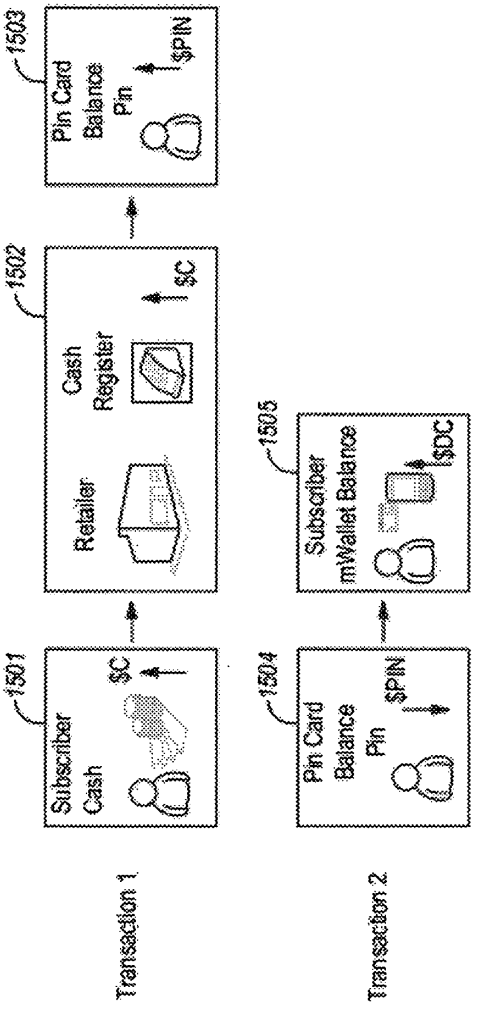
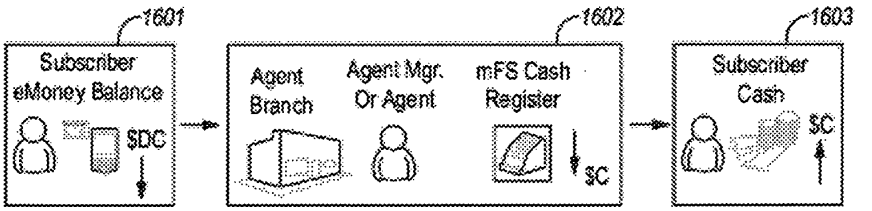


FIG. 15

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 50 of 381



Subscriber Withdrawal (Agent)

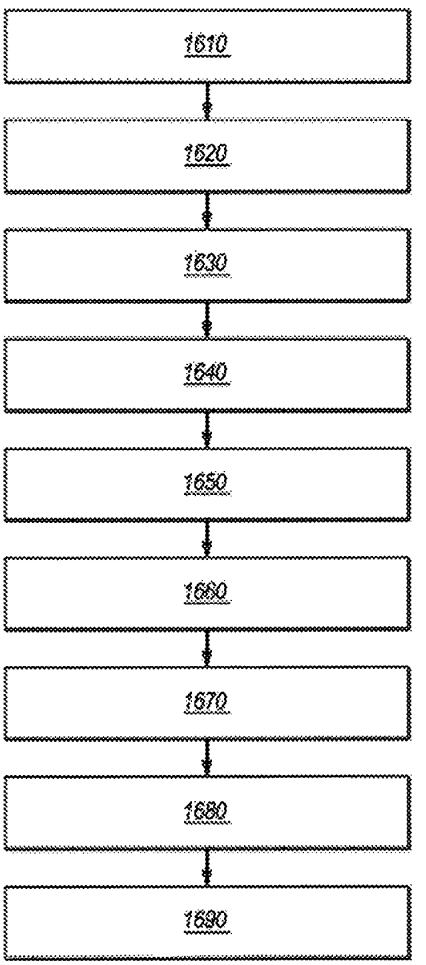
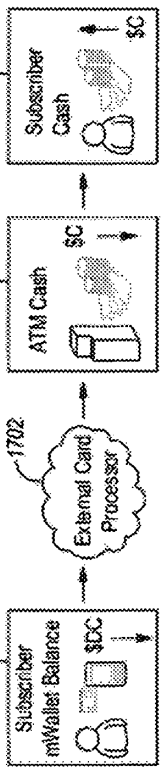
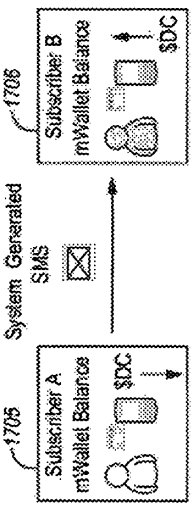


FIG. 16



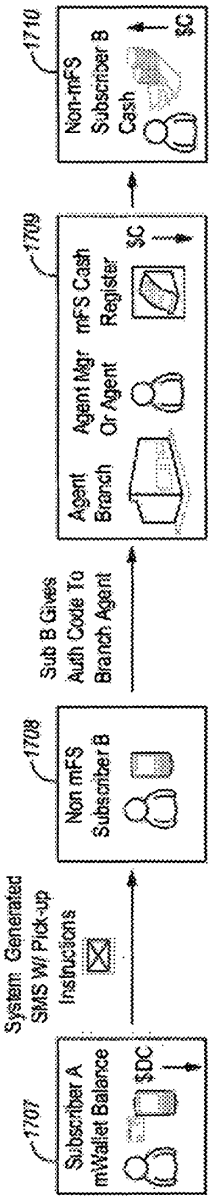
Subscriber Withdrawal (ATM)

FIG. 17A



Subscriber To Subscriber Money Transfer

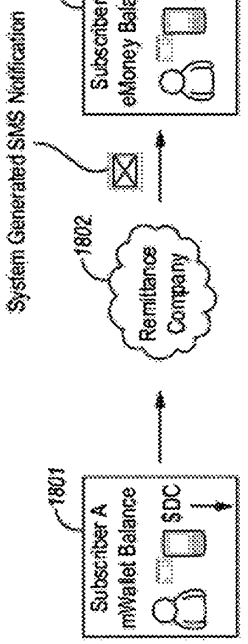
FIG. 17B



Subscriber To Non-Subscriber Money Transfer

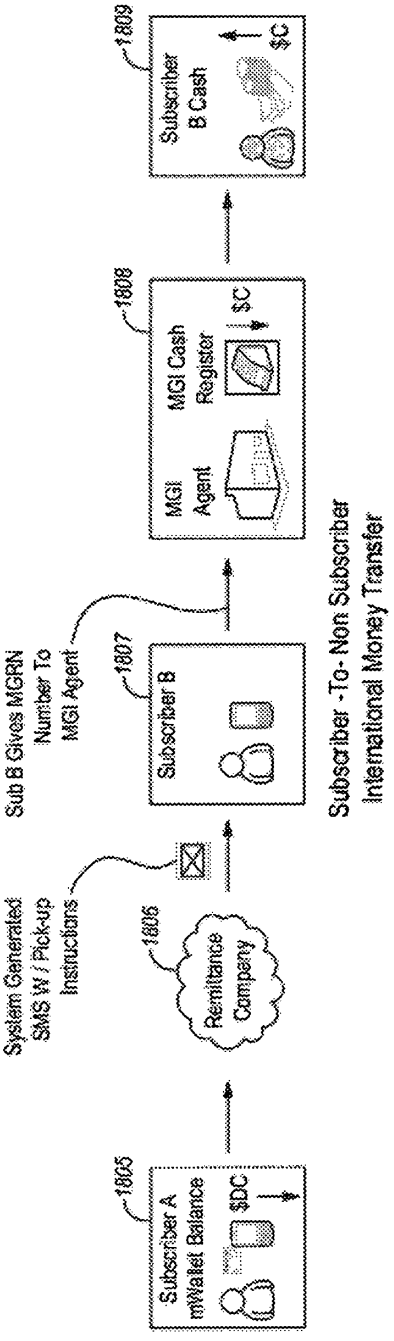
FIG. 17C

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 52 of 381



Subscriber -To- Subscriber
International Money Transfer

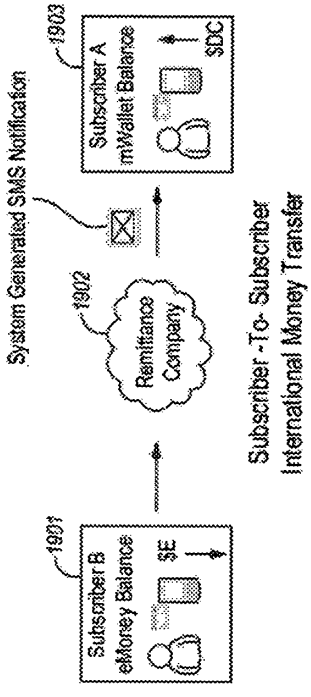
FIG. 18A



Subscriber -To- Non Subscriber
International Money Transfer

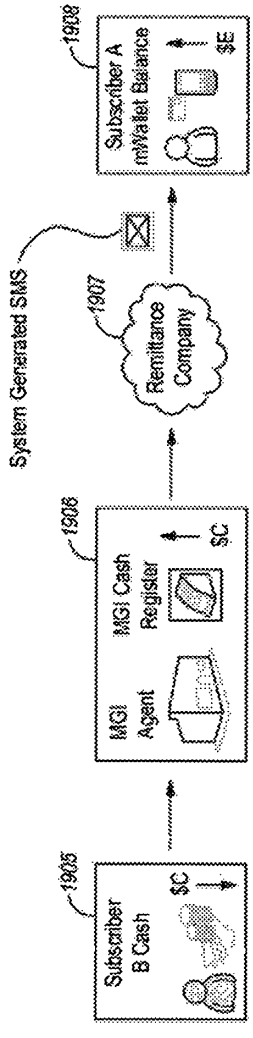
FIG. 18B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 53 of 381



Subscriber -To- Subscriber International Money Transfer

FIG. 19A



Non-Subscriber -To- Subscriber International Money Transfer

FIG. 19B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 54 of 381

MONETARY TRANSACTION SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to and the benefit of U.S. Provisional Application Ser. No. 61/522,099, filed on Aug. 10, 2011, entitled "Mobile Wallet Platform", and also claims priority to and the benefit of U.S. Provisional Application Ser. No. 61/493,064, filed on Jun. 3, 2011, entitled "Mobile Wallet Platform". Both of the aforementioned provisional applications are incorporated by reference in their entirety herein.

BACKGROUND

Mobile phones and other digital devices have become increasingly popular in recent years. Many mobile device users use their devices to perform countless different daily tasks. For instance, mobile devices allow users to check email, send and receive instant messages, check calendar items, take notes, set up reminders, browse the internet, play games or perform any number of different things using specialized applications or "apps". These applications allow mobile devices to communicate with other computer systems and perform a wide variety of network-connected tasks previously not possible with a mobile device.

BRIEF SUMMARY

Embodiments described herein are directed to monetary transaction system for conducting monetary transactions between transaction system subscribers and other entities. In one embodiment, the monetary transaction system includes a mobile device configured to run a monetary transaction system application. The monetary transaction system also includes a monetary transaction system subscriber that has a profile with the system. The subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system. The system further includes a monetary transaction system processor that performs the transactions specified by the subscriber. Performing these transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile.

The monetary transaction system also includes at least one entity that is to be involved in the specified transaction, where the entity has a profile with the monetary transaction system. This entity may be a person, a retail store, an agent or other entity. The subscriber may have access to a bank account, or may be an "unbanked user" that does not have access to a bank account. Each of the terms included above will be described in greater detail below in conjunction with the drawings.

The monetary transaction system may be used for many different tasks including enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a mobile wallet, adding a debit or credit card account to a mobile wallet, depositing funds in a mobile wallet, withdrawing funds from a mobile wallet, paying bills from a mobile wallet, topping up a prepaid mobile account through a mobile wallet, transferring funds through a mobile wallet (nationally or internationally), making in-store purchases using a mobile wallet, and various other tasks as described herein below.

This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

Additional features and advantages will be set forth in the description which follows, and in part will be apparent to one of ordinary skill in the art from the description, or may be learned by the practice of the teachings herein. Features and advantages of embodiments described herein may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. Features of the embodiments described herein will become more fully apparent from the following description and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

To further clarify the above and other features of the embodiments described herein, a more particular description will be rendered by reference to the appended drawings. It is appreciated that these drawings depict only examples of the embodiments described herein and are therefore not to be considered limiting of its scope. The embodiments will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

FIG. **1** illustrates a monetary transaction system architecture in which embodiments described herein may operate.

FIG. **2** illustrates an alternate example embodiment of a monetary transaction system.

FIG. **3** illustrates an example data flow for performing a subscriber deposit via a mobile wallet.

FIG. **4** illustrates an example data flow for performing a subscriber withdrawal via a mobile wallet.

FIGS. **5**A and **5**B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber eMoney transfers via a mobile wallet, respectively.

FIGS. **6**A and **6**B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber international eMoney transfers via a mobile wallet, respectively.

FIG. **7** illustrates an example data flow for performing a subscriber airtime purchase via a mobile wallet.

FIG. **8** illustrates an example data flow for performing a subscriber-initiated bill pay via a mobile wallet.

FIG. **9** illustrates an example data flow for performing a subscriber-initiated retail purchase via a mobile wallet.

FIGS. **10**A and **10**B illustrate example data flows for requesting and repaying micro-loans via a mobile wallet, respectively.

FIG. **11**A illustrates an example data flow of a subscriber receiving a direct deposit via a mobile wallet.

FIG. **11**B illustrates an example data flow of a subscriber receiving a governmental welfare payment via a mobile wallet.

FIG. **12**A illustrates an example data flow of an agent administrator distributing eMoney via a mobile wallet.

FIG. **12**B illustrates an example data flow of an agent company making a deposit using a mobile wallet.

FIG. **13** illustrates an example data flow of an agent company making a withdrawal using a mobile wallet.

FIG. **14** illustrates an example data flow of a subscriber making a deposit at an agent branch using a mobile wallet.

FIG. **15** illustrates an example data flow of a subscriber making a deposit with a non-agent using a mobile wallet.

FIG. **16** illustrates an example data flow of a subscriber making a withdrawal with an agent using a mobile wallet.

FIG. **17**A illustrates an example data flow of a subscriber making a withdrawal from an ATM using a mobile wallet.

FIG. **17**B illustrates an example data flow of a subscriber-to-subscriber money transfer using a mobile wallet.

FIG. **17**C illustrates an example data flow of a subscriber-to-non-subscriber money transfer using a mobile wallet.

FIG. **18**A illustrates an example data flow of a subscriber-to-subscriber international money transfer using a mobile wallet.

FIG. **18**B illustrates an example data flow of a subscriber-to-non-subscriber international money transfer using a mobile wallet.

FIG. **19**A illustrates an example data flow of a subscriber-to-subscriber international money transfer using a mobile wallet.

FIG. **19**B illustrates an example data flow of a non-subscriber-to-subscriber international money transfer using a mobile wallet.

DETAILED DESCRIPTION

Embodiments described herein are directed to monetary transaction system for conducting monetary transactions between transaction system subscribers and other entities. In one embodiment, the monetary transaction system includes a mobile device configured to run a monetary transaction system application. The monetary transaction system also includes a monetary transaction system subscriber that has a profile with the system. The subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system. The system further includes a monetary transaction system processor that performs the transactions specified by the subscriber. Performing these transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile.

The monetary transaction system also includes at least one entity that is to be involved in the specified transaction, where the entity has a profile with the monetary transaction system. This entity may be a person, a retail store, an agent or other entity. The subscriber may have access to a bank account, or may be an "unbanked user" that does not have access to a bank account. Each of the terms included above will be described in greater detail below in conjunction with the drawings.

The monetary transaction system may be used for many different tasks including enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a mobile wallet, adding a debit or credit card account to a mobile wallet, depositing funds in a mobile wallet, withdrawing funds from a mobile wallet, paying bills from a mobile wallet, topping up a prepaid mobile account through a mobile wallet, transferring funds through a mobile wallet (nationally or internationally), making in-store purchases using a mobile wallet, and various other tasks as described herein below.

The following discussion now refers to a number of methods and method steps or acts that may be performed. It should be noted, that although the method steps may be discussed in a certain order or illustrated in a flow chart as occurring in a particular order, no particular ordering is necessarily required unless specifically stated, or required because a step is dependent on another step being completed prior to the step being performed.

Embodiments of the mobile transaction system or "mobile wallet platform" described herein may comprise or utilize a special purpose or general-purpose computer including computer hardware, such as, for example, one or more processors and system memory, as discussed in greater detail below. Embodiments described herein also include physical and other computer-readable media for carrying or storing computer-executable instructions and/or data structures. Such computer-readable media can be any available media that can be accessed by a general purpose or special purpose computer system. Computer-readable media that store computer-executable instructions in the form of data are computer storage media. Computer-readable media that carry computer-executable instructions are transmission media. Thus, by way of example, and not limitation, embodiments described herein can comprise at least two distinctly different kinds of computer-readable media: computer storage media and transmission media.

Computer storage media includes RAM, ROM, EEPROM, CD-ROM, solid state drives (SSDs) that are based on RAM, Flash memory, phase-change memory (PCM), or other types of memory, or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store desired program code means in the form of computer-executable instructions, data or data structures and which can be accessed by a general purpose or special purpose computer.

A "network" is defined as one or more data links and/or data switches that enable the transport of electronic data between computer systems and/or modules and/or other electronic devices. When information is transferred or provided over a network (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a transmission medium. Transmission media can include a network which can be used to carry data or desired program code means in the form of computer-executable instructions or in the form of data structures and which can be accessed by a general purpose or special purpose computer. Combinations of the above should also be included within the scope of computer-readable media.

Further, upon reaching various computer system components, program code means in the form of computer-executable instructions or data structures can be transferred automatically from transmission media to computer storage media (or vice versa). For example, computer-executable instructions or data structures received over a network or data link can be buffered in RAM within a network interface module (e.g., a network interface card or "NIC"), and then eventually transferred to computer system RAM and/or to less volatile computer storage media at a computer system. Thus, it should be understood that computer storage media can be included in computer system components that also (or even primarily) utilize transmission media.

Computer-executable (or computer-interpretable) instructions comprise, for example, instructions which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. The computer executable instructions may be, for example, binaries, intermediate format instructions such as assembly language, or even source code. Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the

appended claims is not necessarily limited to the described features or acts described above. Rather, the described features and acts are disclosed as example forms of implementing the claims.

Those skilled in the art will appreciate that various embodiments may be practiced in network computing environments with many types of computer system configurations, including personal computers, desktop computers, laptop computers, message processors, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, mobile telephones, PDAs, tablets, pagers, routers, switches, and the like. Embodiments described herein may also be practiced in distributed system environments where local and remote computer systems that are linked (either by hardwired data links, wireless data links, or by a combination of hardwired and wireless data links) through a network, each perform tasks (e.g. cloud computing, cloud services and the like). In a distributed system environment, program modules may be located in both local and remote memory storage devices.

In this description and the following claims, "cloud computing" is defined as a model for enabling on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). The definition of "cloud computing" is not limited to any of the other numerous advantages that can be obtained from such a model when properly deployed.

For instance, cloud computing is currently employed in the marketplace so as to offer ubiquitous and convenient on-demand access to the shared pool of configurable computing resources. Furthermore, the shared pool of configurable computing resources can be rapidly provisioned via virtualization and released with low management effort or service provider interaction, and then scaled accordingly.

A cloud computing model can be composed of various characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service, and so forth. A cloud computing model may also come in the form of various service models such as, for example, Software as a Service ("SaaS"), Platform as a Service ("PaaS"), and Infrastructure as a Service ("IaaS"). The cloud computing model may also be deployed using different deployment models such as private cloud, community cloud, public cloud, hybrid cloud, and so forth. In this description and in the claims, a "cloud computing environment" is an environment in which cloud computing is employed.

Additionally or alternatively, the functionally described herein can be performed, at least in part, by one or more hardware logic components. For example, and without limitation, illustrative types of hardware logic components that can be used include Field-programmable Gate Arrays (FPGAs), Program-specific Integrated Circuits (ASICs), Program-specific Standard Products (ASSPs), System-on-a-chip systems (SOCs), Complex Programmable Logic Devices (CPLDs), and other types of programmable hardware.

Still further, system architectures described herein can include a plurality of independent components that each contribute to the functionality of the system as a whole. This modularity allows for increased flexibility when approaching issues of platform scalability and, to this end, provides a variety of advantages. System complexity and growth can be managed more easily through the use of smaller-scale parts with limited functional scope. Platform fault tolerance is enhanced through the use of these loosely coupled modules. Individual components can be grown incrementally as business needs dictate. Modular development also translates to decreased time to market for new functionality. New functionality can be added or subtracted without impacting the core system.

Various terminology will be used herein to describe the monetary transaction system (also referred to as a "mobile wallet platform", "mobile wallet program" or "mobile wallet transaction system"). The term "agent" is used to refer to an individual with mobile financial services (mFS) transaction system tools and training to support specific mFS functions. These mFS functions include subscriber registration and activation, and the deposit and withdrawal of funds from the mFS transaction system. Agents are representatives of the mFS transaction system or "program". Agents can be employees or contractors of the program provider, or other companies and organizations that partner with the program provider to provide these services themselves. Agents may be found in every facet of a typical economy, and may include large retailers, mobile network operators (MNO) airtime sales agents, gas stations, kiosks, or other places of business.

The mobile wallet platform includes a mobile wallet application, web interface or some other type of functionality that allows the user to interact with the mFS platform using their mobile device. The mobile wallet application may include a subscriber identity module (SIM) application, an Unstructured Supplementary Service Data (USSD) application, a smartphone application, a web application, a mobile web application, a Wireless Application Protocol (WAP) application, a Java 2 Platform, Micro Edition (J2ME) application, a tablet application or any other type of application or interface that provides tools for the agent to register, activate, and offer other services to the mFS subscriber.

As used herein, a mobile wallet application is a mobile wallet application installed on a SIM card. A USSD application is an application that implements USSD for various functionality including prepaid callback service, location-based content services, menu-based information services and other mobile wallet platform services. A web application is one that implements or uses the internet to provide mobile wallet platform functionality. A mobile web application is similar to a web application, but is tailored for mobile devices. A WAP application is one that uses the wireless application protocol to communicate with the mobile wallet platform to provide the platform's functionality. A J2ME application is an application developed in Java and is designed to provide mobile wallet functionality on a variety of different hardware. A tablet application is an application specifically designed for a touchscreen-based tablet that provides mobile wallet platform functionality for tablet devices, and as part of configuring the phone on the network. Any of these applications (or any combination thereof) may be provided on the user's mobile device. This functionality can also be made available on a retail point of sale (POS) system or web site.

The term "agent administrator" refers to an individual with mFS program tools and training to administrate the allocation of funds to agent branches (e.g. retail locations). As agents perform mFS transactions with subscribers, such as depositing and withdrawing money, the agents are adding and removing money from their own accounts. If there are insufficient funds in the agent's account to complete a transaction, additional money will need to be transferred from the agent company's master account to that agent branch account to cover that transaction. An agent administrator is responsible for these funds transfers. Any of the applications referred to above may be configured to provide tools used by the agent administrator to view the agent company balance, view the agent branch balances, and transfer funds into and out of

agent branch mobile wallets. This functionality can also be made available on a website for easier access.

The term "agent administrator mobile wallet application" refers to a software program or application installed on the agent administrator's terminal in the agent administrator's mobile device (such as a mobile phone or tablet). This software application provides the agent administrator the ability to securely perform agent administrator functions such as querying the agent company account balance or transferring funds into and out of agent branch accounts. The agent administrator's mobile wallet application may be installed on a global system for mobile communications (GSM) SIM card (or on any other type of SIM card), and may be accessed using a GSM mobile phone. The agent administrator's application may also be installed on a code division multiple access (CDMA) mobile phone, a 3G, 4G, 4G LTE (Long Term Evolution) or other wireless carrier standard. The application may, additionally or alternatively, be installed directly on the agent administrator's mobile device. The application communicates with the mFS transaction system using binary and/or text short message service (SMS) messages. A wireless service provider or MNO provides the GSM SMS network infrastructure on which the mFS platform operates.

In some embodiments, the mFS platform application may utilize triple data encryption standard (3DES) encryption (or some other type of encryption), encrypted message signing, and password security on some or all of its communications with the mFS transaction system in order to ensure that the transactions are properly secured and authenticated.

The term "agent branch" refers to any location where an agent provides support for subscriber services of the mFS platform. Funds are allocated by the agent administrator from the agent company's main account to each agent branch to fund the subscriber mFS functions such as depositing or withdrawing cash, in-store purchases, bill payments, prepaid airtime top-ups and money transfers. In some cases, multiple agents may work in a single branch. However, at least in some cases, monetary funds are allocated to from the agent company's main account on a per branch basis.

The term "agent branch account balance" refers to the amount of money residing in a particular agent branch account at a given time. Funds can be deposited into the branch account by the agent administrator, or the funds can come from participating in subscriber mFS transactions such as depositing or withdrawing cash from the subscriber's mobile wallet accounts, or making retail purchases with the mobile wallet.

Each agent branch is to maintain a balance in their branch account. This applies more strongly in countries where mFS program and financial services infrastructure is still developing. In cases where real-time processing of financial transactions including card processing is not practical, subscribers leverage the applications on their mobile phones to submit transactions and conduct business with retailers, businesses, and other subscribers. The mFS platform manages the balance of mobile wallet accounts for each subscriber as value is transferred from one mobile wallet to another (e.g. from a subscriber's mobile wallet to an agent's mobile wallet in payment for goods or services). This value is referred to herein as "eMoney".

As subscribers conduct business with mFS agents, they deposit or withdraw cash from their mobile wallet accounts. Virtual or eMoney credits are transferred between the subscriber's mobile wallet account and the agent branch's account as a form of currency to support the transaction. As agents accept cash into their cash register by mFS subscribers, they transfer the equivalent amount of eMoney credits into the mFS subscriber's mobile wallet account. For instance, if an mFS subscriber gives an mFS agent $10 to deposit into the subscriber's mobile wallet account, the agent would place the cash into his register and transfer $10 from the agent branch's eMoney account into the subscriber's mobile wallet account. While the agent acquired $10 in his register, he transferred out $10 of eMoney credits from his branch eMoney account.

In some embodiments, in countries with more developed economies, it may be beneficial to use program-issued prepaid debit cards, pre-paid access accounts, stored value accounts or gift cards to conduct business along with the added convenience of card processing networks such as Cirrus, STAR, or Visa for POS and automated teller machine (ATM) functionality. Agents, particularly those in retail outlets and kiosks, can still support subscribers with deposits, withdrawals, and other transfers, but in this case bank external card processors manage the mobile wallet and branch account balances and provide the real-time transfer of funds.

The term "agent branch ledger" refers to a written (or electronic) ledger maintained by the mFS platform. Agent branch transactions are performed on the agent's and subscriber's mobile phones where an electronic record of the transaction is generated and stored on the mFS platform. These electronic transactions are then reconciled with agent branch ledgers to ensure the security and integrity of the transaction. Agent branch ledgers are printed or electronic transaction logs that are distributed to the agent branch locations in hard copy form to serve as a backup record to the electronic transactions.

The term "agent company" refers to a business that registers to participate in the mFS program as a partner of the mFS program provider or owner. The agent company has one or more agent branches which conduct mFS business with mFS program subscribers. In some cases, the agent company may be referred to as a distributor or retailer.

The term "agent company account balance" refers to the sum of the funds deposited at a "partner bank" (defined below) by the agent company to fund the agent company's daily transactions. The funds in the agent company account are then distributed to agent branches by the agent company's agent administrator to conduct everyday business such as accepting cash deposits and cash withdrawals from mFS subscribers. This balance is sometimes referred to as the "agent company float".

An "agent manager" is a supervisor of company agents for a given company. The agent manager has the training and tools to create, delete or modify agent accounts for a company, as well as monitor the transactions performed by agents. The agent manager may have a special application or an increased level of rights to access applications features not available to other users. The special application is a program installed on the agent manager's terminal. This application provides the agent manager the ability to securely perform agent manager functions such as registering and activating new agent accounts.

The mFS agent manager application may be installed on any terminal or device. It communicates with the mFS platform using binary and/or text SMS messages. A wireless service provider or MNO provides the GSM SMS network infrastructure on which the mFS platform operates. The mFS platform mobile wallet applications may utilize 3DES encryption (or any other type of encryption), encrypted message signing, and password security on some or all of its communications with the mFS platform in order to ensure that the transactions are properly secured and authenticated.

The term "agent application" refers to an application that provides all the tools necessary for an agent to register, activate, and offer other services to the mFS subscriber. The agent application is a program installed on the agent's SIM card or otherwise installed in the agent's mobile device's memory. This application provides the agent the ability to securely perform agent functions such as registering and activating new subscribers and depositing and withdrawing funds from mobile wallet accounts. The mFS agent application may be installed on a GSM SIM card or mobile phone and may be accessed using a GSM or CDMA mobile phone. A wireless service provider or MNO provides the data and SMS network infrastructure on which the mFS platform operates.

The terms "mFS platform", "mobile wallet platform" and "monetary transaction system" refer to an overall platform or ecosystem of different components that work together to provide the various functions described herein on a global scale. At least some of the various logic components include the following: the application. The "mobile wallet application" or "mFS application" manages the processing of incoming transactions regardless of their source. The application handles end-user authentication, transaction processing, subscriber profile management, and further manages interactions between the various platform components.

The mFS platform further includes a transaction processor. This component is used when the mFS application is implemented in a country where real-time processing of financial transactions is not practical (or not possible). The transaction processor manages the balance of mobile wallet accounts, agent accounts, and the accounts of any other program participant. The transaction processor handles balance inquiries, credits, debits, and transaction roll-backs.

The mFS platform further includes a rules engine that manages and applies the rules and policy that are defined for transactions as they are processed on the mFS platform. Rules impact transaction fees, limits, velocity limits, and commissions as well as program actor roles and permissions. Rules can be customized for each implementation. The mFS platform also includes an integration interface that manages the integration and interaction between external systems (i.e. external to the mFS platform) and the mFS platform. Connectivity to the wireless service provider's pre-paid airtime billing platform and the program partner bank, for example, are managed by the integration interface.

The mFS platform further includes a transaction database that stores the data that supports the mFS platform. This includes subscriber profiles and subscription data, transaction data and logs, and application configuration and run-time data, among other types of data. Another component of the mFS platform is a handset support service that interfaces with the wireless service provider's SMS network to allow communication between the mobile wallet applications and the back-office systems via SMS messaging or some other form of data transfer. Still further, another component of the mFS platform is a web component that provides a web interface to the mFS program participants that allows the subscriber to perform the same functions in the web interface that they would have available through their applications.

The term "bill pay company" refers to a business that signs-up to participate in the mFS transaction system. As a participant in the mFS transaction system, the company accepts payment from mFS mobile wallet accounts, either in the form of eMoney or through periodic settlements.

At least in some embodiments, financial transactions that take place in the mFS mobile wallet platform are funded through pre-paid mobile wallet accounts. Mobile wallet platform subscribers can deposit cash into their mobile wallet account through a process referred to herein as 'cash-in'. The cash-in process is supported by mFS agents at agent branch locations. The agent accepts the cash from the subscriber and transfers the equivalent amount of eMoney to the subscriber's mobile wallet account. This process is similar to withdrawing cash from a bank account.

As mentioned above, in some embodiments, financial transactions that take place in the mobile wallet platform are funded through pre-paid mobile wallet accounts. Mobile wallet platform subscribers can withdraw cash from their mobile wallet account through a process known as "cash-out". The cash-out process is supported by mFS agents at agent branch locations. The subscriber transfers eMoney from their mobile wallet account to the agent's eMoney account. Upon receiving the eMoney, the agent gives the subscriber cash from their branch cash register.

Accounts managed on the mFS platform by the mFS eMoney transaction processor maintain the mobile wallet balance of mFS program participants including subscribers, agent branches, agent companies, and non-agent companies. eMoney is moved between Mobile Wallet accounts by the transaction processor based on mFS transaction processing. Only when transactions involving cash (i.e. depositing or withdrawing funds from the mFS program) or the movement of money from mFS participants to non-mFS program participants are funds moved from the master bank accounts.

As subscribers, agents, and other mFS program participants conduct business in the mFS program, value is transferred from one account to the next as payment for services rendered or goods purchased. This value can be in the form of real currency or the electronic representation referred to herein as eMoney.

Among other situations, eMoney is used in mFS implementations where the real-time processing of financial transactions including card processing is not practical. The mFS platform utilizes an internal transaction processor for managing the real-time balance of mobile wallet and agent accounts as value (eMoney) is transferred from one mobile wallet to another in payment for services.

As subscribers conduct business with mFS agents, they deposit or withdraw cash from their mobile wallet accounts. Virtual or eMoney credits are transferred between the subscriber mobile wallet accounts and the agent branch accounts as a form of currency to support the transaction. As agents accept cash into their cash register by mFS subscribers, they transfer the equivalent amount of eMoney credits into the mFS subscriber's mobile wallet account. For example, if an mFS subscriber gives an mFS agent $10 to deposit into the subscriber's mobile wallet account, the agent would place the cash into his or her register, and transfer $10 from the agent branch eMoney account into the subscriber's mobile wallet account. While the agent acquired $10 in his or her register, the agent transferred-out $10 of eMoney credits from his or her branch eMoney account. This will be explained in greater detail below.

In some embodiments, employers may wish to participate in the mFS program by allowing the direct deposit of paychecks into subscribers' mobile wallet accounts. Accordingly, each payday, the user's pay is directly transferred to the subscribers' mobile wallet.

The term "know your customer" or "KYC" refers to information collected about an individual that identifies that individual. Such information is used to establish a mobile wallet account with the mobile wallet platform. Regulatory requirements in some countries require that new bank account creation must be preceded by a display of a valid government ID. These KYC regulations may vary from country to country.

Accordingly, different KYC information may be requested from subscribers in different countries in order to establish a mobile wallet account.

The term micro-finance institution (MFI) refers to a lender that issues small loans. MFIs participating in the mFS program lend to mFS program subscribers and accept loan repayment either in the form of eMoney or settlements with the mFS platform provider.

The term "mFS program", like the term "mFS platform" refers to the ecosystem of companies, service providers, and subscribers that participate in providing mobile financial services to their customers. In some embodiments, there may be one mFS program implementation per country. Each program includes a program owner and operator, a program platform, a partner wireless services provider or MNO, and a partner bank.

The term "mFS program master account" refers to a bank account maintained by the mFS program partner bank to provide funds and float for the operation of the mFS platform. Depending on the type of mFS implementation, the master account can include sub-accounts for each of the agent branches and subscriber mobile wallets, giving the bank visibility into all transactions on a per-user basis. The mFS platform can also manage the balance of sub-accounts and interact with the bank's master account when funds need to be deposited or withdrawn from the account.

The term mobile network operator (MNO) refers to a provider of mobile phone service including basic voice, SMS, unstructured supplementary service data (USSD) and data service, and may also be referred to as a "wireless service provider".

The term "mobile wallet" or "mobile wallet account" refers to a stored value account or prepaid access account (PPA) that allows the owner (or "subscriber") to pay for goods and services on the mFS platform from his or her mobile wallet account. When the mFS eMoney transaction processor is used, the mobile wallet balance is maintained by the mFS platform and value is exchanged within the mFS program as eMoney. When the mFS platform is integrated to an external card processor, the mobile wallet utilizes funds from the subscriber's prepaid debit card and bank account to exchange value on the mFS platform.

The term "non-agent company" refers to a mFS program participant who accepts payments from mFS subscribers but does not provide the same services as mFS agent companies. Payment is accepted either in the form of eMoney or through periodic settlements with the mFS platform provider. Examples of non-agent companies include bill pay providers and micro-finance lenders.

The term "non-mFS subscribers" refers to unregistered users that participates in various use cases in the mFS program. Non-mFS subscribers can send money to or receive money from mFS subscribers through interaction with the mFS program agents or with international remittance providers.

The term "partner bank" refers to the primary bank participating in the mFS program. The partner bank is responsible for holding the mFS program master accounts that hold the funds for all mFS services and transactions. A "PIN" refers to a numeric password that may be required to perform a transaction via the mobile wallet application. A "transaction processor" refers to an application or service that manages the mFS program account balances. The transaction processor determines the amount of funds or eMoney is in a particular account at any given time, and manages account balances. Mobile transaction system requests to credit, debit, or view the balance of a particular mobile wallet or program account are handled by the transaction processor (in conjunction with other components of the mobile wallet platform).

The term "sub-accounts" refers to accounts that are maintained within the mFS platform or by an external card processor. A partner bank may elect to maintain a separate bank account for each subscriber and/or agent branch, or a single master account may be established that contains the funds for all of the subscriber mobile wallet and agent branch accounts (at least within a country or other geographical region). The balance of each individual user may be managed by the mFS transaction processor.

When using a master account, the bank is involved only in transactions that require the movement of funds external to the mFS program. For example, subscriber cash-in and cash-out transactions involve the addition and removal of cash from the mFS program and would consequently include a deposit or withdrawal from the master account. Retail purchases from participating mFS program retailers or the exchange of funds between mFS subscribers results in no net change in the mFS program balance and thus do not require involvement by the partner bank.

The term "subscriber" refers to a participant of the mFS mobile wallet platform. The subscriber maintains a mobile wallet balance and performs transactions using the mFS application. An "unbanked subscriber" is a subscriber that does not have (or does not have access to) a bank account or credit union account. The application or "mobile wallet application" provides mobile wallet functionality to the (unbanked) subscriber. The mobile wallet application is installed on a mobile device in the device's memory, on a SIM card (such as a GSM SIM card) or is otherwise accessible to the mobile device. The mobile wallet application provides the subscriber the ability to securely perform subscriber functions such as making retail purchases, paying bills, or transferring money to other mFS subscribers and non-subscribers. The mobile wallet application communicates with the mFS platform using binary and text SMS messages, among other forms of wireless communication. A wireless service provider or MNO provides the GSM network infrastructure on which the mFS platform operates.

FIG. **1** illustrates an example system architecture for a mobile wallet platform. Integration tier **101** is configured to manage mobile wallet sessions and maintain integrity of financial transactions. Integration tier **101** can also include a communication (e.g., Web services) API and/or other communication mechanisms to accept messages from channels **111**. Other mechanisms include, but are not limited to: International Standards Organization ("ISO") 8583 for Point of Sale ("POS") and Automated Teller Machines ("ATM") devices and Advanced Message Queuing Protocol ("AMQP") for queue based interfaces. Each of channels **111** can be integrated to one or more mechanisms for sending messages to integration tier **101**. Notification services **102** is configured to send various notifications through different notification channels **112**, such as, for example, Short Message Peer-to-Peer ("SSMP") for Short Messaging Service ("SMS") and Simple Mail Transfer Protocol ("SMTP") for emails. Notification services **102** can be configured through a web services API.

Service connectors **103** are a set of connectors configure to connect to 3rd party systems **113**. Each connector can be a separate module intended to integrate an external service to the system architecture. Business process services **104** are configured to implement business workflows, including executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects. Payment handler **105** is configured to

wrap APIs of different payment processors, such as, for example, banking accounts, credit/debit cards or processor **121**. Payment handler **105** exposes a common API to facilitate interactions with many different kinds of payment processors.

Security services **106** are configured to perform subscriber authentication. Authorization services **107** are configured to perform client authorization, such as, for example, using a database-based Access Control List ("ACL") table.

Database **108** is configured to manage customer accounts (e.g., storing customer accounts and properties), manage company accounts (e.g., storing company accounts and properties), manage transaction histories (e.g., storing financial transaction details), store customer profiles, storing dictionaries used by the mobile wallet platform, such as, for example, countries, currencies, etc., and managing money containers. Rules engine **109** is configured to gather financial transaction statistics and uses the statistics to provide transaction properties, such as, for example, fees and bonuses. Rules engine **109** is also configured to enforce business constraints, such as, for example, transactions and platform license constraints.

Name matching engine **110** is configured to match different objects according to specified configuration rules. Matching engine **110** can be use to find similarities between names, addresses, etc. Transaction processor **121** is configured to manage financial accounts and transactions. The transaction processor **121** can be used to hold, load, withdraw and deposit funds to mobile wallet accounts. Transaction processor **121** can also be used as a common interface to a third party processor system. When used as a common interface, financial operations may be delegated to the external processor. A Clearing House subsystem of transaction processor **121** can be used to exchange the financial information with a bank.

Components of a mobile wallet platform can be connected to one another over (or be part of) a system bus and/or a network. Networks can include a Local Area Network ("LAN"), a Wide Area Network ("WAN"), and even the Internet. Accordingly, components of the mobile wallet platform can be "in the cloud". As such, mobile wallet platform components as well as any other connected computer systems and their components, can create message related data and exchange message related data (e.g., Internet Protocol ("IP") datagrams and other higher layer protocols that utilize IP datagrams, such as, Transmission Control Protocol ("TCP"), Hypertext Transfer Protocol ("HTTP"), Simple Mail Transfer Protocol ("SMTP"), etc.) over the system bus and/or network.

The components depicted in FIG. **1** can interoperate to provide a number of financial and other services including but not limited to enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a mobile wallet, adding a debit or credit card account to a mobile wallet, depositing funds in a mobile wallet, withdrawing funds from a mobile wallet, paying bills from a mobile wallet, topping up a prepaid mobile account through a mobile wallet, transferring funds through a mobile wallet (nationally or internationally), making in-store purchases using a mobile wallet, and various other tasks as described herein below. These services will be described in greater detail below with regard to system FIGS. **1** and **2**, as well as FIGS. **3-19**B.

FIG. **2** depicts a monetary transaction system **200** similar to that described in FIG. **1**. The monetary transaction system **200** may provide a more simplified system structure in which each of the above services may be provided. The system includes a subscriber **205**. The subscriber may have access to a bank account, or may be an unbanked subscriber. The subscriber has a profile **211** with the monetary transaction system **210**. The profile includes the subscriber's KYC information, as well as any associated bank accounts, credit union accounts, bill pay accounts or other accounts. The subscriber has (or has access to) a mobile device **206** such as a phone or tablet. The mobile device runs the mobile wallet application (or mobile wallet application) **207**.

The subscriber can indicate, using the mobile application **207** which transaction or other action he or she would like to perform. The indicated transaction **208** is sent to the mobile wallet platform **210** to be carried out by the platform. The transaction processor **216** (which may be similar to or the same as transaction processor **121** of FIG. **1**) performs the transaction(s) specified by the (unbanked) subscriber **205**. The transaction processor may implement various other components to perform the transaction including memory **217**, (wireless) communication module **215**, rules engine **210** and/or transaction database **225**.

Performing the specified transactions may include communicating with the monetary transaction database **225** to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile (for instance, whether the subscriber has enough eMoney in his or her stored value account, or has enough money in his or her bank account). Rules engine **220** may also be consulted to determine whether the subscriber has exceeded a specified number of allowed transactions. Then, if funds are available, and the transaction is otherwise permissible, the monetary transaction system can transfer money or eMoney **221** to or from an entity such as a user or agent (e.g. entity **222**) to or from an establishment such as a retail store or agent company (e.g. entity **223**).

In some cases, the monetary transaction system **210** application provides a web interface that allows subscribers to perform the same functions provided by the monetary transaction system application. For instance, mobile wallet application **207** may provide a web interface that allows a user to enroll for a mobile wallet. The web interface (or the mobile wallet application itself) receives a subscriber-initiated transaction over one of a plurality of channels (**111** from FIG. **1**) connected to the monetary transaction system **210**. The web interface or mobile wallet application may prompt for and receive enrollment information (e.g. KYC information) for the (unbanked) subscriber **205** over at least one of the plurality of channels (e.g. web, point-of-sale (POS), interactive voice response (IVR, etc.). The web interface or mobile wallet application may then send activation instructions over the same or a different channel to activate the (unbanked) subscriber **205** and create a subscriber account for the (unbanked) subscriber.

Once the subscriber has an account, the monetary transaction system generates a corresponding mobile wallet for the unbanked subscriber (available via the web interface and/or the mobile wallet application. The system then presents the (unbanked) subscriber's account data associated with the mobile wallet and/or a notification indicating that enrollment was successful to the subscriber. Accordingly, the mobile wallet application or the web interface may be used to provide user enrollment functionality. It should also be understood that either the mobile wallet application or the web interface may be used to provide substantially all of the mobile wallet functionality described herein.

It should also be noted that the mobile device **206** may be any type of plan-based phone or tablet, or prepaid phone or tablet. Many subscribers, such as unbanked subscribers, may primarily use prepaid phones. The mobile wallet application **207** may be installed on both plan-based phones and prepaid

phones. The mobile wallet application may be installed on the device's SIM card, or on the device's main memory. Accordingly, the monetary transaction system **200** may be accessed and used via substantially any type of plan-based or prepaid mobile device.

FIG. **3** shows three different graphics (**301-303**) and corresponding method steps (**310-370**) that illustrate an unbanked subscriber making a deposit using a mobile wallet (and, by extension, using the mobile wallet transaction system **210**). In at least some of the embodiments described below, the actions of each participant are shown and described. This will also, at least in some embodiments, include an illustration of money flow throughout the mobile wallet transaction system. In the graphics, various terms are used as follows: $C=Cash Balance and $E=Electronic Money (eMoney) Balance.

At graphic **301**, it is assumed that the unbanked subscriber (e.g. **205**) has already registered and activated an eMoney account at an agent branch location (e.g. a retail store, gas station, or other location that has registered to be an agent branch). To deposit cash in order to get eMoney credit, the subscriber informs the agent manager or agent that they want to deposit a certain amount of cash (in **301**). The agent manager/agent takes the cash and notifies the mobile wallet transaction system of the deposit using their agent manager or agent application (**302**). The transaction system **210** then credits the subscriber's eMoney account (**303**). Accordingly, any location that has registered to accept eMoney payments from subscribers' mobile wallets can also accept cash deposits. The agent branch's eMoney balance is reduced because their actual money balance was increased by the amount of the deposit. The subscriber's mobile wallet account is credited with eMoney in the amount of the deposit. In this manner, a subscriber can deposit cash into their mobile wallet account (in the form of eMoney) at any retail location or other agent branch location.

Thus, the agent manager receives the physical cash deposit into the subscriber's eMoney account via the agent manager or agent's application. The subscriber gives cash to agent manager or agent, and the mFS platform processes the request, updates the agent branch and subscriber's eMoney balances, logs the transaction, and sends details (such as eMoney account balances, transaction logs, etc.) to bank specified by the mobile wallet platform. These details may be sent instantaneously as transactions occur, or in batches at pre-determined intervals.

In one embodiment, the monetary transaction system **210** of FIG. **2** is implemented to deposit funds at an agent branch using a mobile wallet. The monetary transaction system **210** receives communication from an agent branch over one of a plurality of channels (e.g. **111**) connected to the monetary transaction system (step **310**). The agent communication indicates that the unbanked subscriber **205** desires to deposit a specified amount of funds into the unbanked subscriber's mobile wallet account. The transaction processor **216** then validates the status of the unbanked subscriber's mobile wallet account (step **320**) and determines if the agent branch is authorized to receive deposited money (i.e. determine if it has pre-registered as an official agent branch) (step **330**).

The monetary transaction system may then use rules engine **220** to perform a limit check (to determine whether sufficient funds are available) and/or a velocity check (to determine whether the user has exceeded a specified number of (hourly, daily, or weekly) transactions) on the unbanked subscriber's mobile wallet account (step **340**). The transaction system then credits the unbanked subscriber's mobile wallet account with the specified amount of funds (step **350**) and returns a notification to the agent branch confirming the deposit (step **360**) and returns another notification to the subscriber notifying the subscriber that the specified amount of funds was deposited in the their mobile wallet account (step **370**). Any of channels **111** may be used to perform these communications.

FIG. **4** shows three different graphics (**401-403**) and corresponding method steps (**410-490**) that illustrate an unbanked subscriber making a withdrawal using a mobile wallet (and, by extension, using the mobile wallet transaction system **210**). As above, the terms in the graphics include "SC" representing cash balance and "SE" representing eMoney balance.

To withdraw cash at an agent branch, a subscriber submits a withdrawal request using their application (**401**). The subscriber may also enter information about the agent branch (e.g. name of establishment, name of agent, location or other information) that allows the monetary transaction system **210** to identify the agent branch. The transaction processor **216** may then determine whether the unbanked subscriber has enough eMoney to withdraw the requested amount. If he or she does have enough eMoney, then the subscriber's eMoney is deducted and that amount is transferred to the agent branch's eMoney account (**402**). Then, the agent branch gives the subscriber the requested amount of cash (**403**). In this manner, any entity that has established itself as an agent branch (including retail stores, gas stations, service providers, etc.) can provide cash withdrawal to a mobile wallet subscriber (whether banked or unbanked). The agent's or agent manager's role is to verify the withdrawal request (e.g. via SMS on the agent's or agent manager's phone) and gives the cash to subscriber. The subscriber requests cash withdrawal from agent branch's eMoney account via the application, and receives physical cash from agent manager/agent. The mobile wallet platform processes the request, updates the agent branch's and subscriber's eMoney balances, logs the transaction, and sends transaction details to a specified bank at pre-determined intervals.

In one embodiment, the monetary transaction system **210** is implemented to withdraw funds at an agent branch using a mobile wallet. The communication module **215** receives a communication from an unbanked subscriber over one of a plurality of channels **111** connected to the monetary transaction system **210** (step **410**). The communication indicates that the unbanked subscriber **205** desires to withdraw a specified amount of funds from the unbanked subscriber's mobile wallet account at the agent branch. The monetary transaction system **210** validates the status of the unbanked subscriber's mobile wallet account (step **420**) and determines if the balance of the unbanked subscriber's mobile wallet account is sufficient to accommodate the requested withdrawal for the specified amount of funds (step **430**).

The transaction processor **216** performs one or more of a limit check (to verify sufficient funds) and a velocity check (to verify the subscriber hasn't exceeded specified transfer limits) on the unbanked subscriber's mobile wallet account (step **440**). The monetary transaction system **210** then returns a secure, perishable withdrawal code to the subscriber **205** over at least one of the plurality of channels **111** connected to the monetary transaction system (step **450**). The monetary transaction system **210** receives subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system indicating that the withdrawal code has been presented to the agent branch (step **460**). The monetary transaction system **210** then debits the unbanked subscriber's mobile wallet account by the specified amount of funds (step **470**), returns a notification to the agent

branch confirming the withdrawal (step **480**) and notifies the subscriber that the specified amount of funds was withdrawn from the unbanked subscriber's mobile wallet account over at least one of the channels **111** connected to the monetary transaction system (step **490**). Accordingly, the monetary transaction system **210** may be used to allow subscribers to withdraw cash using their mobile wallet applications at any store or other entity registered as an agent branch.

FIG. **5**A depicts a subscriber-to-subscriber eMoney transfer. To perform such a transfer, subscriber A (**501**) enters some type of identification information identifying subscriber B (e.g. subscriber B's phone number) and an amount of money he or she wishes to transfer. The transaction processor **216** of the monetary transaction system **210** determines if there are sufficient funds to complete the transfer. If sufficient funds are available, the monetary transaction system **210** decrements subscriber A's account and credits subscriber B's account (**502**). The system then sends some kind of notification (e.g. SMS) to subscriber B indicating that a certain amount of money was transferred to their account. Subscriber A may also receive a notification that the transfer was successful. Accordingly, eMoney may be transferred between two mFS platform subscribers, one or both of which may be unbanked. The monetary transaction system **210** processes the subscribers' requests, updates the subscribers' eMoney balances, logs the transactions, and sends transaction information to a specified bank when needed.

FIG. **5**B illustrates a subscriber-to-non-subscriber eMoney transfer. In graphic **505**, subscriber A wishes to send eMoney to another individual that is not a subscriber to the mFS platform. The transaction is initiated in the same fashion as the subscriber-to-subscriber transfer scenario. However, since non-subscriber B does not have a mobile wallet account, the monetary transaction system **210** cannot credit them with eMoney. Instead, the monetary transaction system **210** sends a notification (e.g. via SMS) to non-subscriber B with instructions for how to pick-up the transferred money, along with an authorization code (**506**). The monetary transaction system **210** puts a hold on subscriber A's account for the amount transferred. Subscriber B then has a specified number of days to pick up the cash before the hold expires and the amount is credited back to subscriber A's eMoney account by the monetary transaction system **210**.

When non-subscriber B goes to pick up the money at an agent branch, the agent branch's manager or agent verifies the authorization code via an agent manager or agent mobile wallet application (that, in turn, accesses the mFS platform). Once the transfer has been validated, the agent gives the cash to non-subscriber B. The agent branch's mFS account is credited with the transfer amount (**507**) and the user leaves with the cash in hand (**508**). The mFS platform processes the transfer request, updates subscriber A's eMoney balance, logs the transaction, and sends transaction details to a platform-specified bank.

FIG. **6**A illustrates a subscriber-to-subscriber international eMoney transfer. This embodiment is, at least in some respects, similar to sending eMoney to an mFS subscriber domestically. In this case the monetary transaction system **210** leverages one or more existing international money transfer organizations or "remittance companies" such as MoneyGram®. In some embodiments, MoneyGram® is pre-integrated to the monetary transaction system **210**, but other international money transfer organizations may also be used. Still further, at least in some embodiments, subscriber B may need to have an eMoney account with a foreign mFS program that is also affiliated with MoneyGram® or another international money transfer organization.

In FIG. **6**A, subscriber A initiates the international eMoney transfer at **601**, the international money transfer organization (e.g. MoneyGram®) transfers the eMoney to subscriber B at **602** and subscriber B's eMoney balance is increased by the transferred amount. Thus, subscriber A requests to send eMoney from his or her eMoney account via the mobile wallet application. The eMoney is transferred using an international money transfer organization, and subscriber B receives a notification (that may, for example, include a reference number, among other information) that their eMoney balance has increased by the transfer amount. The monetary transfer system **210** processes subscriber A's request, updates subscriber A's and subscriber B's eMoney balances, logs the transaction, and send transaction details to a mFS platform-specified bank.

FIG. **6**B illustrates a subscriber-to-non-subscriber international eMoney transfer. In this illustration, subscriber A wishes to send cash to subscriber B who is not an mFS program subscriber. Similar to the scenario described in FIG. **6**A, the monetary transaction system **210** leverages various international money transfer organizations or remittance companies such as MoneyGram® to transfer the eMoney. Subscriber A initiates a typical eMoney transfer at **605** by providing non-subscriber B's identification information, as well as the amount to be transferred. The Monetary transaction system **210** recognizes the eMoney transfer is not destined for a domestic phone number and routes the request to the international money transfer organization (e.g. MoneyGram®) (**606**).

The international money transfer organization sends non-subscriber B a notification (e.g. via SMS) with instructions for how and where to pick up the money (in embodiments where MoneyGram® transfers the eMoney, the notification may include a MoneyGram® reference number (MGRN)) (**607**). Non-subscriber B can then show the MGRN to an agent at an agent branch (**608**) and then receive the cash (**609**). The monetary transaction system **210** then decrements subscriber A's eMoney account for the transferred amount. The monetary transfer system **210** thus processes subscriber A's transfer request, updates subscriber A's eMoney balance, logs the transaction, and sends transaction detail to a platform-specified bank. It should also be noted that an mFS subscriber may also receive money in a foreign country from either a subscriber or a non-subscriber in a similar manner.

FIG. **7** illustrates a subscriber purchasing airtime using a mobile wallet. Mobile wallet platform subscribers may buy airtime by using their mobile wallet application **207**. The monetary transaction system **210** will reload their airtime account within the mobile network operator's (MNO's) systems. The subscriber requests to purchase airtime by entering the request via the mobile wallet application or via a mobile wallet web interface. The monetary transaction system **210** then decrements the subscriber's eMoney account (**701**), while crediting the mFS platform's eMoney account (**702**). The purchased airtime is then added to the subscriber's airtime balance (**703**). The monetary transaction system **210** processes the subscriber's request, updates the subscriber's eMoney balances as well as its own eMoney balance, logs the transaction, and sends transaction detail to a mFS platform-specified bank.

In one embodiment, the monetary transaction system **210** is implemented to top up a prepaid mobile account from a mobile wallet. The communication module **215** of the monetary transaction system **210** receives a subscriber communication over one of a plurality of channels **111** connected to the monetary transaction system (step **710**). The subscriber communication indicates that an unbanked subscriber **205** desires

to top up a prepaid mobile account by a specified amount using a specified payment method from the unbanked subscriber's mobile wallet. The transaction processor **216** validates the status of the selected payment method (step **720**) and performs a limit check and/or a velocity check on the selected payment method (step **730**). The monetary transaction system **210** then debits the specified payment method by the specified amount of funds (step **740**) and processes the mobile top-up via a billing system integrator and/or an aggregator (step **750**), and notifies the subscriber that the prepaid mobile account was topped up over at least one of the channels connected to the monetary transaction system (step **760**).

FIG. **8** illustrates an embodiment where a mFS subscriber pays a bill using a mobile wallet. At least in some embodiments, the company that the subscriber wishes to pay needs to have signed-up to be part of the mFS platform. The mFS platform may publish a list of company names that have registered to be part of the mFS platform. This list of companies may include company IDs so that subscribers can know which company ID to enter in their mobile wallet application. Once the company ID is known, the subscriber can pay a bill by entering the company ID and the amount to be paid. The monetary transaction system **210** then decrements the subscriber's eMoney account (**801**) and credits the identified company's eMoney account (**802**). Accordingly, in response to the subscriber's request to pay bill via their mobile wallet application, the monetary transaction system **210** processes the request, updates the bill pay company's and the subscriber's eMoney balances, logs the transaction, and sends transaction details to the mFS platform-specified bank.

In one embodiment, the monetary transaction system **210** is implemented to pay a bill from a mobile wallet. The communications module **215** of the monetary transaction system **215** receives a subscriber communication over a communication channel **111** connected to the monetary transaction system (step **810**). The subscriber communication indicates that unbanked subscriber **205** desires to pay a bill for a specified amount using a specified payment method from the unbanked subscriber's mobile wallet (e.g. eMoney). The monetary transaction system **210** validates the status of the selected payment method (step **820**) and performs a limit check and/or a velocity check on the selected payment method to ensure the eMoney transfer is permissible (step **830**). The monetary transaction system then debits the specified payment method by the specified amount of funds (step **840**), processes the bill payment via a direct biller connection or a bill pay aggregator (step **850**), and notifies the unbanked subscriber that the bill was paid using a communication channel (e.g. SMS) connected to the monetary transaction system (step **860**). Thus, in this manner, a subscriber may use a mobile wallet to pay various bills including rent, utility, mortgage, phone, cable, medical and other bills.

FIG. **9** illustrates a mobile wallet subscriber making a retail purchase. Mobile wallet subscribers can make retail purchases at agent branches directly from their mobile device. Agent branches, as explained above, are retail stores or other entities that have registered with the mFS system and are able to accept mobile wallet payments. Accordingly, a subscriber can select the items they wish to purchase, and indicate (via the mobile wallet application) to the agent branch that they wish to pay for the items. The mobile wallet application then communicates with the agent branch and the monetary transaction system to indicate the price of the transaction. The monetary transaction system **210** then debits the subscriber's eMoney account (**901**) and credits the agent branch's eMoney account (**902**). The agent branch (and/or the agent manager or agent) receives confirmation that subscriber paid for the purchase. The subscriber may also receive a summary of the retail purchase and may be asked to confirm the purchase by entering a PIN. The monetary transaction system processes the purchase request, updates the agent branch and subscriber's eMoney balances, logs the transaction, and sends transaction details to a mFS platform-specified bank.

In one embodiment, the monetary transaction system **210** is implemented to make a purchase from a mobile wallet. The communications module **215** of the monetary transaction system **210** receives a communication from a subscriber over a communication channels **111** (step **910**). The subscriber communication indicates that an unbanked subscriber **205** desires to purchase an item for a specified amount of funds using a specified payment method from the unbanked subscriber's mobile wallet.

The monetary transaction system **210** then returns a secure, perishable purchase code to the unbanked subscriber over at least one of the channels connected to the monetary transaction system (step **920**) and receives a subsequent agent branch communication over a channel indicating that the purchase code has been presented to an agent (branch) (step **930**). The monetary transaction system **210** validates the status of the specified payment method (step **940**), determines if the specified payment method can accommodate a purchase for the specified amount (step **950**), performs a limit check and/or a velocity check on the selected payment method (**960**), debits the specified payment method by the specified amount of funds (**970**), returns a notification to the agent branch authorizing the purchase (**980**) and sends a receipt to the unbanked subscriber over a communication channel. The monetary transaction system **210** may thus be used to make a retail purchase using a mobile wallet.

FIG. **10**A illustrates a subscriber requesting a micro-loan. Financial institutions and potentially other mFS program participants may sign up to become money or eMoney lenders. Mobile wallet subscribers may be able to use their mobile wallets to request micro-loans from these approved lenders. The micro-loans are tracked by the monetary transaction system **210**, and repayment reminders, interest and commissions are managed by the monetary transaction system. The subscriber requests a micro-loan from a lender, indicating the amount in the request, as well as other information such as the repayment date and the commission (i.e. interest rate). Potential lenders then have a chance to counter the loan request with their own terms. Once the lender approves the subscriber's request, the lender's eMoney account balance is debited for the specified amount (**1001**) and the subscriber's eMoney account is credited with the requested amount (**1002**). The monetary transaction system **210** processes the micro-loan requests, update the lender and subscriber's eMoney balances, sets up repayment schedules and reminders, logs the transaction, and sends transaction detail to a mFS bank. It should also be noted that while the term "micro-loan" is used herein, the loan may be for substantially any amount of money.

Following on the embodiment described in FIG. **10**A, FIG. **10**B illustrates a subscriber repaying a micro-loan. The subscriber may repay the loan using functionality provided in the mobile wallet application or in a similar web interface. Repayments can be made in installments or in full depending on the rules of the micro-loan. The subscriber enters the amount they wish to repay and the loan ID. The subscriber's eMoney account is then debited for the specified amount (**1005**), while the lender's eMoney account is credited the specified amount (**1006**). Both the lender and the subscriber may receive confirmation that the loan has been repaid via SMS or some other communication channel. The mFS plat-

form thus processes the subscriber's micro-loan repayment request, updates lender and subscriber's eMoney balances, updates repayment schedule and reminders, logs the transaction, and sends transaction details to a specified mFS platform bank.

FIG. **11**A illustrates a subscriber receiving a direct deposit from an employer or other entity. Subscribers to the mFS platform have the ability to receive any direct deposit into their eMoney account. Subscribers may be asked by their employers to provide account information in order to set up direct deposit. The employer then submits a direct deposit request using their existing processes (i.e the processes they use for a normal checking or savings bank account). Once the direct deposit is set up and a payday arrives, the employer's bank account is debited for the proper amount (**1101**) and the employer's mFS account is credited with that amount (**1102**). Then, once the funds have been received at the mFS platform bank, the mFS platform bank sweeps the employers direct deposit balance (**1103**) into a mFS platform master account (**1104**) and notifies the mFS platform of each account to be incremented (including the subscriber's mobile wallet (eMoney) account). The subscriber's eMoney account is then credited with the paycheck amount (**1105**) upon which the eMoney may be used to pay for goods, pay bills, top up airtime, transfer to other entities or for cash withdrawal.

The subscriber does not need to have a bank account to participate in direct deposit. The employer's bank can communicate with the mFS platform's bank to perform the necessary steps in directly depositing the subscriber's paycheck in his or her eMoney mobile wallet account. The bank facilitates monetary deposit into the employer's bank account for direct deposit and performs an automated sweep of recent deposits from the employer's bank account into the mFS platform's master bank account. The bank also sends transaction details to the monetary transaction system **210** including transaction logs. The monetary transaction system receives a list of eMoney accounts that are to be credited directly from the employer (or bank), processes the list and requests to establish a direct deposit, updates subscriber's eMoney balance, log the transaction, and sends transaction details to the mFS platform bank.

In a similar manner, a subscriber may receive a government welfare payment directly on their mobile device. FIG. **11**B illustrates a subscriber receiving a government social welfare payment directly into their eMoney account. In some embodiments, subscribers may need to opt-in and register with the government program for which they choose to receive the payment via their mobile wallet. Once the funds have been received, the subscriber can use that eMoney for any goods or services, as described above. Once the direct deposit has been established and a payout has been initiated, the government's welfare account deposits the money (**1110**) into the government's bank account for welfare payments (**1111**) and performs an automated sweep of recent deposits from the government's bank account (**1112**) into the mFS program's master bank account (**1113**). The bank then sends transaction details to the monetary transaction system **210** regarding the deposit. The subscriber receives a notification that the welfare payment has been credited to their eMoney account (**1114**). The mFS platform receives an indication of eMoney accounts that are to be credited from the government, processes the welfare payments, updates the subscriber's eMoney balance, logs the transactions, and sends transaction details to the mFS platform bank.

FIG. **12**A illustrates an agent administrator distributing eMoney to various recipients. An agent administrator, as explained above, is a person who acts as an agent company's representative. The agent administrator deposits, withdraws, and distributes funds into and out of the agent company's bank account. When an agent administrator deposits cash into an agent company's bank account, it is credited as eMoney to the agent company's account. In order to provide the agent branches with eMoney, the agent administrator first moves the eMoney from the agent company's account (**1201**) to the branch accounts (**1202**). This is performed using the agent administrator's mobile wallet application or portal. In an agent administrator money transfer, the monetary transaction system **210** processes the administrator's eMoney transfer request, updates the agent company and agent branch eMoney balances, logs the transaction, and sends transaction details to the mFS platform bank.

FIG. **12**B illustrates an agent company deposit. The agent company has an eMoney account in the monetary transaction system **210** that may also include a corresponding bank account (that may be created automatically upon creation of the agent company's eMoney account). After the agent company's bank account has been set up, the agent administrator can make deposits into that account. As FIG. **12**B shows, once cash (**1205**) has been deposited into the bank account (**1206**), it is transferred to a mFS platform master account (**1208**) that includes all or a part of the mFS platform's funds. The agent company's bank account is decreased by the deposit amount (**1207**), while the agent company's eMoney account balance is correspondingly increased (**1210**). At this time, the agent company account is credited with eMoney. The agent company's bank facilitates a physical cash deposit into the agent company's bank account and performs an automated sweep (**1209**) of recent deposits from the agent company's bank account into the mFS platform's master bank account. The agent company's bank then sends transaction details to the monetary transaction system **210**. The agent administrator physically delivers the cash (or form of money such as a check or money order) to a bank branch for deposit. The monetary transfer system receives transaction details from the agent company's bank about recent transactions (including deposits, as shown in FIG. **12**B.

FIG. **13** illustrates an agent company withdrawal. To make a cash withdrawal for an agent company, the agent administrator requests a withdrawal using the agent administrator mobile wallet application. The monetary transaction system **210** then notifies the bank that a certain amount of eMoney is to be transferred from the master mFS account (**1302**) to the agent company bank account (**1303**). When the money is in the agent company bank account, the agent administrator can withdraw the cash by traditional withdrawal means. The mFS master bank receives transaction details from the monetary transaction system **210** about recent transactions (recent withdrawals in this case). The mFS master bank performs an automated sweep (**1304**) of the mFS platform's master bank account to reflect the recent withdrawal request from agent the agent company (**1301**). The agent company's eMoney account is reduced by the amount of the withdrawal. The agent company also sends transaction details to the monetary transaction system **210**. The agent administrator can request withdrawal via the agent administrator mobile wallet application and physically withdrawal cash (**1305**) from the agent company's bank branch (**1306**). The mFS platform processes the agent company's withdrawal request, updates agent company and agent branch eMoney balances, logs the transaction, and sends transaction details to an mFS platform-specified bank.

Attention will now be turned to embodiments in which subscribers have bank accounts associated with their mobile wallets. The monetary transaction system **210** provides simi-

lar functionality to consumers that have bank or credit union accounts. Although many different transactions are presented herein, many more and varied types of transactions may be processed by the monetary transaction system. In the following figures, "$C" refers to cash balance, "$DC" refers to a debit card (prepaid) balance and "$PIN" refers to a recharge PIN value.

FIG. **14** describes a subscriber deposit at an agent branch. The subscriber has a registered and activated (prepaid) debit card at an agent branch location. The prepaid debit card is associated with the mobile wallet application in the subscriber's mobile device. As such, the debit card is linked to the subscriber's account in the monetary transaction system **210**. To deposit cash onto the mobile wallet, the subscriber informs the agent that they want to deposit a specified amount of cash (**1401**). The agent takes the cash and notifies the monetary transaction system **210** of the deposit using their point of sale (POS) system or the agent mobile wallet application (**1402**), and the monetary transaction system **210** credits the subscriber's mobile wallet account (**1403**). The funds collected at the cash register typically do not reach a bank account until the reconciliation and settlement of funds occurs between the agent and the mFS owner's bank.

The subscriber's bank then receives a settlement report from the card processor and receives funds from the agent's bank. The agent or agent manager physically deposits the cash into the subscriber's mobile wallet account via their POS system or agent manager/agent mobile wallet application. The monetary transaction system processes the deposit request, increments the subscriber's mobile wallet balance within the card processor and logs the transaction. An external card processor increments the subscriber's mobile wallet balance and sends reports to the bank for settlement on a regular (e.g. nightly) basis.

In one embodiment, the monetary transaction system **210** is implemented to deposit funds into a bank or credit union account using a mobile wallet. The communications module **215** of the monetary transaction system **210** receives communication from an agent branch over a communication channel (step **1410**). The agent communication indicates that a subscriber **205** desires to deposit a specified amount of funds into a bank or credit union account. The transaction processor **216** validates the status of the bank or credit union account (step **1420**), determines if the agent branch is authorized to deposit money (step **1430**), and performs a limit check and/or a velocity check on the bank or credit union account (step **1440**). The monetary transaction system then credits the bank or credit union account with the specified amount of funds (step **1450**), returns a notification to the agent branch confirming the deposit (step **1460**) and notifies the subscriber that the specified amount of funds was deposited in the bank or credit union account using at least one of the communication channels connected to the monetary transaction system (step **1470**). Accordingly, cash may be deposited into a bank or credit union account associated with a subscriber's mobile wallet.

FIG. **15** illustrates a subscriber deposit that is performed with a non-agent. In some economies, subscribers may have the ability to leverage other channels outside of agents to deposit funds onto their card. One deposit method is a PIN-based recharge that allows a subscriber to purchase a PIN worth the deposit value. The PIN can then be redeemed via an interactive voice response (IVR) system or via the subscriber's mobile wallet application. The mobile wallet application will allow the monetary transaction system **210** to deposit the funds onto the subscriber's card. The retailer's bank settles with the PIN card provider's bank and the PIN card provider's bank settles with the mFS platform's bank for the deposit. The subscriber gives cash to the agent (**1501**) which increases the agent company's physical cash (**1502**). The subscriber uses IVR or their SIM Application to recharge mobile wallet account using a PIN card (**1503**). In some cases, an agent may provide the PIN card (i.e. the prepaid debit card) to the subscriber. The monetary transaction system **210** processes the subscriber deposit request, increments the subscriber's mobile wallet balance within the card processor and logs the transaction. An external card processor decreases the subscriber's PIN card balance (**1504**), increments the subscriber's mobile wallet balance (**1505**) and send reports to the mFS platform bank for settlement.

FIG. **16** illustrates a subscriber withdrawal at an agent branch. To withdraw cash at an agent branch from a (prepaid) debit card, a subscriber submits a withdrawal request using the mobile wallet application on their mobile device. The subscriber may also need to enter details about the agent branch that allows the monetary transaction system **210** to determine if the subscriber has sufficient funds on their debit card. The mFS platform then notifies the agent branch that it can give cash to the subscriber. If the subscriber has sufficient funds, the monetary transaction system **210** will decrement the subscriber's funds from their card (**1601**) and transfer it to the mobile wallet owner's account within the same card processor or bank. The agent branch (**1602**) then provides the withdrawn cash to the subscriber (**1603**).

Accordingly, the subscriber requests a cash withdrawal from their own mobile wallet account via the mobile wallet application. The agent or agent manager verifies the withdrawal request via POS authorization or SMS received on agent's phone and, once verified, gives cash to the subscriber. The monetary transaction system **210** processes the subscriber's withdrawal request, decrements the subscriber's mobile wallet balance within the card processor and logs the transaction. An external card processor decrements the subscriber's mobile wallet balance and sends reports to the bank for settlement on a periodic basis.

In one embodiment, the monetary transaction system **210** is implemented to withdraw funds from a bank or credit union account using a mobile wallet. The communication module **215** of the monetary transaction system **210** receives a communication from a subscriber **205** over a communication channel **111** (step **1610**). The subscriber communication indicates that subscriber **205** desires to withdraw a specified amount of funds from a bank or credit union account. The transaction processor validates the status of the bank or credit union account (step **1620**), determines if the balance of the bank or credit union account is sufficient to accommodate the requested withdrawal for the specified amount of funds (step **1630**) and performs a limit check and/or a velocity check on the bank or credit union account (step **1640**).

The monetary transaction system **210** then returns a secure, perishable withdrawal code to the subscriber **205** over at least one of the communication channels (step **1650**) and receives a subsequent agent branch communication indicating that the withdrawal code has been presented to an agent (step **1660**). The monetary transaction system **210** then debits the bank or credit union account by the specified amount of funds (step **1670**), returns a notification to the agent branch confirming the withdrawal (**1680**) and notifies the subscriber that the specified amount of funds were withdrawn from the bank or credit union account using at least one of the communication channels connected to the monetary transaction system (step **1690**). Accordingly, a subscriber can withdraw cash stored on their mobile wallet from an agent branch or a non-agent branch.

FIG. **17**A illustrates a subscriber withdrawal using an automated teller machine (ATM). Subscribers in many countries have access to ATM machines and can use their mobile wallets to perform withdrawals using their (prepaid) debit card at most ATMs. Banks provide ATMs to their customers (typically at no charge) and to non-customers (typically for a small charge). The subscriber requests a cash withdrawal from the subscriber's mobile wallet via the subscriber's debit card that is associated with the mobile wallet. The bank providing the debit card may receive settlement reports from the card processor and may transfer and/or settle funds from subscriber's account to the ATM network bank. An extern card processor decrements the subscriber's mobile wallet balance (**1701**) and sends transaction reports to the bank for settlement. Accordingly, once the withdrawal request has been received and the external card processor (e.g. Visa® or MasterCard®) (**1702**) has debited the debit card account, the ATM (**1703**) dispenses the withdrawn cash to the subscriber (**1704**).

FIG. **17**B illustrates a subscriber-to-subscriber money transfer. An mFS subscriber (**1705**) may send money to another mFS subscriber (**1706**). To do so, subscriber A enters information identifying subscriber B (e.g. a phone number, email address or other identifier). The monetary transaction system **210** determines if there are enough funds to complete the transaction, and if so, the monetary transaction system **210** decrements subscriber A's debit card and credits subscriber B's debit card. The subscriber, accordingly, may request to send money from their own mobile wallet (i.e. money stored on a (prepaid) debit card) account via the subscriber mobile wallet application. The other subscriber receives a notification that the balance of the debit card associated with their mobile wallet has increased. The bank receives a settlement report from the debit card processor and transfers or settles funds from subscriber A's account to subscriber B's account (if necessary). The monetary transaction system **210** processes the transfer request, updates subscriber A's and subscriber B's debit cards that are associated with their mobile wallets and logs the transaction. The external card processor decrements subscriber A's debit card balance, increments subscriber B's debit card balance and sends transaction reports to the mFS platform bank for settlement.

FIG. **17**C illustrates subscriber-to-non-subscriber money transfers. In this embodiment, subscriber A (an mFS subscriber) wishes to send money to another subscriber (a non-mFS subscriber). The transaction is initiated in the same fashion as described above in FIG. **17**B. However, since subscriber B does not have an mFS account, the monetary transaction system **210** cannot credit them with money. Instead, the monetary transaction system **210** sends a communication (e.g. a SMS) to subscriber B (**1708**) with an authorization code and instructions for how to pick up the cash. The monetary transaction system **210** puts a hold on subscriber A's debit card for the amount transferred (**1707**). Subscriber B has a specified time period in which to pick up the cash before the hold expires and the amount is credited back to the debit card associated with subscriber A's mobile wallet account. The agent branch verifies the authorization code via POS or their agent mobile wallet application (**1709**) and gives the cash to the non-subscriber (**1710**). (In some countries, an agent network needs to be capable of giving cash to a subscriber based on the money transfer reference number).

The mFS bank receives a settlement report from the card processor and transfer and settle funds from subscriber A's debit card to the agent's bank (if necessary). The monetary transaction system **210** processes the money transfer request, decrements subscriber A's mobile wallet balance within the card processor, generates a money transfer reference number, authorizes the reference number to be paid out by the agent and logs the transaction. An external card processor decrements subscriber A's mobile wallet balance and sends periodic transaction reports to the bank for settlement. Thus, as seen in FIGS. **17**B and **17**C, money may be transferred from subscriber to subscriber and from subscriber to non-subscriber.

Subscribers may similarly send money internationally to both subscribers and non-subscribers. FIG. **18**A illustrates a subscriber-to-subscriber international money transfer. In this embodiment, subscriber A wishes to send cash to subscriber B who resides in another country. As in the embodiments described above where money was transferred internationally, the monetary transaction system **210** may use one or more international money transfer organizations or remittance companies such as MoneyGram® to transfer the money. Subscriber A initiates the international money transfer using his or her phone. Subscriber A's debit card account is decremented by the transfer amount (**1801**). The money is transferred between countries using an international money transfer organization (**1802**). In this case, subscriber B has an mFS eMoney account with a foreign mFS platform that is also affiliated with the selected international money transfer organization. That organization can then credit subscriber B's eMoney account directly (**1803**).

Thus, subscriber A requests to send money from their debit card account via the subscriber mobile wallet application. Subscriber B receives a notification (including a MoneyGram® Reference Number (MGRN) (or other reference number when other international money transfer organizations are used) and instructions on how to access the eMoney) that their eMoney balance has increased. The mFS bank receives settlement reports from the debit card processor and transfers and/or settles funds from subscriber's account to the international organization's bank. The monetary transfer system **210** processes the transfer request, update subscriber A's and subscriber B's eMoney balances and logs the transaction. An external card processor decrements subscriber A's mobile wallet balance and sends periodic transaction reports to the bank for settlement.

FIG. **18**B illustrates a subscriber-to-non-subscriber international money transfer. In this embodiment, subscriber A wishes to send cash to subscriber B who resides in another country. As above, the monetary transaction system **210** uses an international money transfer organization (**1806**) to transfer the money between countries. Once the transfer has been initiated by subscriber A, the international money transfer organization debits subscriber A's debit card account (**1805**) and transfers that money to subscriber B. Subscriber B (**1807**) receives a notification (e.g. via SMS) with pick up instructions and a transfer ID number. Subscriber B can then go to an agent company (**1808**), show them the notification (including, perhaps an authorization code), and receive the transferred money (**1809**).

Similar to the transaction described in FIG. **18**A, the embodiment of **19**A illustrates a transaction where a subscriber receives an international money transfer. Subscriber B (**1901**) initiates a money transfer using their mobile wallet application. The international money transfer organization (**1902**) debits subscriber B's eMoney account balance. This money is then transferred by the international money transfer organization to subscriber A. Subscriber A receives a notification along with a transfer ID number indicating that their debit card account has been credited with the transferred money (**1903**).

FIG. **19**B illustrates a non-subscriber-to-subscriber international money transfer. This scenario is very similar to that

described in FIG. **19**A from the mFS subscriber's perspective, except that their eMoney account is credited here, and their debit card account was credited in **19**A. The initiator, subscriber B (**1905**), does not have an mFS account and, as a result, takes their cash to an international money transfer organization (e.g. MoneyGram®) or other remittance company's agent (**1906**) to send it to subscriber A's mobile wallet eMoney account. The international money transfer organization (**1907**) then transfers the specified amount to subscriber A (**1908**) and subscriber A's mobile wallet eMoney account is credited with the amount of the transfer. Subscriber A may receive a transaction ID number, along with an indication that the transfer has occurred. The mFS bank may receive settlement reports from the card processor and settle funds from the international money transfer organization's bank to subscriber A's mobile wallet account. The monetary transaction system processes the money transfer request, updates subscriber A's mobile wallet balance within the card processor and logs the transaction. An external card processor increments subscriber A's mobile wallet balance and sends periodic transaction reports to the mFS bank for settlement.

Other functionality described above in relation to using an eMoney mobile wallet account may also apply to banked subscribers using a debit card associated with their mobile wallet. Such subscribers may buy airtime for their mobile device, pay bills, make retail purchases, receive direct deposits, and perform other functionality.

In one embodiment, the monetary transaction system **210** is implemented to add a mobile wallet platform stored value account to a mobile wallet. The stored value account may include eMoney or other monetary credits. In the embodiment, communication module **215** of monetary transaction system **210** may receive subscriber data for an unbanked subscriber **205** over a communication channel. The transaction processor may perform validation checks on the unbanked subscriber to validate that the unbanked subscriber is not exceeding a specified allowable number of accounts per subscriber. The monetary transaction system **210** may then send subscriber data to another entity (such as a third party verification system) for identification of the unbanked subscriber. The monetary transaction system **210** receives results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber, creates a stored value account for the unbanked subscriber that maintains a recorded balance for the created stored value account, adds the stored value account to the unbanked subscriber's mobile wallet and notifies the unbanked subscriber of the addition of the stored value account over at least one communication channel connected to the mobile wallet platform.

In another embodiment, the monetary transaction system **210** is implemented to add a third party stored value account to a mobile wallet. The monetary transaction system **210** receives unbanked subscriber data, including account details, over a communication channel. The transaction processor **216** performs a validation check on the unbanked subscriber to validate that the unbanked subscriber is not exceeding a specified allowable number of accounts per subscriber. If the validation check is ok, the monetary transaction system **210** sends subscriber data to a third party verification system for identification of the unbanked subscriber. In some cases, validating the status of the sender or the recipient includes performing a check on the specified sender or recipient to comply with the office of foreign assets control. The monetary transaction system **210** then receives results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber, and submits the unbanked subscriber's account details to a third party account processor. The monetary transaction system **210** receives an indication from the third party account processor that third party account processor created a third party stored value account for the subscriber. The transaction processor maintains a link between the subscriber data and the third party stored value account and adds the third party stored value account to the unbanked subscriber's mobile wallet. The monetary transaction system **210** then notifies the unbanked subscriber of the addition of the third party stored value account over a communication channels connected to the monetary transaction system.

In another embodiment, the monetary transaction system **210** is implemented to add a bank or credit union account to a mobile wallet. The communication module **215** receives subscriber data, including bank or credit union account details, over a communication channel **111**. The transaction processor **216** performs validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber and sends subscriber data to a third party verification system for identification of the subscriber. The communication module then receives results from the third party verification system indicating that the subscriber data appropriately identifies the subscriber. Upon receiving these results, the monetary transaction system **210** submits bank or credit union account details for validation by the transaction processor, receives an indication that the bank or credit union account details correspond to a valid bank or credit union account, maintains a link between the subscriber data and the bank or credit union account and notifies the subscriber of the bank or credit union account validation over a communication channel.

In still another embodiment, the monetary transaction system is implemented to add a debit or credit card account to a mobile wallet. The communication module **215** receives subscriber data, including a debit or credit card account number, over a communication channel **111** connected to the monetary transaction system. The transaction processor performs validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber. The communication module sends subscriber data to a third party verification system for identification of the subscriber and receives results from the third party system indicating that the subscriber data appropriately identifies the subscriber. The monetary transaction system **210** securely stores the debit or credit card account number for access by the mobile wallet (e.g. in memory **217** or transaction database **225**), adds the debit or credit card account number to the subscriber's mobile wallet, and notifies the subscriber of the addition of the debit or credit card account number. It should be noted that many other transactions can take place over the monetary transaction system, and that the embodiments described herein should not be read as limiting.

Embodiments of the invention can adhere to Know Your Customer (KYC) rules in the US by performing Customer Identification Program (CIP) checks as required by the Bank Secrecy Act and US PATRIOT Act. A minimum amount of information can be gathered about a customer, such as, for example, first name, last name, date of birth, government ID Type, government ID number and address. The CIP processes are designed to validate customer identity against government blacklists and assists in the prevention of money laundering and terrorist financing. A combination of non-documentary and documentary verification can be used to ensure beyond a reasonable doubt the identity of the customer.

Non-documentary verification can occur through the presentment of the information that was collected from the user

to an external third party, such as, for example, Lexis Nexis®. Documentary verification can occur if non-documentary verification fails, then the user is asked to present an unexpired government ID. Various differ forms of identification including driver's license, passport, alien identification (e.g., green card or work visa), and Mexican Consular identification card, can be accepted.

Embodiments of the invention can perform Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) checks. AML and CFT checks can be performed using transaction monitoring methods to flag names and suspicious transactions for further investigation. The mobile wallet platform can perform AML and CFT checks on all electronic financial transactions to ensure that electronic funds are not being used for money laundering or terrorism. Transaction limits can be placed on user accounts. The transaction limits are fully configurable for each particular use case, channel and payment method that allows maximum flexibility to restrict higher risk use cases. Velocity checks can also be performed. Velocity Checks ensure that subscribers are not abusing the mobile wallet platform within the allowable limits.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

I claim:

1. A monetary transaction system for conducting monetary transactions between unbanked subscribers and other entities, the system comprising: a mobile device configured to run a monetary transaction system application; an unbanked monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the unbanked subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system;

a monetary transaction system processor that performs the one or more transactions specified by the unbanked subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile;

at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system; and

wherein the monetary transaction system is implemented to deposit funds at an agent branch through a mobile wallet, including performing the following steps:

receiving communication from an agent branch over one of a plurality of channels connected to the monetary transaction system, the agent communication indicating that the unbanked subscriber desires to deposit a specified amount of funds into the unbanked subscriber's mobile wallet account;

validating the status of the unbanked subscriber's mobile wallet account; determining if the agent branch is authorized to receive deposited money; performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account, the limit check determining whether sufficient funds are available to make the deposit amount, the velocity check determining whether the unbanked subscriber has exceeded a specified number of transactions within a specified time period;

crediting the unbanked subscriber's mobile wallet account with the specified amount of funds when the agent bank is authorized to receive the deposited money;

returning a notification to the agent branch confirming the deposit; and notifying the subscriber that the specified amount of funds was deposited in the unbanked subscriber's mobile wallet account over at least one of the plurality of channels connected to the monetary transaction system.

2. The monetary transaction system of claim 1, wherein the monetary transaction system application provides a web interface that allows subscribers to perform the same functions provided by the monetary transaction system application.

3. The monetary transaction system of claim 1, wherein the monetary transaction system application is provided on a prepaid or postpaid phone.

4. A monetary transaction system for conducting monetary transactions between subscribers and other entities, the system comprising:

a mobile device configured to run a monetary transaction system application;

a monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system;

a monetary transaction system processor that performs the one or more transactions specified by the subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile;

at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system;

wherein the monetary transaction system is implemented to withdraw funds at an agent branch using a mobile wallet, including performing the following steps:

receiving a communication from the unbanked subscriber over one of a plurality of channels connected to the monetary transaction system, the communication indicating that the unbanked subscriber desires to withdraw a specified amount of funds from the unbanked subscriber's mobile wallet account at the agent branch;

validating the status of the unbanked subscriber's mobile wallet account;

determining if the balance of the unbanked subscriber's mobile wallet account is sufficient to accommodate the requested withdrawal for the specified amount of funds;

performing one or more of a limit check and a velocity check on the unbanked subscriber's mobile wallet account, the limit check determining whether sufficient funds are available to make the deposit amount, the velocity check determining whether the unbanked subscriber has exceeded a specified number of transactions within a specified time period;

returning a secure, perishable withdrawal code to the subscriber over at least one of the plurality of channels connected to the monetary transaction system;

receiving subsequent agent branch communication over at least one of the plurality of channels connected to

the monetary transaction system, the agent branch communication indicating that the withdrawal code has been presented to the agent branch;

debiting the unbanked subscriber's mobile wallet account by the specified amount of funds;

returning a notification to the agent branch confirming the withdrawal; and

notifying the subscriber that the specified amount of funds was withdrawn from the unbanked subscriber's mobile wallet account over at least one of the channels connected to the monetary transaction system.

5. A monetary transaction system for conducting monetary transactions between unbanked subscribers and other entities, the system comprising:

a mobile device configured to run a monetary transaction system application;

a monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system;

a monetary transaction system processor that performs the one or more transactions specified by the subscriber, wherein performing the specified transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile;

at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system; and

wherein the monetary transaction system is implemented to transfer money between mobile wallets, including performing the following steps:

receiving subscriber communication over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to transfer a specified amount of funds to specified recipient using a specified payment method from the subscriber's mobile wallet;

validating the status of the selected payment method;

performing at least one of a limit check and a velocity check on the selected payment method, the limit check determining whether sufficient funds are available to make the deposit amount, the velocity check determining whether the unbanked subscriber has exceeded a specified number of transactions within a specified time period;

validating the status of the specified recipient to ensure the specified recipient has a valid mobile wallet account;

debiting the specified payment method by the specified amount of funds;

transferring the specified amount of funds to the specified recipient over at least one of the plurality of channels connected to the monetary transaction system;

notifying the unbanked subscriber that the specified amount of funds was transferred to the specified recipient over at least one of the plurality of channels connected to the monetary transaction system.

6. The monetary transaction system of claim **5**, wherein validating the status of the specified recipient comprises performing a check on the specified recipient to comply with the office of foreign assets control.

7. The monetary transaction system of claim **5**, wherein the money is transferred internationally between the mobile wallets.

* * * * *

Exhibit B
PayPal Infringement Chart for
U.S. Patent No. 8,538,845

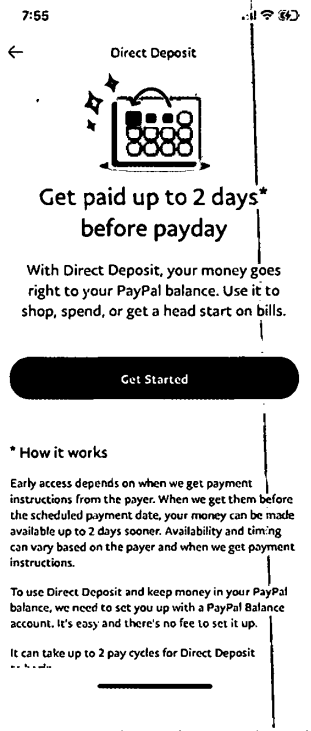
U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
5. A monetary transaction system for conducting monetary transactions between unbanked subscribers and other entities, the system comprising:	Upon information and belief, PayPal manages a transaction system and payment application that allows users to make monetary transactions between parties, including parties that do not have PayPal accounts. The transactions do not need to be linked to a bank account and can consist of cash payments deposited into the account or direct deposits made into the account. SEND AND REQUEST MONEY FOR FREE • When funded by a bank account or with your PayPal balance, it's free and secure to send money or ask for it back from friends and family in the US. • Just type a name, email or phone number and PayPal will find the right person for you if they have an account. • Request money quickly and securely from friends or family and personalize your payments with animations, stickers, emojis and more. *See* https://apps.apple.com/app/id283646709?mt=8 (last accessed on February 25, 2022).

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

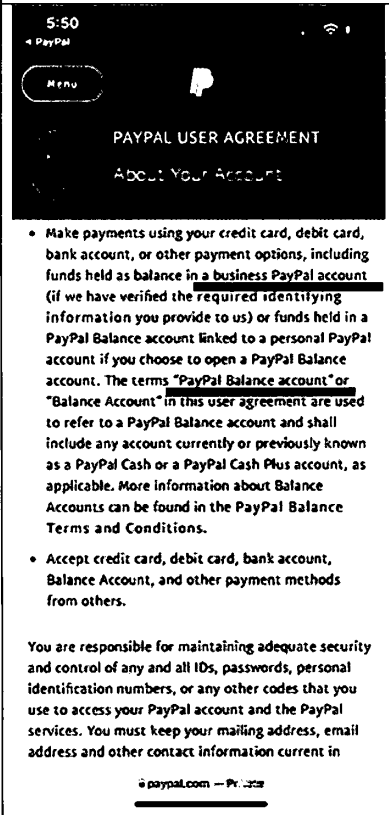
U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* Screenshot of PayPal Mobile Balance Account showing zero balance.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 73 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* Screenshot of PayPal Mobile Balance Account with option to directly deposit wages etc. into the account.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* PayPal User Agreement on PayPal Mobile App identifying both business and private PayPal balance accounts.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 75 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	Money sent by someone else to your personal PayPal account will automatically be placed in your Balance Account. To receive money in a currency your Balance Account is not currently configured to accept, it may be necessary to create a balance in your Balance Account in that currency or convert the money into another currency. Certain currencies can only be received by converting the money into another currency that PayPal allows you to hold. If the money is converted, PayPal's transaction exchange rate (including our currency conversion spread) will be used. You can load funds into your Balance Account at retail stores or you can load funds into it using the remote check capture feature. Fees associated with in-store cash reload and some remote check capture transactions can be found in the PayPal Balance Long Form Disclosure. You may arrange to have all or part of your paycheck or any federal or state government benefit or payment (e.g., Federal tax refunds or Social Security payment) transferred directly into your Balance Account by your employer or government payer, as applicable, by using the Direct Deposit feature. To enroll, you will need to provide your employer or the government payer, as applicable, with the account and routing numbers found in the Direct Deposit section available in the PayPal app. Your employer or government payer may also ask you to fill out their own direct deposit form. We do not charge any fees to set up or maintain Direct Deposit. *See* https://www.paypal.com/us/webapps/mpp/ua/useragreement-full (last accessed on February 25, 2022). About Payment Methods PayPal allows you to make payments using a variety of methods including: PayPal balance, a bank account, PayPal Credit, debit or credit cards, and rewards balance. This page does not address unauthorized transactions. For information on your protection against unauthorized transactions, please see the Error Resolution section of the PayPal User Agreement. *See* https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022).

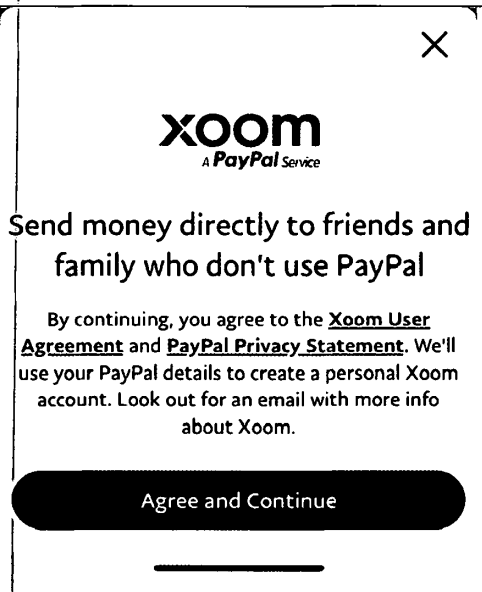
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 76 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

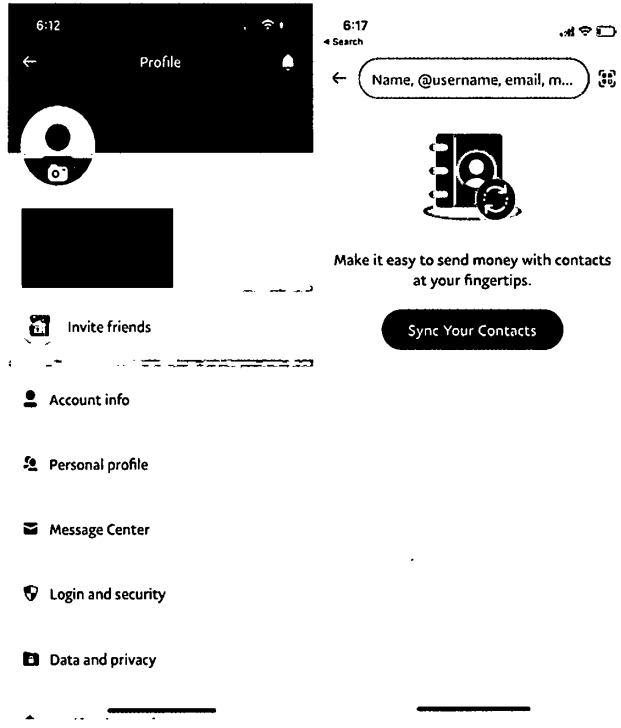
U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	How do I send a payment using my PayPal balance? Payments are automatically made using your PayPal balance first if the currency of your payment is the same as the one of your balance. To send a payment: 1. Click **Send and Request** at the top of the page. 2. Click **Pay for goods or services.** 3. Enter the recipient's email address, and click **Next.** 4. Enter the amount you want to send, and click **Continue.** 5. Review your payment information, and click **Send Payment Now.** *See* https://www.paypal.com/bs/smarthelp/article/how-do-i-send-a-payment-using-my-paypal-balance-faq1844 (last accessed on February 25, 2022).

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 77 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* Screenshot PayPal Mobile Application identifying Xoom service.
1[a] a mobile device configured to run a monetary transaction system application;	Upon information and belief, the PayPal System uses a mobile device loaded with the PayPal application that can be obtained through third party application stores. The application stores allow end users to download the PayPal application and perform monetary transactions through the PayPal System. On information and belief, the PayPal user and/or PayPal facilitates and derives the beneficial use of the claimed system. *See* Claim 5 preamble.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
1[b] a monetary transaction system subscriber that has a profile with the monetary transaction system, wherein the subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system; a monetary transaction system processor that performs the one or more transactions specified by the subscriber, wherein performing the specified transactions includes communicating with a monetary	Upon information and belief, the PayPal system allows users to create a profile and perform transactions using the PayPal System.  *See* Screenshots of PayPal Mobile app showing personal profile screen and contact screen for initiating mobile transactions. *See also* Preamble.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 79 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

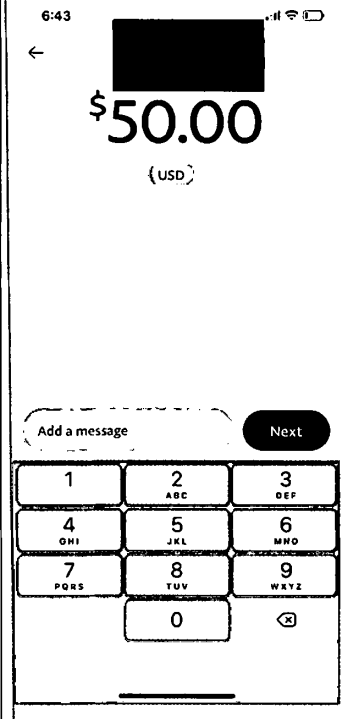
	U.S. Patent No. 8,538,845 (Claim 5)
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile;	
1[c] at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system; and	Upon information and belief, the PayPal system allows users to create a profile and perform transactions using the PayPal System. The users can make transactions if one user has a PayPal profile. *See* Preamble and element 1[b]. SEND AND REQUEST MONEY FOR FREE • When funded by a bank account or with your PayPal balance, it's free and secure to send money or ask for it back from friends and family in the US. • Just type a name, email or phone number and PayPal will find the right person for you if they have an account. • Request money quickly and securely from friends or family and personalize your payments with animations, stickers, emojis and more. *See* https://apps.apple.com/app/id283646709?mt=8 (last accessed on February 25, 2022).
1[d] wherein the monetary transaction system is implemented to	Upon information and belief, the PayPal System allows users to transfer money between mobile wallets.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
transfer money between mobile wallets, including performing the following steps:	 *See* Screenshot of PayPal Mobile Application identifying specified amount of funds to be transferred.
1[e] receiving subscriber communication	Upon information and belief, the PayPal System, including the backend system receives a notification from the user indicating a desire to transfer funds to a payment recipient. The notification indicates an amount and the payment method to be used.

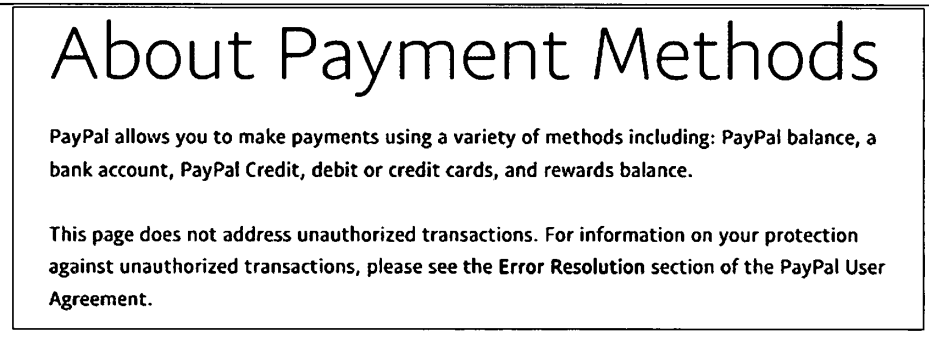
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 81 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
over one of a plurality of channels connected to the monetary transaction system, the subscriber communication indicating that an unbanked subscriber desires to transfer a specified amount of funds to specified recipient using a specified payment method from the subscriber's mobile wallet;	 *See* Screenshot of PayPal Mobile Application identifying specified amount of funds to be transferred.

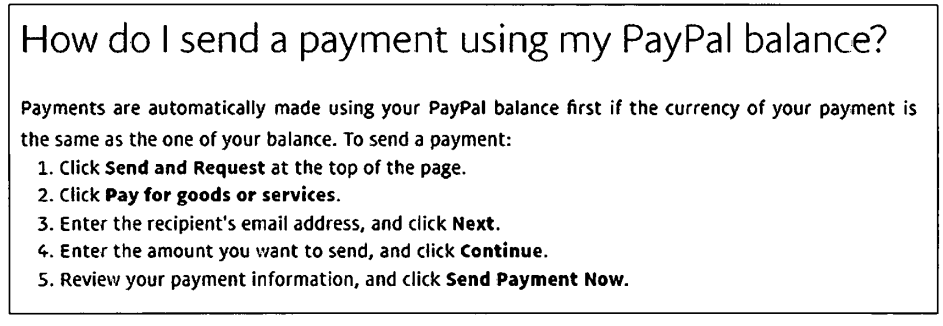
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 82 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

<table>
<tr><th colspan="2">U.S. Patent No. 8,538,845 (Claim 5)</th></tr>
<tr><th>Claims</th><th>Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")</th></tr>
<tr><td></td><td> 

See https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022).</td></tr>
<tr><td>1[f], 1[g], and 1[h] validating the status of the selected payment method;

performing at least one of a limit check and a velocity check on the selected payment method, the limit check determining whether sufficient funds are available to make the deposit</td><td>Upon information and belief, the PayPal System, checks the status of the selected payment method. For example, the PayPal system checks to determine whether the payment method can be used.

 
</td></tr>
</table>

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 83 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

	U.S. Patent No. 8,538,845 (Claim 5)
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
amount, the velocity check determining whether the unbanked subscriber has exceeded a specified number of transactions within a specified time period; validating the status of the specified recipient to ensure the specified recipient has a valid mobile wallet account;	*See* https://www.paypal.com/bs/smarthelp/article/how-do-i-send-a-payment-using-my-paypal-balance-faq1844 (last accessed on February 25, 2022). Upon information and belief, the PayPal System also performs a limit check to determine if there are sufficient available funds in the balance account to complete a transaction. Upon information and belief, the PayPal system also performs velocity check, including to identify fraud, to address regulatory requirements, or filter for transaction issues. Upon information and belief, the PayPal System includes velocity checks. These checks for example, monitor the number of transactions the user receive by minute, hour, etc. and the IP addresses of the user's customers. PayPal's Fraud Protection Services in the PayPal System include velocity checks along with many other filters to help assist in preventing fraud. Account number velocity filter The account number velocity filter is triggered for excessive use of a card within a short period of time. What does the filter do? The account number velocity filter triggers when any credit card account number is used five times within a three-day (72-hour) period. *See e.g.* https://developer.paypal.com/api/nvp-soap/payflow/fraud-protection/ (showing velocity functionality) (last accessed on February 25, 2022). Upon information and belief, the PayPal system includes functionality to further determine that the mobile wallet application is a valid account and is associated with the correct user. *See e.g.* https://developer.paypal.com/api/nvp-soap/payflow/fraud-protection/ (showing validating functionality) (last accessed on February 25, 2022).

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 84 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	Why are limitations placed on an account? There can be several reasons for an account limitation: • *An unauthorized person may be using your account.* If PayPal believes someone is using your account without your knowledge, the account could be limited to protect you from fraudulent charges while PayPal investigates the suspicious transactions. Similar steps may be taken if your debit or credit card issuer or bank notifies PayPal that someone has used your card or bank account without permission. • *The account is out of compliance with regulatory requirements.* Limitations can also be placed on an account that has been found to be out of compliance with regulatory requirements. For example, if you receive donations, you're required to provide documents confirming you're a registered nonprofit organization. PayPal may limit your account while you gather those documents or while we're working with you to satisfy any other regulatory requirements. The same is true if you don't follow PayPal's **Acceptable Use Policy**—selling banned items, such as prescription drugs or guns, for example. • *Your account has a high number of claims and chargebacks.* When there's a high number of **buyer claims and chargebacks** to your account, we may review your account. While we're reviewing, you may experience an account limitation. • *Sudden, rapid changes in what or how much you sell.* If you start to sell an entirely new type of product, specifically higher-end items like jewelry; or there's a rapid increase in sales volume, your account may be limited while PayPal reviews it. *See* https://www.paypal.com/us/brc/article/understanding-account-limitations (last accessed on February 25, 2022).

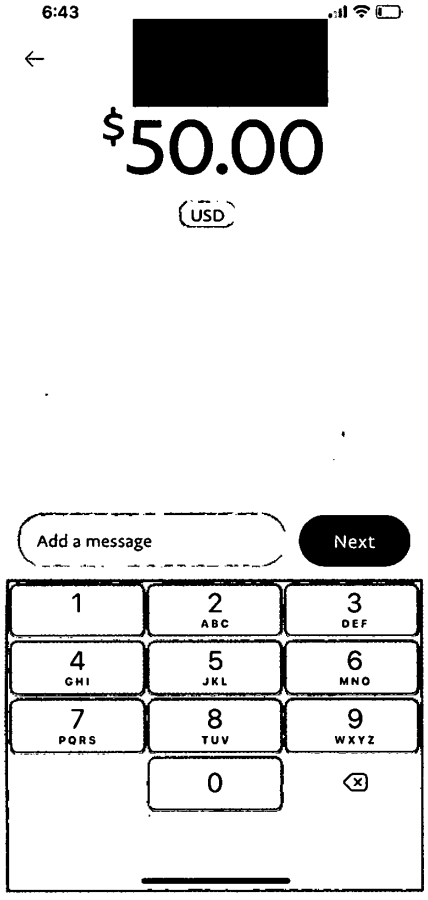
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 85 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
1[i], 1[j], and 1[k] debiting the specified payment method by the specified amount of funds; transferring the specified amount of funds to the specified recipient over at least one of the plurality of channels connected to the monetary transaction system; notifying the unbanked subscriber that the specified amount of funds was transferred to the specified recipient over at least one of the plurality of channels connected to the monetary transaction system.	Upon information and belief, the PayPal System, checks the status of the selected payment method. For example, the PayPal system checks to determine whether the payment method can be used. About Payment Methods PayPal allows you to make payments using a variety of methods including: PayPal balance, a bank account, PayPal Credit, debit or credit cards, and rewards balance. This page does not address unauthorized transactions. For information on your protection against unauthorized transactions, please see the Error Resolution section of the PayPal User Agreement. *See* https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022).

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 86 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 87 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 8,538,845 (Claim 5)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	See Screenshot of PayPal Mobile Application identifying specified amount of funds to be transferred.  *See* Screenshot of PayPal Mobile Application confirming notification of payment to second entity.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 88 of 381

Exhibit C
U.S. Patent No. 9,892,386

US009892386B2

(12) **United States Patent**
Liberty

(10) **Patent No.: US 9,892,386 B2**
(45) **Date of Patent: Feb. 13, 2018**

(54) **MONETARY TRANSACTION SYSTEM**

(71) Applicant: **Mozido, Inc.**, Austin, TX (US)
(72) Inventor: **Michael A. Liberty**, Orlando, FL (US)
(73) Assignee: **MOZIDO, INC.**, Austin, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **15/201,152**

(22) Filed: **Jul. 1, 2016**

(65) **Prior Publication Data**

US 2016/0314443 A1 Oct. 27, 2016

Related U.S. Application Data

(63) Continuation of application No. 14/213,543, filed on Mar. 14, 2014, now abandoned, which is a (Continued)

(51) **Int. Cl.**
G06Q 40/00 (2012.01)
G06Q 20/00 (2012.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G06Q 20/10*** (2013.01); ***G06Q 20/0855*** (2013.01); ***G06Q 20/322*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC G06Q 20/0855
USPC 705/40, 78
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,717,374 A 2/1998 Smith
5,828,739 A 10/1998 Nakanishi
(Continued)

FOREIGN PATENT DOCUMENTS

CA 2666616 4/2008
CN 101606400 12/2009
(Continued)

OTHER PUBLICATIONS

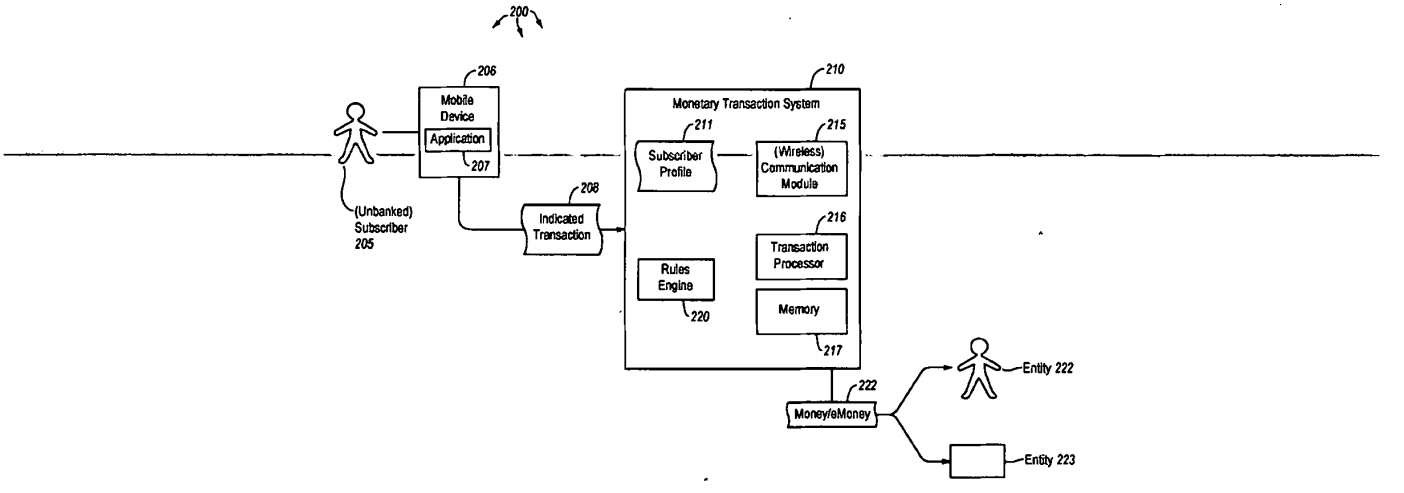
Chen, Jiajun Jim et al, Short-Range Wireless Technologies with Mobile Payments Systems. Proceedings of the 6th International Conference on Electronic Commerce [Online] 2004, pp. 649-656.
(Continued)

Primary Examiner — Edward Chang
(74) *Attorney, Agent, or Firm* — Workman Nydegger

(57) **ABSTRACT**

Embodiments are directed to monetary transaction system for conducting monetary transactions between transaction system subscribers and other entities. In one scenario, the monetary transaction system includes a mobile device that runs a monetary transaction system application. The monetary transaction system also includes a subscriber that has a profile with the system. The subscriber indicates a transaction that is to be performed with the monetary transaction system. The system further includes a monetary transaction system processor that performs the transactions specified by the subscriber including communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile. The monetary transaction system also includes at least one entity that is to be involved in the specified transaction, where the entity has a profile with the monetary transaction system. This entity may be a person, a retail store, an agent or other entity.

3 Claims, 46 Drawing Sheets



Related U.S. Application Data

continuation of application No. 13/964,707, filed on Aug. 12, 2013, now abandoned, which is a continuation of application No. 13/484,199, filed on May 30, 2012, now Pat. No. 8,538,845.

(60) Provisional application No. 61/522,099, filed on Aug. 10, 2011, provisional application No. 61/493,064, filed on Jun. 3, 2011.

(51) **Int. Cl.**

G06Q 20/10	(2012.01)
G06Q 20/08	(2012.01)
G06Q 40/02	(2012.01)
G06Q 20/32	(2012.01)
G06Q 20/40	(2012.01)
G06Q 20/36	(2012.01)
H04L 29/06	(2006.01)

(52) **U.S. Cl.**

CPC ***G06Q 20/3255*** (2013.01); ***G06Q 20/36*** (2013.01); ***G06Q 20/405*** (2013.01); ***G06Q 40/02*** (2013.01); ***H04L 63/101*** (2013.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,991,749	A	11/1999	Morrill	
6,021,397	A	2/2000	Jones et al.	
6,175,823	B1	1/2001	Van Dusen	
6,185,545	B1	2/2001	Resnick	
6,250,557	B1	6/2001	Forslund	
6,415,156	B1	7/2002	Stadelmann	
6,622,015	B1	9/2003	Himmel	
6,697,839	B2	2/2004	Sini	
6,714,797	B1	3/2004	Rautila	
6,736,322	B2	5/2004	Gobburu	
6,819,219	B1	11/2004	Bolle	
6,840,448	B2	1/2005	Fukushima	
6,862,575	B1	3/2005	Antilla et al.	
6,873,974	B1	3/2005	Schutzer	
6,957,342	B2	10/2005	Vatanen	
7,016,532	B2	3/2006	Boncyk	
7,024,174	B2 *	4/2006	Nagy	G06Q 20/04 455/408
7,054,430	B2	5/2006	Lynam	
7,069,001	B2	6/2006	Rupp	
7,089,208	B1	8/2006	Levchin	
7,099,850	B1	8/2006	Mann	
7,100,821	B2	9/2006	Rasti	
7,107,247	B2	9/2006	Kinoshita	
7,110,972	B1	9/2006	Handa	
7,221,939	B2	5/2007	Ylitalo	
7,240,836	B2	7/2007	Vrotsos	
7,248,855	B2	7/2007	Joyce	
7,255,264	B2	8/2007	De Leon	
7,275,685	B2	10/2007	Gray	
7,322,043	B2	1/2008	Letsinger	
7,325,132	B2	1/2008	Takayama	
7,334,720	B2	2/2008	Hulst et al.	
7,347,361	B2	3/2008	Lovett	
7,349,871	B2	3/2008	Labrou	
7,353,382	B2	4/2008	Labrou	
7,363,261	B2	4/2008	Whitehead	
7,370,017	B1	5/2008	Lindeman	
7,403,652	B2	7/2008	Boncyk	
7,421,410	B1	9/2008	Schechtman et al.	
7,461,010	B2	12/2008	Kwan	
7,461,028	B2	12/2008	Wronski	
7,477,780	B2	1/2009	Boncyk	
7,494,055	B2	2/2009	Fernandes	
7,512,098	B2	3/2009	Jiang	
7,527,194	B2	5/2009	Truitt	
7,548,915	B2	6/2009	Ramer	
7,562,818	B1	7/2009	Bierbaum	
7,564,469	B2	7/2009	Cohen	
7,565,008	B2	7/2009	Boncyk	
7,606,560	B2	10/2009	Labrou	
7,657,489	B2	2/2010	Stambaugh	
7,677,973	B2	3/2010	Van Luchene	
7,680,324	B2	3/2010	Boncyk	
7,689,506	B2	3/2010	Fei et al.	
7,694,876	B2	4/2010	Barnes et al.	
7,699,218	B2	4/2010	Garcia	
7,708,194	B2	5/2010	Vawter	
7,729,963	B1	6/2010	Lego	
7,729,987	B1	6/2010	Wakim	
7,748,618	B2	7/2010	Vawter	
7,774,076	B2	8/2010	Skowronek	
7,774,231	B2	8/2010	Pond	
7,775,437	B2	8/2010	Cohen	
7,784,684	B2	8/2010	Labrou	
7,801,826	B2	9/2010	Labrou	
7,819,307	B2	10/2010	Lyons	
7,822,688	B2	10/2010	Labrou	
7,823,772	B2	11/2010	Vawter	
7,848,500	B2	12/2010	Lynam	
7,848,504	B2	12/2010	Lynam	
7,865,414	B2	1/2011	Fung	
7,865,431	B2	1/2011	Takayama	
7,877,605	B2	1/2011	Labrou	
7,881,529	B2	2/2011	Boncyk	
7,886,962	B2	2/2011	Vawter	
7,890,424	B1	2/2011	Wakim	
7,899,243	B2	3/2011	Boncyk	
7,899,252	B2	3/2011	Boncyk	
7,937,302	B1	5/2011	Lego	
7,937,305	B1	5/2011	Lego	
7,942,317	B2	5/2011	Racz et al.	
7,958,052	B2	6/2011	Powell	
7,967,196	B1	6/2011	Bierbaum	
7,979,026	B2	7/2011	Hulvey	
7,988,060	B2	8/2011	Killian	
8,016,185	B2	9/2011	Modi	
8,019,365	B2	9/2011	Fisher	
8,033,458	B2	10/2011	Hulst et al.	
8,041,338	B2	10/2011	Chen	
8,052,042	B2	11/2011	Kolinski-Schultz	
8,060,012	B2	11/2011	Sklovsky	
8,061,598	B2	11/2011	Racz et al.	
8,073,783	B2	12/2011	Felsted	
8,077,042	B2	12/2011	Peeters	
8,090,945	B2	1/2012	Singhal	
8,095,113	B2	1/2012	Kean	
8,116,734	B2	2/2012	Vawter	
8,116,773	B2	2/2012	Chitrapu	
8,118,221	B2	2/2012	Racz et al.	
8,121,945	B2	2/2012	Rackley	
8,130,242	B2	3/2012	Cohen	
8,145,568	B2	3/2012	Rackley	
8,160,959	B2	4/2012	Rackley	
8,170,485	B2	5/2012	Hulvey	
8,190,087	B2	5/2012	Fisher	
8,195,576	B1	6/2012	Grigg	
8,196,131	B1	6/2012	von Behren	
8,213,470	B2	7/2012	Gu	
8,218,873	B2	7/2012	Boncyk	
8,229,354	B2	7/2012	Sklovsky	
8,239,325	B2	8/2012	Schwarz	
8,275,312	B2	9/2012	Fisher	
8,290,433	D2	10/2012	Fisher	
8,332,272	B2	12/2012	Fisher	
8,333,319	B2	12/2012	Roth	
8,336,772	B2	12/2012	Racz et al.	
8,352,323	B2	1/2013	Fisher	
8,355,670	B2	1/2013	White	
8,359,265	B2	1/2013	Van Rensburg	
8,360,329	B2	1/2013	Grigg	
8,374,916	B2	2/2013	White	
8,380,177	B2	2/2013	Laracey	
8,396,793	B2	3/2013	Hill	
8,487,771	B2	7/2013	Hsieh et al.	
8,538,845	B2	9/2013	Liberty	

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,577,803 B2 11/2013 Chatterjee et al.
8,612,325 B2 12/2013 Stacy et al.
8,632,000 B2 1/2014 Laracey
9,208,488 B2 12/2015 Liberty
2001/0011248 A1 8/2001 Himmel
2001/0037264 A1 11/2001 Husemann
2001/0042785 A1 11/2001 Walker et al.
2002/0042776 A1 4/2002 Woo
2002/0052754 A1 5/2002 Joyce
2002/0060246 A1 5/2002 Gobburu
2002/0065774 A1 5/2002 Young
2002/0069123 A1 6/2002 Soderlind
2002/0131404 A1 9/2002 Mehta
2002/0141586 A1 10/2002 Margalit
2002/0152177 A1 10/2002 Wolf
2002/0161708 A1 10/2002 Offer
2003/0001010 A1 1/2003 Schmidt
2003/0026404 A1 2/2003 Joyce
2003/0055735 A1 3/2003 Cameron
2003/0071115 A1 4/2003 Horn
2003/0154165 A1 8/2003 Horn
2003/0195842 A1 10/2003 Reece
2004/0117302 A1 6/2004 Weichert et al.
2004/0181531 A1 9/2004 Becker
2004/0205618 A1 10/2004 Sini
2004/0235450 A1 11/2004 Rosenberg
2004/0248554 A1 12/2004 Khan
2005/0070265 A1 3/2005 Korpinen
2005/0071512 A1 3/2005 Kim et al.
2005/0080697 A1 4/2005 Foss
2005/0199709 A1 9/2005 Linior
2005/0222961 A1 10/2005 Staib
2005/0283434 A1 12/2005 Hahn-Carlson
2006/0116892 A1 6/2006 Grimes
2006/0136901 A1 6/2006 Nichols
2006/0165060 A1 7/2006 Dua
2006/0179452 A1 8/2006 Amodeo
2006/0200427 A1 9/2006 Morrison
2006/0253335 A1 11/2006 Keena et al.
2006/0287004 A1 12/2006 Fuqua
2007/0006327 A1 1/2007 Lal et al.
2007/0033285 A1 2/2007 Shiigi
2007/0106564 A1 5/2007 Matotek
2007/0123305 A1 5/2007 Chen
2007/0125838 A1 6/2007 Law
2007/0125840 A1 6/2007 Law
2007/0162471 A1 7/2007 Samuelsson
2007/0179885 A1 8/2007 Bird
2007/0198432 A1 8/2007 Pitroda
2007/0203850 A1 8/2007 Singh
2007/0241189 A1 10/2007 Slavin
2007/0244811 A1 10/2007 Tumminaro
2007/0255620 A1 11/2007 Tumminaro et al.
2007/0255652 A1 11/2007 Tumminaro et al.
2007/0255653 A1 11/2007 Tumminaro
2007/0265984 A1 11/2007 Santhana
2008/0006685 A1 1/2008 Rackley
2008/0010191 A1 1/2008 Rackley
2008/0010196 A1 1/2008 Rackley
2008/0010204 A1 1/2008 Rackley
2008/0010215 A1 1/2008 Rackley
2008/0011825 A1 1/2008 Giordano
2008/0017704 A1 1/2008 VanDeburg
2008/0040265 A1 2/2008 Rackley
2008/0040285 A1 2/2008 Wankmueller
2008/0052192 A1 2/2008 Fisher
2008/0065490 A1 3/2008 Novick et al.
2008/0097851 A1 4/2008 Bemmel
2008/0126145 A1 5/2008 Rackley
2008/0126929 A1 5/2008 Bykov
2008/0143487 A1 6/2008 Hulvey
2008/0197190 A1 8/2008 Fujita
2008/0204358 A1 8/2008 Sato
2008/0208743 A1 8/2008 Arthur
2008/0208744 A1 8/2008 Arthur
2008/0208762 A1 8/2008 Arthur
2008/0210751 A1 9/2008 Kim
2008/0249927 A1 10/2008 Rethorn
2008/0249928 A1 10/2008 Hill
2008/0249930 A1 10/2008 Hill
2008/0249933 A1 10/2008 Rethorn
2008/0255947 A1 10/2008 Friedman
2008/0275779 A1 11/2008 Lakshminarayanan
2008/0281737 A1 11/2008 Fajardo
2009/0024526 A1 1/2009 Erickson
2009/0037326 A1 2/2009 Chitti
2009/0055322 A1 2/2009 Bykov
2009/0063312 A1 3/2009 Hurst
2009/0081989 A1 3/2009 Wuhrer
2009/0098854 A1 4/2009 Park
2009/0104888 A1 4/2009 Cox
2009/0106148 A1 4/2009 Prada
2009/0108015 A1 4/2009 Kreamer
2009/0119190 A1 5/2009 Realini
2009/0132362 A1 5/2009 Fisher
2009/0132392 A1 5/2009 Davis
2009/0138366 A1 5/2009 Bemmel
2009/0144161 A1 6/2009 Fisher
2009/0156190 A1 6/2009 Fisher
2009/0157546 A1 6/2009 Garcia
2009/0177578 A1 7/2009 Garcia
2009/0177581 A1 7/2009 Garcia
2009/0210308 A1 8/2009 Toomer
2009/0222353 A1 9/2009 Guest
2009/0222358 A1 9/2009 Bednarek
2009/0234751 A1 9/2009 Chan et al.
2009/0248537 A1 10/2009 Sarkeshik
2009/0254440 A1 10/2009 Pharris
2009/0254479 A1 10/2009 Pharris
2009/0265272 A1 10/2009 Dill et al.
2009/0281904 A1 11/2009 Pharris
2009/0288012 A1 11/2009 Hertel
2009/0299844 A1 12/2009 Reilly
2009/0307132 A1 12/2009 Phillips
2010/0010964 A1 1/2010 Skowronek
2010/0023449 A1 1/2010 Skowronek
2010/0030651 A1 2/2010 Matotek et al.
2010/0044430 A1 2/2010 Song
2010/0048226 A1 2/2010 Owen
2010/0049599 A1 2/2010 Owen
2010/0051685 A1 3/2010 Royyuru
2010/0057614 A1 3/2010 Rainey
2010/0057619 A1 3/2010 Weller
2010/0057624 A1 3/2010 Hurt
2010/0063895 A1 3/2010 Dominguez
2010/0088188 A1 4/2010 Kumar
2010/0114739 A1 5/2010 Johnston
2010/0125495 A1 5/2010 Smith
2010/0125510 A1 5/2010 Smith
2010/0146607 A1 6/2010 Piepenbrink et al.
2010/0151790 A1 6/2010 Hoeksel et al.
2010/0197326 A1 8/2010 Ngo
2010/0223110 A1 9/2010 Slavin
2010/0235283 A1 9/2010 Gerson
2010/0248710 A1 9/2010 Sklovsky
2010/0250356 A1 9/2010 Gillenson
2010/0250436 A1 9/2010 Loevenguth
2010/0260388 A1 10/2010 Garrett
2010/0333129 A1 12/2010 Alhadeff et al.
2011/0047016 A1 2/2011 Cook
2011/0057025 A1 3/2011 Denzer
2011/0087529 A1 4/2011 Angell
2011/0087610 A1 4/2011 Batada
2011/0105022 A1 5/2011 Vawter
2011/0113473 A1 5/2011 Corda
2011/0145049 A1 6/2011 Hertel
2011/0145149 A1 6/2011 Valdes
2011/0179113 A1 7/2011 Thomas
2011/0196788 A1 8/2011 Lu et al.
2011/0218911 A1 9/2011 Spodak
2011/0246284 A1 10/2011 Chaikin
2011/0250866 A1 10/2011 Fisher
2011/0251941 A1 10/2011 Dunwoody
2011/0258024 A1 10/2011 Prince

(56) **References Cited**

U.S. PATENT DOCUMENTS

2011/0258115 A1 10/2011 Mulhim
2011/0276417 A1 11/2011 Campbell
2011/0295750 A1 12/2011 Rammal
2011/0302016 A1 12/2011 Haddad
2011/0302406 A1 12/2011 Machani
2011/0313924 A1 12/2011 Carell
2011/0320243 A1 12/2011 Khan
2011/0320293 A1 12/2011 Khan
2011/0320294 A1 12/2011 Votaw
2011/0320345 A1 12/2011 Taveau
2012/0005076 A1 1/2012 Dessert
2012/0011058 A1 1/2012 Pitroda et al.
2012/0011063 A1 1/2012 Killian
2012/0028612 A1 2/2012 Hurst
2012/0029990 A1 2/2012 Fisher
2012/0047070 A1 2/2012 Pharris
2012/0074232 A1 3/2012 Spodak
2012/0078735 A1 3/2012 Bauer
2012/0079521 A1 3/2012 Garg et al.
2012/0084203 A1 4/2012 Mehew
2012/0095855 A1 4/2012 Sterling
2012/0095856 A1 4/2012 Sanjeev
2012/0122447 A1 5/2012 Craft
2012/0123841 A1 5/2012 Taveau
2012/0123868 A1 5/2012 Brudnicki
2012/0123880 A1 5/2012 Craft
2012/0123935 A1 5/2012 Brudnicki
2012/0123937 A1 5/2012 Spodak
2012/0131653 A1 5/2012 Pasquero
2012/0143752 A1 6/2012 Wong
2012/0150669 A1 6/2012 Langley
2012/0158589 A1 6/2012 Katzin
2012/0166311 A1 6/2012 Dwight
2012/0171992 A1 7/2012 Cheong
2012/0172026 A1 7/2012 Kwon
2012/0172089 A1 7/2012 Bae
2012/0174189 A1 7/2012 Lim
2012/0191557 A1 7/2012 Fisher
2012/0191612 A1 7/2012 Spodak
2012/0196586 A1 8/2012 Grigg
2012/0197691 A1 8/2012 Grigg
2012/0197740 A1 8/2012 Grigg
2012/0197743 A1 8/2012 Grigg
2012/0197745 A1 8/2012 Fisher
2012/0197787 A1 8/2012 Grigg
2012/0203610 A1 8/2012 Grigg et al.
2012/0203632 A1 8/2012 Blum
2012/0209688 A1 8/2012 Lamothe
2012/0209749 A1 8/2012 Hammad
2012/0215701 A1 8/2012 Mehta
2012/0221421 A1 8/2012 Hammad
2012/0221475 A1 8/2012 Grigg
2012/0226610 A1 9/2012 Gill
2012/0229647 A1 9/2012 Calman
2012/0229657 A1 9/2012 Calman
2012/0231424 A1 9/2012 Calman
2012/0231425 A1 9/2012 Calman
2012/0232937 A1 9/2012 Calman
2012/0232977 A1 9/2012 Calman
2012/0232983 A1 9/2012 Bertha
2012/0245986 A1 9/2012 Regan
2012/0253852 A1 10/2012 Pourfallah
2012/0259686 A1 10/2012 Yurrow
2012/0259698 A1 10/2012 Yurrow
2012/0259732 A1 10/2012 Sasankan
2012/0265677 A1 10/2012 Rackley
2012/0265685 A1 10/2012 Brudnicki
2012/0271712 A1 10/2012 Katzin
2012/0284131 A1 11/2012 Soffer
2012/0286928 A1 11/2012 Mullen
2012/0290376 A1 11/2012 Dryer
2012/0290449 A1 11/2012 Mullen
2012/0290478 A1 11/2012 Crofts et al.
2012/0293303 A1 11/2012 Khan
2012/0296708 A1 11/2012 Bachmann
2012/0296720 A1 11/2012 Pirillo
2012/0296722 A1 11/2012 Gosavi
2012/0296741 A1 11/2012 Dykes
2012/0297204 A1 11/2012 Buer
2012/0302204 A1 11/2012 Gupta
2012/0303425 A1 11/2012 Katzin
2012/0310720 A1 12/2012 Balsan
2012/0310760 A1 12/2012 Phillips
2012/0310824 A1 12/2012 Liberty
2012/0310826 A1 12/2012 Chatterjee
2012/0316950 A1 12/2012 LaPorte
2012/0316951 A1 12/2012 Fisher
2012/0316992 A1 12/2012 Oborne
2012/0317019 A1 12/2012 Carnes
2012/0323653 A1 12/2012 Fisher
2012/0323664 A1 12/2012 Klems
2012/0323670 A1 12/2012 Fisher
2012/0323777 A1 12/2012 Liberty
2012/0329394 A1 12/2012 Fisher
2012/0330737 A1 12/2012 Liberty
2012/0330792 A1 12/2012 Kashanian
2013/0012125 A1 1/2013 Fisher
2013/0012126 A1 1/2013 Fisher
2013/0012131 A1 1/2013 Fisher
2013/0013352 A1 1/2013 Fisher
2013/0013353 A1 1/2013 Fisher
2013/0013355 A1 1/2013 Fisher
2013/0013432 A1 1/2013 Fisher
2013/0013434 A1 1/2013 Fisher
2013/0013490 A1 1/2013 Keller
2013/0013498 A1 1/2013 Fisher
2013/0013499 A1 1/2013 Kalgi
2013/0013501 A1 1/2013 Rackley
2013/0017784 A1 1/2013 Fisher
2013/0018738 A1 1/2013 Faires
2013/0018740 A1 1/2013 Fisher
2013/0018742 A1 1/2013 Fisher
2013/0018793 A1 1/2013 Wong
2013/0023209 A1 1/2013 Fisher
2013/0023294 A1 1/2013 Singh
2013/0024220 A1 1/2013 Fisher
2013/0024221 A1 1/2013 Fisher
2013/0024223 A1 1/2013 Thomas
2013/0024280 A1 1/2013 Fisher
2013/0024364 A1 1/2013 Shrivastava et al.
2013/0024371 A1 1/2013 Hariramani
2013/0024372 A1 1/2013 Spodak
2013/0024377 A1 1/2013 Stong
2013/0029646 A1 1/2013 Chowdhury
2013/0030828 A1 1/2013 Pourfallah
2013/0030960 A1 1/2013 Kashanian
2013/0030997 A1 1/2013 Spodak
2013/0035035 A1 2/2013 Fisher
2013/0035036 A1 2/2013 Fisher
2013/0035037 A1 2/2013 Fisher
2013/0035068 A1 2/2013 Fisher
2013/0035069 A1 2/2013 Fisher
2013/0035070 A1 2/2013 Fisher
2013/0035071 A1 2/2013 Fisher
2013/0035072 A1 2/2013 Fisher
2013/0035087 A1 2/2013 Fisher
2013/0035967 A1 2/2013 Fisher
2013/0035968 A1 2/2013 Fisher
2013/0035969 A1 2/2013 Fisher
2013/0035970 A1 2/2013 Fisher
2013/0040568 A1 2/2013 Fisher
2013/0040569 A1 2/2013 Fisher
2013/0041699 A1 2/2013 Fisher
2013/0041700 A1 2/2013 Fisher
2013/0041701 A1 2/2013 Roth
2013/0041736 A1 2/2013 Coppinger
2013/0041743 A1 2/2013 Coppinger
2013/0041744 A1 2/2013 Coppinger
2013/0041745 A1 2/2013 Coppinger
2013/0041769 A1 2/2013 Fisher
2013/0046608 A1 2/2013 Coppinger
2013/0046634 A1 2/2013 Grigg
2013/0046645 A1 2/2013 Grigg
2013/0048723 A1 2/2013 King

(56) **References Cited**

U.S. PATENT DOCUMENTS

2013/0052952	A1	2/2013	Fisher
2013/0054336	A1	2/2013	Graylin
2013/0054337	A1	2/2013	Brendell
2013/0054412	A1	2/2013	Brendell
2013/0054441	A1	2/2013	Kamdar
2013/0057392	A1	3/2013	Bullock
2013/0060618	A1	3/2013	Barton
2013/0073373	A1	3/2013	Fisher
2013/0073377	A1	3/2013	Heath
2013/0073458	A1	3/2013	Sherwin
2013/0080228	A1	3/2013	Fisher
2013/0080229	A1	3/2013	Fisher
2013/0080230	A1	3/2013	Fisher
2013/0080231	A1	3/2013	Fisher
2013/0080232	A1	3/2013	Fisher
2013/0080233	A1	3/2013	Fisher
2013/0080240	A1	3/2013	Fisher
2013/0080241	A1	3/2013	Fisher
2013/0080329	A1	3/2013	Royyuru
2013/0091012	A1	4/2013	Liberty
2013/0132219	A1	5/2013	Liberty
2013/0238455	A1	9/2013	Laracey
2013/0246141	A1	9/2013	Liberty
2013/0246203	A1	9/2013	Laracey
2013/0317928	A1	11/2013	Laracey
2013/0332347	A1	12/2013	Liberty
2013/0346309	A1	12/2013	Giori
2014/0006048	A1	1/2014	Liberty
2014/0014721	A1	1/2014	Lindeman
2014/0201070	A1	7/2014	Liberty
2015/0039517	A1	2/2015	Liberty
2016/0055483	A1	2/2016	Liberty
2016/0055583	A1	2/2016	Liberty

FOREIGN PATENT DOCUMENTS

CN	102073958	5/2011
DE	10119808	9/2002
EP	1280115	1/2003
JP	2001-297198	10/2001
JP	2001357164	12/2001
JP	2002-99716	4/2002
KR	10-2002-0065989	8/2002
KR	10-2003-0068603	8/2003
KR	10-2007-0092400	9/2007
WO	9834203	8/1998
WO	9913636	3/1999
WO	0171627	9/2001
WO	0197118	12/2001
WO	02071354	9/2002
WO	03012717	2/2003
WO	2004010393	1/2004
WO	2004023353	3/2004
WO	2004053640	6/2004
WO	2004088641	10/2004
WO	2005079254	9/2005
WO	2005086593	9/2005
WO	2007145500	12/2007
WO	2008008735	1/2008
WO	2012025824	3/2012
WO	2013009444	1/2013
WO	2013009446	1/2013
WO	2013025273	2/2013
WO	2013078176	5/2013
WO	2013166174	11/2013

OTHER PUBLICATIONS

Labrou, Yannis et al, Wireless Wallet. Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services [Online] 2004, pp. 1-10.

Motorola, Motorola M-Wallet Solution. [Online] 2006 http://www.motorola.com/networkoperators/pdfs/M-Wallet-Brochure.pdf (Accessed Oct. 4, 2012).

Valcourt, E. et al., "Investigating Mobile Payment," Wireless And Mobile Computing, Networking and Communications, 2005. (WiMob'2005), IEEE International Conference on Aug. 22-24, 2005, Aug. 2005, vol. 4, pp. 29-36.

Gao, Jerry, et al., "P2P-Paid: A Peer-to-Peer Wireless Payment System," Proceedings of the 2005 Second IEEE International Workshop on Mobile Commerce and Services (WMCS'05) Jul. 2005, 10 pages.

Edwin, et al., "Technobiography," Oct. 2004, 29 pages.

International Search Report and Written Opinion for PCT/US2012/066013 dated Jan. 29, 2013.

International Search Report and Written Opinion for PCT/US2012/040131 dated Jan. 29, 2013.

International Search Report and Written Opinion for PCT/US2012/043321 dated Sep. 6, 2012.

International Search Report and Written Opinion for PCT/US2012/058849 dated Jan. 4, 2013.

International Search Report and Written Opinion for PCT/US2013/039100 dated Aug. 23, 2013.

European Search Report for EP12824344 dated Sep. 29, 2014.

Sykes, et al. "Securing Mobile Banking," Credit Union Management, Nov. 2010, vol. 33 No. 11; ISSN 0273-9267.

Clarke, Irvine III, "Emerging Value Propositions for M-commerce," *Journal of Business Strategies*, vol. 25, Issue 2, Fall 2008, p. 41-57; ISSN: 0887-2058.

Wei, et al., "Development of a Web-Based Mobile Airline Ticketing Model with Usability Features," 2005, Industrial Management + Data Systems; vol. 105 No. 9, ISSN: 0263-5577.

International Search Report and Written Opinion for PCT/US2012/43458 dated Aug. 17, 2012.

International Search Report and Written Opinion for PCT/US2015/58886 dated Feb. 4, 2016.

European Search Report for EP12851211 dated Feb. 18, 2016.

U.S. Appl. No. 13/484,199, Dec. 26, 2012, Office Action.

U.S. Appl. No. 13/484,199, Jun. 7, 2013, Notice of Allowance.

U.S. Appl. No. 13/527,466, Apr. 15, 2013, Office Action.

U.S. Appl. No. 13/527,466, Dec. 4, 2013, Final Office Action.

U.S. Appl. No. 13/964,707, Feb. 24, 2014, Office Action.

U.S. Appl. No. 14/213,543, May 6, 2014, Office Action.

U.S. Appl. No. 13/680,824, Jun. 16, 2014, Office Action.

U.S. Appl. No. 13/528,720, Jun. 25, 2014, Office Action.

U.S. Appl. No. 13/964,707, Jul. 10, 2014, Office Action.

U.S. Appl. No. 13/527,466, Aug. 1, 2014, Office Action.

U.S. Appl. No. 14/012,822, Aug. 7, 2014, Office Action.

U.S. Appl. No. 13/528,720, Dec. 10, 2014, Final Office Action.

U.S. Appl. No. 14/012,822, Jan. 7, 2015, Final Office Action.

U.S. Appl. No. 13/680,824, Feb. 6, 2015, Final Office Action.

U.S. Appl. No. 13/964,707, Mar. 16, 2015, Final Office Action.

U.S. Appl. No. 14/213,543, Apr. 8, 2015, Office Action.

U.S. Appl. No. 13/874,192, Jul. 14, 2015, Office Action.

U.S. Appl. No. 13/527,466, Jul. 16, 2015, Office Action.

U.S. Appl. No. 13/528,720, Jul. 22, 2015, Office Action.

U.S. Appl. No. 14/012,822, Sep. 11, 2015, Office Action.

U.S. Appl. No. 13/680,824, Sep. 18, 2015, Notice of Allowance.

U.S. Appl. No. 14/213,543, Jan. 6, 2016, Final Office Action.

U.S. Appl. No. 13/528,720, Mar. 2, 2016, Final Office Action.

U.S. Appl. No. 13/527,466, Apr. 1, 2016, Office Action.

U.S. Appl. No. 13/874,192, Apr. 18, 2016, Final Office Action.

U.S. Appl. No. 14/012,822, May 6, 2016, Final Office Action.

U.S. Appl. No. 13/527,466, Dec. 14, 2016, Office Action.

Office Action U.S. Appl. No. 13/527,466, dated Aug. 9, 2017.

Ron White, How Computers Work, Oct. 15, 2003, Paul Boger, Illustrated by Timothy Edward Dwons, 7th Edition (Year: 2003).

U.S. Appl. No. 14/341,605, dated Nov. 27, 2017, Office Action.

* cited by examiner

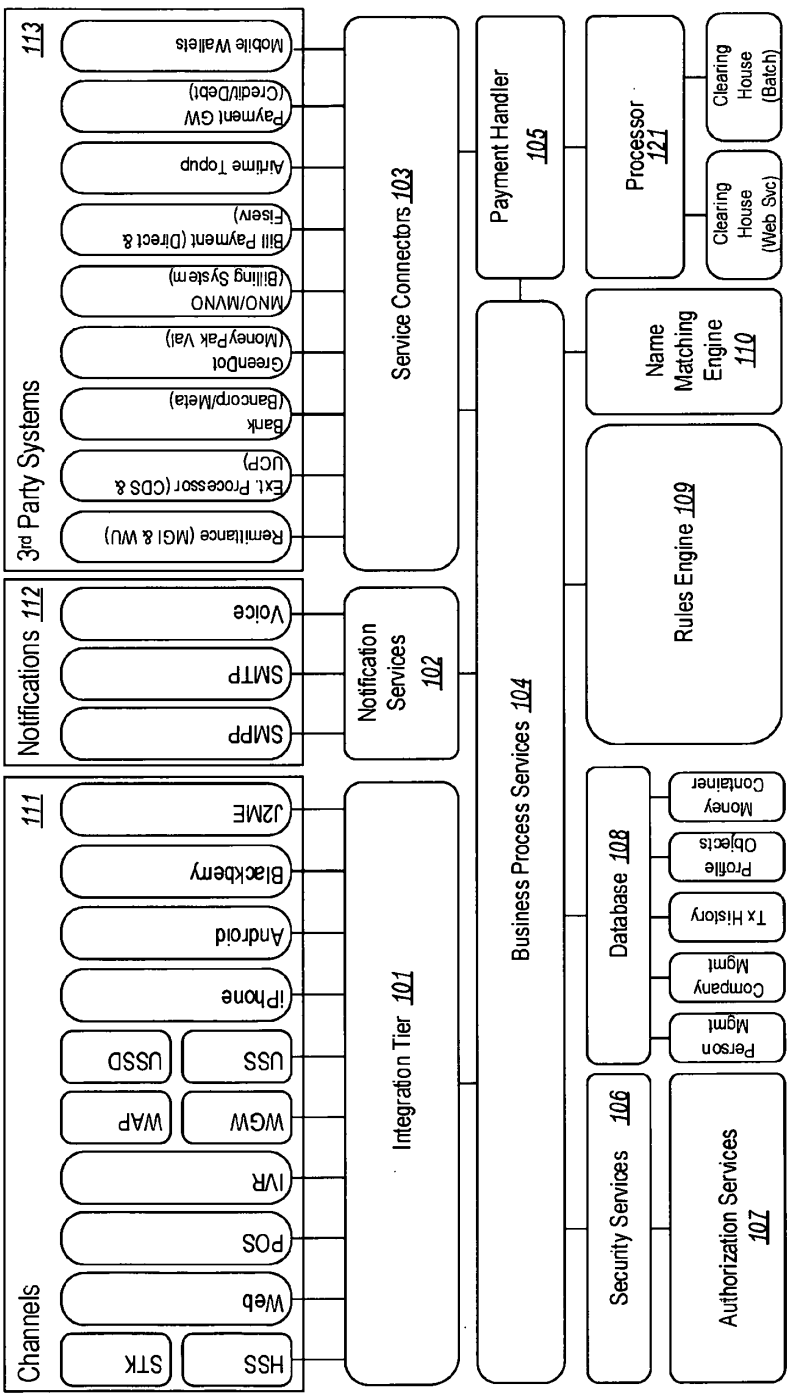


Figure 1

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 95 of 381

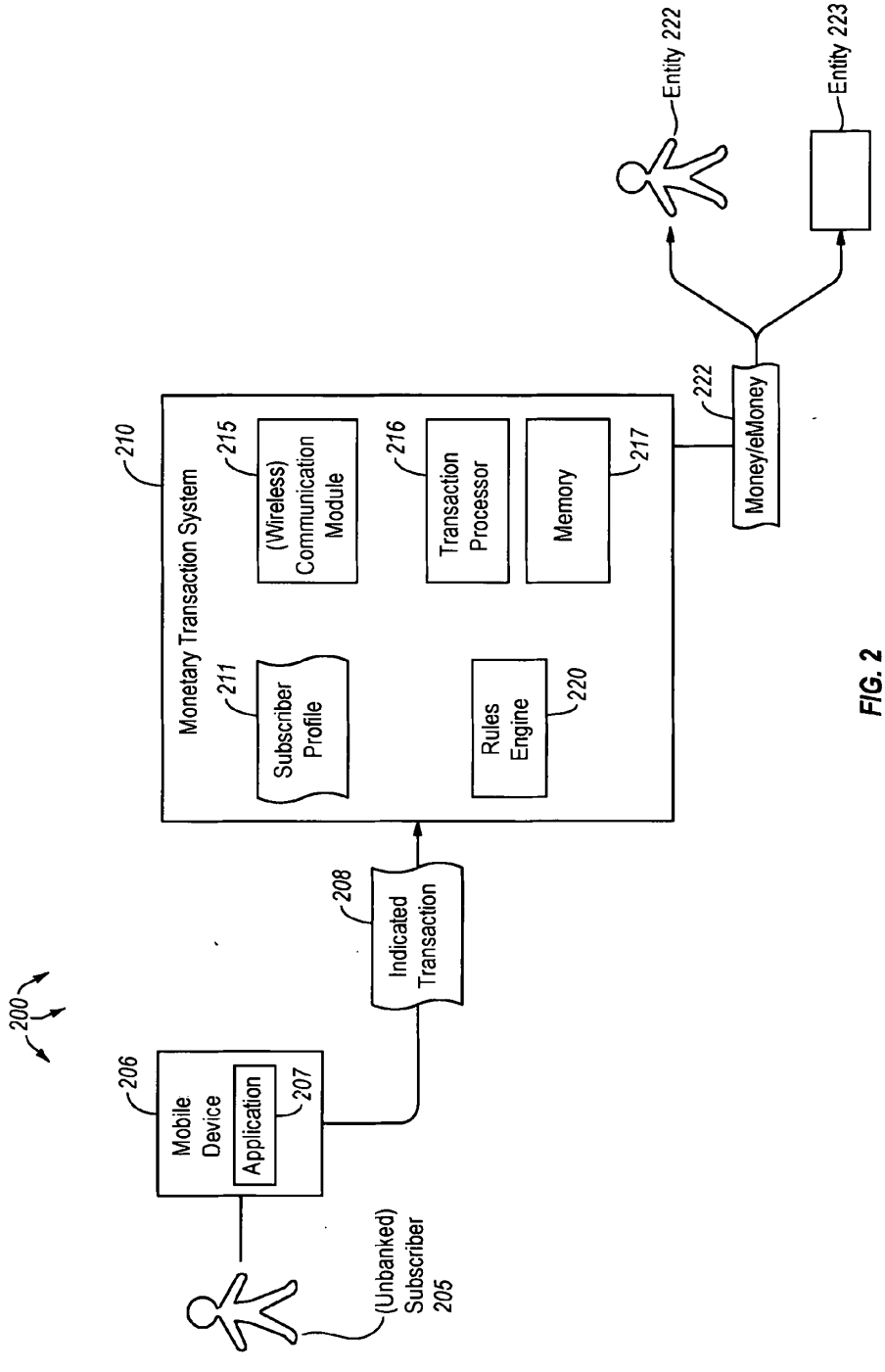
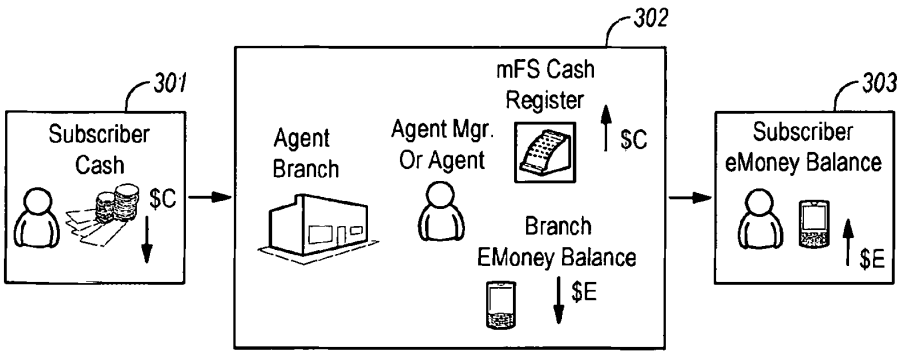


FIG. 2

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 96 of 381



Subscriber Deposit

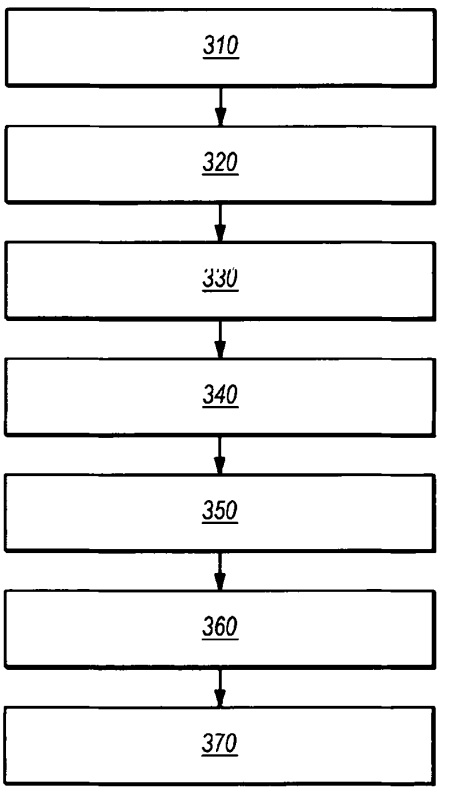
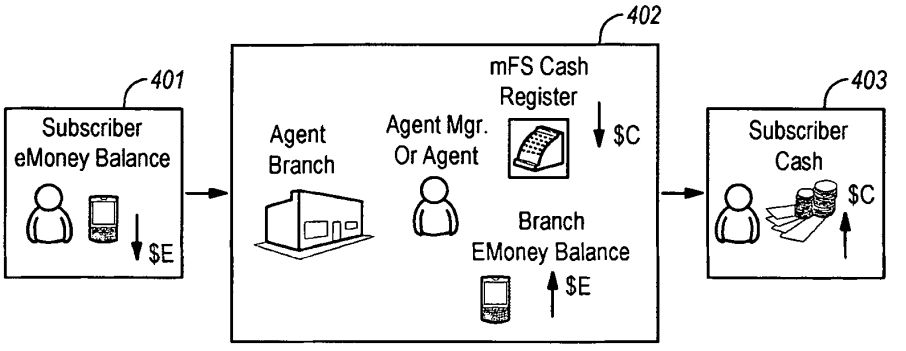


FIG. 3



Subscriber Withdrawal

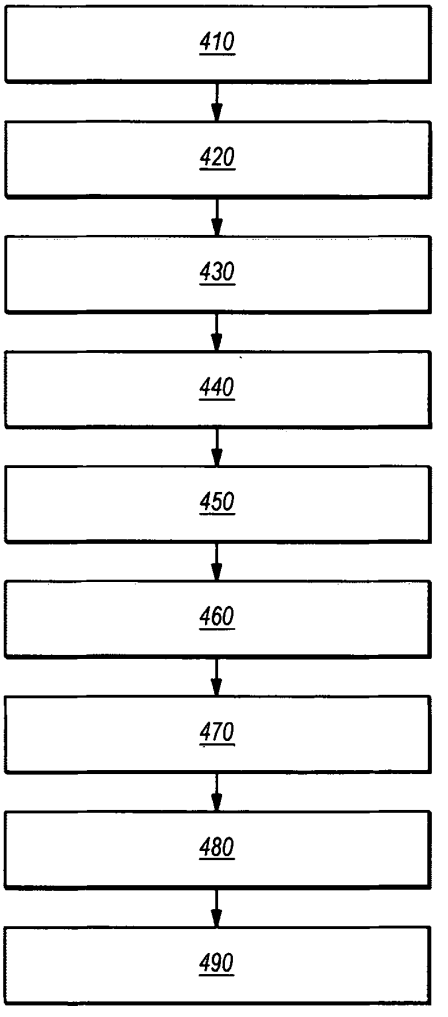
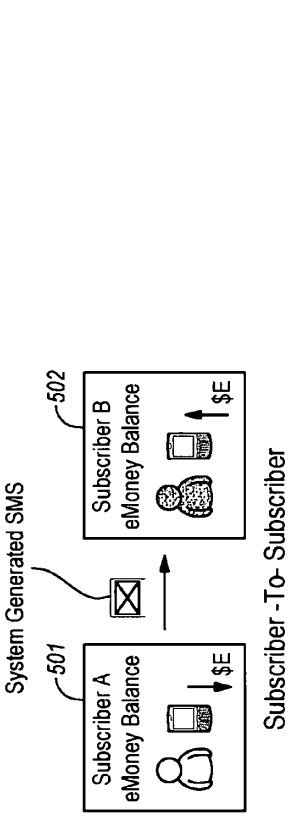
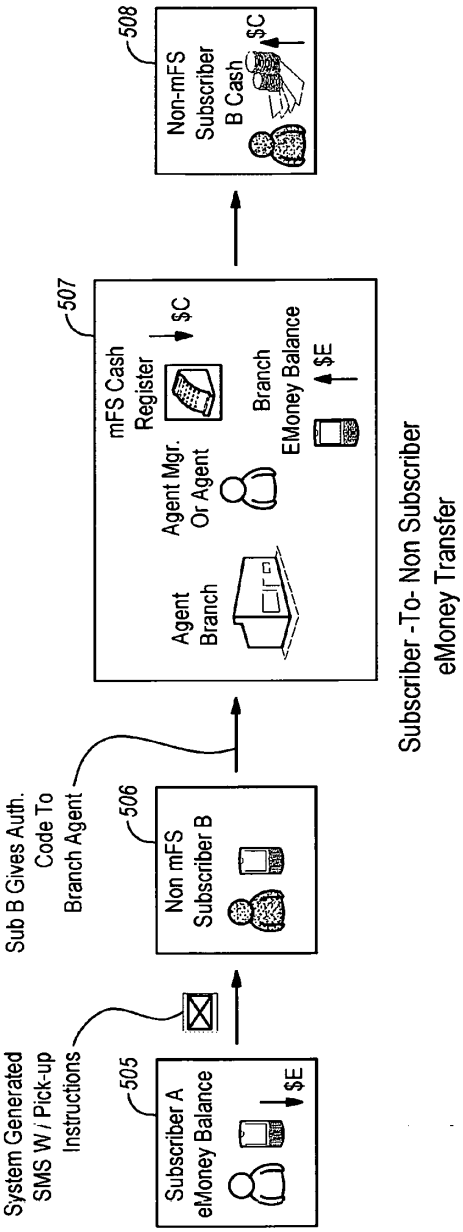


FIG. 4



Subscriber -To- Subscriber eMoney Transfer

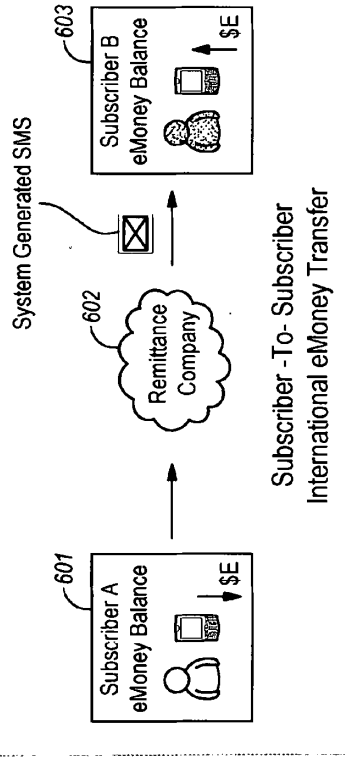
FIG. 5A



Subscriber -To- Non Subscriber eMoney Transfer

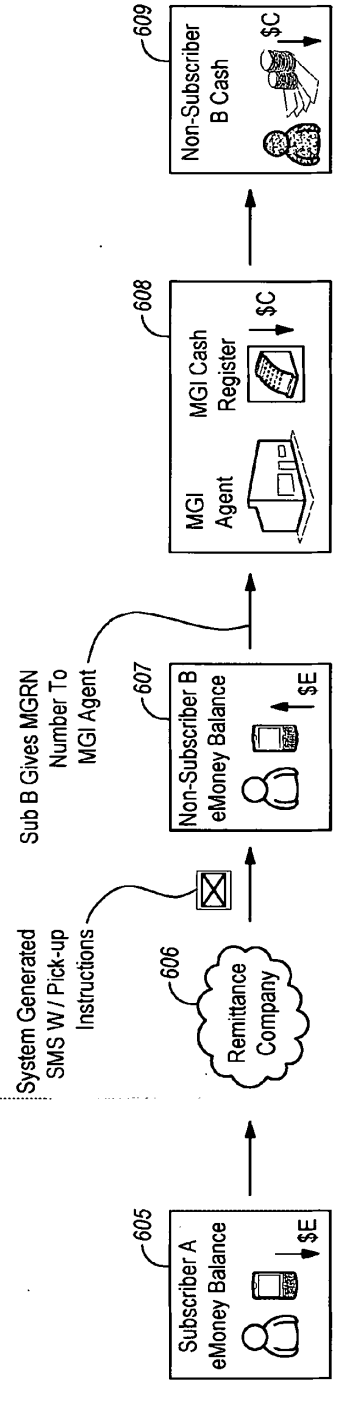
FIG. 5B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 99 of 381



Subscriber -To- Subscriber
International eMoney Transfer

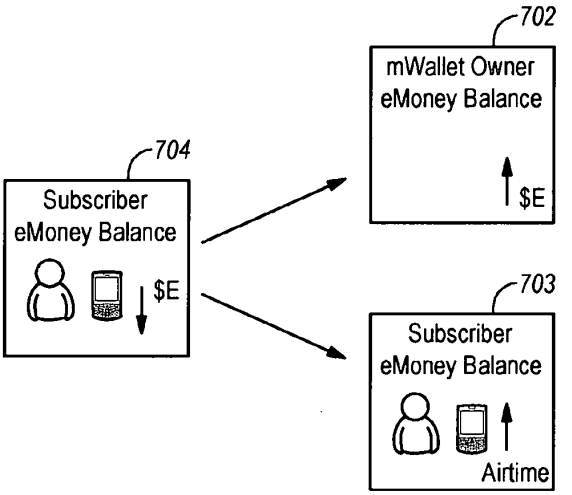
FIG. 6A



Subscriber -To- Non Subscriber
International eMoney Transfer

FIG. 6B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 100 of 381



Subscriber Buys Airtime

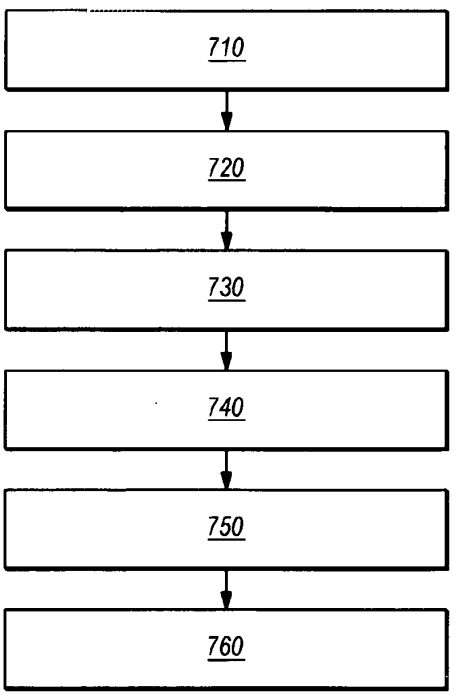
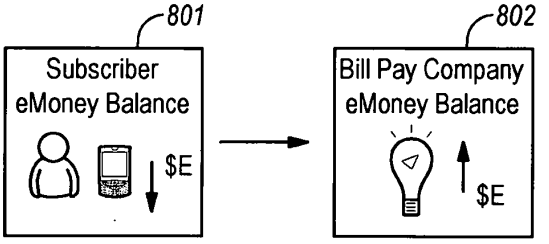


FIG. 7



Subscriber Pays Bill

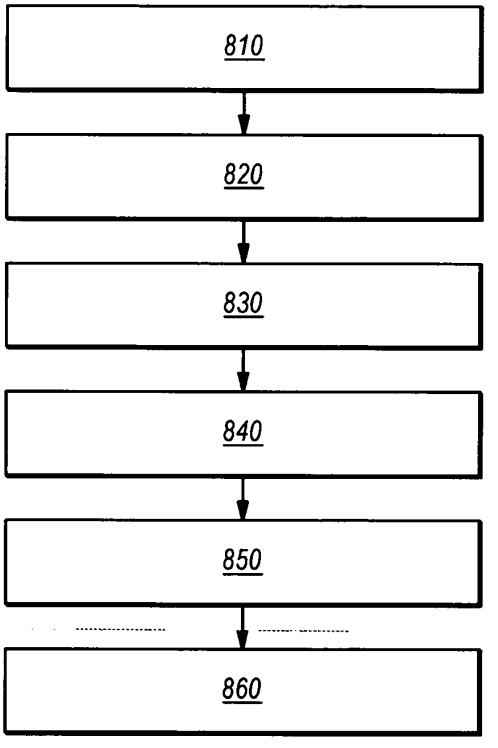
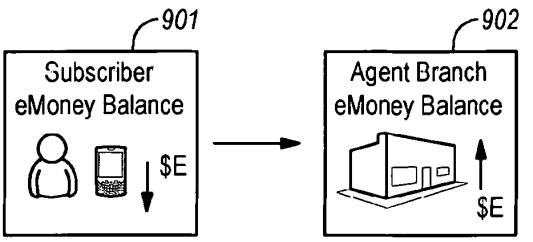


FIG. 8



Subscriber Makes Retail Purchase

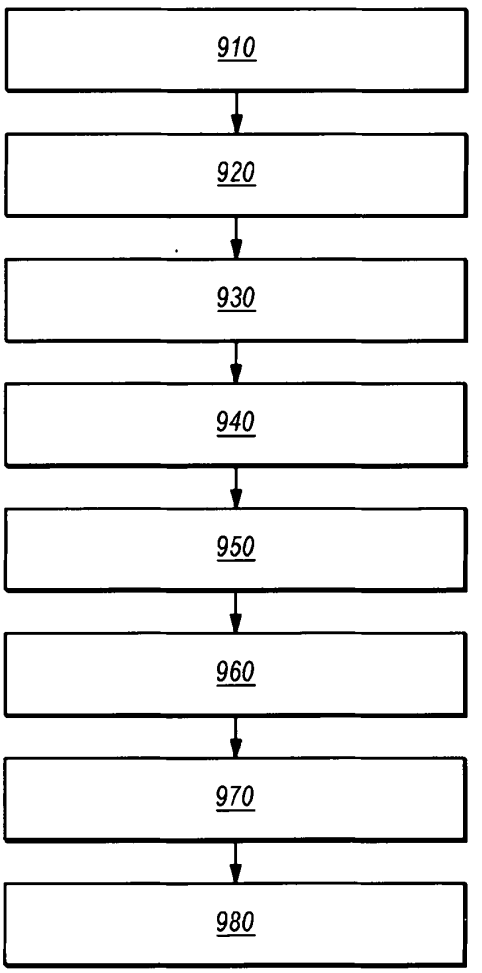
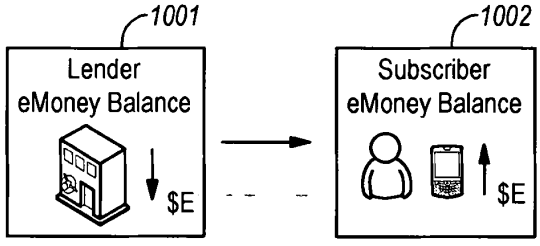
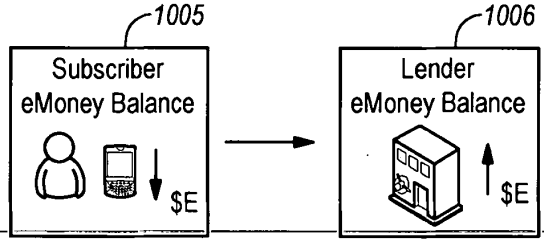


FIG. 9



Subscriber Requests Micro-Loan

FIG. 10A



Subscriber Repays Micro-Loan

FIG. 10B

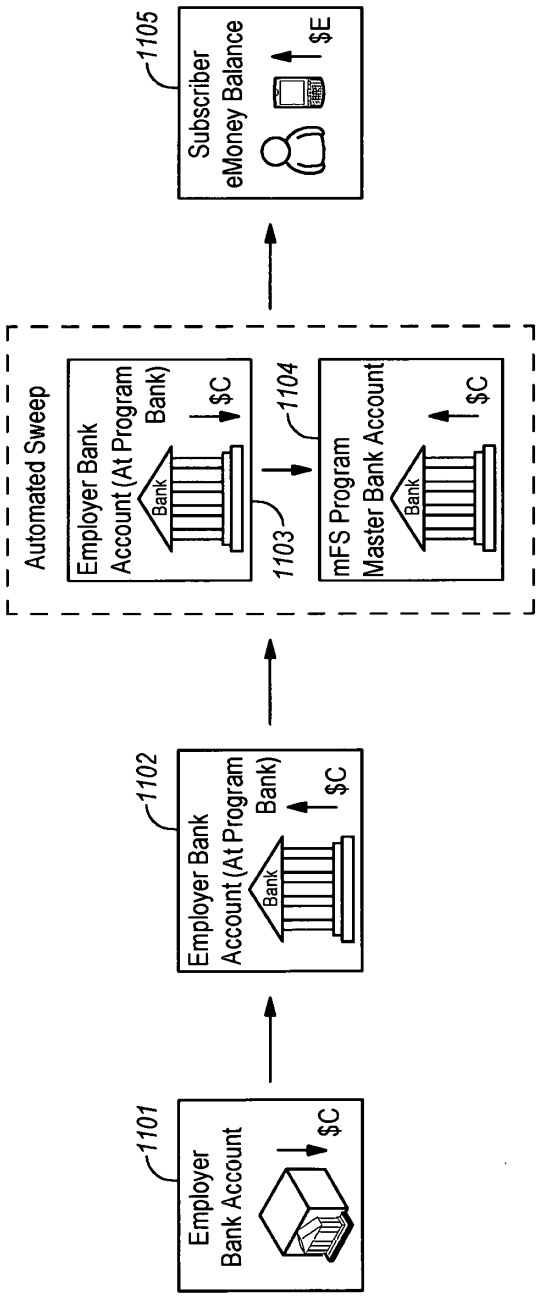


FIG. 11A

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 105 of 381

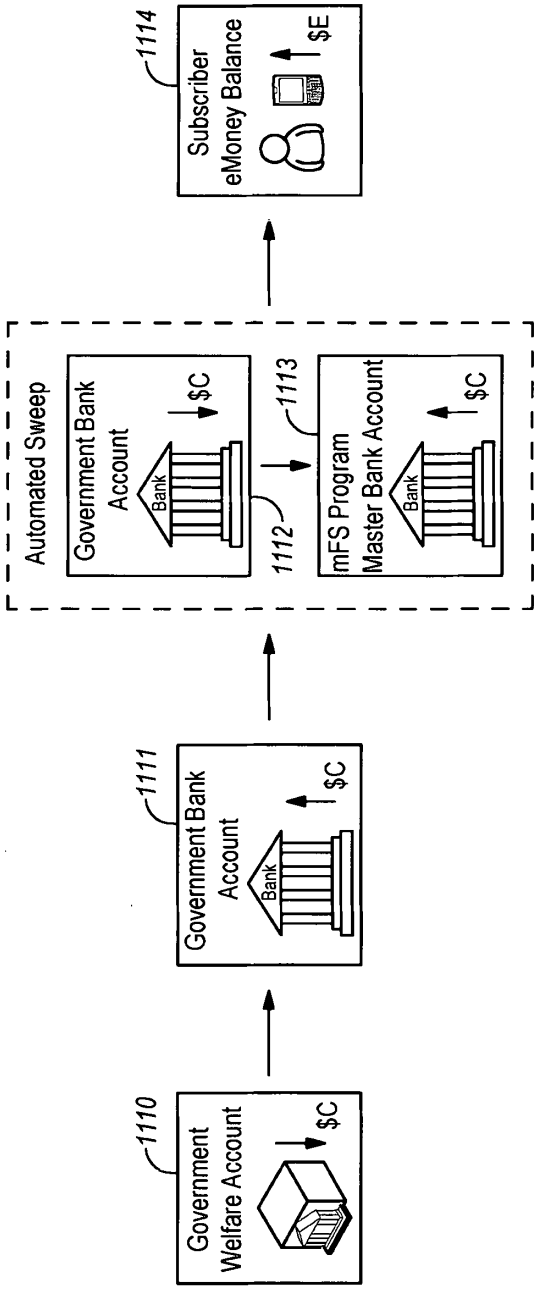


FIG. 11B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 106 of 381

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 107 of 381

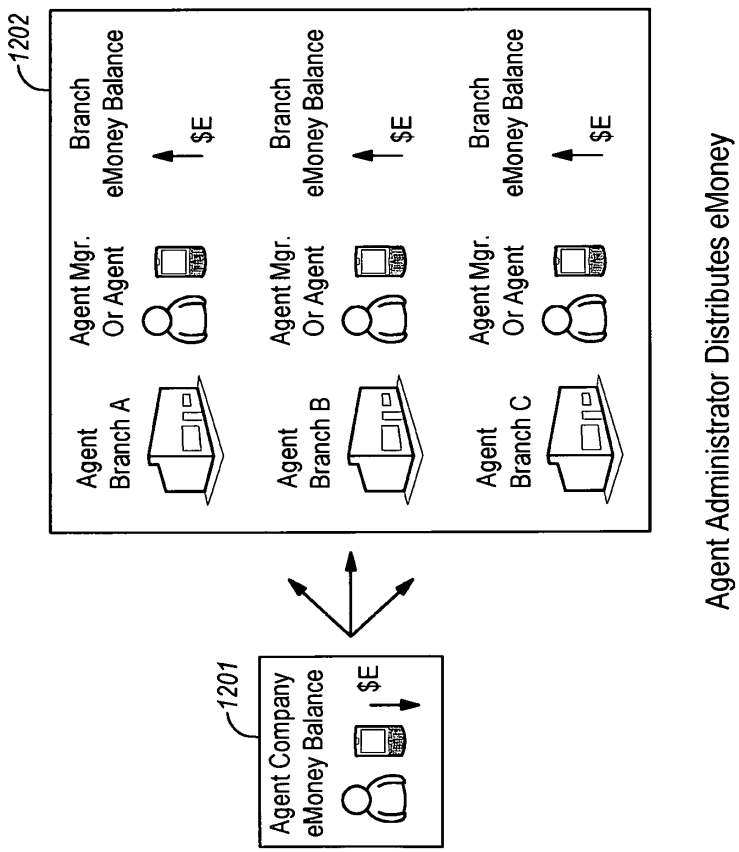


FIG. 12A

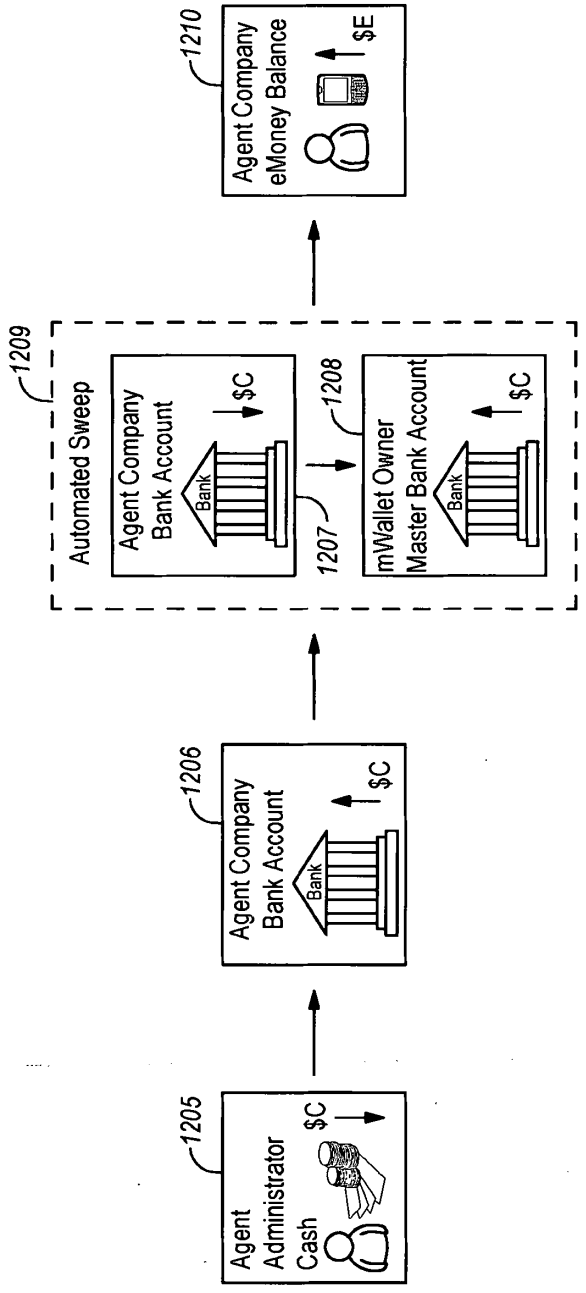


FIG. 12B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 108 of 381

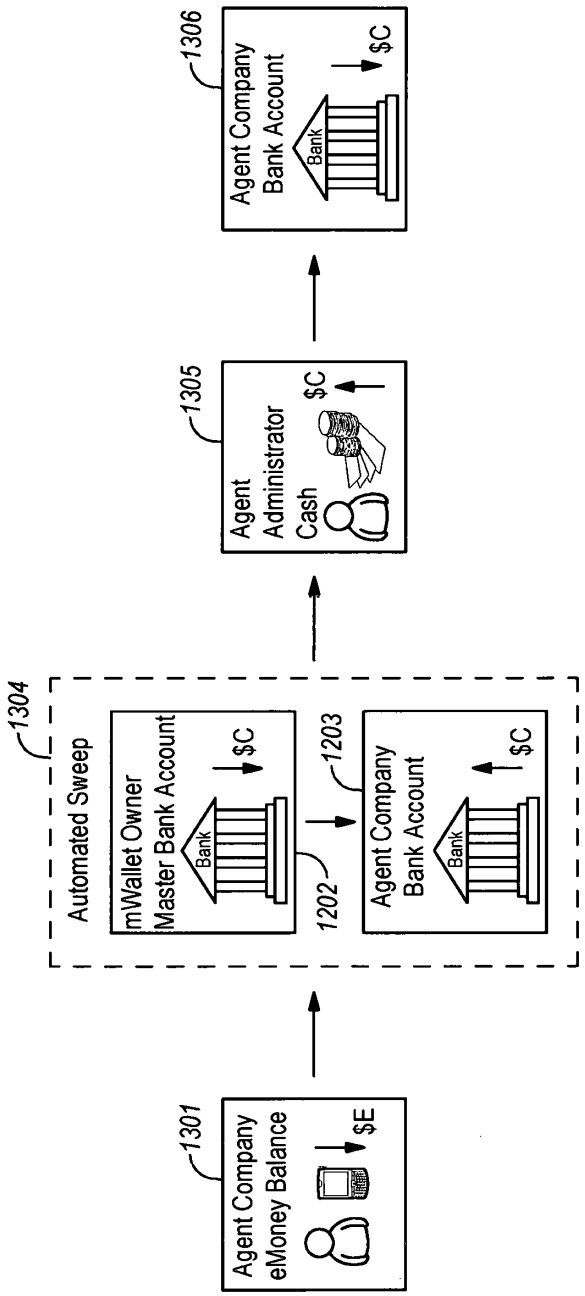
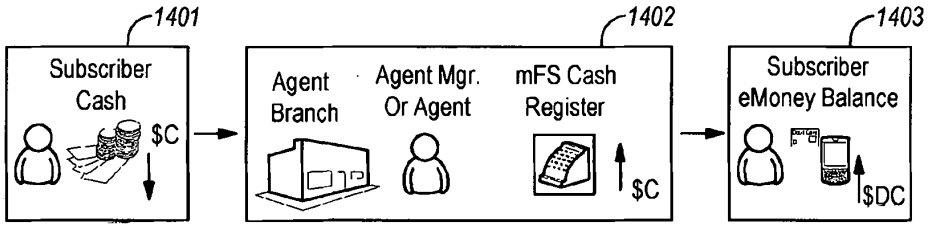


FIG. 13

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 109 of 381



Subscriber Deposit At Agent Branch

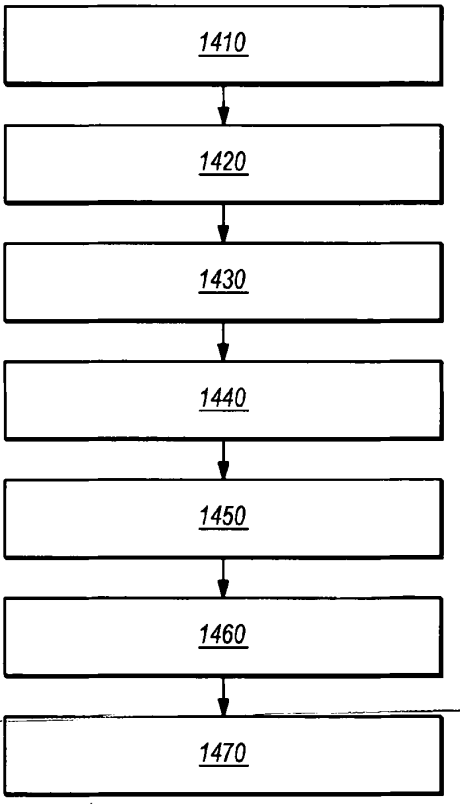


FIG. 14

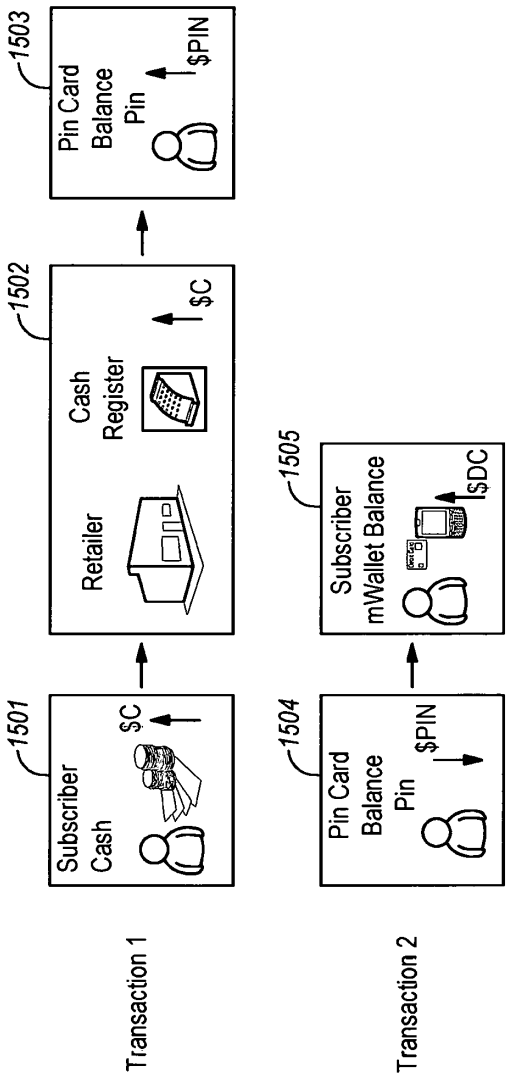
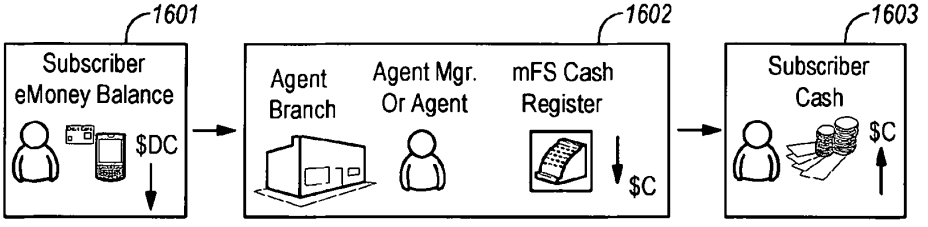


FIG. 15

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 111 of 381



Subscriber Withdrawal (Agent)

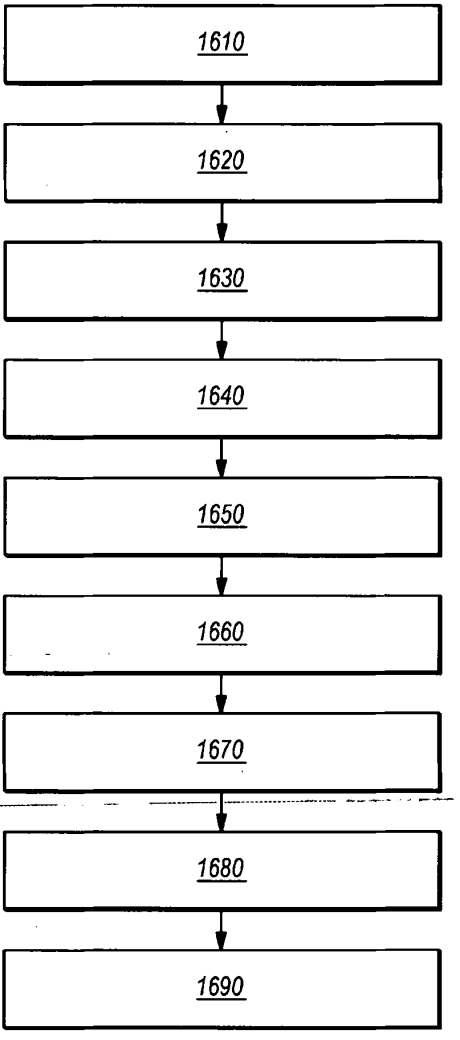
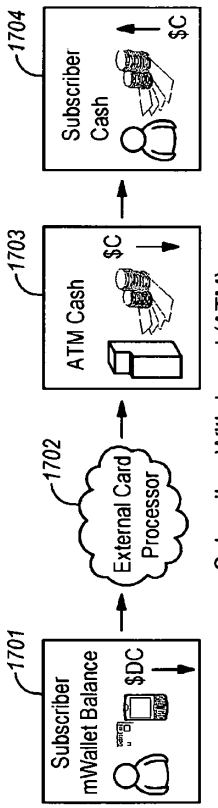
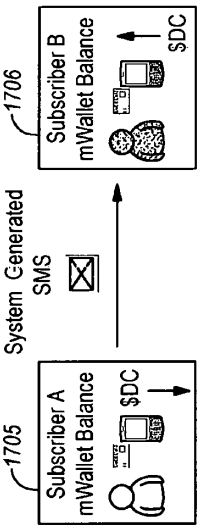


FIG. 16



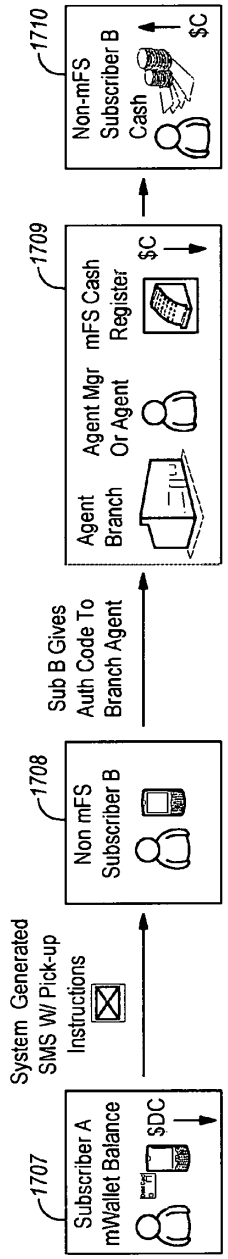
Subscriber Withdrawal (ATM)

FIG. 17A



Subscriber To Subscriber Money Transfer

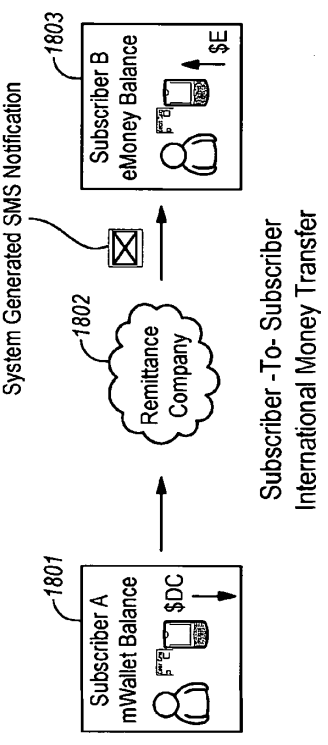
FIG. 17B



Subscriber To Non-Subscriber Money Transfer

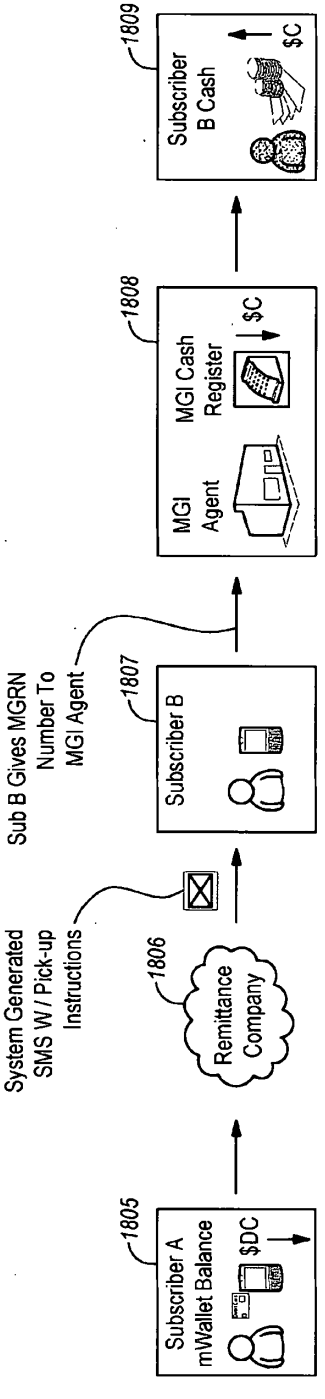
FIG. 17C

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 113 of 381



Subscriber -To- Subscriber
International Money Transfer

FIG. 18A



Subscriber -To- Non Subscriber
International Money Transfer

FIG. 18B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 114 of 381

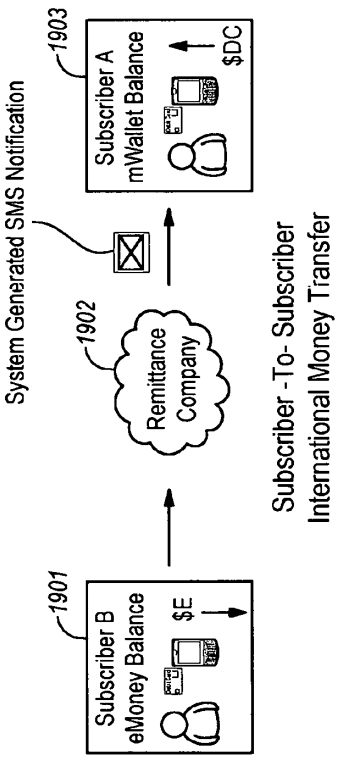


FIG. 19A

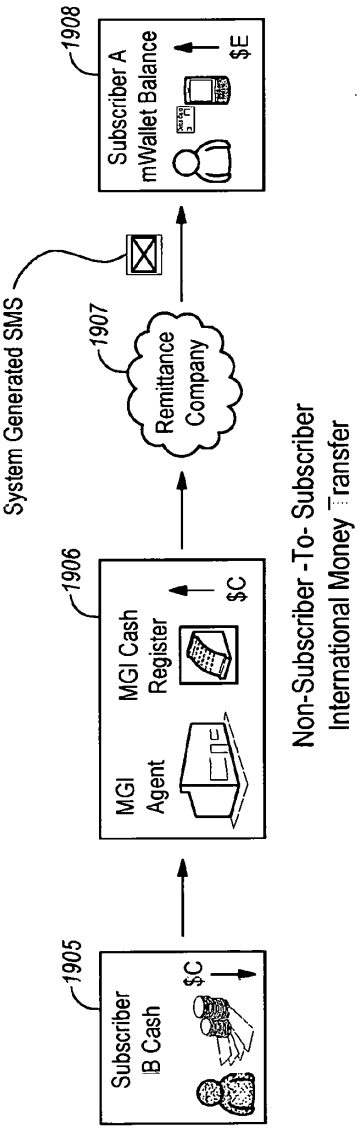


FIG. 19B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 115 of 381

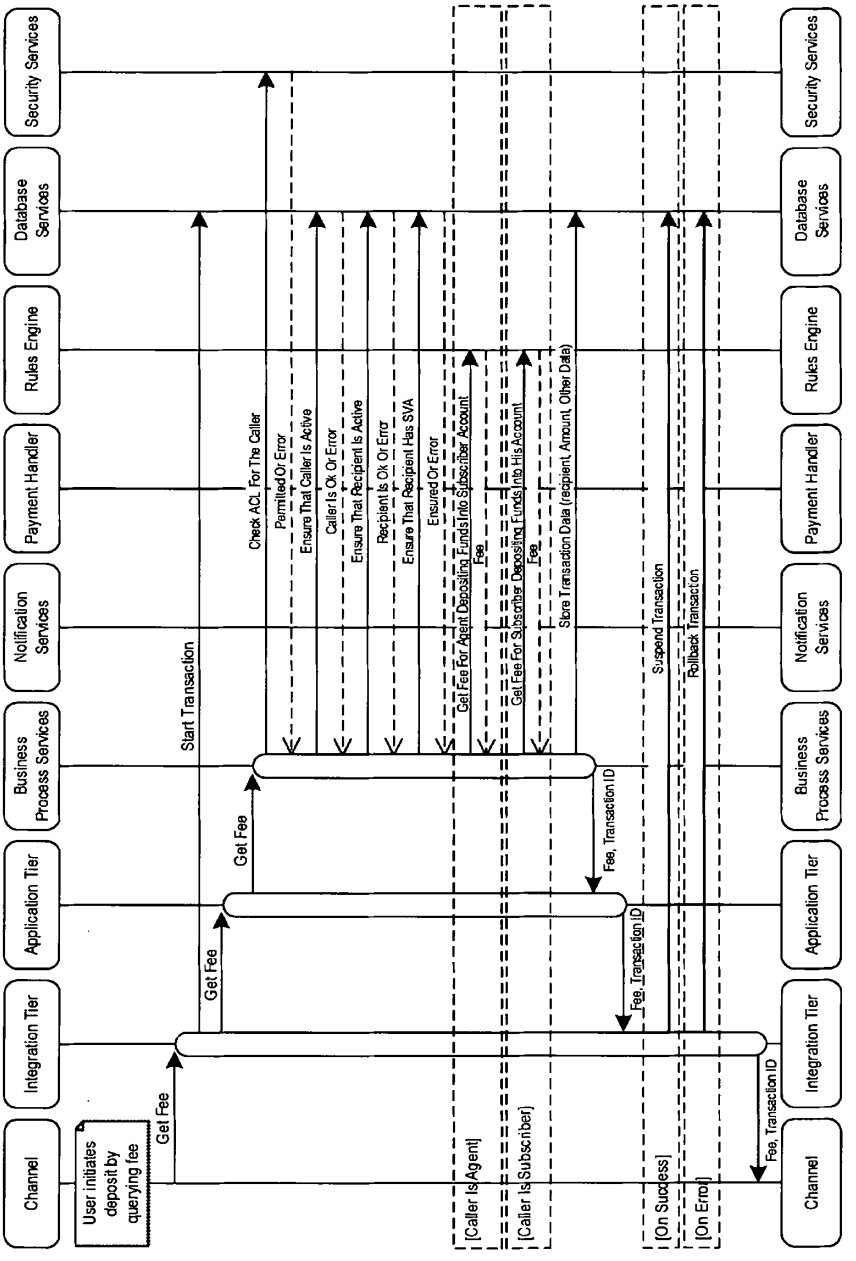


Figure 20A

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 116 of 381

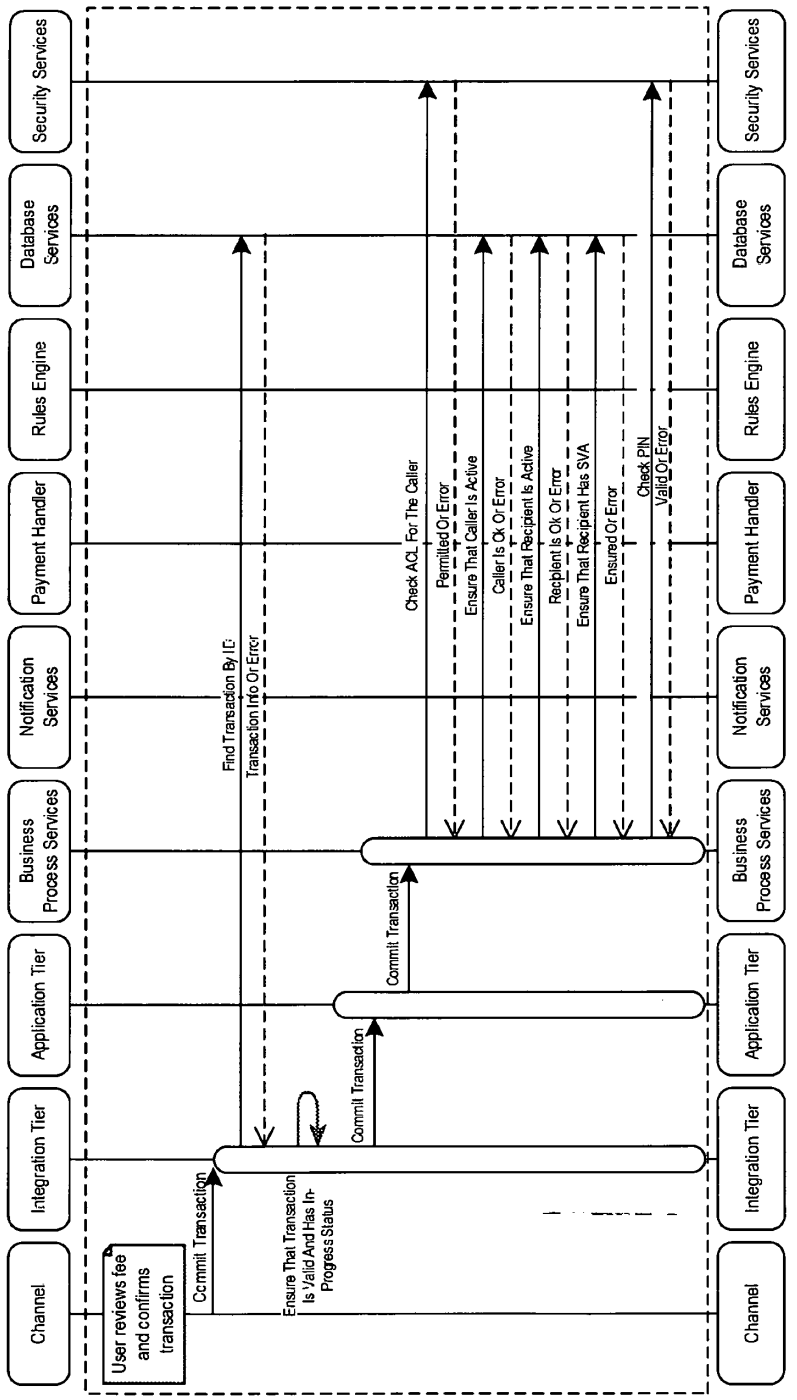


Figure 20B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 117 of 381

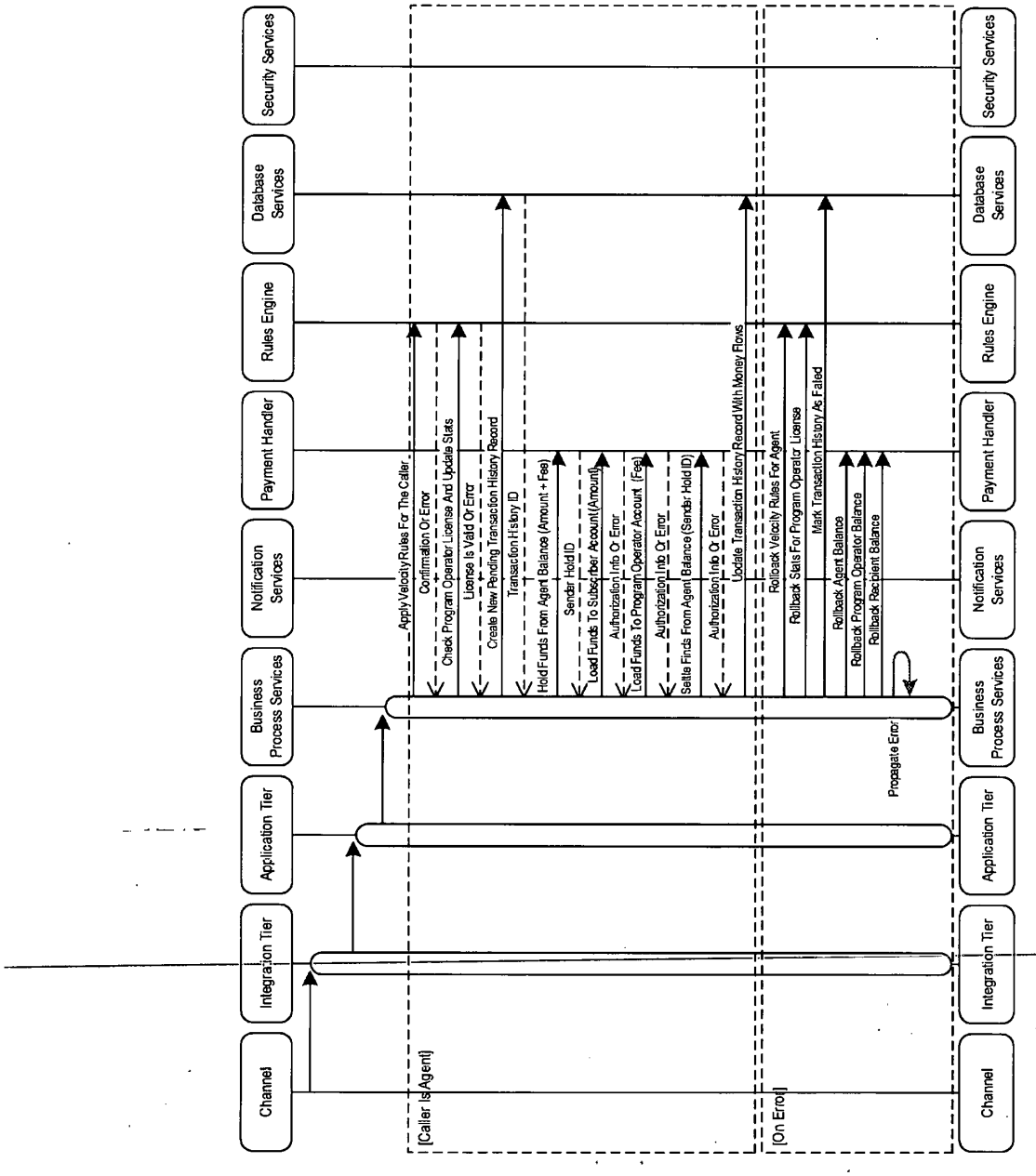


Figure 20C

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 118 of 381

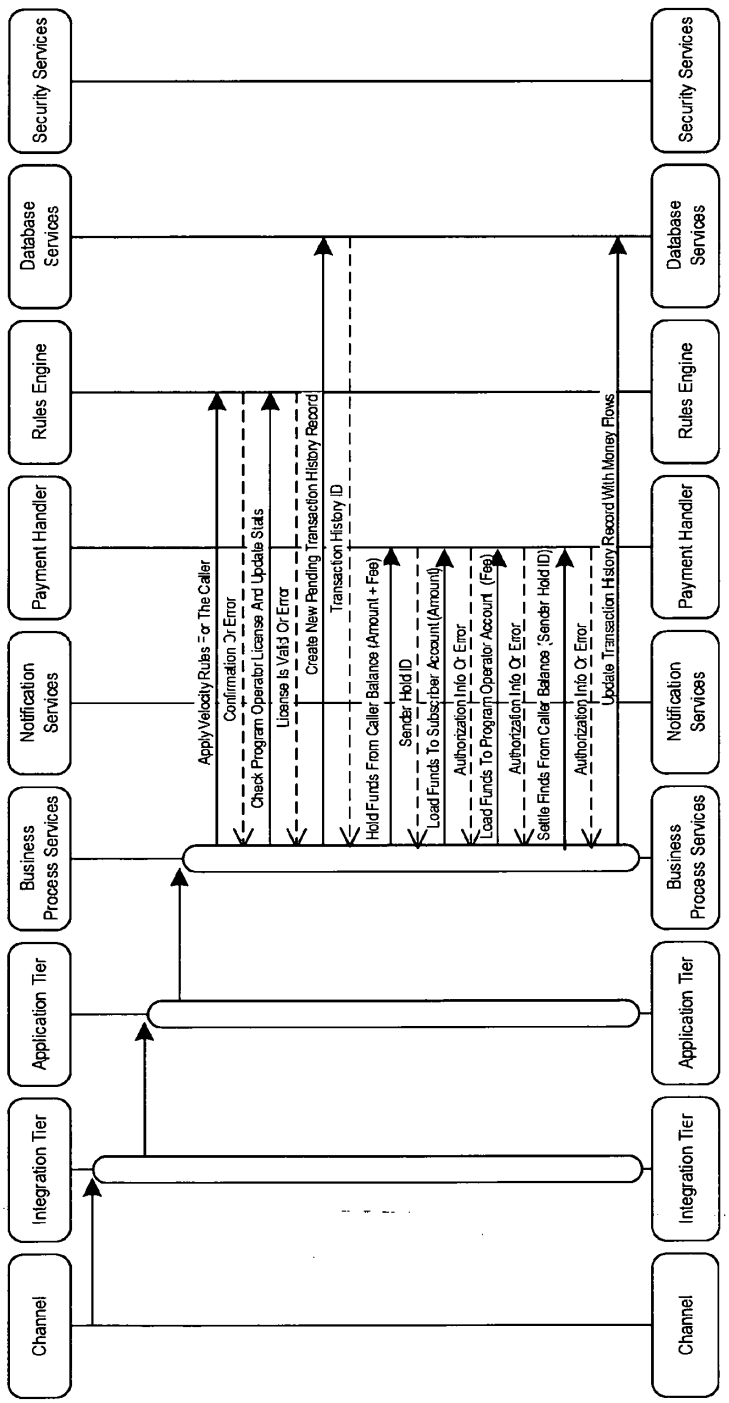


Figure 20D

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 119 of 381

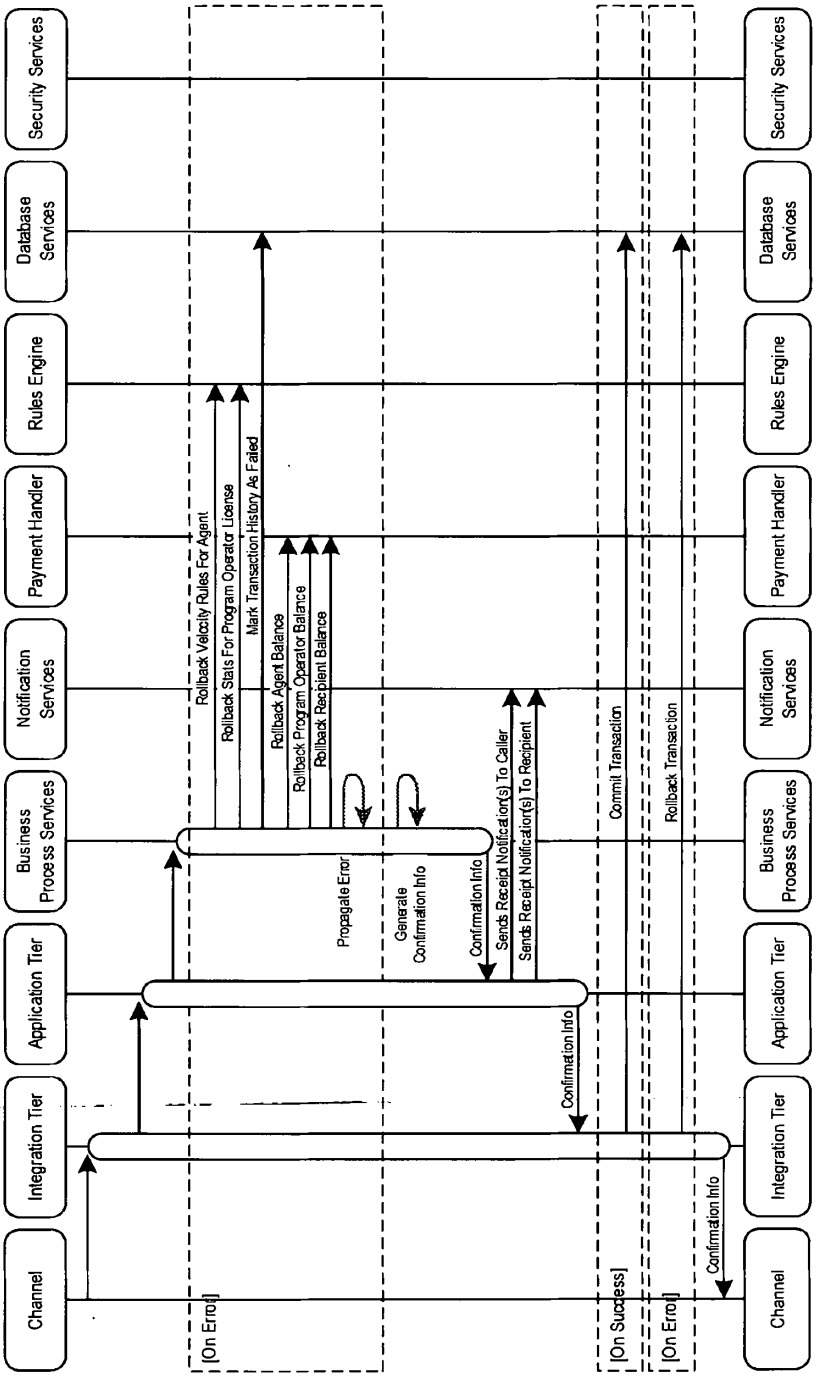


Figure 20E

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 120 of 381

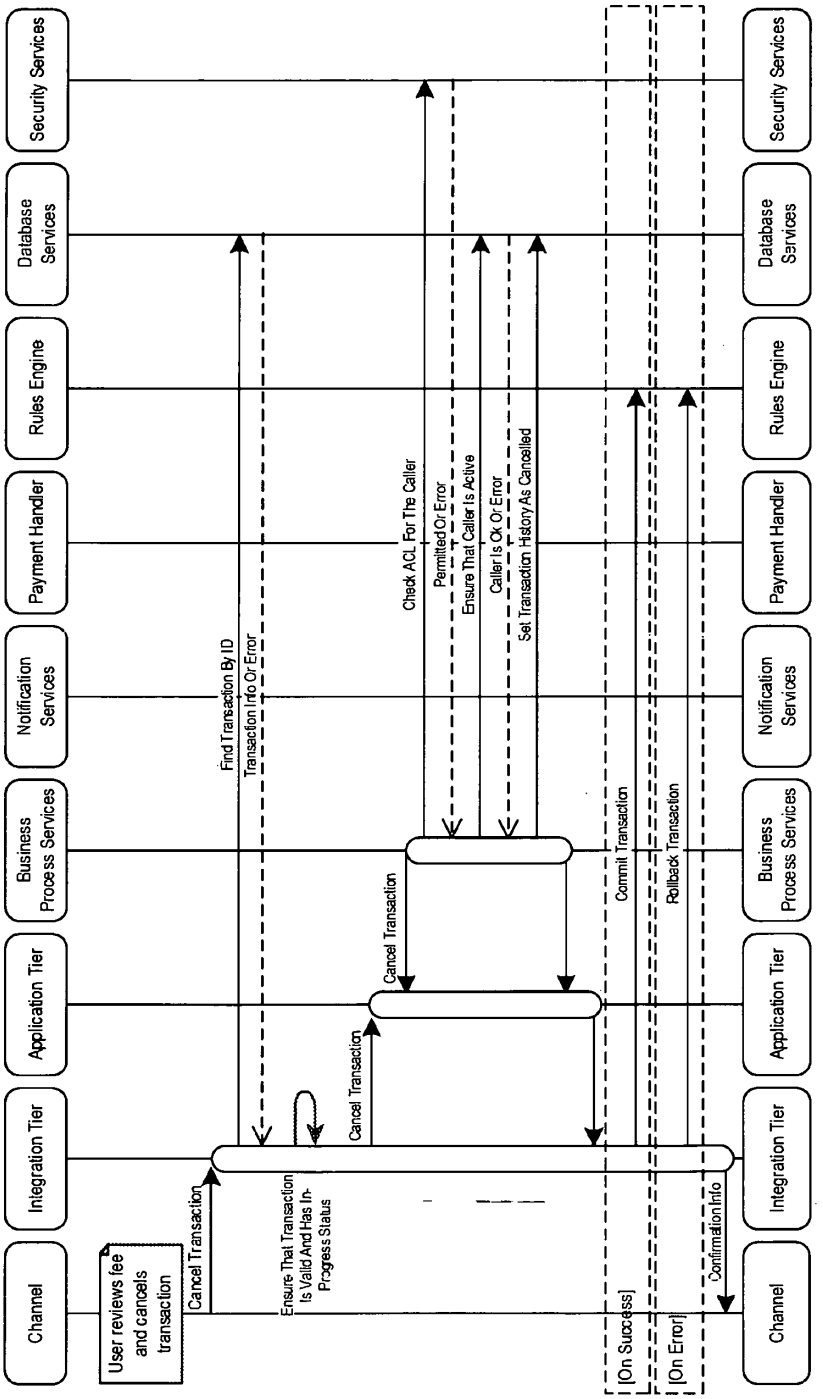


Figure 20F

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 121 of 381

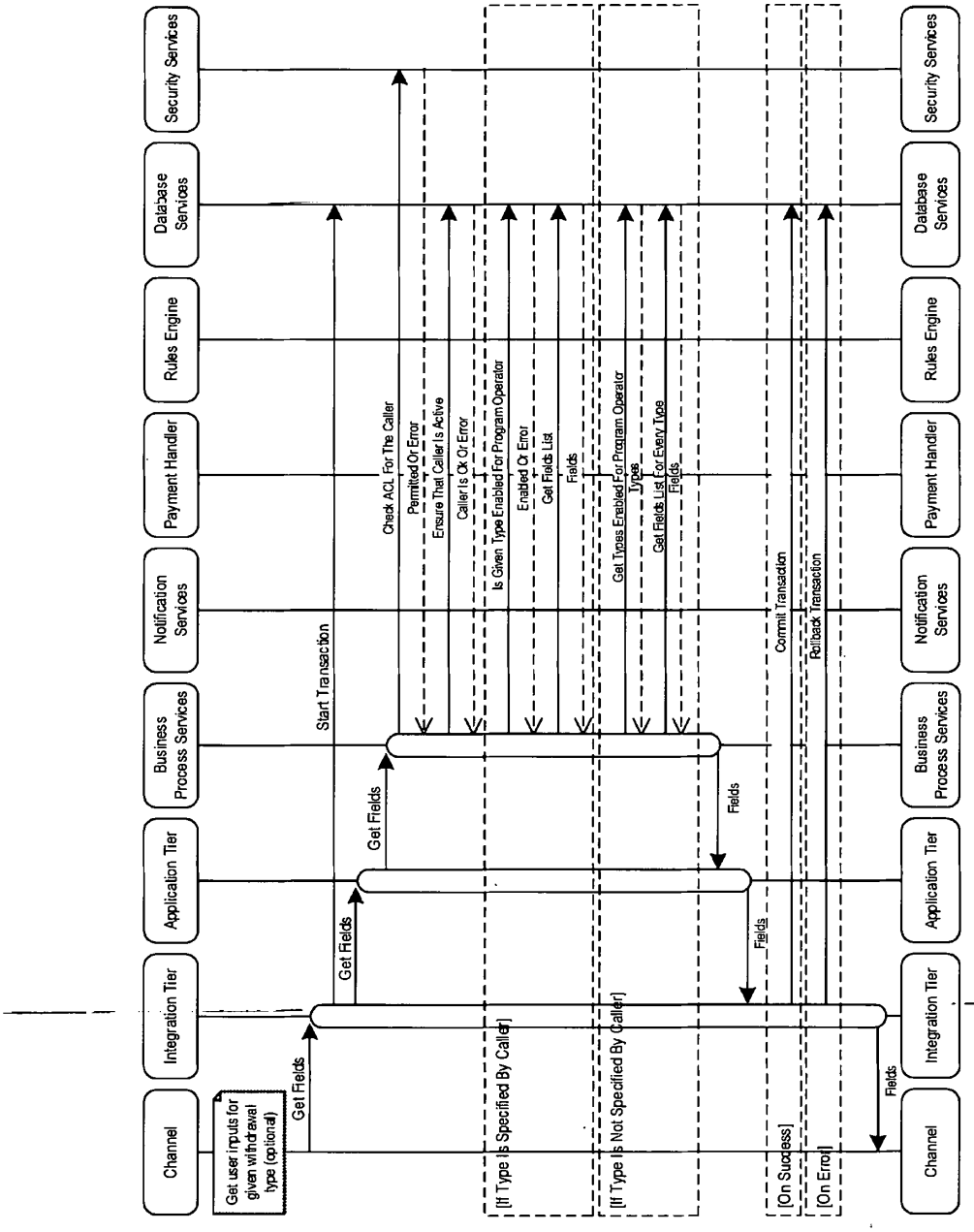


Figure 21A

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 122 of 381

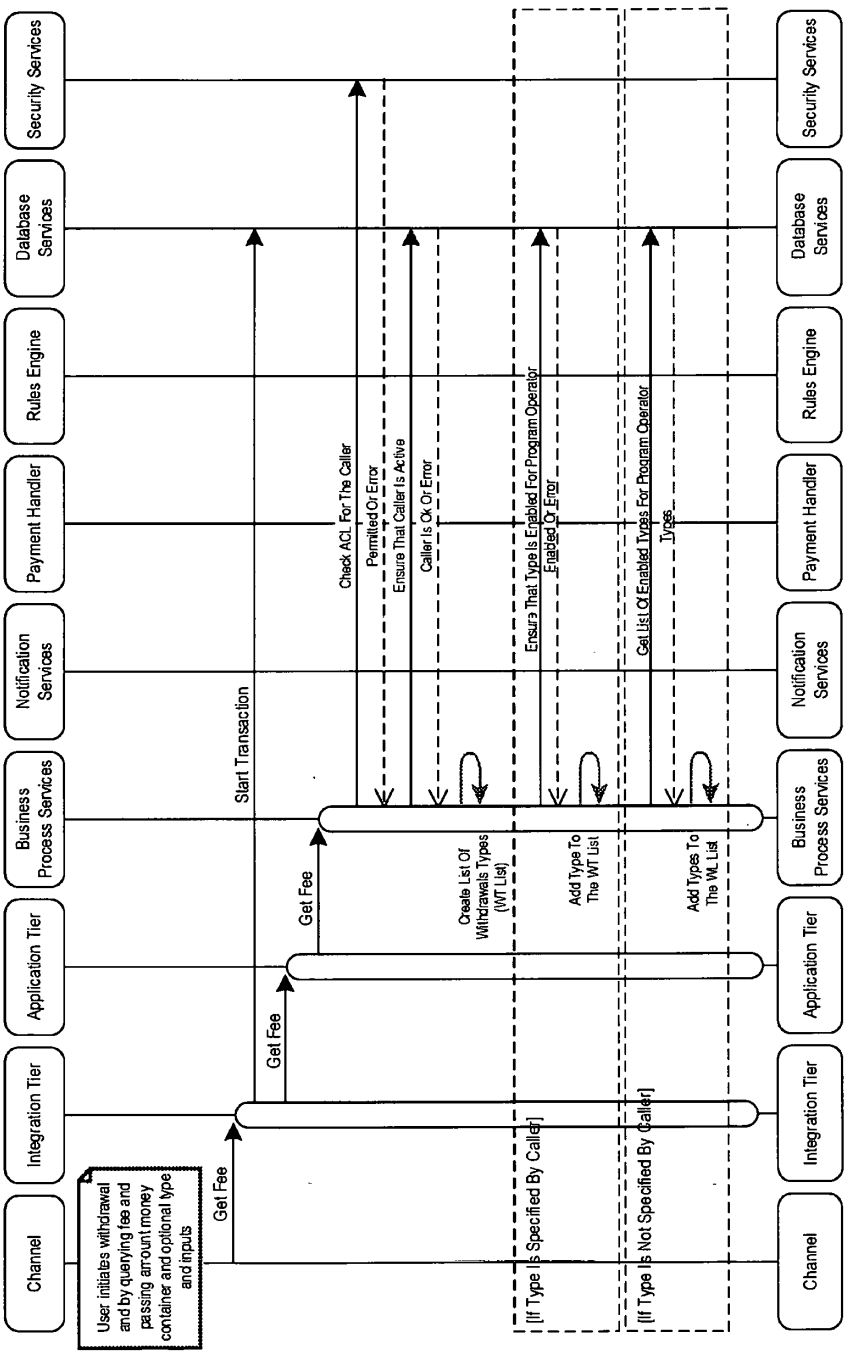


Figure 21B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 123 of 381

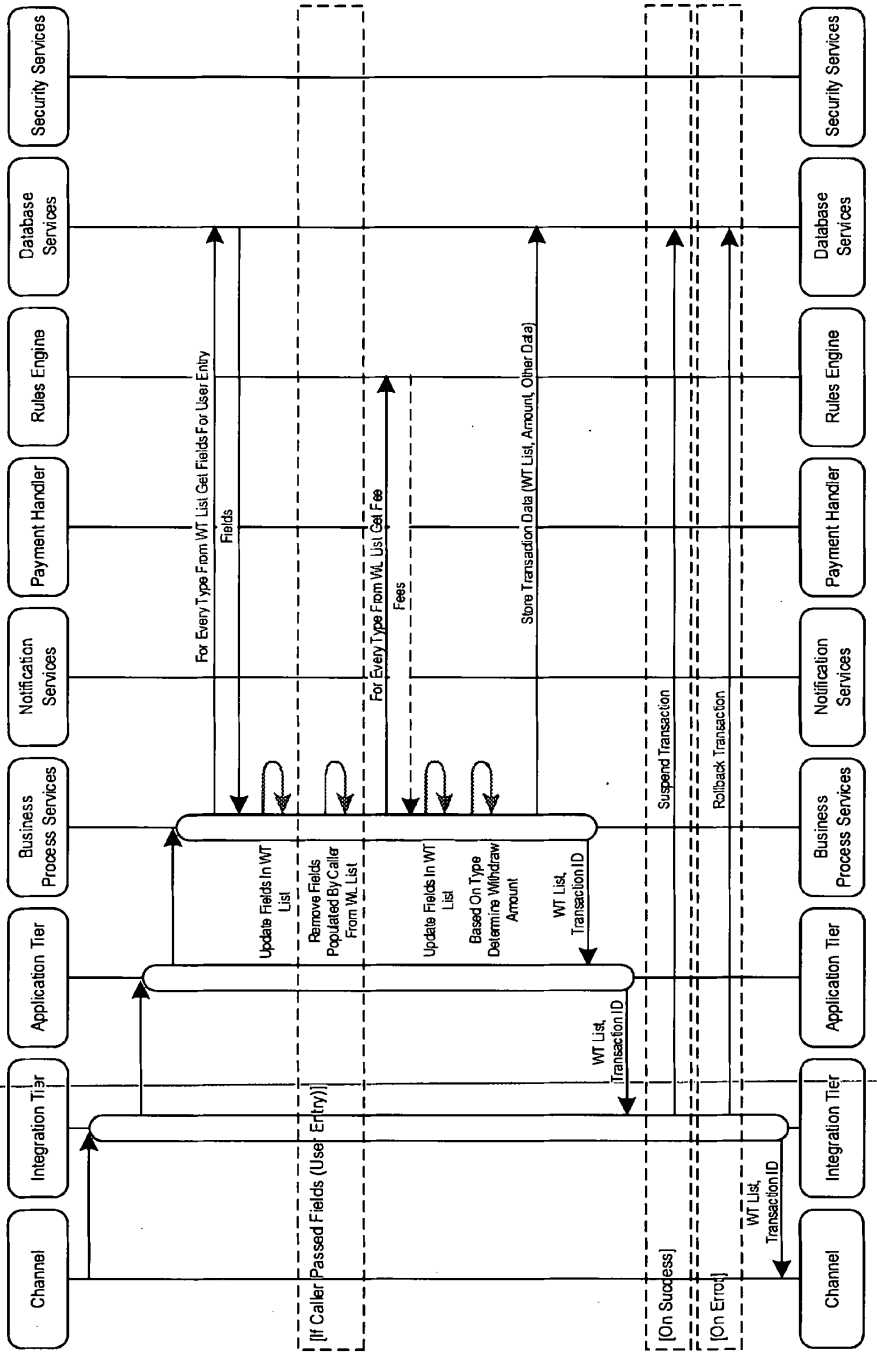


Figure 21C

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 124 of 381

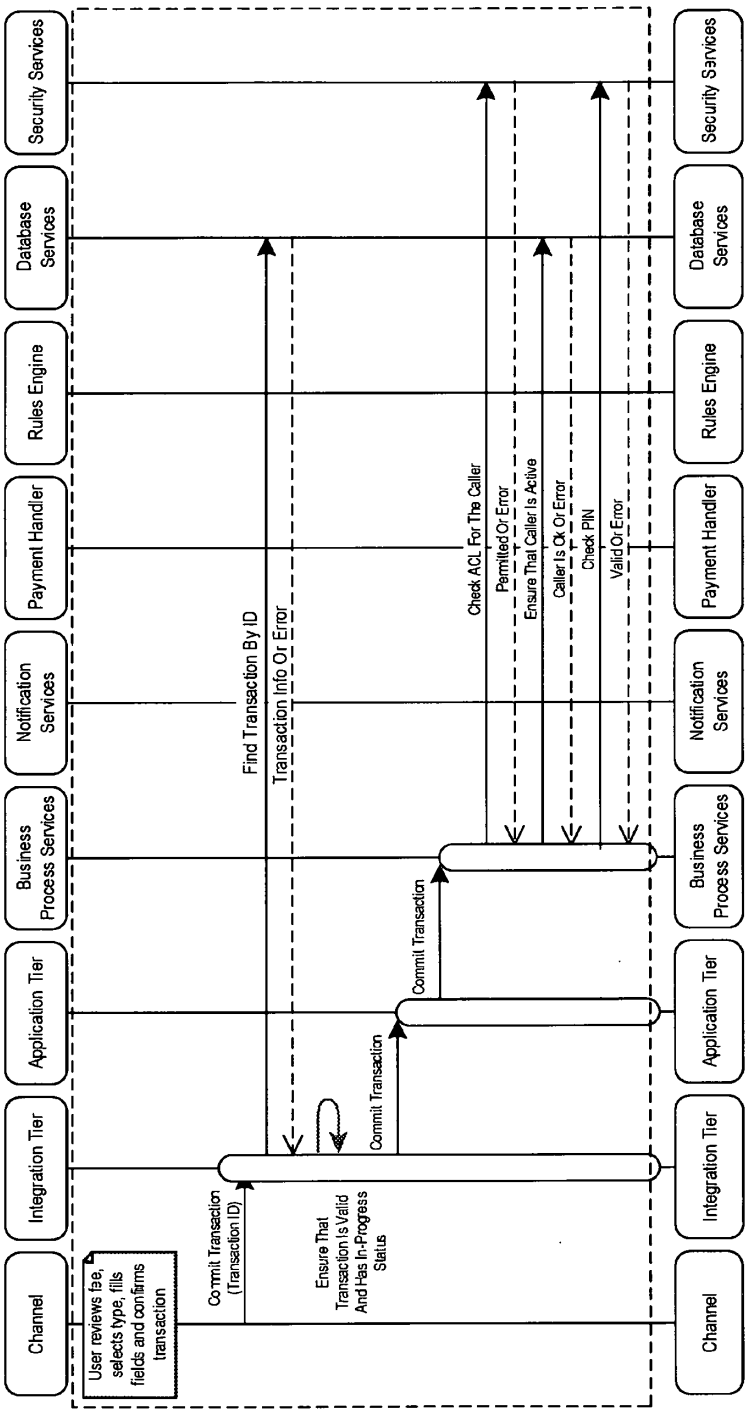


Figure 21D

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 125 of 381

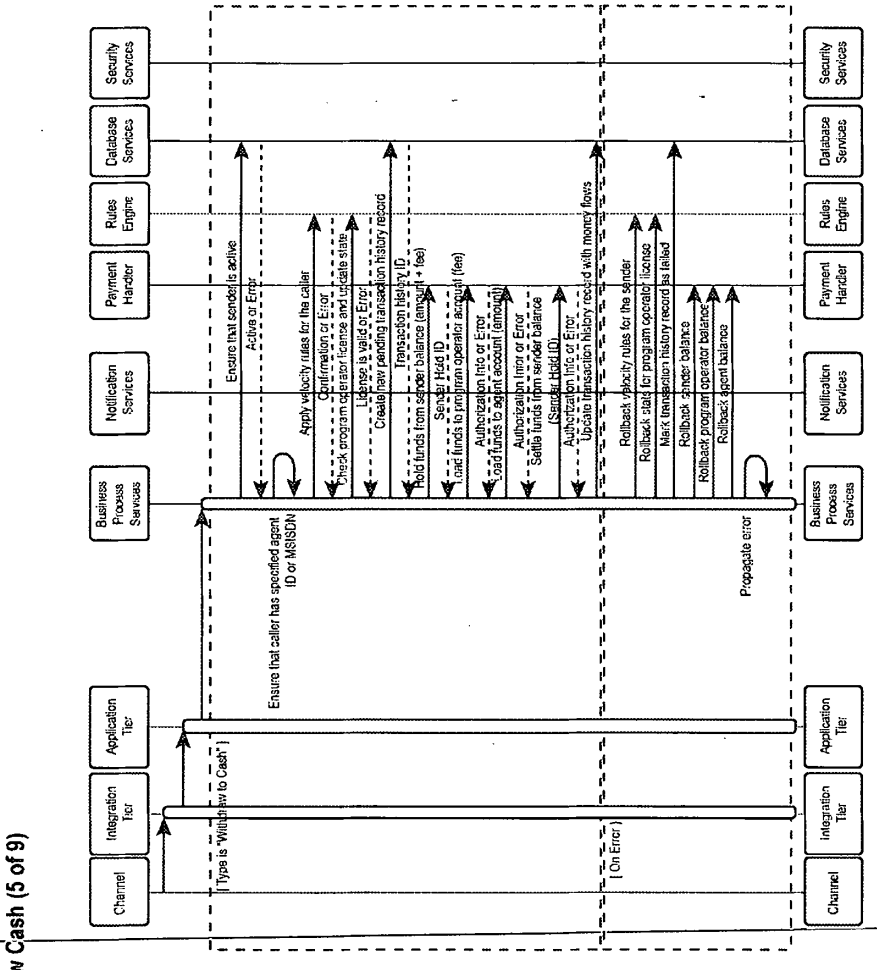


Figure 21E

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 126 of 381

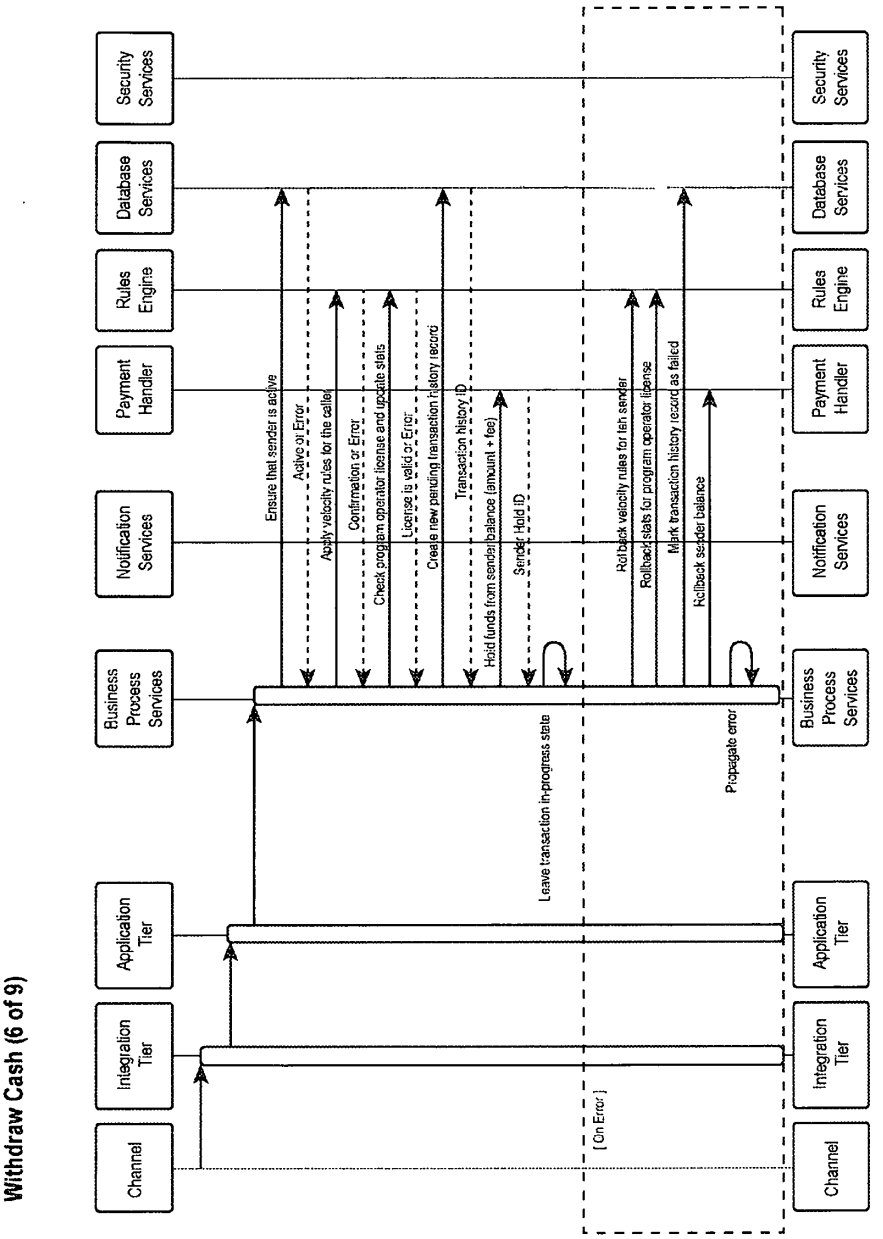


Figure 21F

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 127 of 381

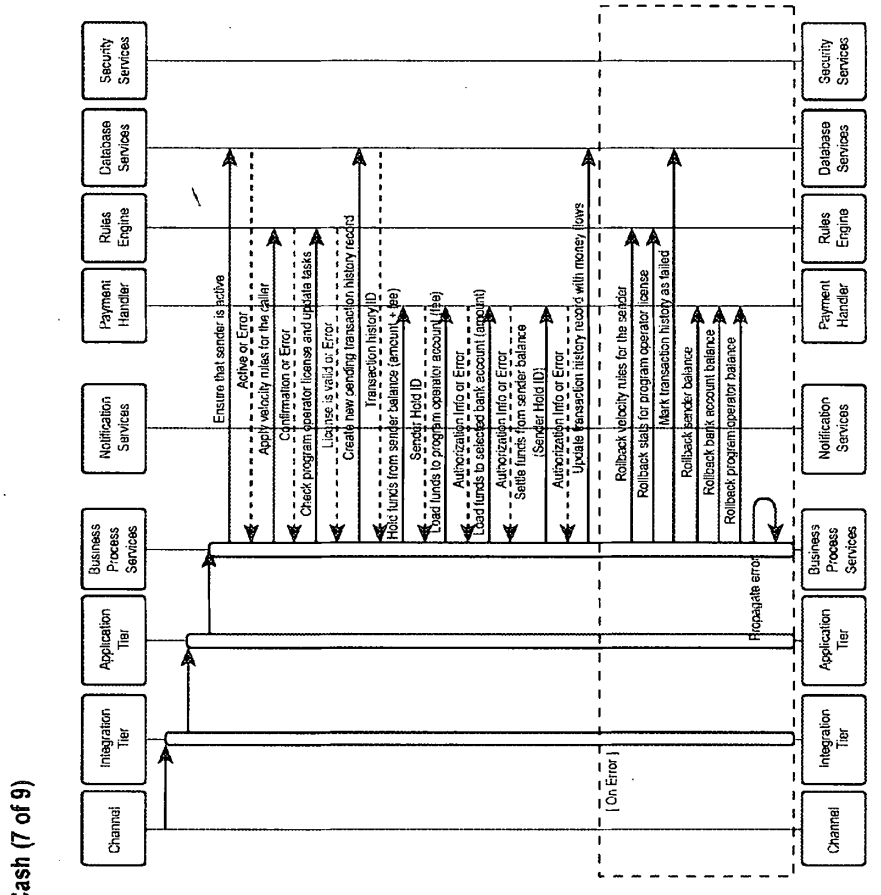


Figure 21G

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 128 of 381

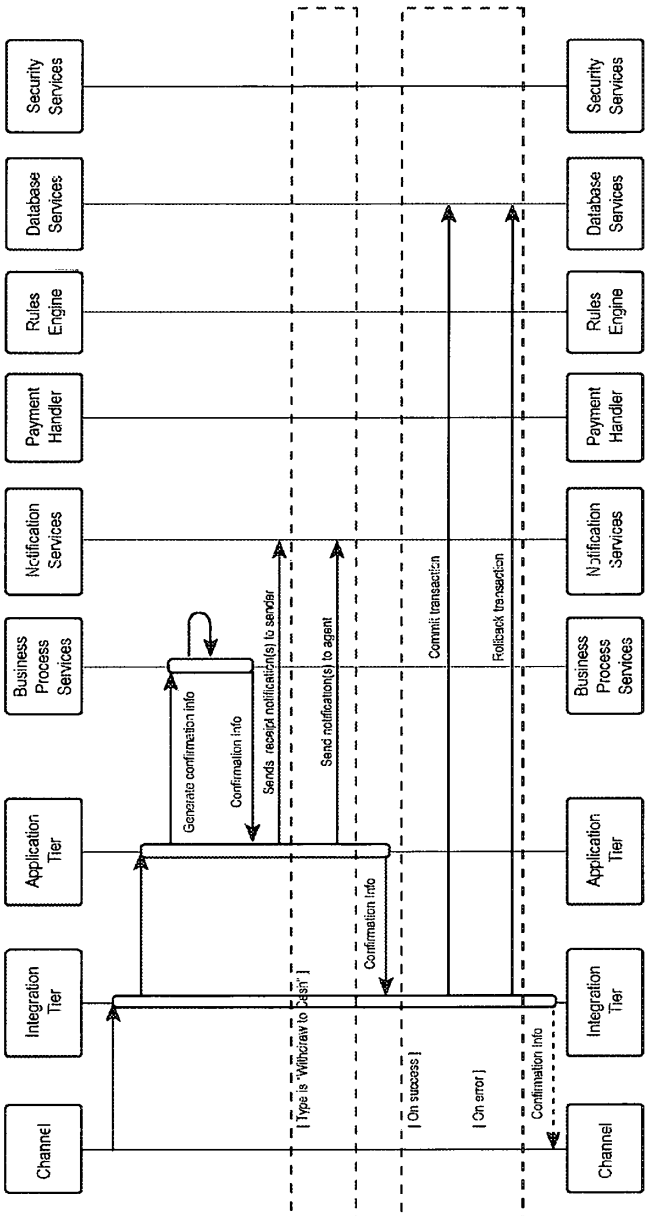


Figure 21H

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 129 of 381

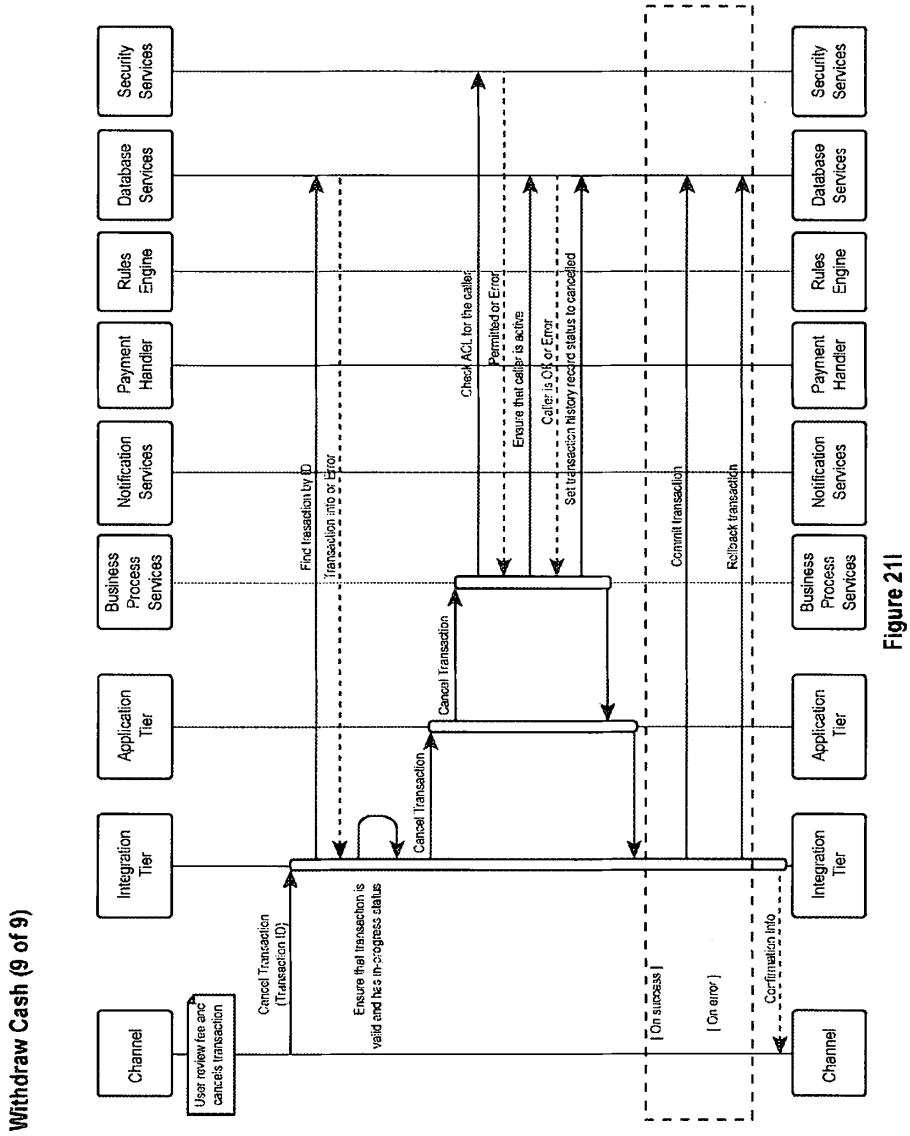


Figure 21I

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 130 of 381

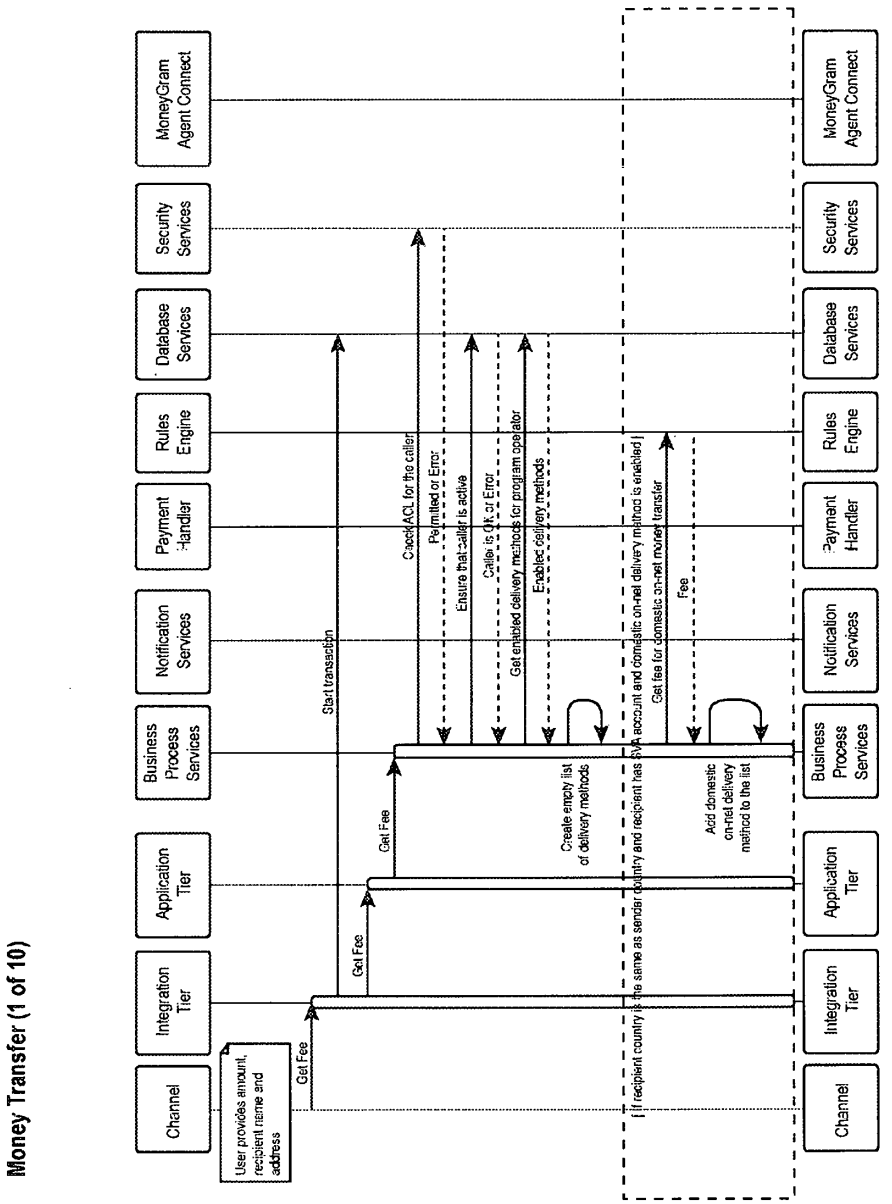


Figure 22A

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 131 of 381

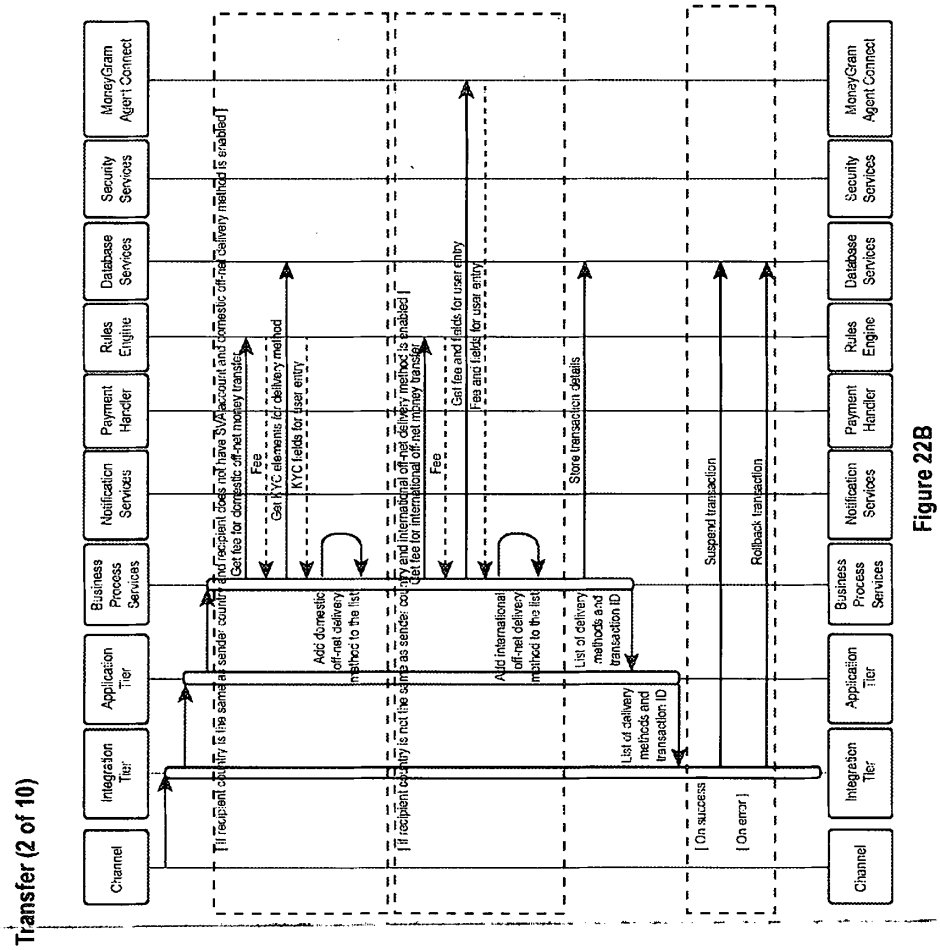


Figure 22B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 132 of 381

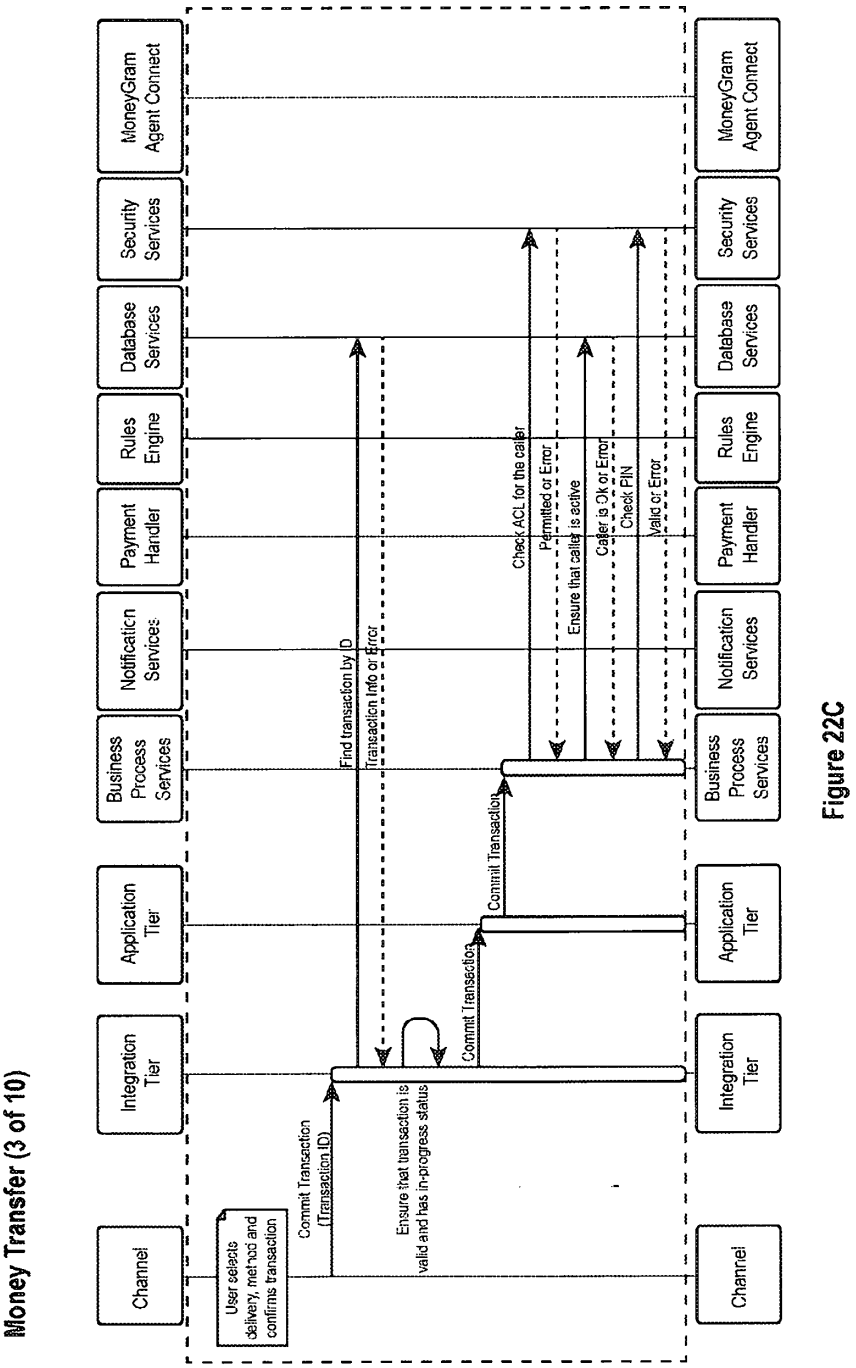


Figure 22C

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 133 of 381

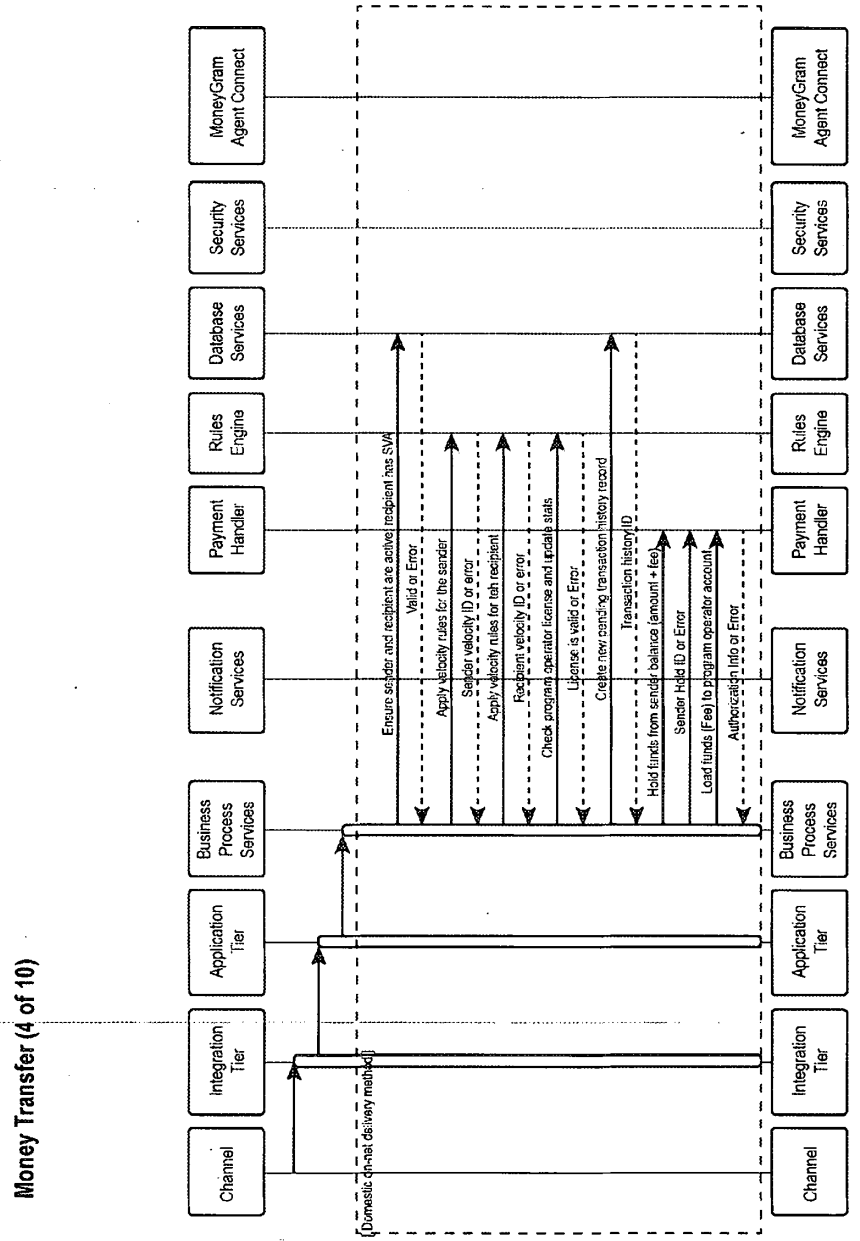


Figure 22D

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 134 of 381

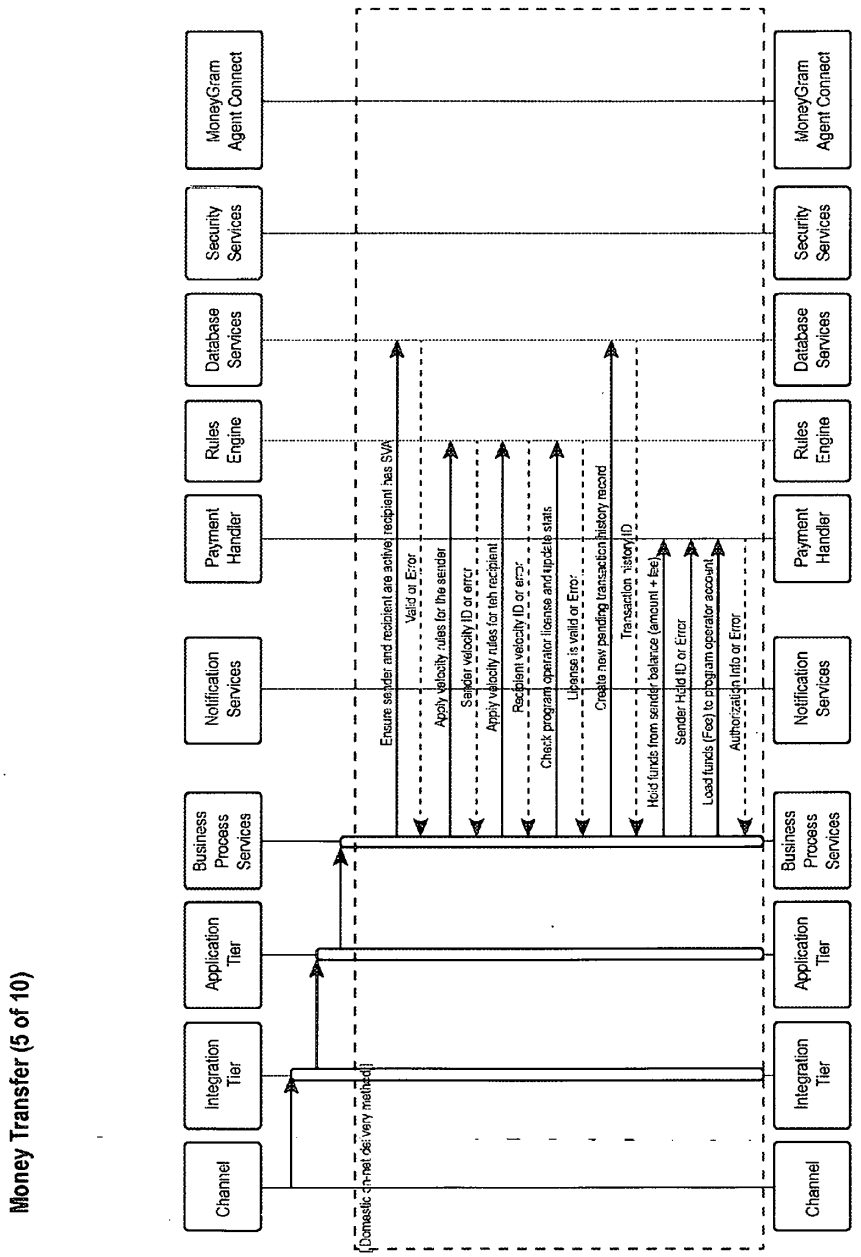


Figure 22E

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 135 of 381

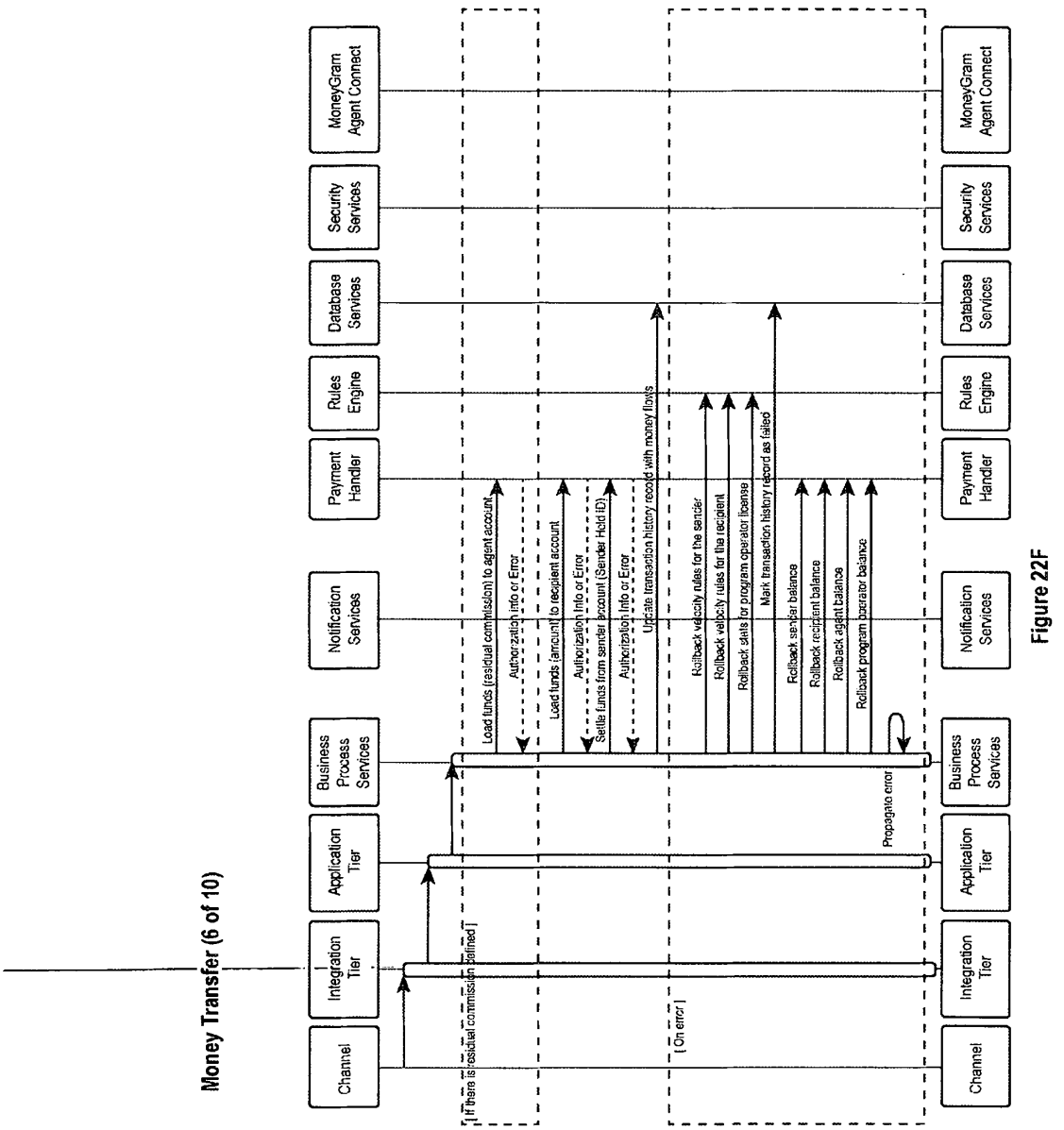


Figure 22F

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 136 of 381

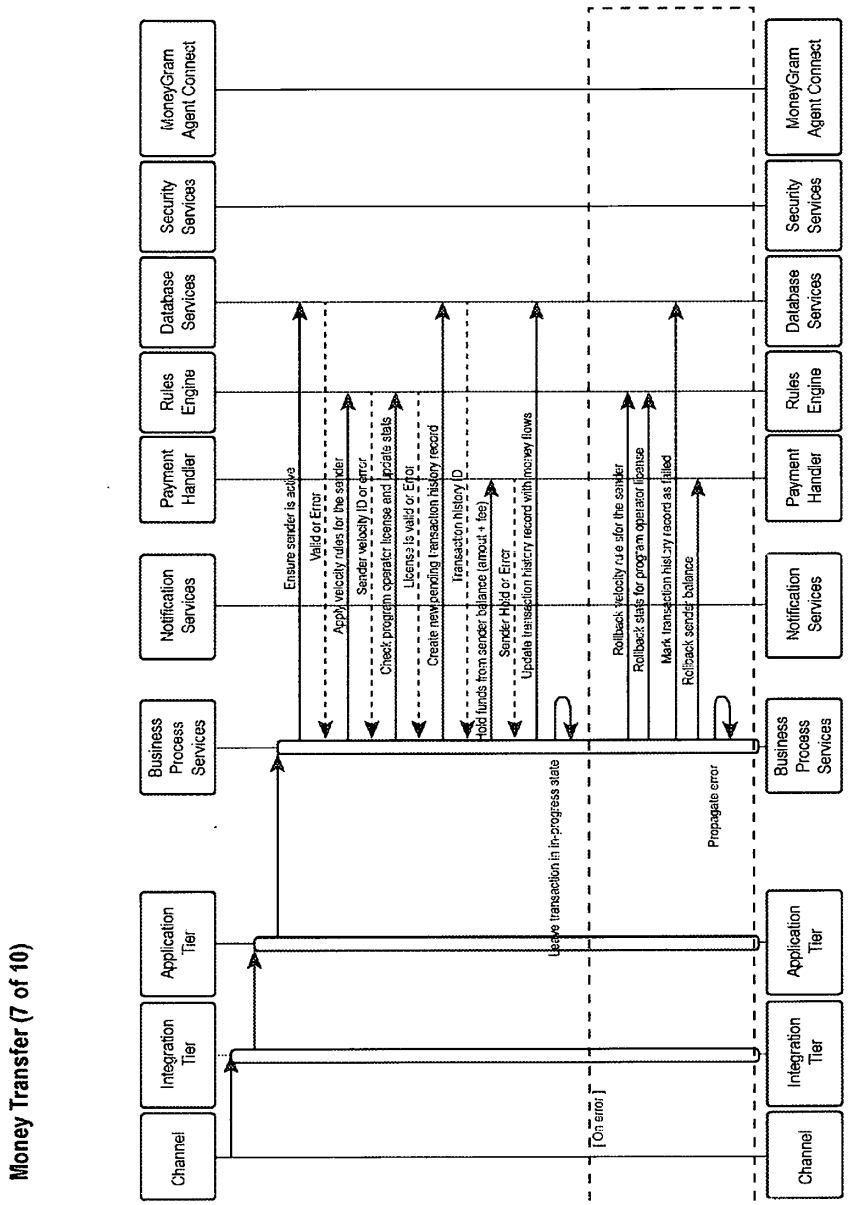


Figure 22G

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 137 of 381

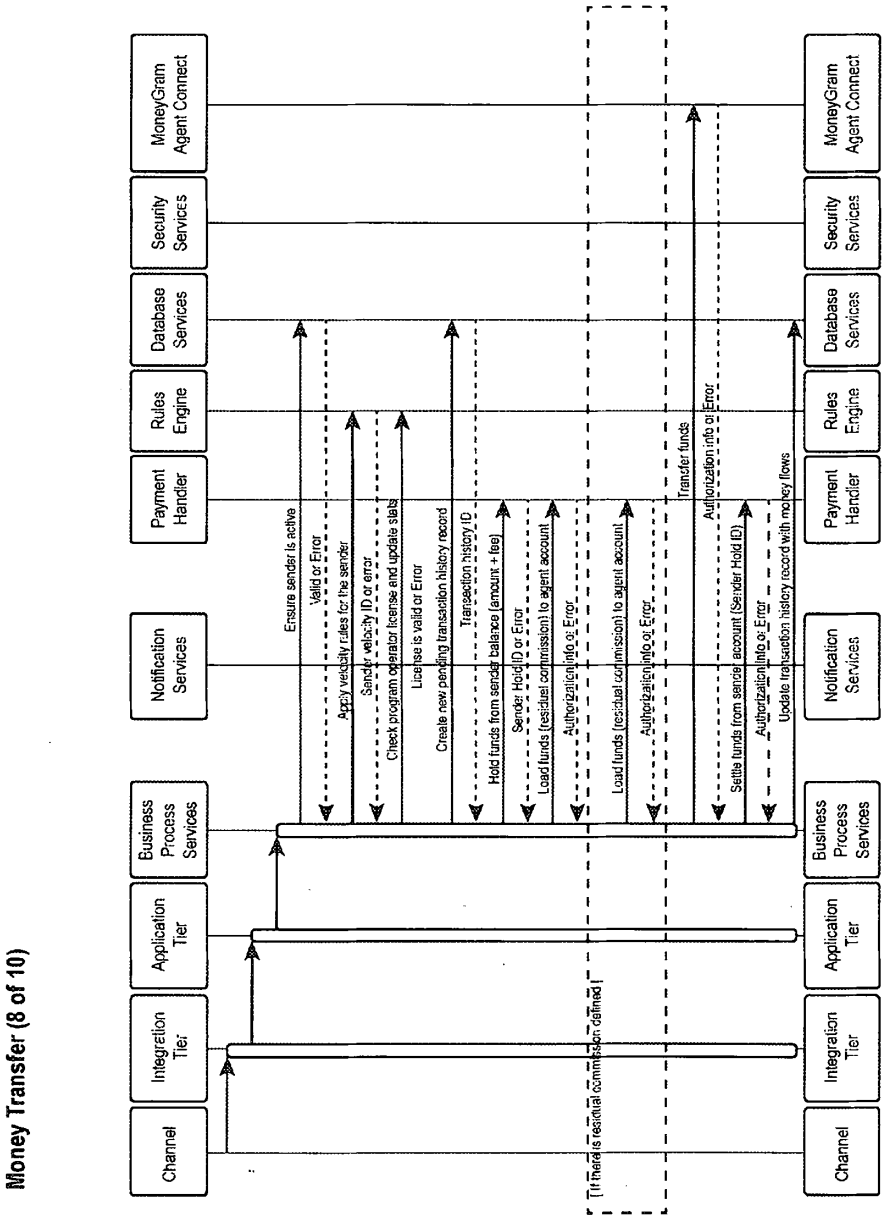


Figure 22H

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 138 of 381

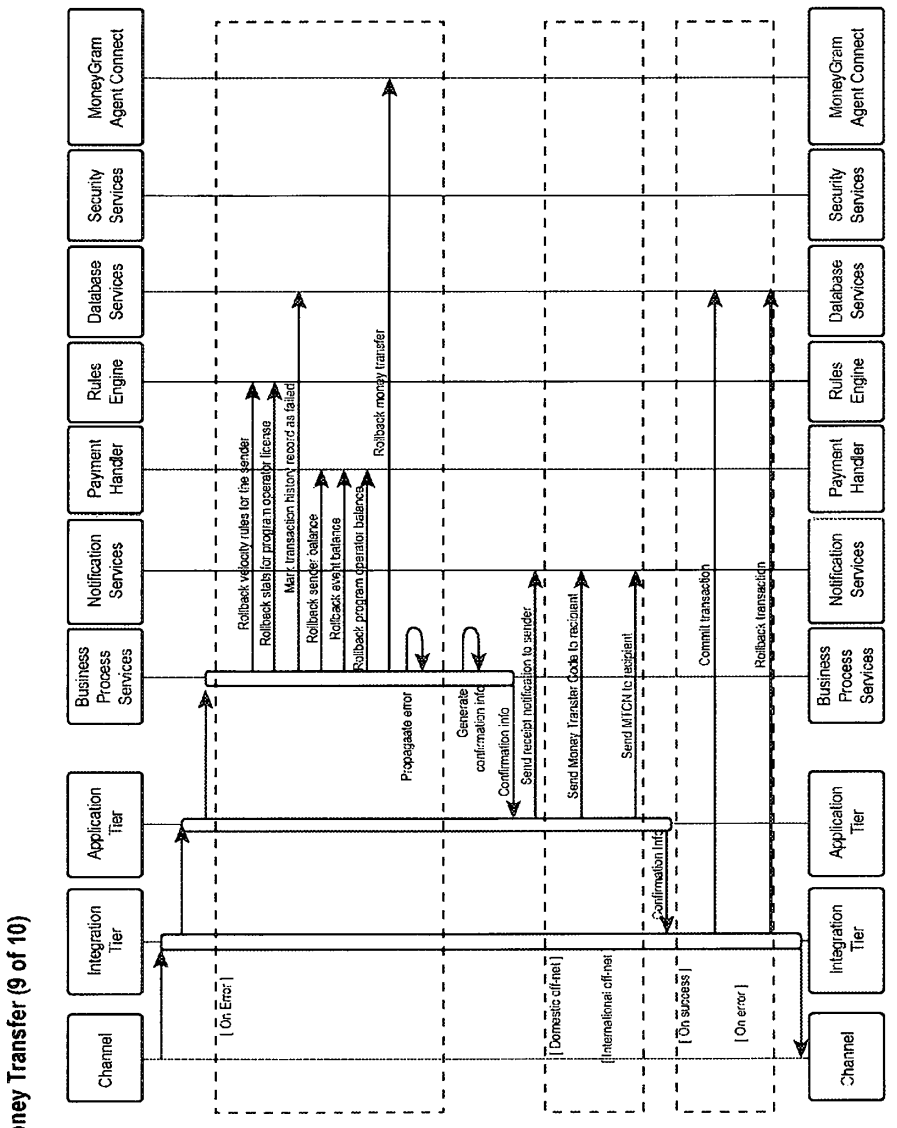


Figure 22I

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 139 of 381

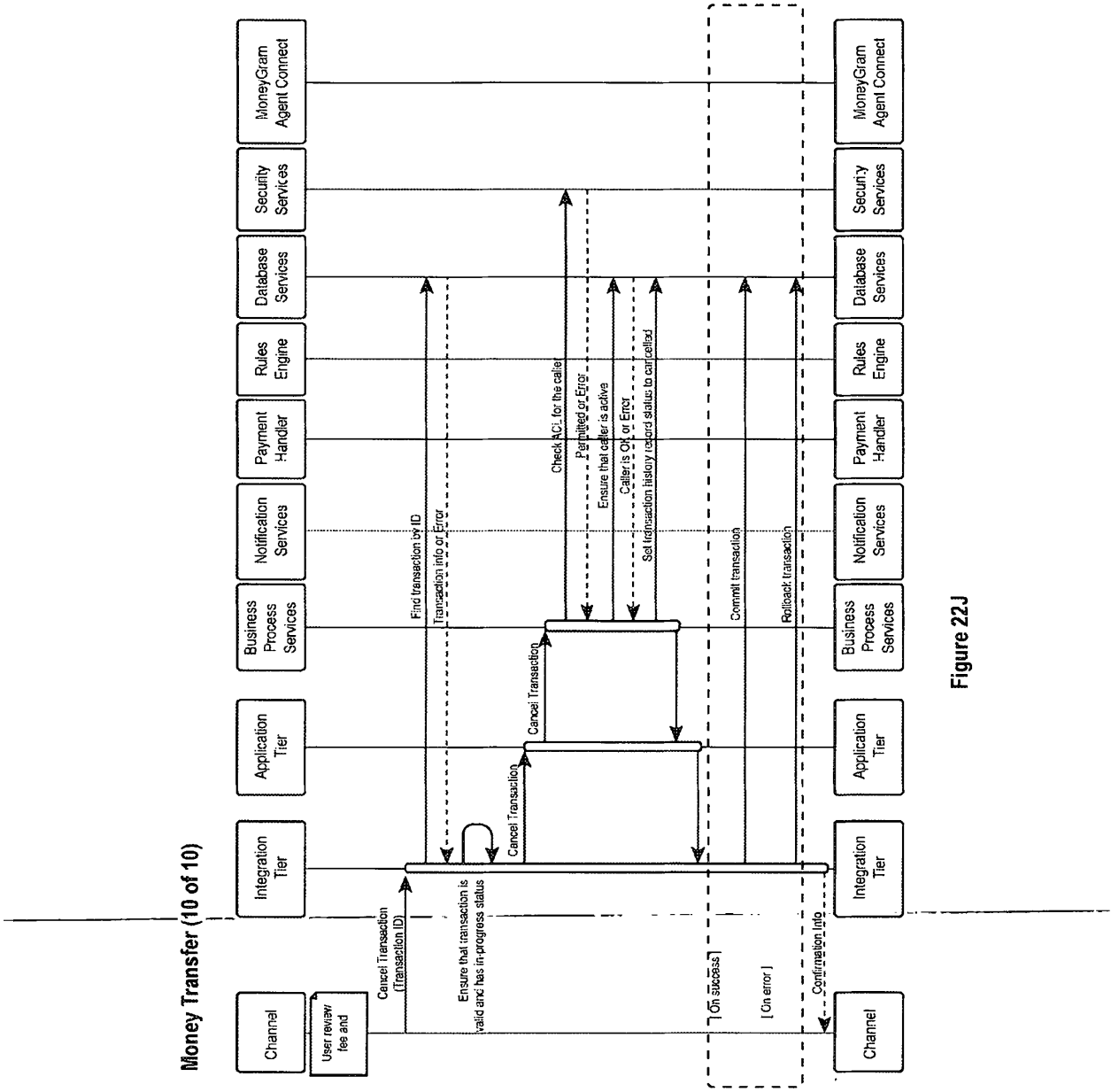


Figure 22J

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 140 of 381

MONETARY TRANSACTION SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 14/213,543, entitled "Monetary Transaction System", filed Mar. 14, 2014, which is a continuation of U.S. patent application Ser. No. 13/964,707, entitled "Monetary Transaction system", filed Aug. 12, 2013, which application is a continuation of U.S. patent application Ser. No. 13/484,199, filed May 30, 2012, entitled "Monetary Transaction System", which application claims priority to and the benefit of U.S. Provisional Application Ser. No. 61/522,099, filed on Aug. 10, 2011, entitled "Mobile Wallet Platform", and also claims priority to and the benefit of U.S. Provisional Application Ser. No. 61/493,064, filed on Jun. 3, 2011, entitled "Mobile Wallet Platform". All of the aforementioned applications are incorporated by reference herein in their entirety.

BACKGROUND

Mobile phones and other digital devices have become increasingly popular in recent years. Many mobile device users use their devices to perform countless different daily tasks. For instance, mobile devices allow users to check email, send and receive instant messages, check calendar items, take notes, set up reminders, browse the internet, play games or perform any number of different things using specialized applications or "apps". These applications allow mobile devices to communicate with other computer systems and perform a wide variety of network-connected tasks previously not possible with a mobile device.

BRIEF SUMMARY

Embodiments described herein are directed to monetary transaction system for conducting monetary transactions between transaction system subscribers and other entities. In one embodiment, the monetary transaction system includes a mobile device configured to run a monetary transaction system application. The monetary transaction system also includes a monetary transaction system subscriber that has a profile with the system. The subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system. The system further includes a monetary transaction system processor that performs the transactions specified by the subscriber. Performing these transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile.

The monetary transaction system also includes at least one entity that is to be involved in the specified transaction, where the entity has a profile with the monetary transaction system. This entity may be a person, a retail store, an agent or other entity. The subscriber may have access to a bank account, or may be an "unbanked user" that does not have access to a bank account. Each of the terms included above will be described in greater detail below in conjunction with the drawings.

The monetary transaction system may be used for many different tasks including enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a mobile wallet, adding a debit or credit card account to a mobile wallet, depositing funds in a mobile wallet, withdrawing funds from a mobile wallet, paying bills from a mobile wallet, topping up a prepaid mobile account through a mobile wallet, transferring funds through a mobile wallet (nationally or internationally), making in-store purchases using a mobile wallet, and various other tasks as described herein below.

This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

Additional features and advantages will be set forth in the description which follows, and in part will be apparent to one of ordinary skill in the art from the description, or may be learned by the practice of the teachings herein. Features and advantages of embodiments described herein may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. Features of the embodiments described herein will become more fully apparent from the following description and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

To further clarify the above and other features of the embodiments described herein, a more particular description will be rendered by reference to the appended drawings. It is appreciated that these drawings depict only examples of the embodiments described herein and are therefore not to be considered limiting of its scope. The embodiments will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

FIG. **1** illustrates a monetary transaction system architecture in which embodiments described herein may operate.

FIG. **2** illustrates an alternate example embodiment of a monetary transaction system.

FIG. **3** illustrates an example data flow for performing a subscriber deposit via a mobile wallet.

FIG. **4** illustrates an example data flow for performing a subscriber withdrawal via a mobile wallet.

FIGS. **5**A and **5**B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber eMoney transfers via a mobile wallet, respectively.

FIGS. **6**A and **6**B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber international eMoney transfers via a mobile wallet, respectively.

FIG. **7** illustrates an example data flow for performing a subscriber airtime purchase via a mobile wallet.

FIG. **8** illustrates an example data flow for performing a subscriber-initiated bill pay via a mobile wallet.

FIG. **9** illustrates an example data flow for performing a subscriber-initiated retail purchase via a mobile wallet.

FIGS. **10**A and **10**B illustrate example data flows for requesting and repaying micro-loans via a mobile wallet, respectively.

FIG. **11**A illustrates an example data flow of a subscriber receiving a direct deposit via a mobile wallet.

FIG. **11**B illustrates an example data flow of a subscriber receiving a governmental welfare payment via a mobile wallet.

FIG. **12**A illustrates an example data flow of an agent administrator distributing eMoney via a mobile wallet.

FIG. **12**B illustrates an example data flow of an agent company making a deposit using a mobile wallet.

FIG. **13** illustrates an example data flow of an agent company making a withdrawal using a mobile wallet.

FIG. **14** illustrates an example data flow of a subscriber making a deposit at an agent branch using a mobile wallet.

FIG. **15** illustrates an example data flow of a subscriber making a deposit with a non-agent using a mobile wallet.

FIG. **16** illustrates an example data flow of a subscriber making a withdrawal with an agent using a mobile wallet.

FIG. **17**A illustrates an example data flow of a subscriber making a withdrawal from an ATM using a mobile wallet.

FIG. **17**B illustrates an example data flow of a subscriber-to-subscriber money transfer using a mobile wallet.

FIG. **17**C illustrates an example data flow of a subscriber-to-non-subscriber money transfer using a mobile wallet.

FIG. **18**A illustrates an example data flow of a subscriber-to-subscriber international money transfer using a mobile wallet.

FIG. **18**B illustrates an example data flow of a subscriber-to-non-subscriber international money transfer using a mobile wallet.

FIG. **19**A illustrates an example data flow of a subscriber-to-subscriber international money transfer using a mobile wallet.

FIG. **19**B illustrates an example data flow of a non-subscriber-to-subscriber international money transfer using a mobile wallet.

FIGS. **20**A-**20**F illustrate embodiments of communications between specific components within a monetary transaction system during an operation to deposit of funds within a financial account.

FIGS. **21**A-**21**I illustrate embodiments of communications between specific components within a monetary transaction system during an operation to withdraw of funds from a financial account.

FIGS. **22**A-**22**J illustrate embodiments of communications between specific components within a monetary transaction system during an operation to transfer funds between financial accounts.

DETAILED DESCRIPTION

Embodiments described herein are directed to monetary transaction system for conducting monetary transactions between transaction system subscribers and other entities. In one embodiment, the monetary transaction system includes a mobile device configured to run a monetary transaction system application. The monetary transaction system also includes a monetary transaction system subscriber that has a profile with the system. The subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system. The system further includes a monetary transaction system processor that performs the transactions specified by the subscriber. Performing these transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile.

The monetary transaction system also includes at least one entity that is to be involved in the specified transaction, where the entity has a profile with the monetary transaction system. This entity may be a person, a retail store, an agent or other entity. The subscriber may have access to a bank account, or may be an "unbanked user" that does not have access to a bank account. Each of the terms included above will be described in greater detail below in conjunction with the drawings.

The monetary transaction system may be used for many different tasks including enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a mobile wallet, adding a debit or credit card account to a mobile wallet, depositing funds in a mobile wallet, withdrawing funds from a mobile wallet, paying bills from a mobile wallet, topping up a prepaid mobile account through a mobile wallet, transferring funds through a mobile wallet (nationally or internationally), making in-store purchases using a mobile wallet, and various other tasks as described herein below.

The following discussion now refers to a number of methods and method steps or acts that may be performed. It should be noted, that although the method steps may be discussed in a certain order or illustrated in a flow chart as occurring in a particular order, no particular ordering is necessarily required unless specifically stated, or required because a step is dependent on another step being completed prior to the step being performed.

Embodiments of the mobile transaction system or "mobile wallet platform" described herein may comprise or utilize a special purpose or general-purpose computer including computer hardware, such as, for example, one or more processors and system memory, as discussed in greater detail below. Embodiments described herein also include physical and other computer-readable media for carrying or storing computer-executable instructions and/or data structures. Such computer-readable media can be any available media that can be accessed by a general purpose or special purpose computer system. Computer-readable media that store computer-executable instructions in the form of data are computer storage media. Computer-readable media that carry computer-executable instructions are transmission media. Thus, by way of example, and not limitation, embodiments described herein can comprise at least two distinctly different kinds of computer-readable media: computer storage media and transmission media.

Computer storage media includes RAM, ROM, EEPROM, CD-ROM, solid state drives (SSDs) that are based on RAM, Flash memory, phase-change memory (PCM), or other types of memory, or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store desired program code means in the form of computer-executable instructions, data or data structures and which can be accessed by a general purpose or special purpose computer.

A "network" is defined as one or more data links and/or data switches that enable the transport of electronic data between computer systems and/or modules and/or other electronic devices. When information is transferred or provided over a network (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a transmission medium. Transmission media can include a network which can be used to carry data or desired program code means in the form of computer-executable instructions or in the form of data structures and which can be accessed by a general purpose or special purpose computer. Combinations of the above should also be included within the scope of computer-readable media.

Further, upon reaching various computer system components, program code means in the form of computer-executable instructions or data structures can be transferred automatically from transmission media to computer storage media (or vice versa). For example, computer-executable

instructions or data structures received over a network or data link can be buffered in RAM within a network interface module (e.g., a network interface card or "NIC"), and then eventually transferred to computer system RAM and/or to less volatile computer storage media at a computer system. Thus, it should be understood that computer storage media can be included in computer system components that also (or even primarily) utilize transmission media.

Computer-executable (or computer-interpretable) instructions comprise, for example, instructions which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. The computer executable instructions may be, for example, binaries, intermediate format instructions such as assembly language, or even source code. Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the described features or acts described above. Rather, the described features and acts are disclosed as example forms of implementing the claims.

Those skilled in the art will appreciate that various embodiments may be practiced in network computing environments with many types of computer system configurations, including personal computers, desktop computers, laptop computers, message processors, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, mobile telephones, PDAs, tablets, pagers, routers, switches, and the like. Embodiments described herein may also be practiced in distributed system environments where local and remote computer systems that are linked (either by hardwired data links, wireless data links, or by a combination of hardwired and wireless data links) through a network, each perform tasks (e.g. cloud computing, cloud services and the like). In a distributed system environment, program modules may be located in both local and remote memory storage devices.

In this description and the following claims, "cloud computing" is defined as a model for enabling on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). The definition of "cloud computing" is not limited to any of the other numerous advantages that can be obtained from such a model when properly deployed.

For instance, cloud computing is currently employed in the marketplace so as to offer ubiquitous and convenient on-demand access to the shared pool of configurable computing resources. Furthermore, the shared pool of configurable computing resources can be rapidly provisioned via virtualization and released with low management effort or service provider interaction, and then scaled accordingly.

A cloud computing model can be composed of various characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service, and so forth. A cloud computing model may also come in the form of various service models such as, for example, Software as a Service ("SaaS"), Platform as a Service ("PaaS"), and Infrastructure as a Service ("IaaS"). The cloud computing model may also be deployed using different deployment models such as private cloud, community cloud, public cloud, hybrid cloud, and so forth. In this description and in the claims, a "cloud computing environment" is an environment in which cloud computing is employed.

Additionally or alternatively, the functionally described herein can be performed, at least in part, by one or more hardware logic components. For example, and without limitation, illustrative types of hardware logic components that can be used include Field-programmable Gate Arrays (FPGAs), Program-specific Integrated Circuits (ASICs), Program-specific Standard Products (ASSPs), System-on-a-chip systems (SOCs), Complex Programmable Logic Devices (CPLDs), and other types of programmable hardware.

Still further, system architectures described herein can include a plurality of independent components that each contribute to the functionality of the system as a whole. This modularity allows for increased flexibility when approaching issues of platform scalability and, to this end, provides a variety of advantages. System complexity and growth can be managed more easily through the use of smaller-scale parts with limited functional scope. Platform fault tolerance is enhanced through the use of these loosely coupled modules. Individual components can be grown incrementally as business needs dictate. Modular development also translates to decreased time to market for new functionality. New functionality can be added or subtracted without impacting the core system.

Various terminology will be used herein to describe the monetary transaction system (also referred to as a "mobile wallet platform", "mobile wallet program" or "mobile wallet transaction system"). The term "agent" is used to refer to an individual with mobile financial services (mFS) transaction system tools and training to support specific mFS functions. These mFS functions include subscriber registration and activation, and the deposit and withdrawal of funds from the mFS transaction system. Agents are representatives of the mFS transaction system or "program". Agents can be employees or contractors of the program provider, or other companies and organizations that partner with the program provider to provide these services themselves. Agents may be found in every facet of a typical economy, and may include large retailers, mobile network operators (MNO) airtime sales agents, gas stations, kiosks, or other places of business.

The mobile wallet platform includes a mobile wallet application, web interface or some other type of functionality that allows the user to interact with the mFS platform using their mobile device. The mobile wallet application may include a subscriber identity module (SIM) application, an Unstructured Supplementary Service Data (USSD) application, a smartphone application, a web application, a mobile web application, a Wireless Application Protocol (WAP) application, a Java 2 Platform, Micro Edition (J2ME) application, a tablet application or any other type of application or interface that provides tools for the agent to register, activate, and offer other services to the mFS subscriber.

As used herein, a mobile wallet application is a mobile wallet application installed on a SIM card. A USSD application is an application that implements USSD for various functionality including prepaid callback service, location-based content services, menu-based information services and other mobile wallet platform services. A web application is one that implements or uses the internet to provide mobile wallet platform functionality. A mobile web application is similar to a web application, but is tailored for mobile devices. A WAP application is one that uses the wireless application protocol to communicate with the mobile wallet platform to provide the platform's functionality. A J2ME application is an application developed in Java and is

designed to provide mobile wallet functionality on a variety of different hardware. A tablet application is an application specifically designed for a touchscreen-based tablet that provides mobile wallet platform functionality for tablet devices, and as part of configuring the phone on the network. Any of these applications (or any combination thereof) may be provided on the user's mobile device. This functionality can also be made available on a retail point of sale (POS) system or web site.

The term "agent administrator" refers to an individual with mFS program tools and training to administrate the allocation of funds to agent branches (e.g. retail locations). As agents perform mFS transactions with subscribers, such as depositing and withdrawing money, the agents are adding and removing money from their own accounts. If there are insufficient funds in the agent's account to complete a transaction, additional money will need to be transferred from the agent company's master account to that agent branch account to cover that transaction. An agent administrator is responsible for these funds transfers. Any of the applications referred to above may be configured to provide tools used by the agent administrator to view the agent company balance, view the agent branch balances, and transfer funds into and out of agent branch mobile wallets. This functionality can also be made available on a website for easier access.

The term "agent administrator mobile wallet application" refers to a software program or application installed on the agent administrator's terminal in the agent administrator's mobile device (such as a mobile phone or tablet). This software application provides the agent administrator the ability to securely perform agent administrator functions such as querying the agent company account balance or transferring funds into and out of agent branch accounts. The agent administrator's mobile wallet application may be installed on a global system for mobile communications (GSM) SIM card (or on any other type of SIM card), and may be accessed using a GSM mobile phone. The agent administrator's application may also be installed on a code division multiple access (CDMA) mobile phone, a 3 G, 4G, 4G LTE (Long Term Evolution) or other wireless carrier standard. The application may, additionally or alternatively, be installed directly on the agent administrator's mobile device. The application communicates with the mFS transaction system using binary and/or text short message service (SMS) messages. A wireless service provider or MNO provides the GSM SMS network infrastructure on which the mFS platform operates.

In some embodiments, the mFS platform application may utilize triple data encryption standard (3DES) encryption (or some other type of encryption), encrypted message signing, and password security on some or all of its communications with the mFS transaction system in order to ensure that the transactions are properly secured and authenticated.

The term "agent branch" refers to any location where an agent provides support for subscriber services of the mFS platform. Funds are allocated by the agent administrator from the agent company's main account to each agent branch to fund the subscriber mFS functions such as depositing or withdrawing cash, in-store purchases, bill payments, prepaid airtime top-ups and money transfers. In some cases, multiple agents may work in a single branch. However, at least in some cases, monetary funds are allocated to from the agent company's main account on a per branch basis.

The term "agent branch account balance" refers to the amount of money residing in a particular agent branch account at a given time. Funds can be deposited into the branch account by the agent administrator, or the funds can come from participating in subscriber mFS transactions such as depositing or withdrawing cash from the subscriber's mobile wallet accounts, or making retail purchases with the mobile wallet.

Each agent branch is to maintain a balance in their branch account. This applies more strongly in countries where mFS program and financial services infrastructure is still developing. In cases where real-time processing of financial transactions including card processing is not practical, subscribers leverage the applications on their mobile phones to submit transactions and conduct business with retailers, businesses, and other subscribers. The mFS platform manages the balance of mobile wallet accounts for each subscriber as value is transferred from one mobile wallet to another (e.g. from a subscriber's mobile wallet to an agent's mobile wallet in payment for goods or services). This value is referred to herein as "eMoney".

As subscribers conduct business with mFS agents, they deposit or withdraw cash from their mobile wallet accounts. Virtual or eMoney credits are transferred between the subscriber's mobile wallet account and the agent branch's account as a form of currency to support the transaction. As agents accept cash into their cash register by mFS subscribers, they transfer the equivalent amount of eMoney credits into the mFS subscriber's mobile wallet account. For instance, if an mFS subscriber gives an mFS agent $10 to deposit into the subscriber's mobile wallet account, the agent would place the cash into his register and transfer $10 from the agent branch's eMoney account into the subscriber's mobile wallet account. While the agent acquired $10 in his register, he transferred out $10 of eMoney credits from his branch eMoney account.

In some embodiments, in countries with more developed economies, it may be beneficial to use program-issued pre-paid debit cards, pre-paid access accounts, stored value accounts or gift cards to conduct business along with the added convenience of card processing networks such as Cirrus, STAR, or Visa for POS and automated teller machine (ATM) functionality. Agents, particularly those in retail outlets and kiosks, can still support subscribers with deposits, withdrawals, and other transfers, but in this case bank external card processors manage the mobile wallet and branch account balances and provide the real-time transfer of funds.

The term "agent branch ledger" refers to a written (or electronic) ledger maintained by the mFS platform. Agent branch transactions are performed on the agent's and subscriber's mobile phones where an electronic record of the transaction is generated and stored on the mFS platform. These electronic transactions are then reconciled with agent branch ledgers to ensure the security and integrity of the transaction. Agent branch ledgers are printed or electronic transaction logs that are distributed to the agent branch locations in hard copy form to serve as a backup record to the electronic transactions.

The term "agent company" refers to a business that registers to participate in the mFS program as a partner of the mFS program provider or owner. The agent company has one or more agent branches which conduct mFS business with mFS program subscribers. In some cases, the agent company may be referred to as a distributor or retailer.

The term "agent company account balance" refers to the sum of the funds deposited at a "partner bank" (defined below) by the agent company to fund the agent company's daily transactions. The funds in the agent company account are then distributed to agent branches by the agent compa-

ny's agent administrator to conduct everyday business such as accepting cash deposits and cash withdrawals from mFS subscribers. This balance is sometimes referred to as the "agent company float".

An "agent manager" is a supervisor of company agents for a given company. The agent manager has the training and tools to create, delete or modify agent accounts for a company, as well as monitor the transactions performed by agents. The agent manager may have a special application or an increased level of rights to access applications features not available to other users. The special application is a program installed on the agent manager's terminal. This application provides the agent manager the ability to securely perform agent manager functions such as registering and activating new agent accounts.

The mFS agent manager application may be installed on any terminal or device. It communicates with the mFS platform using binary and/or text SMS messages. A wireless service provider or MNO provides the GSM SMS network infrastructure on which the mFS platform operates. The mFS platform mobile wallet applications may utilize 3DES encryption (or any other type of encryption), encrypted message signing, and password security on some or all of its communications with the mFS platform in order to ensure that the transactions are properly secured and authenticated.

The term "agent application" refers to an application that provides all the tools necessary for an agent to register, activate, and offer other services to the mFS subscriber. The agent application is a program installed on the agent's SIM card or otherwise installed in the agent's mobile device's memory. This application provides the agent the ability to securely perform agent functions such as registering and activating new subscribers and depositing and withdrawing funds from mobile wallet accounts. The mFS agent application may be installed on a GSM SIM card or mobile phone and may be accessed using a GSM or CDMA mobile phone. A wireless service provider or MNO provides the data and SMS network infrastructure on which the mFS platform operates.

The terms "mFS platform", "mobile wallet platform" and "monetary transaction system" refer to an overall platform or ecosystem of different components that work together to provide the various functions described herein on a global scale. At least some of the various logic components include the following: the application. The "mobile wallet application" or "mFS application" manages the processing of incoming transactions regardless of their source. The application handles end-user authentication, transaction processing, subscriber profile management, and further manages interactions between the various platform components.

The mFS platform further includes a transaction processor. This component is used when the mFS application is implemented in a country where real-time processing of financial transactions is not practical (or not possible). The transaction processor manages the balance of mobile wallet accounts, agent accounts, and the accounts of any other program participant. The transaction processor handles balance inquiries, credits, debits, and transaction roll-backs.

The mFS platform further includes a rules engine that manages and applies the rules and policy that are defined for transactions as they are processed on the mFS platform. Rules impact transaction fees, limits, velocity limits, and commissions as well as program actor roles and permissions. Rules can be customized for each implementation. The mFS platform also includes an integration interface that manages the integration and interaction between external systems (i.e. external to the mFS platform) and the mFS platform. Connectivity to the wireless service provider's pre-paid airtime billing platform and the program partner bank, for example, are managed by the integration interface.

The mFS platform further includes a transaction database that stores the data that supports the mFS platform. This includes subscriber profiles and subscription data, transaction data and logs, and application configuration and runtime data, among other types of data. Another component of the mFS platform is a handset support service that interfaces with the wireless service provider's SMS network to allow communication between the mobile wallet applications and the back-office systems via SMS messaging or some other form of data transfer. Still further, another component of the mFS platform is a web component that provides a web interface to the mFS program participants that allows the subscriber to perform the same functions in the web interface that they would have available through their applications.

The term "bill pay company" refers to a business that signs-up to participate in the mFS transaction system. As a participant in the mFS transaction system, the company accepts payment from mFS mobile wallet accounts, either in the form of eMoney or through periodic settlements.

At least in some embodiments, financial transactions that take place in the mFS mobile wallet platform are funded through pre-paid mobile wallet accounts. Mobile wallet platform subscribers can deposit cash into their mobile wallet account through a process referred to herein as 'cash-in'. The cash-in process is supported by mFS agents at agent branch locations. The agent accepts the cash from the subscriber and transfers the equivalent amount of eMoney to the subscriber's mobile wallet account. This process is similar to withdrawing cash from a bank account.

As mentioned above, in some embodiments, financial transactions that take place in the mobile wallet platform are funded through pre-paid mobile wallet accounts. Mobile wallet platform subscribers can withdraw cash from their mobile wallet account through a process known as "cash-out". The cash-out process is supported by mFS agents at agent branch locations. The subscriber transfers eMoney from their mobile wallet account to the agent's eMoney account. Upon receiving the eMoney, the agent gives the subscriber cash from their branch cash register.

Accounts managed on the mFS platform by the mFS eMoney transaction processor maintain the mobile wallet balance of mFS program participants including subscribers, agent branches, agent companies, and non-agent companies. eMoney is moved between Mobile Wallet accounts by the transaction processor based on mFS transaction processing. Only when transactions involving cash (i.e. depositing or withdrawing funds from the mFS program) or the movement of money from mFS participants to non-mFS program participants are funds moved from the master bank accounts.

As subscribers, agents, and other mFS program participants conduct business in the mFS program, value is transferred from one account to the next as payment for services rendered or goods purchased. This value can be in the form of real currency or the electronic representation referred to herein as eMoney.

Among other situations, eMoney is used in mFS implementations where the real-time processing of financial transactions including card processing is not practical. The mFS platform utilizes an internal transaction processor for managing the real-time balance of mobile wallet and agent accounts as value (eMoney) is transferred from one mobile wallet to another in payment for services.

As subscribers conduct business with mFS agents, they deposit or withdraw cash from their mobile wallet accounts. Virtual or eMoney credits are transferred between the subscriber mobile wallet accounts and the agent branch accounts as a form of currency to support the transaction. As agents accept cash into their cash register by mFS subscribers, they transfer the equivalent amount of eMoney credits into the mFS subscriber's mobile wallet account. For example, if an mFS subscriber gives an mFS agent $10 to deposit into the subscriber's mobile wallet account, the agent would place the cash into his or her register, and transfer $10 from the agent branch eMoney account into the subscriber's mobile wallet account. While the agent acquired $10 in his or her register, the agent transferred-out $10 of eMoney credits from his or her branch eMoney account. This will be explained in greater detail below.

In some embodiments, employers may wish to participate in the mFS program by allowing the direct deposit of paychecks into subscribers' mobile wallet accounts. Accordingly, each payday, the user's pay is directly transferred to the subscribers' mobile wallet.

The term "know your customer" or "KYC" refers to information collected about an individual that identifies that individual. Such information is used to establish a mobile wallet account with the mobile wallet platform. Regulatory requirements in some countries require that new bank account creation must be preceded by a display of a valid government ID. These KYC regulations may vary from country to country. Accordingly, different KYC information may be requested from subscribers in different countries in order to establish a mobile wallet account.

The term micro-finance institution (MFI) refers to a lender that issues small loans. MFIs participating in the mFS program lend to mFS program subscribers and accept loan repayment either in the form of eMoney or settlements with the mFS platform provider.

The term "mFS program", like the term "mFS platform" refers to the ecosystem of companies, service providers, and subscribers that participate in providing mobile financial services to their customers. In some embodiments, there may be one mFS program implementation per country. Each program includes a program owner and operator, a program platform, a partner wireless services provider or MNO, and a partner bank.

The term "mFS program master account" refers to a bank account maintained by the mFS program partner bank to provide funds and float for the operation of the mFS platform. Depending on the type of mFS implementation, the master account can include sub-accounts for each of the agent branches and subscriber mobile wallets, giving the bank visibility into all transactions on a per-user basis. The mFS platform can also manage the balance of sub-accounts and interact with the bank's master account when funds need to be deposited or withdrawn from the account.

The term mobile network operator (MNO) refers to a provider of mobile phone service including basic voice, SMS, unstructured supplementary service data (USSD) and data service, and may also be referred to as a "wireless service provider".

The term "mobile wallet" or "mobile wallet account" refers to a stored value account or prepaid access account (PPA) that allows the owner (or "subscriber") to pay for goods and services on the mFS platform from his or her mobile wallet account. When the mFS eMoney transaction processor is used, the mobile wallet balance is maintained by the mFS platform and value is exchanged within the mFS program as eMoney. When the mFS platform is integrated to an external card processor, the mobile wallet utilizes funds from the subscriber's prepaid debit card and bank account to exchange value on the mFS platform.

The term "non-agent company" refers to a mFS program participant who accepts payments from mFS subscribers but does not provide the same services as mFS agent companies. Payment is accepted either in the form of eMoney or through periodic settlements with the mFS platform provider. Examples of non-agent companies include bill pay providers and micro-finance lenders.

The term "non-mFS subscribers" refers to unregistered users that participates in various use cases in the mFS program. Non-mFS subscribers can send money to or receive money from mFS subscribers through interaction with the mFS program agents or with international remittance providers.

The term "partner bank" refers to the primary bank participating in the mFS program. The partner bank is responsible for holding the mFS program master accounts that hold the funds for all mFS services and transactions. A "PIN" refers to a numeric password that may be required to perform a transaction via the mobile wallet application. A "transaction processor" refers to an application or service that manages the mFS program account balances. The transaction processor determines the amount of funds or eMoney is in a particular account at any given time, and manages account balances. Mobile transaction system requests to credit, debit, or view the balance of a particular mobile wallet or program account are handled by the transaction processor (in conjunction with other components of the mobile wallet platform).

The term "sub-accounts" refers to accounts that are maintained within the mFS platform or by an external card processor. A partner bank may elect to maintain a separate bank account for each subscriber and/or agent branch, or a single master account may be established that contains the funds for all of the subscriber mobile wallet and agent branch accounts (at least within a country or other geographical region). The balance of each individual user may be managed by the mFS transaction processor.

When using a master account, the bank is involved only in transactions that require the movement of funds external to the mFS program. For example, subscriber cash-in and cash-out transactions involve the addition and removal of cash from the mFS program and would consequently include a deposit or withdrawal from the master account. Retail purchases from participating mFS program retailers or the exchange of funds between mFS subscribers results in no net change in the mFS program balance and thus do not require involvement by the partner bank.

The term "subscriber" refers to a participant of the mFS mobile wallet platform. The subscriber maintains a mobile wallet balance and performs transactions using the mFS application. An "unbanked subscriber" is a subscriber that does not have (or does not have access to) a bank account or credit union account. The application or "mobile wallet application" provides mobile wallet functionality to the (unbanked) subscriber. The mobile wallet application is installed on a mobile device in the device's memory, on a SIM card (such as a GSM SIM card) or is otherwise accessible to the mobile device. The mobile wallet application provides the subscriber the ability to securely perform subscriber functions such as making retail purchases, paying bills, or transferring money to other mFS subscribers and non-subscribers. The mobile wallet application communicates with the mFS platform using binary and text SMS messages, among other forms of wireless communication. A

wireless service provider or MNO provides the GSM network infrastructure on which the mFS platform operates.

FIG. **1** illustrates an example system architecture for a mobile wallet platform. Integration tier **101** is configured to manage mobile wallet sessions and maintain integrity of financial transactions. Integration tier **101** can also include a communication (e.g., Web services) API and/or other communication mechanisms to accept messages from channels **111**. Other mechanisms include, but are not limited to: International Standards Organization ("ISO") **8583** for Point of Sale ("POS") and Automated Teller Machines ("ATM") devices and Advanced Message Queuing Protocol ("AMQP") for queue based interfaces. Each of channels **111** can be integrated to one or more mechanisms for sending messages to integration tier **101**. Notification services **102** is configured to send various notifications through different notification channels **112**, such as, for example, Short Message Peer-to-Peer ("SSMP") for Short Messaging Service ("SMS") and Simple Mail Transfer Protocol ("SMTP") for emails. Notification services **102** can be configured through a web services API.

Service connectors **103** are a set of connectors configure to connect to 3rd party systems **113**. Each connector can be a separate module intended to integrate an external service to the system architecture. Business process services **104** are configured to implement business workflows, including executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects. Payment handler **105** is configured to wrap APIs of different payment processors, such as, for example, banking accounts, credit/debit cards or processor **121**. Payment handler **105** exposes a common API to facilitate interactions with many different kinds of payment processors.

Security services **106** are configured to perform subscriber authentication. Authorization services **107** are configured to perform client authorization, such as, for example, using a database-based Access Control List ("ACL") table.

Database **108** is configured to manage customer accounts (e.g., storing customer accounts and properties), manage company accounts (e.g., storing company accounts and properties), manage transaction histories (e.g., storing financial transaction details), store customer profiles, storing dictionaries used by the mobile wallet platform, such as, for example, countries, currencies, etc., and managing money containers. Rules engine **109** is configured to gather financial transaction statistics and uses the statistics to provide transaction properties, such as, for example, fees and bonuses. Rules engine **109** is also configured to enforce business constraints, such as, for example, transactions and platform license constraints.

Name matching engine **110** is configured to match different objects according to specified configuration rules. Matching engine **110** can be use to find similarities between names, addresses, etc. Transaction processor **121** is configured to manage financial accounts and transactions. The transaction processor **121** can be used to hold, load, withdraw and deposit funds to mobile wallet accounts. Transaction processor **121** can also be used as a common interface to a third party processor system. When used as a common interface, financial operations may be delegated to the external processor. A Clearing House subsystem of transaction processor **121** can be used to exchange the financial information with a bank.

Components of a mobile wallet platform can be connected to one another over (or be part of) a system bus and/or a network. Networks can include a Local Area Network ("LAN"), a Wide Area Network ("WAN"), and even the Internet. Accordingly, components of the mobile wallet platform can be "in the cloud". As such, mobile wallet platform components as well as any other connected computer systems and their components, can create message related data and exchange message related data (e.g., Internet Protocol ("IP") datagrams and other higher layer protocols that utilize IP datagrams, such as, Transmission Control Protocol ("TCP"), Hypertext Transfer Protocol ("HTTP"), Simple Mail Transfer Protocol ("SMTP"), etc.) over the system bus and/or network.

The components depicted in FIG. **1** can interoperate to provide a number of financial and other services including but not limited to enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a mobile wallet, adding a debit or credit card account to a mobile wallet, depositing funds in a mobile wallet, withdrawing funds from a mobile wallet, paying bills from a mobile wallet, topping up a prepaid mobile account through a mobile wallet, transferring funds through a mobile wallet (nationally or internationally), making in-store purchases using a mobile wallet, and various other tasks as described herein below. These services will be described in greater detail below with regard to system FIGS. **1** and **2**, as well as FIGS. **3-19B**.

FIG. **2** depicts a monetary transaction system **200** similar to that described in FIG. **1**. The monetary transaction system **200** may provide a more simplified system structure in which each of the above services may be provided. The system includes a subscriber **205**. The subscriber may have access to a bank account, or may be an unbanked subscriber. The subscriber has a profile **211** with the monetary transaction system **210**. The profile includes the subscriber's KYC information, as well as any associated bank accounts, credit union accounts, bill pay accounts or other accounts. The subscriber has (or has access to) a mobile device **206** such as a phone or tablet. The mobile device runs the mobile wallet application (or mobile wallet application) **207**.

The subscriber can indicate, using the mobile application **207** which transaction or other action he or she would like to perform. The indicated transaction **208** is sent to the mobile wallet platform **210** to be carried out by the platform. The transaction processor **216** (which may be similar to or the same as transaction processor **121** of FIG. **1**) performs the transaction(s) specified by the (unbanked) subscriber **205**. The transaction processor may implement various other components to perform the transaction including memory **217**, (wireless) communication module **215**, rules engine **210** and/or transaction database **225**.

Performing the specified transactions may include communicating with the monetary transaction database **225** to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile (for instance, whether the subscriber has enough eMoney in his or her stored value account, or has enough money in his or her bank account). Rules engine **220** may also be consulted to determine whether the subscriber has exceeded a specified number of allowed transactions. Then, if funds are available, and the transaction is otherwise permissible, the monetary transaction system can transfer money or eMoney **221** to or from an entity such as a user or agent (e.g. entity **222**) to or from an establishment such as a retail store or agent company (e.g. entity **223**).

In some cases, the monetary transaction system **210** application provides a web interface that allows subscribers to perform the same functions provided by the monetary

transaction system application. For instance, mobile wallet application **207** may provide a web interface that allows a user to enroll for a mobile wallet. The web interface (or the mobile wallet application itself) receives a subscriber-initiated transaction over one of a plurality of channels (**111** from FIG. **1**) connected to the monetary transaction system **210**. The web interface or mobile wallet application may prompt for and receive enrollment information (e.g. KYC information) for the (unbanked) subscriber **205** over at least one of the plurality of channels (e.g. web, point-of-sale (POS), interactive voice response (IVR, etc.). The web interface or mobile wallet application may then send activation instructions over the same or a different channel to activate the (unbanked) subscriber **205** and create a subscriber account for the (unbanked) subscriber.

Once the subscriber has an account, the monetary transaction system generates a corresponding mobile wallet for the unbanked subscriber (available via the web interface and/or the mobile wallet application. The system then presents the (unbanked) subscriber's account data associated with the mobile wallet and/or a notification indicating that enrollment was successful to the subscriber. Accordingly, the mobile wallet application or the web interface may be used to provide user enrollment functionality. It should also be understood that either the mobile wallet application or the web interface may be used to provide substantially all of the mobile wallet functionality described herein.

It should also be noted that the mobile device **206** may be any type of plan-based phone or tablet, or prepaid phone or tablet. Many subscribers, such as unbanked subscribers, may primarily use prepaid phones. The mobile wallet application **207** may be installed on both plan-based phones and prepaid phones. The mobile wallet application may be installed on the device's SIM card, or on the device's main memory. Accordingly, the monetary transaction system **200** may be accessed and used via substantially any type of plan-based or prepaid mobile device.

FIG. **3** shows three different graphics (**301**-**303**) and corresponding method steps (**310**-**370**) that illustrate an unbanked subscriber making a deposit using a mobile wallet (and, by extension, using the mobile wallet transaction system **210**). In at least some of the embodiments described below, the actions of each participant are shown and described. This will also, at least in some embodiments, include an illustration of money flow throughout the mobile wallet transaction system. In the graphics, various terms are used as follows: $C=Cash Balance and $E=Electronic Money (eMoney) Balance.

At graphic **301**, it is assumed that the unbanked subscriber (e.g. **205**) has already registered and activated an eMoney account at an agent branch location (e.g. a retail store, gas station, or other location that has registered to be an agent branch). To deposit cash in order to get eMoney credit, the subscriber informs the agent manager or agent that they want to deposit a certain amount of cash (in **301**). The agent manager/agent takes the cash and notifies the mobile wallet transaction system of the deposit using their agent manager or agent application (**302**). The transaction system **210** then credits the subscriber's eMoney account (**303**). Accordingly, any location that has registered to accept eMoney payments from subscribers' mobile wallets can also accept cash deposits. The agent branch's eMoney balance is reduced because their actual money balance was increased by the amount of the deposit. The subscriber's mobile wallet account is credited with eMoney in the amount of the deposit. In this manner, a subscriber can deposit cash into their mobile wallet account (in the form of eMoney) at any retail location or other agent branch location.

Thus, the agent manager receives the physical cash deposit into the subscriber's eMoney account via the agent manager or agent's application. The subscriber gives cash to agent manager or agent, and the mFS platform processes the request, updates the agent branch and subscriber's eMoney balances, logs the transaction, and sends details (such as eMoney account balances, transaction logs, etc.) to bank specified by the mobile wallet platform. These details may be sent instantaneously as transactions occur, or in batches at pre-determined intervals.

In one embodiment, the monetary transaction system **210** of FIG. **2** is implemented to deposit funds at an agent branch using a mobile wallet. The monetary transaction system **210** receives communication from an agent branch over one of a plurality of channels (e.g. **111**) connected to the monetary transaction system (step **310**). The agent communication indicates that the unbanked subscriber **205** desires to deposit a specified amount of funds into the unbanked subscriber's mobile wallet account. The transaction processor **216** then validates the status of the unbanked subscriber's mobile wallet account (step **320**) and determines if the agent branch is authorized to receive deposited money (i.e. determine if it has pre-registered as an official agent branch) (step **330**).

The monetary transaction system may then use rules engine **220** to perform a limit check (to determine whether sufficient funds are available) and/or a velocity check (to determine whether the user has exceeded a specified number of (hourly, daily, or weekly) transactions) on the unbanked subscriber's mobile wallet account (step **340**). The transaction system then credits the unbanked subscriber's mobile wallet account with the specified amount of funds (step **350**) and returns a notification to the agent branch confirming the deposit (step **360**) and returns another notification to the subscriber notifying the subscriber that the specified amount of funds was deposited in the their mobile wallet account (step **370**). Any of channels **111** may be used to perform these communications.

FIG. **4** shows three different graphics (**401**-**403**) and corresponding method steps (**410**-**490**) that illustrate an unbanked subscriber making a withdrawal using a mobile wallet (and, by extension, using the mobile wallet transaction system **210**). As above, the terms in the graphics include "$C" representing cash balance and "$E" representing eMoney balance.

To withdraw cash at an agent branch, a subscriber submits a withdrawal request using their application (**401**). The subscriber may also enter information about the agent branch (e.g. name of establishment, name of agent, location or other information) that allows the monetary transaction system **210** to identify the agent branch. The transaction processor **216** may then determine whether the unbanked subscriber has enough eMoney to withdraw the requested amount. If he or she does have enough eMoney, then the subscriber's eMoney is deducted and that amount is transferred to the agent branch's eMoney account (**402**). Then, the agent branch gives the subscriber the requested amount of cash (**403**). In this manner, any entity that has established itself as an agent branch (including retail stores, gas stations, service providers, etc.) can provide cash withdrawal to a mobile wallet subscriber (whether banked or unbanked). The agent's or agent manager's role is to verify the withdrawal request (e.g. via SMS on the agent's or agent manager's phone) and gives the cash to subscriber. The subscriber requests cash withdrawal from agent branch's eMoney account via the application, and receives physical

cash from agent manager/agent. The mobile wallet platform processes the request, updates the agent branch's and subscriber's eMoney balances, logs the transaction, and sends transaction details to a specified bank at pre-determined intervals.

In one embodiment, the monetary transaction system **210** is implemented to withdraw funds at an agent branch using a mobile wallet. The communication module **215** receives a communication from an unbanked subscriber over one of a plurality of channels **111** connected to the monetary transaction system **210** (step **410**). The communication indicates that the unbanked subscriber **205** desires to withdraw a specified amount of funds from the unbanked subscriber's mobile wallet account at the agent branch. The monetary transaction system **210** validates the status of the unbanked subscriber's mobile wallet account (step **420**) and determines if the balance of the unbanked subscriber's mobile wallet account is sufficient to accommodate the requested withdrawal for the specified amount of funds (step **430**).

The transaction processor **216** performs one or more of a limit check (to verify sufficient funds) and a velocity check (to verify the subscriber hasn't exceeded specified transfer limits) on the unbanked subscriber's mobile wallet account (step **440**). The monetary transaction system **210** then returns a secure, perishable withdrawal code to the subscriber **205** over at least one of the plurality of channels **111** connected to the monetary transaction system (step **450**). The monetary transaction system **210** receives subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system indicating that the withdrawal code has been presented to the agent branch (step **460**). The monetary transaction system **210** then debits the unbanked subscriber's mobile wallet account by the specified amount of funds (step **470**), returns a notification to the agent branch confirming the withdrawal (step **480**) and notifies the subscriber that the specified amount of funds was withdrawn from the unbanked subscriber's mobile wallet account over at least one of the channels **111** connected to the monetary transaction system (step **490**). Accordingly, the monetary transaction system **210** may be used to allow subscribers to withdraw cash using their mobile wallet applications at any store or other entity registered as an agent branch.

FIG. **5**A depicts a subscriber-to-subscriber eMoney transfer. To perform such a transfer, subscriber A (**501**) enters some type of identification information identifying subscriber B (e.g. subscriber B's phone number) and an amount of money he or she wishes to transfer. The transaction processor **216** of the monetary transaction system **210** determines if there are sufficient funds to complete the transfer. If sufficient funds are available, the monetary transaction system **210** decrements subscriber A's account and credits subscriber B's account (**502**). The system then sends some kind of notification (e.g. SMS) to subscriber B indicating that a certain amount of money was transferred to their account. Subscriber A may also receive a notification that the transfer was successful. Accordingly, eMoney may be transferred between two mFS platform subscribers, one or both of which may be unbanked. The monetary transaction system **210** processes the subscribers' requests, updates the subscribers' eMoney balances, logs the transactions, and sends transaction information to a specified bank when needed.

FIG. **5**B illustrates a subscriber-to-non-subscriber eMoney transfer. In graphic **505**, subscriber A wishes to send eMoney to another individual that is not a subscriber to the mFS platform. The transaction is initiated in the same fashion as the subscriber-to-subscriber transfer scenario. However, since non-subscriber B does not have a mobile wallet account, the monetary transaction system **210** cannot credit them with eMoney. Instead, the monetary transaction system **210** sends a notification (e.g. via SMS) to non-subscriber B with instructions for how to pick-up the transferred money, along with an authorization code (**506**). The monetary transaction system **210** puts a hold on subscriber A's account for the amount transferred. Subscriber B then has a specified number of days to pick up the cash before the hold expires and the amount is credited back to subscriber A's eMoney account by the monetary transaction system **210**.

When non-subscriber B goes to pick up the money at an agent branch, the agent branch's manager or agent verifies the authorization code via an agent manager or agent mobile wallet application (that, in turn, accesses the mFS platform). Once the transfer has been validated, the agent gives the cash to non-subscriber B. The agent branch's mFS account is credited with the transfer amount (**507**) and the user leaves with the cash in hand (**508**). The mFS platform processes the transfer request, updates subscriber A's eMoney balance, logs the transaction, and sends transaction details to a platform-specified bank.

FIG. **6**A illustrates a subscriber-to-subscriber international eMoney transfer. This embodiment is, at least in some respects, similar to sending eMoney to an mFS subscriber domestically. In this case the monetary transaction system **210** leverages one or more existing international money transfer organizations or "remittance companies" such as MoneyGram®. In some embodiments, MoneyGram® is pre-integrated to the monetary transaction system **210**, but other international money transfer organizations may also be used. Still further, at least in some embodiments, subscriber B may need to have an eMoney account with a foreign mFS program that is also affiliated with MoneyGram® or another international money transfer organization.

In FIG. **6**A, subscriber A initiates the international eMoney transfer at **601**, the international money transfer organization (e.g. MoneyGram®) transfers the eMoney to subscriber B at **602** and subscriber B's eMoney balance is increased by the transferred amount. Thus, subscriber A requests to send eMoney from his or her eMoney account via the mobile wallet application. The eMoney is transferred using an international money transfer organization, and subscriber B receives a notification (that may, for example, include a reference number, among other information) that their eMoney balance has increased by the transfer amount. The monetary transfer system **210** processes subscriber A's request, updates subscriber A's and subscriber B's eMoney balances, logs the transaction, and send transaction details to a mFS platform-specified bank.

FIG. **6**B illustrates a subscriber-to-non-subscriber international eMoney transfer. In this illustration, subscriber A wishes to send cash to subscriber B who is not an mFS program subscriber. Similar to the scenario described in FIG. **6**A, the monetary transaction system **210** leverages various international money transfer organizations or remittance companies such as MoneyGram® to transfer the eMoney. Subscriber A initiates a typical eMoney transfer at **605** by providing non-subscriber B's identification information, as well as the amount to be transferred. The Monetary transaction system **210** recognizes the eMoney transfer is not destined for a domestic phone number and routes the request to the international money transfer organization (e.g. MoneyGram®) (**606**).

The international money transfer organization sends non-subscriber B a notification (e.g. via SMS) with instructions for how and where to pick up the money (in embodiments where MoneyGram® transfers the eMoney, the notification may include a MoneyGram® reference number (MGRN)) (**607**). Non-subscriber B can then show the MGRN to an agent at an agent branch (**608**) and then receive the cash (**609**). The monetary transaction system **210** then decrements subscriber A's eMoney account for the transferred amount. The monetary transfer system **210** thus processes subscriber A's transfer request, updates subscriber A's eMoney balance, logs the transaction, and sends transaction detail to a platform-specified bank. It should also be noted that an mFS subscriber may also receive money in a foreign country from either a subscriber or a non-subscriber in a similar manner.

FIG. **7** illustrates a subscriber purchasing airtime using a mobile wallet. Mobile wallet platform subscribers may buy airtime by using their mobile wallet application **207**. The monetary transaction system **210** will reload their airtime account within the mobile network operator's (MNO's) systems. The subscriber requests to purchase airtime by entering the request via the mobile wallet application or via a mobile wallet web interface. The monetary transaction system **210** then decrements the subscriber's eMoney account (**701**), while crediting the mFS platform's eMoney account (**702**). The purchased airtime is then added to the subscriber's airtime balance (**703**). The monetary transaction system **210** processes the subscriber's request, updates the subscriber's eMoney balances as well as its own eMoney balance, logs the transaction, and sends transaction detail to a mFS platform-specified bank.

In one embodiment, the monetary transaction system **210** is implemented to top up a prepaid mobile account from a mobile wallet. The communication module **215** of the monetary transaction system **210** receives a subscriber communication over one of a plurality of channels **111** connected to the monetary transaction system (step **710**). The subscriber communication indicates that an unbanked subscriber **205** desires to top up a prepaid mobile account by a specified amount using a specified payment method from the unbanked subscriber's mobile wallet. The transaction processor **216** validates the status of the selected payment method (step **720**) and performs a limit check and/or a velocity check on the selected payment method (step **730**). The monetary transaction system **210** then debits the specified payment method by the specified amount of funds (step **740**) and processes the mobile top-up via a billing system integrator and/or an aggregator (step **750**), and notifies the subscriber that the prepaid mobile account was topped up over at least one of the channels connected to the monetary transaction system (step **760**).

FIG. **8** illustrates an embodiment where a mFS subscriber pays a bill using a mobile wallet. At least in some embodiments, the company that the subscriber wishes to pay needs to have signed-up to be part of the mFS platform. The mFS platform may publish a list of company names that have registered to be part of the mFS platform. This list of companies may include company IDs so that subscribers can know which company ID to enter in their mobile wallet application. Once the company ID is known, the subscriber can pay a bill by entering the company ID and the amount to be paid. The monetary transaction system **210** then decrements the subscriber's eMoney account (**801**) and credits the identified company's eMoney account (**802**). Accordingly, in response to the subscriber's request to pay bill via their mobile wallet application, the monetary transaction system **210** processes the request, updates the bill pay company's and the subscriber's eMoney balances, logs the transaction, and sends transaction details to the mFS platform-specified bank.

In one embodiment, the monetary transaction system **210** is implemented to pay a bill from a mobile wallet. The communications module **215** of the monetary transaction system **215** receives a subscriber communication over a communication channel **111** connected to the monetary transaction system (step **810**). The subscriber communication indicates that unbanked subscriber **205** desires to pay a bill for a specified amount using a specified payment method from the unbanked subscriber's mobile wallet (e.g. eMoney). The monetary transaction system **210** validates the status of the selected payment method (step **820**) and performs a limit check and/or a velocity check on the selected payment method to ensure the eMoney transfer is permissible (step **830**). The monetary transaction system then debits the specified payment method by the specified amount of funds (step **840**), processes the bill payment via a direct biller connection or a bill pay aggregator (step **850**), and notifies the unbanked subscriber that the bill was paid using a communication channel (e.g. SMS) connected to the monetary transaction system (step **860**). Thus, in this manner, a subscriber may use a mobile wallet to pay various bills including rent, utility, mortgage, phone, cable, medical and other bills.

FIG. **9** illustrates a mobile wallet subscriber making a retail purchase.

Mobile wallet subscribers can make retail purchases at agent branches directly from their mobile device. Agent branches, as explained above, are retail stores or other entities that have registered with the mFS system and are able to accept mobile wallet payments. Accordingly, a subscriber can select the items they wish to purchase, and indicate (via the mobile wallet application) to the agent branch that they wish to pay for the items. The mobile wallet application then communicates with the agent branch and the monetary transaction system to indicate the price of the transaction. The monetary transaction system **210** then debits the subscriber's eMoney account (**901**) and credits the agent branch's eMoney account (**902**). The agent branch (and/or the agent manager or agent) receives confirmation that subscriber paid for the purchase. The subscriber may also receive a summary of the retail purchase and may be asked to confirm the purchase by entering a PIN. The monetary transaction system processes the purchase request, updates the agent branch and subscriber's eMoney balances, logs the transaction, and sends transaction details to a mFS platform-specified bank.

In one embodiment, the monetary transaction system **210** is implemented to make a purchase from a mobile wallet. The communications module **215** of the monetary transaction system **210** receives a communication from a subscriber over a communication channels **111** (step **910**). The subscriber communication indicates that an unbanked subscriber **205** desires to purchase an item for a specified amount of funds using a specified payment method from the unbanked subscriber's mobile wallet.

The monetary transaction system **210** then returns a secure, perishable purchase code to the unbanked subscriber over at least one of the channels connected to the monetary transaction system (step **920**) and receives a subsequent agent branch communication over a channel indicating that the purchase code has been presented to an agent (branch) (step **930**). The monetary transaction system **210** validates the status of the specified payment method (step **940**),

determines if the specified payment method can accommodate a purchase for the specified amount (step **950**), performs a limit check and/or a velocity check on the selected payment method (**960**), debits the specified payment method by the specified amount of funds (**970**), returns a notification to the agent branch authorizing the purchase (**980**) and sends a receipt to the unbanked subscriber over a communication channel. The monetary transaction system **210** may thus be used to make a retail purchase using a mobile wallet.

FIG. **10**A illustrates a subscriber requesting a micro-loan. Financial institutions and potentially other mFS program participants may sign up to become money or eMoney lenders. Mobile wallet subscribers may be able to use their mobile wallets to request micro-loans from these approved lenders. The micro-loans are tracked by the monetary transaction system **210**, and repayment reminders, interest and commissions are managed by the monetary transaction system. The subscriber requests a micro-loan from a lender, indicating the amount in the request, as well as other information such as the repayment date and the commission (i.e. interest rate). Potential lenders then have a chance to counter the loan request with their own terms. Once the lender approves the subscriber's request, the lender's eMoney account balance is debited for the specified amount (**1001**) and the subscriber's eMoney account is credited with the requested amount (**1002**). The monetary transaction system **210** processes the micro-loan requests, update the lender and subscriber's eMoney balances, sets up repayment schedules and reminders, logs the transaction, and sends transaction detail to a mFS bank. It should also be noted that while the term "micro-loan" is used herein, the loan may be for substantially any amount of money.

Following on the embodiment described in FIG. **10**A, FIG. **10**B illustrates a subscriber repaying a micro-loan. The subscriber may repay the loan using functionality provided in the mobile wallet application or in a similar web interface. Repayments can be made in installments or in full depending on the rules of the micro-loan. The subscriber enters the amount they wish to repay and the loan ID. The subscriber's eMoney account is then debited for the specified amount (**1005**), while the lender's eMoney account is credited the specified amount (**1006**). Both the lender and the subscriber may receive confirmation that the loan has been repaid via SMS or some other communication channel. The mFS platform thus processes the subscriber's micro-loan repayment request, updates lender and subscriber's eMoney balances, updates repayment schedule and reminders, logs the transaction, and sends transaction details to a specified mFS platform bank.

FIG. **11**A illustrates a subscriber receiving a direct deposit from an employer or other entity. Subscribers to the mFS platform have the ability to receive any direct deposit into their eMoney account. Subscribers may be asked by their employers to provide account information in order to set up direct deposit. The employer then submits a direct deposit request using their existing processes (i.e the processes they use for a normal checking or savings bank account). Once the direct deposit is set up and a payday arrives, the employer's bank account is debited for the proper amount (**1101**) and the employer's mFS account is credited with that amount (**1102**). Then, once the funds have been received at the mFS platform bank, the mFS platform bank sweeps the employers direct deposit balance (**1103**) into a mFS platform master account (**1104**) and notifies the mFS platform of each account to be incremented (including the subscriber's mobile wallet (eMoney) account). The subscriber's eMoney account is then credited with the paycheck amount (**1105**) upon which the eMoney may be used to pay for goods, pay bills, top up airtime, transfer to other entities or for cash withdrawal.

The subscriber does not need to have a bank account to participate in direct deposit. The employer's bank can communicate with the mFS platform's bank to perform the necessary steps in directly depositing the subscriber's paycheck in his or her eMoney mobile wallet account. The bank facilitates monetary deposit into the employer's bank account for direct deposit and performs an automated sweep of recent deposits from the employer's bank account into the mFS platform's master bank account. The bank also sends transaction details to the monetary transaction system **210** including transaction logs. The monetary transaction system receives a list of eMoney accounts that are to be credited directly from the employer (or bank), processes the list and requests to establish a direct deposit, updates subscriber's eMoney balance, log the transaction, and sends transaction details to the mFS platform bank.

In a similar manner, a subscriber may receive a government welfare payment directly on their mobile device. FIG. **11**B illustrates a subscriber receiving a government social welfare payment directly into their eMoney account. In some embodiments, subscribers may need to opt-in and register with the government program for which they choose to receive the payment via their mobile wallet. Once the funds have been received, the subscriber can use that eMoney for any goods or services, as described above. Once the direct deposit has been established and a payout has been initiated, the government's welfare account deposits the money (**1110**) into the government's bank account for welfare payments (**1111**) and performs an automated sweep of recent deposits from the government's bank account (**1112**) into the mFS program's master bank account (**1113**). The bank then sends transaction details to the monetary transaction system **210** regarding the deposit. The subscriber receives a notification that the welfare payment has been credited to their eMoney account (**1114**). The mFS platform receives an indication of eMoney accounts that are to be credited from the government, processes the welfare payments, updates the subscriber's eMoney balance, logs the transactions, and sends transaction details to the mFS platform bank.

FIG. **12**A illustrates an agent administrator distributing eMoney to various recipients. An agent administrator, as explained above, is a person who acts as an agent company's representative. The agent administrator deposits, withdraws, and distributes funds into and out of the agent company's bank account. When an agent administrator deposits cash into an agent company's bank account, it is credited as eMoney to the agent company's account. In order to provide the agent branches with eMoney, the agent administrator first moves the eMoney from the agent company's account (**1201**) to the branch accounts (**1202**). This is performed using the agent administrator's mobile wallet application or portal. In an agent administrator money transfer, the monetary transaction system **210** processes the administrator's eMoney transfer request, updates the agent company and agent branch eMoney balances, logs the transaction, and sends transaction details to the mFS platform bank.

FIG. **12**B illustrates an agent company deposit. The agent company has an eMoney account in the monetary transaction system **210** that may also include a corresponding bank account (that may be created automatically upon creation of the agent company's eMoney account). After the agent company's bank account has been set up, the agent administrator can make deposits into that account. As FIG. **12**B

shows, once cash (**1205**) has been deposited into the bank account (**1206**), it is transferred to a mFS platform master account (**1208**) that includes all or a part of the mFS platform's funds. The agent company's bank account is decreased by the deposit amount (**1207**), while the agent company's eMoney account balance is correspondingly increased (**1210**). At this time, the agent company account is credited with eMoney. The agent company's bank facilitates a physical cash deposit into the agent company's bank account and performs an automated sweep (**1209**) of recent deposits from the agent company's bank account into the mFS platform's master bank account. The agent company's bank then sends transaction details to the monetary transaction system **210**. The agent administrator physically delivers the cash (or form of money such as a check or money order) to a bank branch for deposit. The monetary transfer system receives transaction details from the agent company's bank about recent transactions (including deposits, as shown in FIG. **12**B.

FIG. **13** illustrates an agent company withdrawal. To make a cash withdrawal for an agent company, the agent administrator requests a withdrawal using the agent administrator mobile wallet application. The monetary transaction system **210** then notifies the bank that a certain amount of eMoney is to be transferred from the master mFS account (**1302**) to the agent company bank account (**1303**). When the money is in the agent company bank account, the agent administrator can withdraw the cash by traditional withdrawal means. The mFS master bank receives transaction details from the monetary transaction system **210** about recent transactions (recent withdrawals in this case). The mFS master bank performs an automated sweep (**1304**) of the mFS platform's master bank account to reflect the recent withdrawal request from agent the agent company (**1301**). The agent company's eMoney account is reduced by the amount of the withdrawal. The agent company also sends transaction details to the monetary transaction system **210**. The agent administrator can request withdrawal via the agent administrator mobile wallet application and physically withdrawal cash (**1305**) from the agent company's bank branch (**1306**). The mFS platform processes the agent company's withdrawal request, updates agent company and agent branch eMoney balances, logs the transaction, and sends transaction details to an mFS platform-specified bank.

Attention will now be turned to embodiments in which subscribers have bank accounts associated with their mobile wallets. The monetary transaction system **210** provides similar functionality to consumers that have bank or credit union accounts. Although many different transactions are presented herein, many more and varied types of transactions may be processed by the monetary transaction system. In the following figures, "$C" refers to cash balance, "$DC" refers to a debit card (prepaid) balance and "$PIN" refers to a recharge PIN value.

FIG. **14** describes a subscriber deposit at an agent branch. The subscriber has a registered and activated (prepaid) debit card at an agent branch location. The prepaid debit card is associated with the mobile wallet application in the subscriber's mobile device. As such, the debit card is linked to the subscriber's account in the monetary transaction system **210**. To deposit cash onto the mobile wallet, the subscriber informs the agent that they want to deposit a specified amount of cash (**1401**). The agent takes the cash and notifies the monetary transaction system **210** of the deposit using their point of sale (POS) system or the agent mobile wallet application (**1402**), and the monetary transaction system **210** credits the subscriber's mobile wallet account (**1403**). The funds collected at the cash register typically do not reach a bank account until the reconciliation and settlement of funds occurs between the agent and the mFS owner's bank.

The subscriber's bank then receives a settlement report from the card processor and receives funds from the agent's bank. The agent or agent manager physically deposits the cash into the subscriber's mobile wallet account via their POS system or agent manager/agent mobile wallet application. The monetary transaction system processes the deposit request, increments the subscriber's mobile wallet balance within the card processor and logs the transaction. An external card processor increments the subscriber's mobile wallet balance and sends reports to the bank for settlement on a regular (e.g. nightly) basis.

In one embodiment, the monetary transaction system **210** is implemented to deposit funds into a bank or credit union account using a mobile wallet. The communications module **215** of the monetary transaction system **210** receives communication from an agent branch over a communication channel (step **1410**). The agent communication indicates that a subscriber **205** desires to deposit a specified amount of funds into a bank or credit union account. The transaction processor **216** validates the status of the bank or credit union account (step **1420**), determines if the agent branch is authorized to deposit money (step **1430**), and performs a limit check and/or a velocity check on the bank or credit union account (step **1440**). The monetary transaction system then credits the bank or credit union account with the specified amount of funds (step **1450**), returns a notification to the agent branch confirming the deposit (step **1460**) and notifies the subscriber that the specified amount of funds was deposited in the bank or credit union account using at least one of the communication channels connected to the monetary transaction system (step **1470**). Accordingly, cash may be deposited into a bank or credit union account associated with a subscriber's mobile wallet.

FIG. **15** illustrates a subscriber deposit that is performed with a non-agent. In some economies, subscribers may have the ability to leverage other channels outside of agents to deposit funds onto their card. One deposit method is a PIN-based recharge that allows a subscriber to purchase a PIN worth the deposit value. The PIN can then be redeemed via an interactive voice response (IVR) system or via the subscriber's mobile wallet application. The mobile wallet application will allow the monetary transaction system **210** to deposit the funds onto the subscriber's card. The retailer's bank settles with the PIN card provider's bank and the PIN card provider's bank settles with the mFS platform's bank for the deposit. The subscriber gives cash to the agent (**1501**) which increases the agent company's physical cash (**1502**). The subscriber uses IVR or their SIM Application to recharge mobile wallet account using a PIN card (**1503**). In some cases, an agent may provide the PIN card (i.e. the prepaid debit card) to the subscriber. The monetary transaction system **210** processes the subscriber deposit request, increments the subscriber's mobile wallet balance within the card processor and logs the transaction. An external card processor decreases the subscriber's PIN card balance (**1504**), increments the subscriber's mobile wallet balance (**1505**) and send reports to the mFS platform bank for settlement.

FIG. **16** illustrates a subscriber withdrawal at an agent branch. To withdraw cash at an agent branch from a (prepaid) debit card, a subscriber submits a withdrawal request using the mobile wallet application on their mobile device. The subscriber may also need to enter details about the agent branch that allows the monetary transaction system **210** to

determine if the subscriber has sufficient funds on their debit card. The mFS platform then notifies the agent branch that it can give cash to the subscriber. If the subscriber has sufficient funds, the monetary transaction system **210** will decrement the subscriber's funds from their card (**1601**) and transfer it to the mobile wallet owner's account within the same card processor or bank. The agent branch (**1602**) then provides the withdrawn cash to the subscriber (**1603**).

Accordingly, the subscriber requests a cash withdrawal from their own mobile wallet account via the mobile wallet application. The agent or agent manager verifies the withdrawal request via POS authorization or SMS received on agent's phone and, once verified, gives cash to the subscriber. The monetary transaction system **210** processes the subscriber's withdrawal request, decrements the subscriber's mobile wallet balance within the card processor and logs the transaction. An external card processor decrements the subscriber's mobile wallet balance and sends reports to the bank for settlement on a periodic basis.

In one embodiment, the monetary transaction system **210** is implemented to withdraw funds from a bank or credit union account using a mobile wallet. The communication module **215** of the monetary transaction system **210** receives a communication from a subscriber **205** over a communication channel **111** (step **1610**). The subscriber communication indicates that subscriber **205** desires to withdraw a specified amount of funds from a bank or credit union account. The transaction processor validates the status of the bank or credit union account (step **1620**), determines if the balance of the bank or credit union account is sufficient to accommodate the requested withdrawal for the specified amount of funds (step **1630**) and performs a limit check and/or a velocity check on the bank or credit union account (step **1640**).

The monetary transaction system **210** then returns a secure, perishable withdrawal code to the subscriber **205** over at least one of the communication channels (step **1650**) and receives a subsequent agent branch communication indicating that the withdrawal code has been presented to an agent (step **1660**). The monetary transaction system **210** then debits the bank or credit union account by the specified amount of funds (step **1670**), returns a notification to the agent branch confirming the withdrawal (**1680**) and notifies the subscriber that the specified amount of funds were withdrawn from the bank or credit union account using at least one of the communication channels connected to the monetary transaction system (step **1690**). Accordingly, a subscriber can withdraw cash stored on their mobile wallet from an agent branch or a non-agent branch.

FIG. **17**A illustrates a subscriber withdrawal using an automated teller machine (ATM). Subscribers in many countries have access to ATM machines and can use their mobile wallets to perform withdrawals using their (prepaid) debit card at most ATMs. Banks provide ATMs to their customers (typically at no charge) and to non-customers (typically for a small charge). The subscriber requests a cash withdrawal from the subscriber's mobile wallet via the subscriber's debit card that is associated with the mobile wallet. The bank providing the debit card may receive settlement reports from the card processor and may transfer and/or settle funds from subscriber's account to the ATM network bank. An extern card processor decrements the subscriber's mobile wallet balance (**1701**) and sends transaction reports to the bank for settlement. Accordingly, once the withdrawal request has been received and the external card processor (e.g. Visa® or MasterCard®) (**1702**) has debited the debit card account, the ATM (**1703**) dispenses the withdrawn cash to the subscriber (**1704**).

FIG. **17**B illustrates a subscriber-to-subscriber money transfer. An mFS subscriber (**1705**) may send money to another mFS subscriber (**1706**). To do so, subscriber A enters information identifying subscriber B (e.g. a phone number, email address or other identifier). The monetary transaction system **210** determines if there are enough funds to complete the transaction, and if so, the monetary transaction system **210** decrements subscriber A's debit card and credits subscriber B's debit card. The subscriber, accordingly, may request to send money from their own mobile wallet (i.e. money stored on a (prepaid) debit card) account via the subscriber mobile wallet application. The other subscriber receives a notification that the balance of the debit card associated with their mobile wallet has increased. The bank receives a settlement report from the debit card processor and transfers or settles funds from subscriber A's account to subscriber B's account (if necessary). The monetary transaction system **210** processes the transfer request, updates subscriber A's and subscriber B's debit cards that are associated with their mobile wallets and logs the transaction. The external card processor decrements subscriber A's debit card balance, increments subscriber B's debit card balance and sends transaction reports to the mFS platform bank for settlement.

FIG. **17**C illustrates subscriber-to-non-subscriber money transfers. In this embodiment, subscriber A (an mFS subscriber) wishes to send money to another subscriber (a non-mFS subscriber). The transaction is initiated in the same fashion as described above in FIG. **17**B. However, since subscriber B does not have an mFS account, the monetary transaction system **210** cannot credit them with money. Instead, the monetary transaction system **210** sends a communication (e.g. a SMS) to subscriber B (**1708**) with an authorization code and instructions for how to pick up the cash. The monetary transaction system **210** puts a hold on subscriber A's debit card for the amount transferred (**1707**). Subscriber B has a specified time period in which to pick up the cash before the hold expires and the amount is credited back to the debit card associated with subscriber A's mobile wallet account. The agent branch verifies the authorization code via POS or their agent mobile wallet application (**1709**) and gives the cash to the non-subscriber (**1710**). (In some countries, an agent network needs to be capable of giving cash to a subscriber based on the money transfer reference number).

The mFS bank receives a settlement report from the card processor and transfer and settle funds from subscriber A's debit card to the agent's bank (if necessary). The monetary transaction system **210** processes the money transfer request, decrements subscriber A's mobile wallet balance within the card processor, generates a money transfer reference number, authorizes the reference number to be paid out by the agent and logs the transaction. An external card processor decrements subscriber A's mobile wallet balance and sends periodic transaction reports to the bank for settlement. Thus, as seen in FIGS. **17**B and **17**C, money may be transferred from subscriber to subscriber and from subscriber to non-subscriber.

Subscribers may similarly send money internationally to both subscribers and non-subscribers. FIG. **18**A illustrates a subscriber-to-subscriber international money transfer. In this embodiment, subscriber A wishes to send cash to subscriber B who resides in another country. As in the embodiments described above where money was transferred internation-

ally, the monetary transaction system **210** may use one or more international money transfer organizations or remittance companies such as MoneyGram® to transfer the money. Subscriber A initiates the international money transfer using his or her phone. Subscriber A's debit card account is decremented by the transfer amount (**1801**). The money is transferred between countries using an international money transfer organization (**1802**). In this case, subscriber B has an mFS eMoney account with a foreign mFS platform that is also affiliated with the selected international money transfer organization. That organization can then credit subscriber B's eMoney account directly (**1803**).

Thus, subscriber A requests to send money from their debit card account via the subscriber mobile wallet application. Subscriber B receives a notification (including a MoneyGram® Reference Number (MGRN) (or other reference number when other international money transfer organizations are used) and instructions on how to access the eMoney) that their eMoney balance has increased. The mFS bank receives settlement reports from the debit card processor and transfers and/or settles funds from subscriber's account to the international organization's bank. The monetary transfer system **210** processes the transfer request, update subscriber A's and subscriber B's eMoney balances and logs the transaction. An external card processor decrements subscriber A's mobile wallet balance and sends periodic transaction reports to the bank for settlement.

FIG. **18**B illustrates a subscriber-to-non-subscriber international money transfer. In this embodiment, subscriber A wishes to send cash to subscriber B who resides in another country. As above, the monetary transaction system **210** uses an international money transfer organization (**1806**) to transfer the money between countries. Once the transfer has been initiated by subscriber A, the international money transfer organization debits subscriber A's debit card account (**1805**) and transfers that money to subscriber B. Subscriber B (**1807**) receives a notification (e.g. via SMS) with pick up instructions and a transfer ID number. Subscriber B can then go to an agent company (**1808**), show them the notification (including, perhaps an authorization code), and receive the transferred money (**1809**).

Similar to the transaction described in FIG. **18**A, the embodiment of **19**A illustrates a transaction where a subscriber receives an international money transfer. Subscriber B (**1901**) initiates a money transfer using their mobile wallet application. The international money transfer organization (**1902**) debits subscriber B's eMoney account balance. This money is then transferred by the international money transfer organization to subscriber A. Subscriber A receives a notification along with a transfer ID number indicating that their debit card account has been credited with the transferred money (**1903**).

FIG. **19**B illustrates a non-subscriber-to-subscriber international money transfer. This scenario is very similar to that described in FIG. **19**A from the mFS subscriber's perspective, except that their eMoney account is credited here, and their debit card account was credited in **19**A. The initiator, subscriber B (**1905**), does not have an mFS account and, as a result, takes their cash to an international money transfer organization (e.g. MoneyGram®) or other remittance company's agent (**1906**) to send it to subscriber A's mobile wallet eMoney account. The international money transfer organization (**1907**) then transfers the specified amount to subscriber A (**1908**) and subscriber A's mobile wallet eMoney account is credited with the amount of the transfer. Subscriber A may receive a transaction ID number, along with an indication that the transfer has occurred. The mFS bank may receive settlement reports from the card processor and settle funds from the international money transfer organization's bank to subscriber A's mobile wallet account. The monetary transaction system processes the money transfer request, updates subscriber A's mobile wallet balance within the card processor and logs the transaction. An external card processor increments subscriber A's mobile wallet balance and sends periodic transaction reports to the mFS bank for settlement.

Other functionality described above in relation to using an eMoney mobile wallet account may also apply to banked subscribers using a debit card associated with their mobile wallet. Such subscribers may buy airtime for their mobile device, pay bills, make retail purchases, receive direct deposits, and perform other functionality.

In one embodiment, the monetary transaction system **210** is implemented to add a mobile wallet platform stored value account to a mobile wallet. The stored value account may include eMoney or other monetary credits. In the embodiment, communication module **215** of monetary transaction system **210** may receive subscriber data for an unbanked subscriber **205** over a communication channel. The transaction processor may perform validation checks on the unbanked subscriber to validate that the unbanked subscriber is not exceeding a specified allowable number of accounts per subscriber. The monetary transaction system **210** may then send subscriber data to another entity (such as a third party verification system) for identification of the unbanked subscriber. The monetary transaction system **210** receives results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber, creates a stored value account for the unbanked subscriber that maintains a recorded balance for the created stored value account, adds the stored value account to the unbanked subscriber's mobile wallet and notifies the unbanked subscriber of the addition of the stored value account over at least one communication channel connected to the mobile wallet platform.

In another embodiment, the monetary transaction system **210** is implemented to add a third party stored value account to a mobile wallet. The monetary transaction system **210** receives unbanked subscriber data, including account details, over a communication channel. The transaction processor **216** performs a validation check on the unbanked subscriber to validate that the unbanked subscriber is not exceeding a specified allowable number of accounts per subscriber. If the validation check is ok, the monetary transaction system **210** sends subscriber data to a third party verification system for identification of the unbanked subscriber. In some cases, validating the status of the sender or the recipient includes performing a check on the specified sender or recipient to comply with the office of foreign assets control. The monetary transaction system **210** then receives results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber, and submits the unbanked subscriber's account details to a third party account processor. The monetary transaction system **210** receives an indication from the third party account processor that third party account processor created a third party stored value account for the subscriber. The transaction processor maintains a link between the subscriber data and the third party stored value account and adds the third party stored value account to the unbanked subscriber's mobile wallet. The monetary transaction system **210** then notifies the unbanked subscriber of the addition of the third party stored value account over a communication channels connected to the monetary transaction system.

In another embodiment, the monetary transaction system **210** is implemented to add a bank or credit union account to a mobile wallet. The communication module **215** receives subscriber data, including bank or credit union account details, over a communication channel **111**. The transaction processor **216** performs validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber and sends subscriber data to a third party verification system for identification of the subscriber. The communication module then receives results from the third party verification system indicating that the subscriber data appropriately identifies the subscriber. Upon receiving these results, the monetary transaction system **210** submits bank or credit union account details for validation by the transaction processor, receives an indication that the bank or credit union account details correspond to a valid bank or credit union account, maintains a link between the subscriber data and the bank or credit union account and notifies the subscriber of the bank or credit union account validation over a communication channel.

In still another embodiment, the monetary transaction system is implemented to add a debit or credit card account to a mobile wallet. The communication module **215** receives subscriber data, including a debit or credit card account number, over a communication channel **111** connected to the monetary transaction system. The transaction processor performs validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber. The communication module sends subscriber data to a third party verification system for identification of the subscriber and receives results from the third party system indicating that the subscriber data appropriately identifies the subscriber. The monetary transaction system **210** securely stores the debit or credit card account number for access by the mobile wallet (e.g. in memory **217** or transaction database **225**), adds the debit or credit card account number to the subscriber's mobile wallet, and notifies the subscriber of the addition of the debit or credit card account number. It should be noted that many other transactions can take place over the monetary transaction system, and that the embodiments described herein should not be read as limiting.

Embodiments of the invention can adhere to Know Your Customer (KYC) rules in the US by performing Customer Identification Program (CIP) checks as required by the Bank Secrecy Act and US PATRIOT Act. A minimum amount of information can be gathered about a customer, such as, for example, first name, last name, date of birth, government ID Type, government ID number and address. The CIP processes are designed to validate customer identity against government blacklists and assists in the prevention of money laundering and terrorist financing. A combination of non-documentary and documentary verification can be used to ensure beyond a reasonable doubt the identity of the customer.

Non-documentary verification can occur through the presentment of the information that was collected from the user to an external third party, such as, for example, Lexis Nexis®. Documentary verification can occur if non-documentary verification fails, then the user is asked to present an unexpired government ID. Various differ forms of identification including driver's license, passport, alien identification (e.g., green card or work visa), and Mexican Consular identification card, can be accepted.

Embodiments of the invention can perform Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) checks. AML and CFT checks can be performed using transaction monitoring methods to flag names and suspicious transactions for further investigation. The mobile wallet platform can perform AML and CFT checks on all electronic financial transactions to ensure that electronic funds are not being used for money laundering or terrorism. Transaction limits can be placed on user accounts. The transaction limits are fully configurable for each particular use case, channel and payment method that allows maximum flexibility to restrict higher risk use cases. Velocity checks can also be performed. Velocity Checks ensure that subscribers are not abusing the mobile wallet platform within the allowable limits.

FIGS. **20**A through **20**F depicts relationships between embodiments of various components within the monetary transaction system depicted in FIG. **1**. In particular, FIGS. **20**A through **20**F depict communications between the specific components within the monetary transaction system during an operation to deposit of funds within a financial account. The depicted interactions are representative of computer executed functions that enable the deposit of money through a mobile transaction system that is capable of functioning without an associated bank account.

FIGS. **21**A through **21**I depicts relationships between embodiments of various components within the monetary transaction system depicted in FIG. **1**. In particular, FIGS. **21**A through **21**I depict communications between the specific components within the monetary transaction system during an operation to withdraw of funds from a financial account. The depicted interactions are representative of computer executed functions that enable the withdrawal of money through a mobile transaction system that is capable of functioning without an associated bank account.

FIGS. **22**A through **22**J depicts relationships between embodiments of various components within the monetary transaction system depicted in FIG. **1**. In particular, FIGS. **22**A through **22**J depict communications between the specific components within the monetary transaction system during an operation to transfer funds between financial accounts. The depicted interactions are representative of computer executed functions that enable the transfer of money through a mobile transaction system that is capable of functioning without an associated bank account.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

I claim:

1. A monetary transaction system for conducting monetary transactions between subscribers and other entities, the system comprising one or more of:

an integration tier operable to manage mobile wallet sessions, the integration tier also including a communication application programming interface (API) and other communication mechanisms to accept messages from channels;

notification services operable to send notifications through different notification channels including one or more of short message peer-to-peer, short-message services and simple mail transfer protocol emails;

business process services operable to implement business workflows, including at least one of executing financial

transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects;

database services operable to store financial transaction details, store customer profiles, and manage money containers;

a payment handler service operable to use APIs of different payment processors including one or more APIs of banks, credit and debit cards processors, bill payment processors;

a rules engine operable to gather financial transaction statistics and use the gathered financial transaction statistics to enforce constraints including transaction constraints;

a security service operable to perform subscriber authentication;

at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system: wherein the at least one entity is the agent;

wherein the monetary transaction system is implemented to deposit funds at an agent branch, the funds being deposited by a subscriber at the agent branch using a mobile device configured to run a monetary transaction system application, the monetary transaction system performing the following steps:

receiving a communication message from the mobile device over one of a plurality of channels connected to the monetary transaction system, the communication message being received by an API associated with the integration tier of the monetary transaction system, the communication message indicating that the subscriber desires to deposit a specified amount of funds into the subscriber's account;

validating the status of the subscriber's account, wherein validating the status of the subscriber's account comprises communicating from the integration tier to the database services to query attributes of the subscriber's account;

committing a pending transaction through the business process services, wherein the integration tier communicates a transaction commitment request to the business process services;

receiving a confirmation from the business process services that the pending transaction has been committed;

sending, through the notification services, a receipt notification to the mobile device; and

upon receiving a confirmation of commitment from the business process services, committing the pending transaction to the database services; and

wherein committing the pending transaction further comprises the following steps as orchestrated by the business process services:

ensuring, via the database services, that the subscriber has an active account;

validating, through communication with the security services, one or more of a PIN number and an access control list;

applying with the rules engine, velocity rules;

creating with the database services a new pending transaction history record;

holding funds from the agent account balance using the payment handler,

loading the funds to the subscriber account using the payment handler; and

updating, using the database services, a pending transaction history record to reflect the funds.

2. A monetary transaction system for conducting monetary transactions between subscribers and other entities, the system comprising one or more of:

an integration tier operable to manage mobile wallet sessions and maintain the integrity of financial transactions, the integration tier also including a communication application programming interface (API) and other communication mechanisms to accept messages from channels;

notification services operable to send notifications through different notification channels including one or more of short message peer-to-peer, short-message services and simple mail transfer protocol emails;

business process services operable to implement business workflows, including at least one of executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects;

a security service operable to perform subscriber authentication;

database services operable to store financial transaction details, store customer profiles, and manage money containers;

a mobile device configured to run a monetary transaction system application;

a payment handler service operable to use APIs of different payment processors including one or more APIs of banks, credit and debit cards processors, bill payment processors;

a rules engine operable to gather financial transaction statistics and use the gathered financial transaction statistics to enforce business constraints including transaction constraints;

a security service operable to perform subscriber authentication;

at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system, wherein the at least one entity is the agent;

a monetary transaction system subscriber that has a profile with the monetary transaction system the subscriber profile stored in the database of the monetary transaction system, wherein the subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system;

wherein the monetary transaction system is implemented to withdraw funds at an agent branch using the mobile device configured to run a monetary transaction system application, including performing the following steps:

receiving a communication message from the mobile device over one of a plurality of channels connected to the monetary transaction system, the communication message being received by an API associated with the integration tier of the monetary transaction system, the communication message indicating that the subscriber desires to withdraw a specified amount of funds from an account associated with the subscriber, the communication comprising a secure, perishable code;

determining that the transaction is valid and in progress, wherein determining that the transaction is valid comprises validating the secure, perishable

code and communicating from the integration tier to the database services to query attributes of the subscriber's account;

committing a pending transaction through the business process services, wherein the integration tier communicates a transaction commitment request to the business process services;

receiving a confirmation from the business process services that a pending transaction has been committed;

sending, through the notification services, a receipt notification to the mobile device; and

upon receiving a confirmation of commitment from the business process services, committing the pending transaction to the database services; and

wherein committing the pending transaction further comprises the following steps as orchestrated by the business process services:

ensuring, via the database services, that the subscriber has an active account;

validating, through communication with the security services, one or more of a PIN number and an access control list;

applying with the rules engine, velocity rules;

creating with the database services a new pending transaction history record;

holding funds from the agent account balance using the payment handler;

loading the funds to the subscriber account using the payment handler; and

updating using the database services, a pending transaction history record to reflect the funds.

3. A monetary transaction system for conducting monetary transactions between subscribers and other entities, the system comprising one or more of:

an integration tier operable to manage mobile wallet sessions and maintain the integrity of financial transactions, the integration tier also including a communication application programming interface (API) and other communication mechanisms to accept messages from channels;

notification services operable to send notifications through different notification channels including one or more of short message peer-to-peer, short-message services and simple mail transfer protocol emails;

business process services operable to implement business workflows, including at least one of executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects;

database services operable to store financial transaction details, store customer profiles, and manage money containers;

a monetary transaction system subscriber that has a profile with the monetary transaction system the subscriber profile stored in the database of the monetary transaction system, wherein the subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system;

a payment handler service operable to use APIs of different payment processors including one or more APIs of banks, credit and debit cards processors, bill payment processors;

a rules engine operable to gather financial transaction statistics and use the gathered financial transaction statistics to enforce business constraints including transaction constraints;

a security service operable to perform subscriber authentication;

at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system; wherein the at least one entity is the agent;

wherein the monetary transaction system is implemented to transfer funds using the mobile device configured to run a monetary transaction system application, including performing the following steps:

receiving a communication message from the mobile device over one of a plurality of channels connected to the monetary transaction system, the communication message being received by an API associated with the integration tier of the monetary transaction system, the communication message indicating that the subscriber desires to transfer a specified amount of funds from the subscriber's account to a recipient;

validating the status of the subscriber's account, wherein validating the status of the subscriber's account comprises communicating from the integration tier to the database services to query attributes of the subscriber's account;

committing a pending transaction through the business process services, wherein the integration tier communicates a transaction commitment request to the business process services;

receiving a confirmation from the business process services that a pending transaction has been committed;

sending, through the notification services, a receipt notification to the mobile device; and

upon receiving a confirmation of commitment from the business process services, committing the pending transaction to the database services; and

wherein committing the pending transaction further comprises the following steps as orchestrated by the business process services:

ensuring, via the database services, that the subscriber has an active account;

validating, through communication with the security services, one or more of a PIN number and an access control list;

applying with the rules engine, velocity rules;

creating with the database services a new pending transaction history record;

holding funds from the agent account balance using the payment handler;

loading the funds to the subscriber account using the payment handler; and

updating, using the database services, a pending transaction history record to reflect the funds.

* * * * *

Exhibit D
PayPal Infringement Chart for
U.S. Patent No. 9,892,386

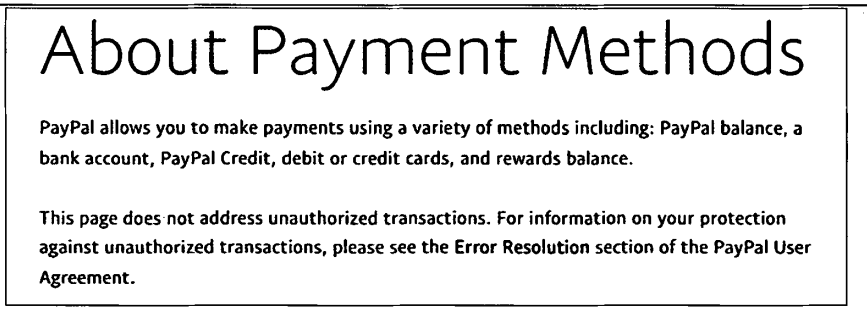
U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
1. A monetary transaction system for conducting monetary transactions between subscribers and other entities, the system comprising one or more of:	Upon information and belief, PayPal manages a transaction system and payment application that allows users to make monetary transactions between subscribers and other entities. SEND AND REQUEST MONEY FOR FREE • When funded by a bank account or with your PayPal balance, it's free and secure to send money or ask for it back from friends and family in the US. • Just type a name, email or phone number and PayPal will find the right person for you if they have an account. • Request money quickly and securely from friends or family and personalize your payments with animations, stickers, emojis and more. *See* https://apps.apple.com/app/id283646709?mt=8 (last accessed on February 25, 2022).

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 • Make payments using your credit card, debit card, bank account, or other payment options, including funds held as balance in a business PayPal account (if we have verified the required identifying information you provide to us) or funds held in a PayPal Balance account linked to a personal PayPal account if you choose to open a PayPal Balance account. The terms "PayPal Balance account" or "Balance Account" in this user agreement are used to refer to a PayPal Balance account and shall include any account currently or previously known as a PayPal Cash or a PayPal Cash Plus account, as applicable. More information about Balance Accounts can be found in the PayPal Balance Terms and Conditions. • Accept credit card, debit card, bank account, Balance Account, and other payment methods from others. You are responsible for maintaining adequate security and control of any and all IDs, passwords, personal identification numbers, or any other codes that you use to access your PayPal account and the PayPal services. You must keep your mailing address, email address and other contact information current in paypal.com *See* PayPal User Agreement on PayPal Mobile App.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 160 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022).
1[a] an integration tier operable to manage mobile wallet sessions, the integration tier also including a communication application programming interface (API) and other communication mechanisms to accept messages from channels;	Upon information and belief, the PayPal System includes an integration tier. The integration tier is configured to manage mobile wallet sessions. The integration tier handles communications from different mobile phones (e.g. Apple and/or Android) and uses API and other communication mechanisms to communicate.

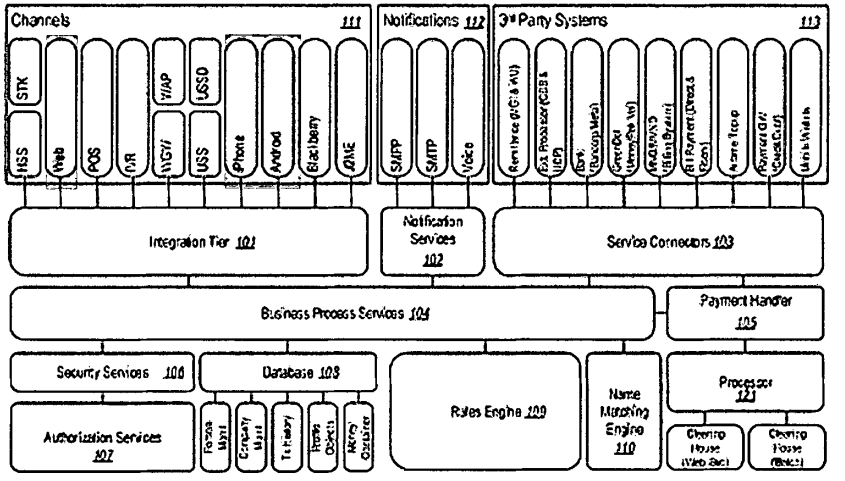
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 161 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 We have versions of our app for iOS, Android, and Windows. In a few moments you can log on to PayPal, check your balance, pay bills, and more. It is easy, fast, and secure. With PayPal there are no borders. Download Now: iPhone | Android https://www.paypal.com/bs/webapps/mpp/shop/apps (last accessed on February 25, 2022).

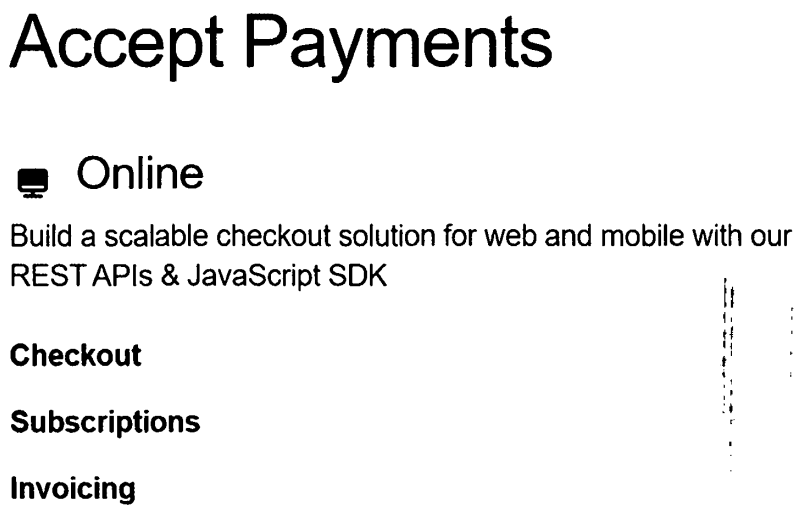
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 162 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 ***Figure 1*** *See e.g.* '386 Patent Figure 1. Upon information and belief, the PayPal System provides REST APIs for new integrations. These APIs use HTTP methods, a RESTful endpoint structure, the OAuth 2.0 protocol, and JSON-formatted payloads. The REST APIs can be used to incorporate the PayPal System's functionality

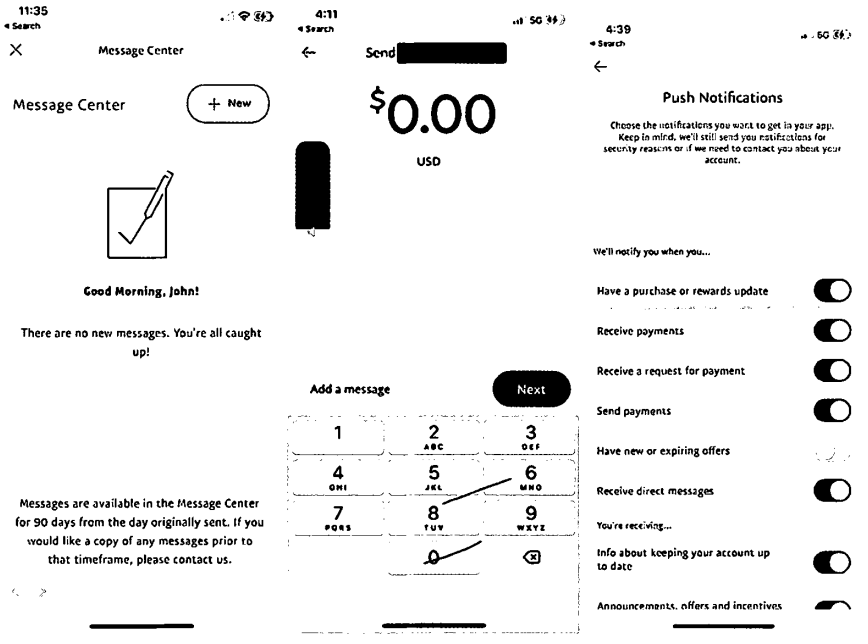
U.S. Patent Feb. 13, 2018 Sheet 1 of 46 US 9,892,386 B2

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	into a user's web and mobile apps. Standard PayPal APIs can be accessed via the PayPal Developer Portal (*see* http://developer.paypal.com (last accessed on February 25, 2022)). 
1[b] notification services operable to send notifications through different notification channels including one or more of short message peer-to-peer, short-message services and	Upon information and belief, the PayPal system includes notification services that are capable of sending notifications though various communication channels including short message peer-to-peer, short-message services and simple mail transfer protocol emails.

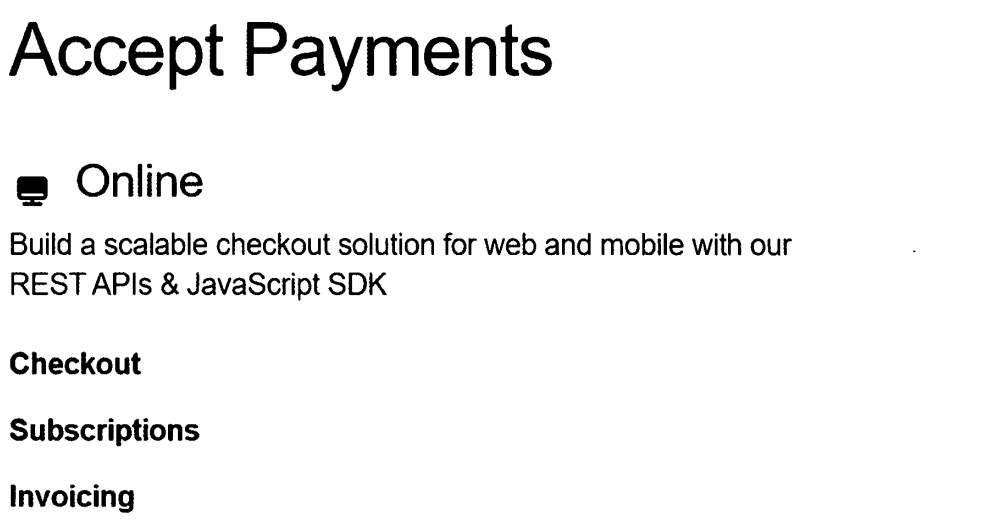
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 164 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
simple mail transfer protocol emails;	 *See* Screenshots of PayPal Mobile app (above) showing ability to receive messages. Upon information and belief, the PayPal System provides REST APIs for new integrations. These APIs use HTTP methods, a RESTful endpoint structure, the OAuth 2.0 protocol, and JSON-formatted payloads. The REST APIs can be used to incorporate the PayPal System's functionality into a user's web and mobile apps. Standard PayPal APIs can be accessed via the PayPal Developer Portal (*see* http://developer.paypal.com (last accessed on February 25, 2022)).

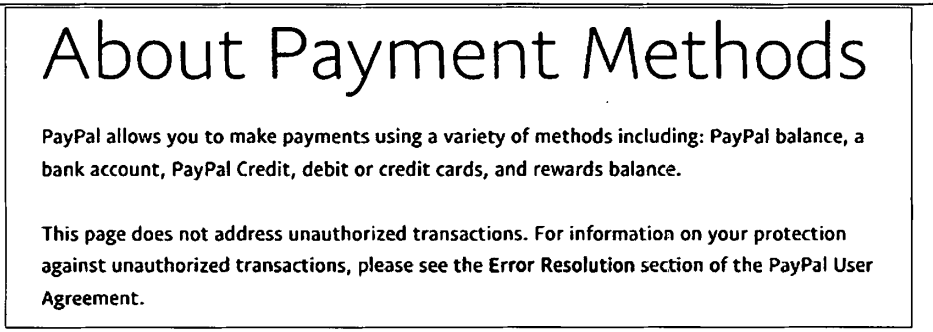
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 165 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	
1[c] business process services operable to implement business workflows, including at least one of executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects;	Upon information and belief, the PayPal system includes business process services which include at least executing financial transactions as well as other business services.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 166 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

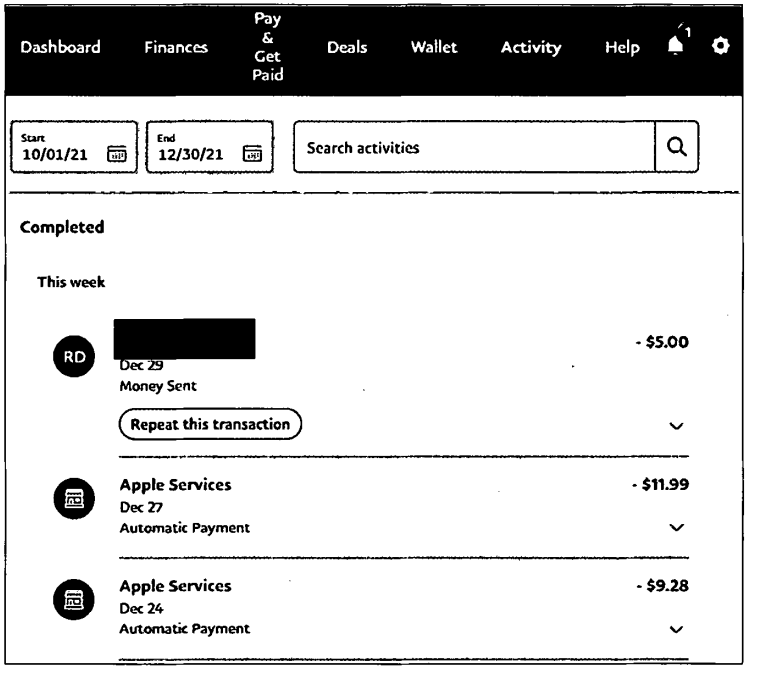
U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022).

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	Why are limitations placed on an account? There can be several reasons for an account limitation: • *An unauthorized person may be using your account.* If PayPal believes someone is using your account without your knowledge, the account could be limited to protect you from fraudulent charges while PayPal investigates the suspicious transactions. Similar steps may be taken if your debit or credit card issuer or bank notifies PayPal that someone has used your card or bank account without permission. • *The account is out of compliance with regulatory requirements.* Limitations can also be placed on an account that has been found to be out of compliance with regulatory requirements. For example, if you receive donations, you're required to provide documents confirming you're a registered nonprofit organization. PayPal may limit your account while you gather those documents or while we're working with you to satisfy any other regulatory requirements. The same is true if you don't follow PayPal's **Acceptable Use Policy**—selling banned items, such as prescription drugs or guns, for example. • *Your account has a high number of claims and chargebacks.* When there's a high number of **buyer claims and chargebacks** to your account, we may review your account. While we're reviewing, you may experience an account limitation. • *Sudden, rapid changes in what or how much you sell.* If you start to sell an entirely new type of product, specifically higher-end items like jewelry; or there's a rapid increase in sales volume, your account may be limited while PayPal reviews it. *See* https://www.paypal.com/us/brc/article/understanding-account-limitations (last accessed on February 25, 2022).
1[d] database services operable to store financial transaction details, store	Upon information and belief, the PayPal System includes database servers that store financial transaction details, store customer profiles and manage money containers. For example, financial transactions are stored and can be accessed via the Paypal website and the

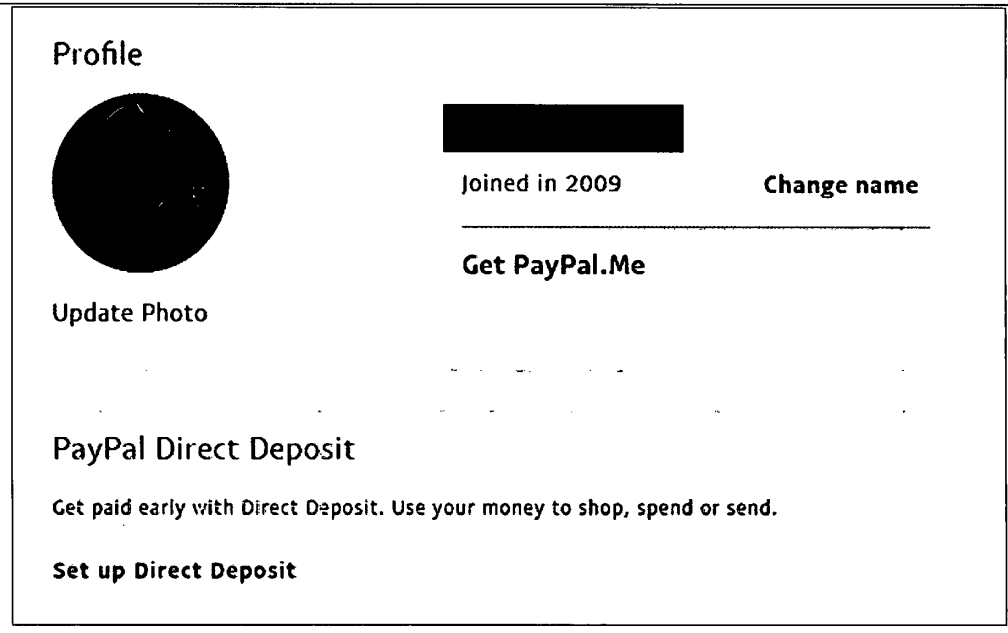
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 168 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
customer profiles, and manage money containers;	user Login. The user profile and money containers can also be accessed. 

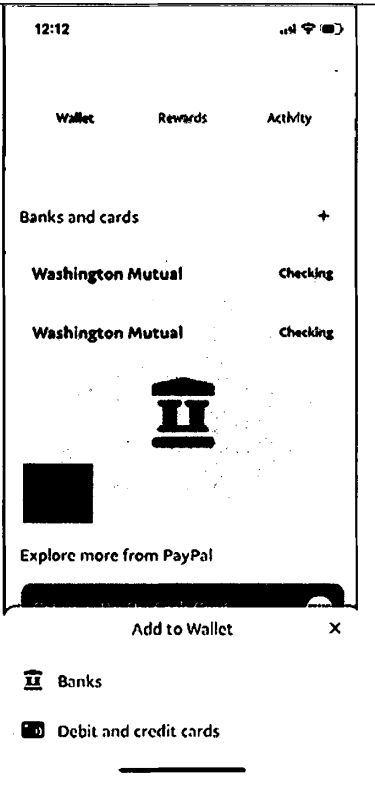
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 169 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* Screenshots of PayPay website accessing stored information. Upon information and belief, the PayPal System allows a user to make payments using a variety of methods including: PayPal balance, a bank account, PayPal Credit, debit or credit cards, and rewards balance.
1[e] a payment handler service operable to use APIs of different payment	Upon information and belief, the PayPal System, includes a payment handler which can interface with APIs of payment processors for banks, credit card, debit card, and bill payment processors.

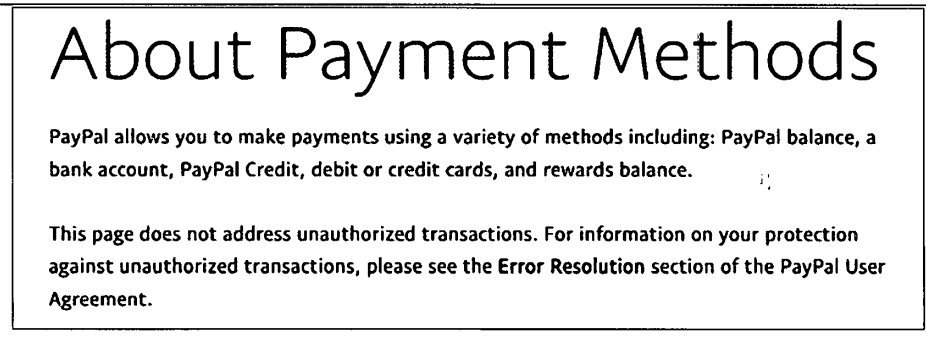
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 170 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
processors including one or more APIs of banks, credit and debit cards processors, bill payment processors;	 *See* Screenshot of PayPal Mobile Application identifying bank account with option to add credit and debit cards.

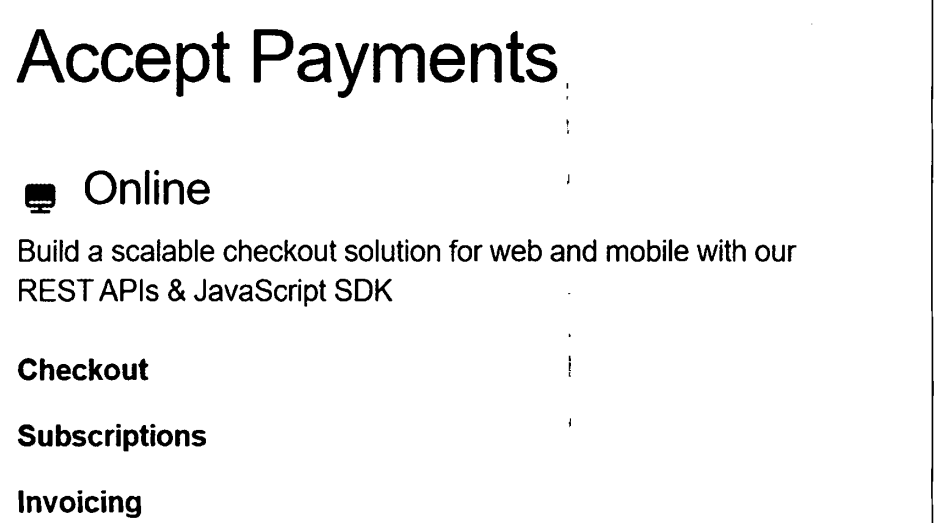
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 171 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022). Upon information and belief, the PayPal System provides REST APIs for new integrations. These APIs use HTTP methods, a RESTful endpoint structure, the OAuth 2.0 protocol, and JSON-formatted payloads. The REST APIs can be used to incorporate the PayPal System's functionality into a user's web and mobile apps. Standard PayPal APIs can be accessed via the PayPal Developer Portal (*see* http://developer.paypal.com (last accessed on February 25, 2022)).

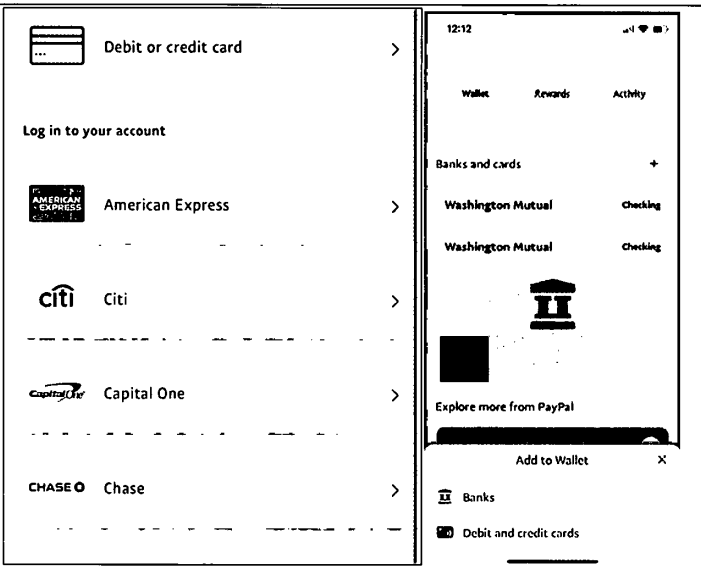
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 172 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	
1[f] and 1[g] a rules engine operable to gather financial transaction statistics and use the gathered financial transaction statistics to enforce constraints including transaction constraints; a security service operable to perform subscriber authentication;	Upon information and belief, the PayPal System, includes a rule engine that track financial transactions and enforce constraints including transaction constraints. Upon information and belief, the PayPal System also discloses a security service that authenticates a subscriber.

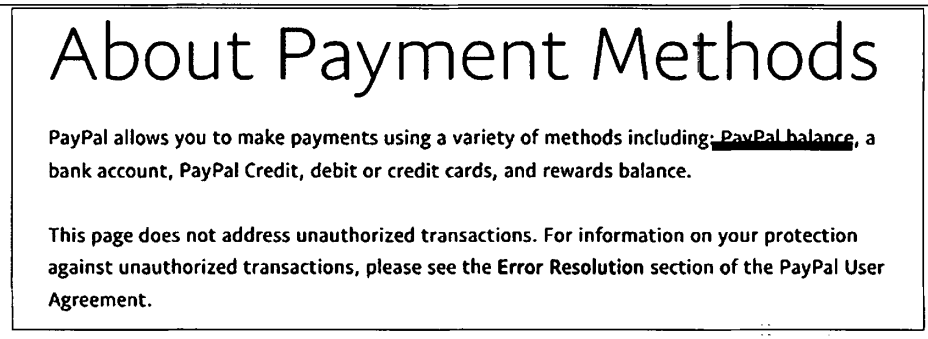
U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	Why are limitations placed on an account? There can be several reasons for an account limitation: • *An unauthorized person may be using your account.* If PayPal believes someone is using your account without your knowledge, the account could be limited to protect you from fraudulent charges while PayPal investigates the suspicious transactions. Similar steps may be taken if your debit or credit card issuer or bank notifies PayPal that someone has used your card or bank account without permission. • *The account is out of compliance with regulatory requirements.* Limitations can also be placed on an account that has been found to be out of compliance with regulatory requirements. For example, if you receive donations, you're required to provide documents confirming you're a registered nonprofit organization. PayPal may limit your account while you gather those documents or while we're working with you to satisfy any other regulatory requirements. The same is true if you don't follow PayPal's **Acceptable Use Policy**—selling banned items, such as prescription drugs or guns, for example. • *Your account has a high number of claims and chargebacks.* When there's a high number of **buyer claims and chargebacks** to your account, we may review your account. While we're reviewing, you may experience an account limitation. • *Sudden, rapid changes in what or how much you sell.* If you start to sell an entirely new type of product, specifically higher-end items like jewelry; or there's a rapid increase in sales volume, your account may be limited while PayPal reviews it. *See* https://www.paypal.com/us/brc/article/understanding-account-limitations (last accessed on February 25, 2022).
1[g] at least one entity that is to be involved in the specified transaction, the at least one entity having a profile with the monetary transaction system: wherein the at least one entity is the agent; wherein the monetary transaction system is implemented to deposit	Upon information and belief, the PayPal System allows a user to deposit funds as part of a transaction into an agent branch, including for example, Chase Bank account that is linked to the PayPal account.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
funds at an agent branch, the funds being deposited by a subscriber at the agent branch using a mobile device configured to run a monetary transaction system application, the monetary transaction system performing the following steps:	 *See* Screenshot of PayPal Mobile Application allowing users to link bank accounts to the PayPal System and showing an active legacy Washington Mutual account.

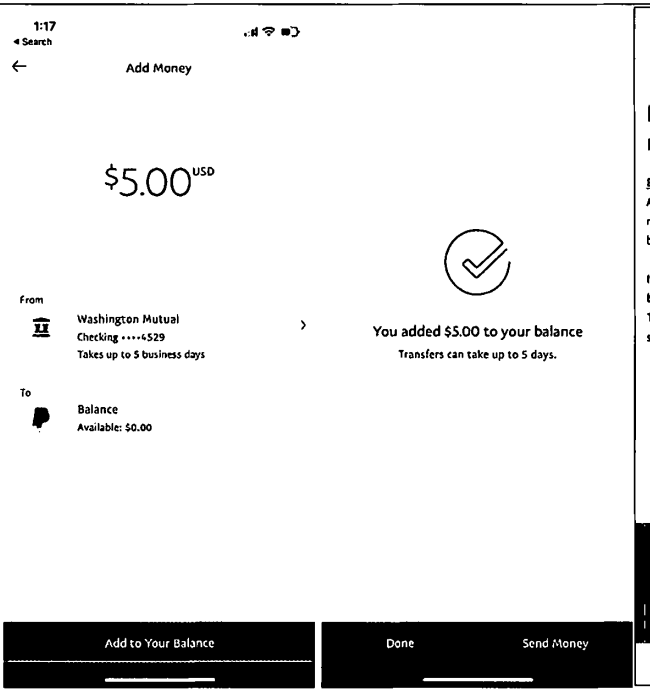
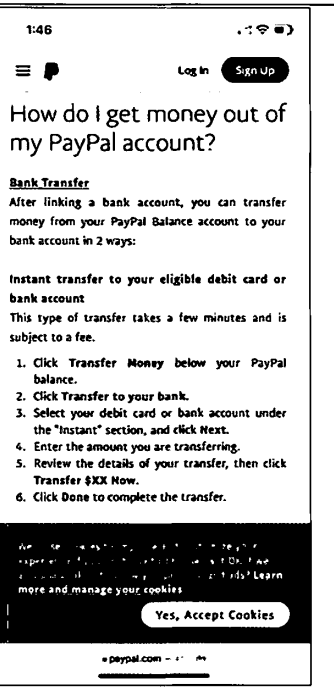
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 175 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

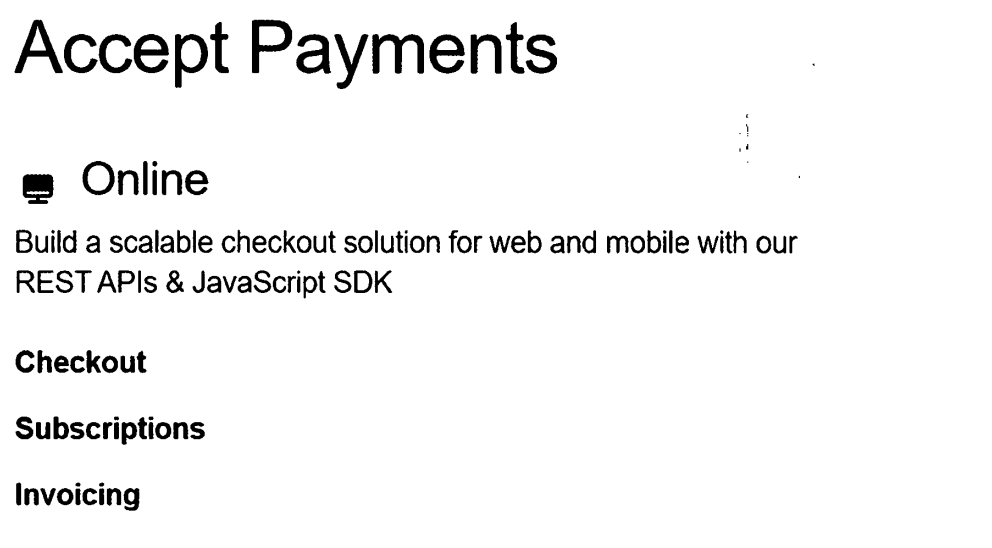
U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022).
receiving a communication message from the mobile device over one of a plurality of channels connected to the monetary transaction system, the communication message being received by an API associated with the integration tier of the monetary transaction system, the communication message indicating that the subscriber desires to deposit a specified amount of funds into the subscriber's account; validating the status of the subscriber's account, wherein	Upon information and belief, the PayPal System meets the following limitations and is capable of facilitating a deposit of funds to and from a PayPal account linked to a bank, for example chase Bank. Discovery and review of PayPal internal documents are needed for this limitation.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 176 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
validating the status of the subscriber's account comprises communicating from the integration tier to the database services to query attributes of the subscriber's account; committing a pending transaction through the business process services, wherein the integration tier communicates a transaction commitment request to the business process services; receiving a confirmation from the business process services that the pending transaction has been committed; sending, through the notification services, a receipt notification to the mobile device; and upon receiving a confirmation of commitment from the business process services, committing the pending transaction to the database services; and	  Upon information and belief, the PayPal System provides REST APIs for new integrations. These APIs use HTTP methods, a RESTful endpoint structure, the OAuth 2.0 protocol, and JSON-formatted payloads. The REST APIs can be used to incorporate the PayPal System's functionality into a user's web and mobile apps. Standard PayPal APIs can be accessed via the PayPal Developer Portal (*see* http://developer.paypal.com (last accessed on February 25, 2022)).

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	
wherein committing the pending transaction further comprises the following steps as orchestrated by the business process services: ensuring, via the database services, that the subscriber has an active account; validating, through communication with the security services, one or more of a PIN number and an access control list;	Upon information and belief, the PayPal System, checks the status of the selected payment method. For example, the PayPal system checks to determine whether the payment method can be used.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 178 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
applying with the rules engine, velocity rules; creating with the database services a new pending transaction history record; holding funds from the agent account balance using the payment handler, loading the funds to the subscriber account using the payment handler; and updating, using the database services, a pending transaction history record to reflect the funds.	How do I send a payment using my PayPal balance? Payments are automatically made using your PayPal balance first if the currency of your payment is the same as the one of your balance. To send a payment: 1. Click **Send and Request** at the top of the page. 2. Click **Pay for goods or services**. 3. Enter the recipient's email address, and click **Next**. 4. Enter the amount you want to send, and click **Continue**. 5. Review your payment information, and click **Send Payment Now**. *See* https://www.paypal.com/bs/smarthelp/article/how-do-i-send-a-payment-using-my-paypal-balance-faq1844 (last accessed on February 25, 2022). Upon information and belief, the PayPal System also performs a limit check to determine if there are sufficient available funds in the balance account to complete a transaction. Upon information and belief, the PayPal system also performs velocity check, including to identify fraud, to address regulatory requirements, or filter for transaction issues. Upon information and belief, the PayPal System includes velocity checks. These checks for example, monitor the number of transactions the user receive by minute, hour, etc. and the IP addresses of the user's customers. PayPal's Fraud Protection Services in the PayPal System include velocity checks along with many other filters to help assist in preventing fraud.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 179 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	Account number velocity filter The account number velocity filter is triggered for excessive use of a card within a short period of time. What does the filter do? The account number velocity filter triggers when any credit card account number is used five times within a three-day (72-hour) period. *See e.g.* https://developer.paypal.com/api/nvp-soap/payflow/fraud-protection/ (showing velocity functionality) (last accessed on February 25, 2022). Upon information and belief, the PayPal system includes functionality to further determine that the mobile wallet application is a valid account and is associated with the correct user.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 180 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	Existing Payflow parameters used by the filters The following existing Payflow parameters (described in the Payflow Gateway Develcper's Guide and Reference) are also used by the filters (if they are provided in the transaction request or response): User Authentication • PARTNER • VENDOR • USER • PWD Transaction Information • TRXTYPE • TENDER • ACCT • EXPDATE *See e.g.* https://developer.paypal.com/api/nvp-soap/payflow/fraud-protection/ (showing validating functionality) (last accessed on February 25, 2022).

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 181 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	Why are limitations placed on an account? There can be several reasons for an account limitation: • *An unauthorized person may be using your account.* If PayPal believes someone is using your account without your knowledge, the account could be limited to protect you from fraudulent charges while PayPal investigates the suspicious transactions. Similar steps may be taken if your debit or credit card issuer or bank notifies PayPal that someone has used your card or bank account without permission. • *The account is out of compliance with regulatory requirements.* Limitations can also be placed on an account that has been found to be out of compliance with regulatory requirements. For example, if you receive donations, you're required to provide documents confirming you're a registered nonprofit organization. PayPal may limit your account while you gather those documents or while we're working with you to satisfy any other regulatory requirements. The same is true if you don't follow PayPal's **Acceptable Use Policy**—selling banned items, such as prescription drugs or guns, for example. • *Your account has a high number of claims and chargebacks.* When there's a high number of **buyer claims and chargebacks** to your account, we may review your account. While we're reviewing, you may experience an account limitation. • *Sudden, rapid changes in what or how much you sell.* If you start to sell an entirely new type of product, specifically higher-end items like jewelry; or there's a rapid increase in sales volume, your account may be limited while PayPal reviews it. *See* https://www.paypal.com/us/brc/article/understanding-account-limitations (last accessed on February 25, 2022). Upon information and belief, the PayPal System utilizes a PayPal Security Key, which is an additional layer of security at login. In addition to the user's password, the user can enter a One-Time PIN (OTP) that's unique for each login attempt.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 182 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,892,386 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 **PayPal Security Key** This is your free additional layer of security at login. In addition to your password, you'll enter a One-Time PIN (OTP) that's unique for each login attempt. Register your mobile phone to use PayPal Security Key Upon information and belief, the PayPal System includes an access-control list (ACL) such as a list of permissions associated with system resources. A user can manually grant the PayPal System permissions to a third party to access specific information in the user's account at the PayPal system and perform PayPal API operations on the user's behalf. For example, if the user is integrating with a third-party shopping cart, the cart owner needs permission to the user's PayPal account to perform specific operations on behalf of the user. Upon information and belief, by way of example, the PayPal systems utilizes OAuth 2.0 protocol to provide authenticated and/or authorized access to various protected resources. In particular, OAuth 2.0 scopes are used to specify or limit the type of access (i.e., ACL) that is associated with a granted access token. *See* https://oauth.net/2/scope/ (last accessed on February 25, 2022); https://developer.paypal.com/api/rest/ (last accessed on February 25, 2022).

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 183 of 381

Exhibit E
U.S. Patent No. 11,120,413

US011120413B2

(12) **United States Patent**
Liberty et al.

(10) **Patent No.: US 11,120,413 B2**
(45) **Date of Patent: *Sep. 14, 2021**

(54) **MONETARY TRANSACTION SYSTEM**

(71) Applicant: **Fintiv, Inc.**, Austin, TX (US)

(72) Inventors: **Michael A. Liberty**, Orlando, FL (US); **Felipe Fernandes**, Austin, TX (US)

(73) Assignee: **Fintiv, Inc.**, Austin, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/569,348**

(22) Filed: **Sep. 12, 2019**

(65) **Prior Publication Data**

US 2020/0005257 A1 Jan. 2, 2020

Related U.S. Application Data

(63) Continuation of application No. 15/809,872, filed on Nov. 10, 2017, which is a continuation of application
(Continued)

(51) **Int. Cl.**
G06Q 20/00 (2012.01)
G06Q 20/10 (2012.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G06Q 20/10*** (2013.01); ***G06Q 20/0855*** (2013.01); ***G06Q 20/322*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC G06Q 20/10
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,221,838 A 6/1993 Gutman et al.
5,717,374 A 2/1998 Smith
(Continued)

FOREIGN PATENT DOCUMENTS

AU 2007312879 A1 4/2008
CA 2666616 4/2008
(Continued)

OTHER PUBLICATIONS

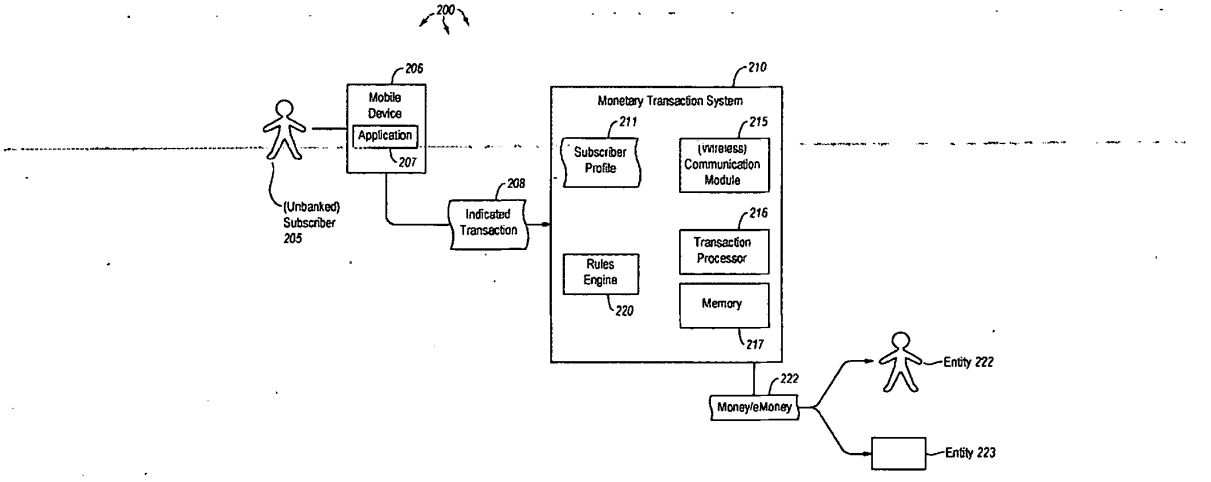
Final Office Action received for U.S. Appl. No. 13/644,312, dated May 20, 2015.
(Continued)

Primary Examiner — Edward Chang
(74) *Attorney, Agent, or Firm* — Workman Nydegger

(57) **ABSTRACT**

Embodiments are directed to monetary transaction system for conducting monetary transactions between transaction system subscribers and other entities. In one scenario, the monetary transaction system includes a mobile device that runs a monetary transaction system application. The monetary transaction system also includes a subscriber that has a profile with the system. The subscriber indicates a transaction that is to be performed with the monetary transaction system. The system further includes a monetary transaction system processor that performs the transactions specified by the subscriber including communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile. The monetary transaction system also includes at least one entity that is to be involved in the specified transaction, where the entity has a profile with the monetary transaction system. This entity may be a person, a retail store, an agent or other entity.

7 Claims, 46 Drawing Sheets



Related U.S. Application Data

No. 15/201,152, filed on Jul. 1, 2016, now Pat. No. 9,892,386, which is a continuation of application No. 14/213,543, filed on Mar. 14, 2014, now abandoned, which is a continuation of application No. 13/964,707, filed on Aug. 12, 2013, now abandoned, which is a continuation of application No. 13/484,199, filed on May 30, 2012, now Pat. No. 8,538,845.

(60) Provisional application No. 61/522,099, filed on Aug. 10, 2011, provisional application No. 61/493,064, filed on Jun. 3, 2011.

(51) **Int. Cl.**

G06Q 20/08	(2012.01)
G06Q 40/02	(2012.01)
G06Q 20/40	(2012.01)
G06Q 20/32	(2012.01)
G06Q 20/36	(2012.01)
H04L 29/06	(2006.01)

(52) **U.S. Cl.**

CPC ***G06Q 20/3255*** (2013.01); ***G06Q 20/36*** (2013.01); ***G06Q 20/405*** (2013.01); ***G06Q 40/02*** (2013.01); ***H04L 63/101*** (2013.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,828,739	A	10/1998	Nakanishi	
5,991,749	A	11/1999	Morrill	
6,021,397	A	2/2000	Jones et al.	
6,175,823	B1	1/2001	Van Dusen	
6,185,545	B1	2/2001	Resnick	
6,199,762	B1	3/2001	Hohle	
6,250,557	B1	6/2001	Forslund	
6,256,614	B1	7/2001	Wecker et al.	
6,356,908	B1	3/2002	Brown et al.	
6,415,156	B1	7/2002	Stadelmann	
6,480,957	B1	11/2002	Liao et al.	
6,487,403	B2	11/2002	Carroll	
6,622,015	B1	9/2003	Himmel	
6,697,839	B2	2/2004	Sini	
6,714,797	B1	3/2004	Rautila	
6,732,179	B1	5/2004	Brown et al.	
6,736,322	B2	5/2004	Gobburu	
6,819,219	B1	11/2004	Bolle	
6,840,448	B2	1/2005	Fukushima	
6,862,575	B1	3/2005	Antilla et al.	
6,873,974	B1	3/2005	Schutzer	
6,950,939	B2	9/2005	Tobin	
6,957,342	B2	10/2005	Vatanen	
7,016,532	B2	3/2006	Boncyk	
7,024,174	B2 *	4/2006	Nagy	G06Q 20/04 455/408
7,024,390	B1	4/2006	Mori et al.	
7,054,430	B2	5/2006	Lynam	
7,065,341	B2	6/2006	Kamiyama et al.	
7,069,001	B2	6/2006	Rupp	
7,089,208	B1	8/2006	Levchin	
7,099,850	B1	8/2006	Mann	
7,100,821	B2	9/2006	Rasti	
7,107,247	B2	9/2006	Kinoshita	
7,110,972	B1	9/2006	Handa	
7,146,159	B1	12/2006	Zhu	
7,149,545	B2	12/2006	Hurst et al.	
7,155,411	B1	12/2006	Blinn et al.	
7,197,297	B2	3/2007	Myles et al.	
7,221,939	B2	5/2007	Ylitalo	
7,233,785	B2	6/2007	Yamagishi et al.	
7,233,926	B2	6/2007	Durand et al.	
7,236,742	B2	6/2007	Hall et al.	
7,240,836	B2	7/2007	Vrotsos	
7,248,855	B2	7/2007	Joyce	
7,255,264	B2	8/2007	De Leon	
7,275,685	B2	10/2007	Gray	
7,286,818	B2	10/2007	Rosenberg	
7,322,043	B2	1/2008	Letsinger	
7,325,132	B2	1/2008	Takayama	
7,334,720	B2	2/2008	Hulst et al.	
7,347,361	B2	3/2008	Lovett	
7,349,871	B2	3/2008	Labrou	
7,353,382	B2	4/2008	Labrou	
7,363,261	B2	4/2008	Whitehead	
7,370,017	B1	5/2008	Lindeman	
7,389,123	B2	6/2008	Rydgren et al.	
7,403,652	B2	7/2008	Boncyk	
7,415,721	B2	8/2008	Fransdonk	
7,421,410	B1	9/2008	Schechtman et al.	
7,447,494	B2	11/2008	Law et al.	
7,454,233	B2	11/2008	Lu et al.	
7,461,010	B2	12/2008	Kwan	
7,461,028	B2	12/2008	Wronski	
7,469,151	B2	12/2008	Khan et al.	
7,477,780	B2	1/2009	Boncyk	
7,490,775	B2	2/2009	Biderman	
7,494,055	B2	2/2009	Fernandes	
7,512,098	B2	3/2009	Jiang	
7,527,194	B2	5/2009	Truitt	
7,527,208	B2	5/2009	Hammad et al.	
7,548,915	B2	6/2009	Ramer	
7,562,818	B1	7/2009	Bierbaum	
7,564,469	B2	7/2009	Boncyk	
7,565,008	B2	7/2009	Boncyk	
7,606,560	B2	10/2009	Labrou	
7,628,322	B2	12/2009	Holtmanns et al.	
7,657,489	B2	2/2010	Stambaugh	
7,677,973	B2	3/2010	Van Luchene	
7,680,324	B2	3/2010	Boncyk	
7,689,205	B2	3/2010	Toy et al.	
7,689,506	B2	3/2010	Fei et al.	
7,689,508	B2	3/2010	Davis et al.	
7,694,876	B2	4/2010	Barnes et al.	
7,699,218	B2	4/2010	Garcia	
7,707,113	B1	4/2010	DiMartino et al.	
7,708,194	B2	5/2010	Vawter	
7,711,392	B2	5/2010	Brown et al.	
7,729,963	B1	6/2010	Lego	
7,729,987	B1	6/2010	Wakim	
7,748,618	B2	7/2010	Vawter	
7,774,076	B2	8/2010	Skowronek	
7,774,231	B2	8/2010	Pond	
7,775,437	B2	8/2010	Boncyk	
7,784,684	B2	8/2010	Labrou	
7,801,826	B2	9/2010	Labrou	
7,819,307	B2	10/2010	Lyons	
7,822,439	B2	10/2010	Teicher	
7,822,688	B2	10/2010	Labrou	
7,823,772	B2	11/2010	Vawter	
7,848,500	B2	12/2010	Lynam	
7,848,504	B2	12/2010	Lynam	
7,865,414	B2	1/2011	Fung	
7,865,431	B2	1/2011	Takayama	
7,877,605	B2	1/2011	Labrou	
7,881,529	B2	2/2011	Boncyk	
7,886,962	B2	2/2011	Vawter	
7,890,424	B1	2/2011	Wakim	
7,899,243	B2	3/2011	Boncyk	
7,899,252	B2	3/2011	Boncyk	
7,937,302	B1	5/2011	Lego	
7,937,305	B1	5/2011	Lego	
7,942,317	B2	5/2011	Racz et al.	
7,958,052	B2	6/2011	Powell	
7,967,196	B1	6/2011	Bierbaum	
7,979,026	B2	7/2011	Hulvey	
7,988,060	B2	8/2011	Killian	
8,016,185	B2	9/2011	Modi	
8,019,365	B2	9/2011	Fisher	
8,033,458	B2	10/2011	Hulst et al.	
8,041,338	B2	10/2011	Chen	
8,052,042	B2	11/2011	Kolinski-Schultz	
8,060,012	B2	11/2011	Sklovsky	
8,061,598	B2	11/2011	Racz et al.	

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,073,783 B2 12/2011 Felsted
8,077,042 B2 12/2011 Peeters
8,090,945 B2 1/2012 Singhal
8,095,113 B2 1/2012 Kean
8,116,734 B2 2/2012 Vawter
8,116,773 B2 2/2012 Chitrapu
8,118,221 B2 2/2012 Racz et al.
8,121,945 B2 2/2012 Rackley
8,130,242 B2 3/2012 Boncyk
8,145,568 B2 3/2012 Rackley
8,160,959 B2 4/2012 Rackley
8,170,485 B2 5/2012 Hulvey
8,190,087 B2 5/2012 Fisher
8,195,576 B1 6/2012 Grigg
8,196,131 B1 6/2012 von Behren
8,213,470 B2 7/2012 Gu
8,218,873 B2 7/2012 Boncyk
8,229,354 B2 7/2012 Sklovsky
8,239,325 B2 8/2012 Schwarz
8,275,312 B2 9/2012 Fisher
8,290,433 B2 10/2012 Fisher
8,332,272 B2 12/2012 Fisher
8,333,319 B2 12/2012 Roth
8,336,772 B2 12/2012 Racz et al.
8,352,323 B2 1/2013 Fisher
8,355,670 B2 1/2013 White
8,359,265 B2 1/2013 Van Rensburg
8,360,329 B2 1/2013 Grigg
8,374,916 B2 2/2013 White
8,380,177 B2 2/2013 Laracey
8,396,793 B2 3/2013 Hill
8,487,771 B2 7/2013 Hsieh et al.
8,538,845 B2 9/2013 Liberty
8,577,803 B2 11/2013 Chatterjee et al.
8,612,325 B2 11/2013 Laracey
8,632,000 B2 1/2014 Laracey
8,843,125 B2 9/2014 Kwon et al.
9,208,488 B2 12/2015 Liberty
9,892,386 B2 2/2018 Liberty
10,438,196 B2 10/2019 Liberty
2001/0011248 A1 8/2001 Himmel
2001/0037264 A1 11/2001 Husemann
2001/0042785 A1 11/2001 Walker et al.
2002/0042776 A1 4/2002 Woo
2002/0052754 A1 5/2002 Joyce
2002/0060246 A1 5/2002 Gobburu
2002/0065774 A1 5/2002 Young
2002/0069123 A1 6/2002 Soderlind
2002/0131404 A1 9/2002 Mehta
2002/0141586 A1 10/2002 Margalit
2002/0152177 A1 10/2002 Wolf
2002/0161708 A1 10/2002 Offei
2003/0001010 A1 1/2003 Schmidt
2003/0026404 A1 2/2003 Joyce
2003/0055735 A1 3/2003 Cameron
2003/0071115 A1 4/2003 Horn
2003/0154165 A1 8/2003 Horn
2003/0195842 A1 10/2003 Reece
2004/0117302 A1 6/2004 Weichert et al.
2004/0181531 A1 9/2004 Becker
2004/0205618 A1 10/2004 Sini
2004/0215491 A1 10/2004 Clark et al.
2004/0235450 A1 11/2004 Rosenberg
2004/0248554 A1 12/2004 Khan
2005/0070265 A1 3/2005 Korpinen
2005/0071512 A1 3/2005 Kim et al.
2005/0080697 A1 4/2005 Foss
2005/0187873 A1 8/2005 Labrou et al.
2005/0199709 A1 9/2005 Linior
2005/0222961 A1 10/2005 Staib
2005/0283434 A1 12/2005 Hahn-Carlson
2006/0116892 A1 6/2006 Grimes
2006/0136901 A1 6/2006 Nichols
2006/0165060 A1 7/2006 Dua
2006/0179452 A1 8/2006 Amodeo
2006/0200427 A1 9/2006 Morrison
2006/0253335 A1 11/2006 Keena et al.
2006/0287004 A1 12/2006 Fuqua
2007/0006327 A1 1/2007 Lal et al.
2007/0033285 A1 2/2007 Shiigi
2007/0088852 A1 4/2007 Levkovitz
2007/0106564 A1 5/2007 Matotek
2007/0123305 A1 5/2007 Chen
2007/0125838 A1 6/2007 Law
2007/0125840 A1 6/2007 Law
2007/0162471 A1 7/2007 Samuelsson
2007/0179885 A1 8/2007 Bird
2007/0198432 A1 8/2007 Pitroda
2007/0203850 A1 8/2007 Singh
2007/0241189 A1 10/2007 Slavin
2007/0244811 A1 10/2007 Tumminaro
2007/0255620 A1 11/2007 Tumminaro et al.
2007/0255652 A1 11/2007 Tumminaro et al.
2007/0255653 A1 11/2007 Tumminaro
2007/0265984 A1 11/2007 Santhana
2008/0005018 A1 1/2008 Powell
2008/0006685 A1 1/2008 Rackley
2008/0010191 A1 1/2008 Rackley
2008/0010196 A1 1/2008 Rackley
2008/0010204 A1 1/2008 Rackley
2008/0010215 A1 1/2008 Rackley
2008/0011825 A1 1/2008 Giordano
2008/0017704 A1 1/2008 VanDeburg
2008/0040265 A1 2/2008 Rackley
2008/0040285 A1 2/2008 Wankmueller
2008/0052192 A1 2/2008 Fisher
2008/0065490 A1 3/2008 Novick et al.
2008/0097851 A1 4/2008 Bemmel
2008/0126145 A1 5/2008 Rackley
2008/0126929 A1 5/2008 Bykov
2008/0143487 A1 6/2008 Hulvey
2008/0197190 A1 8/2008 Fujita
2008/0204358 A1 8/2008 Sato
2008/0208741 A1 8/2008 Arthur et al.
2008/0208742 A1 8/2008 Arthur et al.
2008/0208743 A1 8/2008 Arthur
2008/0208744 A1 8/2008 Arthur
2008/0208762 A1 8/2008 Arthur
2008/0210751 A1 9/2008 Kim
2008/0249927 A1 10/2008 Rethorn
2008/0249928 A1 10/2008 Hill
2008/0249930 A1 10/2008 Hill
2008/0249933 A1 10/2008 Rethorn
2008/0255947 A1 10/2008 Friedman
2008/0275779 A1 11/2008 Lakshminarayanan
2008/0281737 A1 11/2008 Fajardo
2009/0024526 A1 1/2009 Erickson
2009/0037326 A1 2/2009 Chitti
2009/0055322 A1 2/2009 Bykov
2009/0063312 A1 3/2009 Hurst
2009/0081989 A1 3/2009 Wuhrer
2009/0098854 A1 4/2009 Park
2009/0104888 A1 4/2009 Cox
2009/0106132 A1 4/2009 Isturiz
2009/0106148 A1 4/2009 Prada
2009/0108015 A1 4/2009 Kreamer
2009/0119190 A1 5/2009 Realini
2009/0124234 A1 5/2009 Fisher et al.
2009/0132362 A1 5/2009 Fisher
2009/0132392 A1 5/2009 Davis
2009/0138366 A1 5/2009 Bemmel
2009/0144161 A1 6/2009 Fisher
2009/0156190 A1 6/2009 Fisher
2009/0157546 A1 6/2009 Garcia
2009/0177578 A1 7/2009 Garcia
2009/0177581 A1 7/2009 Garcia
2009/0210308 A1 8/2009 Toomer
2009/0222353 A1 9/2009 Guest
2009/0222358 A1 9/2009 Bednarek
2009/0234751 A1 9/2009 Chan et al.
2009/0248537 A1 10/2009 Sarkeshik
2009/0254440 A1 10/2009 Pharris
2009/0254479 A1 10/2009 Pharris
2009/0265272 A1 10/2009 Dill et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2009/0281904 A1 11/2009 Pharris
2009/0288012 A1 11/2009 Hertel
2009/0299844 A1 12/2009 Reilly
2009/0307132 A1 12/2009 Phillips
2009/0307139 A1 12/2009 Mardikar et al.
2009/0307140 A1 12/2009 Mardikar
2010/0010964 A1 1/2010 Skowronek
2010/0023449 A1 1/2010 Skowronek
2010/0030651 A1 2/2010 Matotek et al.
2010/0044430 A1 2/2010 Song
2010/0048226 A1 2/2010 Owen
2010/0049599 A1 2/2010 Owen
2010/0051685 A1 3/2010 Royyuru
2010/0057614 A1 3/2010 Raincy
2010/0057619 A1 3/2010 Weller
2010/0057624 A1 3/2010 Hurt
2010/0063895 A1 3/2010 Dominguez
2010/0088188 A1 4/2010 Kumar
2010/0114739 A1 5/2010 Johnston
2010/0125495 A1 5/2010 Smith
2010/0125508 A1 5/2010 Smith
2010/0125510 A1 5/2010 Smith
2010/0138518 A1 6/2010 Aiglstorfer et al.
2010/0145835 A1 6/2010 Davis et al.
2010/0146607 A1 6/2010 Piepenbrink et al.
2010/0151790 A1 6/2010 Hoeksel et al.
2010/0197326 A1 8/2010 Ngo
2010/0205432 A1 8/2010 Corda et al.
2010/0211507 A1 8/2010 Aabye et al.
2010/0223110 A1 9/2010 Slavin
2010/0235283 A1 9/2010 Gerson
2010/0248710 A1 9/2010 Sklovsky
2010/0250356 A1 9/2010 Gillenson
2010/0250436 A1 9/2010 Loevenguth
2010/0260388 A1 10/2010 Garrett
2010/0275242 A1 10/2010 Raffard et al.
2010/0275269 A1 10/2010 Vilmos et al.
2010/0285821 A1 11/2010 Smeeding et al.
2010/0291904 A1 11/2010 Musfeldt et al.
2010/0306107 A1 12/2010 Nahari
2010/0330958 A1 12/2010 Corda et al.
2010/0333129 A1 12/2010 Alhadeff et al.
2011/0047016 A1 2/2011 Cook
2011/0057025 A1 3/2011 Denzer
2011/0078081 A1 3/2011 Pirzadeh et al.
2011/0087529 A1 4/2011 Angell
2011/0087610 A1 4/2011 Batada
2011/0105022 A1 5/2011 Vawter
2011/0113473 A1 5/2011 Corda
2011/0131421 A1 6/2011 Jogand-Coulomb et al.
2011/0145049 A1 6/2011 Hertel
2011/0145149 A1 6/2011 Valdes
2011/0179113 A1 7/2011 Thomas
2011/0196788 A1 8/2011 Lu et al.
2011/0218911 A1 9/2011 Spodak
2011/0246284 A1 10/2011 Chaikin
2011/0250866 A1 10/2011 Fisher
2011/0251941 A1 10/2011 Dunwoody
2011/0258024 A1 10/2011 Prince
2011/0258115 A1 10/2011 Mulhim
2011/0270744 A1 11/2011 Baker
2011/0276417 A1 11/2011 Campbell
2011/0295750 A1 12/2011 Rammal
2011/0302016 A1 12/2011 Haddad
2011/0302406 A1 12/2011 Machani
2011/0313924 A1 12/2011 Carell
2011/0320243 A1 12/2011 Khan
2011/0320293 A1 12/2011 Khan
2011/0320294 A1 12/2011 Votaw
2011/0320345 A1 12/2011 Taveau
2012/0005076 A1 1/2012 Dessert
2012/0011058 A1 1/2012 Pitroda et al.
2012/0011063 A1 1/2012 Killian
2012/0028612 A1 2/2012 Hurst
2012/0029990 A1 2/2012 Fisher
2012/0047070 A1 2/2012 Pharris
2012/0074232 A1 3/2012 Spodak
2012/0078735 A1 3/2012 Bauer
2012/0079521 A1 3/2012 Garg et al.
2012/0084203 A1 4/2012 Mehew
2012/0095655 A1 4/2012 Hyodo et al.
2012/0095855 A1 4/2012 Sterling
2012/0095856 A1 4/2012 Sanjeev
2012/0122447 A1 5/2012 Craft
2012/0123641 A1 5/2012 Ferrin et al.
2012/0123841 A1 5/2012 Taveau
2012/0123868 A1 5/2012 Brudnicki
2012/0123880 A1 5/2012 Craft
2012/0123935 A1 5/2012 Brudnicki
2012/0123937 A1 5/2012 Spodak
2012/0131653 A1 5/2012 Pasquero
2012/0143752 A1 6/2012 Wong
2012/0150669 A1 6/2012 Langley
2012/0158589 A1 6/2012 Katzin
2012/0166311 A1 6/2012 Dwight
2012/0171992 A1 7/2012 Cheong
2012/0172026 A1 7/2012 Kwon
2012/0172089 A1 7/2012 Bae
2012/0174189 A1 7/2012 Lim
2012/0191557 A1 7/2012 Fisher
2012/0191612 A1 7/2012 Spodak
2012/0196586 A1 8/2012 Grigg
2012/0197691 A1 8/2012 Grigg
2012/0197740 A1 8/2012 Grigg
2012/0197743 A1 8/2012 Grigg
2012/0197745 A1 8/2012 Fisher
2012/0197787 A1 8/2012 Grigg
2012/0203610 A1 8/2012 Grigg et al.
2012/0203632 A1 8/2012 Blum
2012/0209688 A1 8/2012 Lamothe
2012/0209749 A1 8/2012 Hammad
2012/0215701 A1 8/2012 Mehta
2012/0221421 A1 8/2012 Hammad
2012/0221475 A1 8/2012 Grigg
2012/0226610 A1 9/2012 Gill
2012/0229647 A1 9/2012 Calman
2012/0229657 A1 9/2012 Calman
2012/0231424 A1 9/2012 Calman
2012/0231425 A1 9/2012 Calman
2012/0232937 A1 9/2012 Calman
2012/0232977 A1 9/2012 Calman
2012/0232983 A1 9/2012 Bertha
2012/0245986 A1 9/2012 Regan
2012/0253852 A1 10/2012 Pourfallah
2012/0259598 A1 10/2012 Jandhyala et al.
2012/0259686 A1 10/2012 Yurow
2012/0259698 A1 10/2012 Yurow
2012/0259732 A1 10/2012 Sasankan
2012/0265677 A1 10/2012 Rackley
2012/0265685 A1 10/2012 Brudnicki
2012/0271712 A1 10/2012 Katzin
2012/0284131 A1 11/2012 Soffer
2012/0286928 A1 11/2012 Mullen
2012/0290376 A1 11/2012 Dryer
2012/0290449 A1 11/2012 Mullen
2012/0290478 A1 11/2012 Crofts et al.
2012/0293303 A1 11/2012 Khan
2012/0296708 A1 11/2012 Bachmann
2012/0296720 A1 11/2012 Pirillo
2012/0296722 A1 11/2012 Gosavi
2012/0296741 A1 11/2012 Dykes
2012/0297204 A1 11/2012 Buer
2012/0302204 A1 11/2012 Gupta
2012/0303425 A1 11/2012 Katzin
2012/0310720 A1 12/2012 Balsan
2012/0310760 A1 12/2012 Phillips
2012/0310824 A1 12/2012 Liberty
2012/0310826 A1 12/2012 Chatterjee
2012/0316591 A1 12/2012 Thorne et al.
2012/0316950 A1 12/2012 LaPorte
2012/0316951 A1 12/2012 Fisher
2012/0316992 A1 12/2012 Oborne
2012/0317019 A1 12/2012 Carnes
2012/0323653 A1 12/2012 Fisher

(56) **References Cited**

U.S. PATENT DOCUMENTS

2012/0323664 A1 12/2012 Klems
2012/0323670 A1 12/2012 Fisher
2012/0323777 A1 12/2012 Liberty
2012/0329394 A1 12/2012 Fisher
2012/0330737 A1 12/2012 Liberty
2012/0330792 A1 12/2012 Kashanian
2013/0012125 A1 1/2013 Fisher
2013/0012126 A1 1/2013 Fisher
2013/0012131 A1 1/2013 Fisher
2013/0013352 A1 1/2013 Fisher
2013/0013353 A1 1/2013 Fisher
2013/0013355 A1 1/2013 Fisher
2013/0013432 A1 1/2013 Fisher
2013/0013434 A1 1/2013 Fisher
2013/0013490 A1 1/2013 Keller
2013/0013498 A1 1/2013 Fisher
2013/0013501 A1 1/2013 Rackley
2013/0017784 A1 1/2013 Fisher
2013/0018738 A1 1/2013 Faires
2013/0018740 A1 1/2013 Fisher
2013/0018742 A1 1/2013 Fisher
2013/0018793 A1 1/2013 Wong
2013/0023209 A1 1/2013 Fisher
2013/0023294 A1 1/2013 Singh
2013/0024220 A1 1/2013 Fisher
2013/0024221 A1 1/2013 Fisher
2013/0024223 A1 1/2013 Thomas
2013/0024280 A1 1/2013 Fisher
2013/0024364 A1 1/2013 Fisher
2013/0024371 A1 1/2013 Hariramani
2013/0024372 A1 1/2013 Spodak
2013/0024377 A1 1/2013 Stong
2013/0029646 A1 1/2013 Chowdhury
2013/0030828 A1 1/2013 Pourfallah
2013/0030960 A1 1/2013 Kashanian
2013/0030997 A1 1/2013 Spodak
2013/0035035 A1 2/2013 Fisher
2013/0035036 A1 2/2013 Fisher
2013/0035037 A1 2/2013 Fisher
2013/0035068 A1 2/2013 Fisher
2013/0035069 A1 2/2013 Fisher
2013/0035070 A1 2/2013 Fisher
2013/0035071 A1 2/2013 Fisher
2013/0035072 A1 2/2013 Fisher
2013/0035087 A1 2/2013 Fisher
2013/0035967 A1 2/2013 Fisher
2013/0035968 A1 2/2013 Fisher
2013/0035969 A1 2/2013 Fisher
2013/0035970 A1 2/2013 Fisher
2013/0040568 A1 2/2013 Fisher
2013/0040569 A1 2/2013 Fisher
2013/0041699 A1 2/2013 Fisher
2013/0041700 A1 2/2013 Fisher
2013/0041701 A1 2/2013 Roth
2013/0041736 A1 2/2013 Coppinger
2013/0041743 A1 2/2013 Coppinger
2013/0041744 A1 2/2013 Coppinger
2013/0041745 A1 2/2013 Coppinger
2013/0041769 A1 2/2013 Fisher
2013/0046608 A1 2/2013 Coppinger
2013/0046634 A1 2/2013 Grigg
2013/0046645 A1 2/2013 Grigg
2013/0048723 A1 2/2013 King
2013/0052952 A1 2/2013 Fisher
2013/0054336 A1 2/2013 Graylin
2013/0054337 A1 2/2013 Brendell
2013/0054412 A1 2/2013 Brendell
2013/0054441 A1 2/2013 Kamdar
2013/0057392 A1 3/2013 Bullock
2013/0060618 A1 3/2013 Barton
2013/0073373 A1 3/2013 Fisher
2013/0073377 A1 3/2013 Heath
2013/0073458 A1 3/2013 Sherwin
2013/0080228 A1 3/2013 Fisher
2013/0080229 A1 3/2013 Fisher
2013/0080230 A1 3/2013 Fisher
2013/0080231 A1 3/2013 Fisher
2013/0080232 A1 3/2013 Fisher
2013/0080233 A1 3/2013 Fisher
2013/0080240 A1 3/2013 Fisher
2013/0080241 A1 3/2013 Fisher
2013/0080329 A1 3/2013 Royyuru
2013/0091012 A1 4/2013 Liberty
2013/0246141 A1 4/2013 Liberty
2013/0132219 A1 5/2013 Liberty
2013/0238455 A1 9/2013 Laracey
2013/0246203 A1 9/2013 Laracey
2013/0013499 A1 10/2013 Kalgi
2013/0317928 A1 11/2013 Laracey
2013/0332347 A1 12/2013 Liberty
2013/0346309 A1 12/2013 Giori
2014/0006048 A1 1/2014 Liberty
2014/0014721 A1 1/2014 Lindeman
2014/0089185 A1 3/2014 Desai et al.
2014/0201070 A1 7/2014 Liberty
2015/0039517 A1 2/2015 Liberty
2015/0073891 A1 3/2015 Dauneria
2015/0100398 A1 4/2015 Narayanaswami et al.
2015/0310489 A1 10/2015 Hussain
2016/0055483 A1 2/2016 Liberty
2016/0055583 A1 2/2016 Liberty
2016/0078493 A1 3/2016 Liberty
2016/0314443 A1 10/2016 Liberty
2018/0130036 A1 5/2018 Liberty
2020/0074454 A1 3/2020 Liberty

FOREIGN PATENT DOCUMENTS

CN 101606400 12/2009
CN 102073958 5/2011
DE 10119808 9/2002
DE 102009041002 3/2011
EP 1280115 1/2003
EP 2084921 A1 8/2009
EP 2284783 2/2011
JP 2001-297198 10/2001
JP 2001357164 12/2001
JP 2002-99716 4/2002
KR 10-2002-0065989 8/2002
KR 10-2003-0068603 8/2003
KR 10-2007-0092400 9/2007
WO 199834203 8/1998
WO 9913636 3/1999
WO 0171627 9/2001
WO 2001097118 12/2001
WO 2002071354 9/2002
WO 2003012717 2/2003
WO 2004010393 1/2004
WO 2004023353 3/2004
WO 2004053640 6/2004
WO 2004088641 10/2004
WO 2005079254 9/2005
WO 2005086593 9/2005
WO 2007145500 12/2007
WO 2008008735 1/2008
WO 2008/046161 A1 4/2008
WO 2008005018 10/2008
WO 2012025824 3/2012
WO 2013009444 1/2013
WO 2013009446 1/2013
WO 2013025273 2/2013
WO 2013/052729 A2 4/2013
WO 2013078176 5/2013
WO 2013166174 11/2013

OTHER PUBLICATIONS

Office Action received for U.S. Appl. No. 13/644,312, dated Oct. 21, 2014.
Office Action received for U.S. Appl. No. 14/928,521, dated Oct. 5, 2018.

(56) **References Cited**

OTHER PUBLICATIONS

U.S. Appl. No. 13/484,199, dated Dec. 26, 2012, Office Action.
GlobalPlatform, Card Specification, Version 2.2, published Mar. 2006.
U.S. Appl. No. 61/493,064, filed Jun. 3, 2011, Liberty, Michael A.
U.S. Appl. No. 61/522,099, filed Aug. 10, 2011, Liberty, Michael A.
U.S. Appl. No. 62/075,657, filed Nov. 5, 2014, Liberty, Michael A.
U.S. Appl. No. 61/498,957, filed Jun. 20, 2011, Liberty, Michael A.
U.S. Appl. No. 61/499,927, filed Jun. 22, 2011, Liberty, Michael A.
U.S. Appl. No. 61/562,301, filed Nov. 21, 2011, Liberty, Michael A.
U.S. Appl. No. 61/694,118, filed Aug. 28, 2012, Liberty, Michael A.
U.S. Appl. No. 61/641,677, filed May 2, 2012, Liberty, Michael A.
U.S. Appl. No. 61/862,437, filed Aug. 5, 2013, Liberty, Michael A.
Chen, Jiajun Jim et al, Short-Range Wireless Technologies with Mobile Payments Systems. Proceedings of the 6th International Conference on Electronic Commerce [Online] 2004, pp. 649-656.
Medhi et al., "Mobile-banking adoption and usage by low-literate, low-income users in the developing world", 2009, N. Aykin (Ed.): Internationalization, Design, LNCS 5623, pp. 485-486.
Mbogo, "The impact of mobile payments on the success and growth of micro-business: the case of M-Pesa in Kenya", The Journal of Language, Technology & Entrepreneurship in Africa, vol. 2, No. 1, 2010, ISSN 1998-1279, pp. 182-203.
Jack et al., "Monetary Theory and electronic money: reflections on the Kenyan experience", economic quarterly, vol. 96, No. 1, first quarter 2010, pp. 83-122.
Comninos et al., "M-banking the unbanked", towards evidence-based ICT policy and regulation, vol. 1, 2008, policy paper 4, pp. 1-15.
Lonie, "M-PESA: finding new ways to serve the unbanked in Kenya", innovations in rural and agricultural finance, Jul. 2010, focus 18, brief 8, pp. 1-3.
Plyler et al., "Community level economic effects of M-PESA in Kenya: initial findings (executive summary)", financial services assessment, IRIS center, university of maryland college park, Mar. 30, 2010, pp. 1-4, accessible at <http://www.fsassessment.umd.edu/>.
Hughes et al., "M-PESA: mobile money for the 'unbanked' turning cellphones into 24-hour tellers in Kenya"; winter & spring 2007, innovations, pp. 63-81.
Omwansa, "M-PESA: Progress and prospects", innovations case discussion: M-PESA, 2009, innovations, mobile world congress, pp. 107-123.
Mas et al., "Designing mobile money services—lessons from M-PESA", innovations, spring 2009, pp. 77-91.
Porteous, "Just how transformational is m-banking?", commissioned by FinMark Trust, bankable frontier associates LLC, Feb. 2007, pp. 1-32.
Morawczynski et al., "Poor people using mobile financial services: observations on customer usage and and impact from M-PESA", CGAP, Aug. 2009, pp. 1-4.
Jack et al., "The economics of M-PESA", Aug. 2010, commissioned by the Centra Bank of Kenya, managed by Financial Sector Deepening, adminstered by the Steadman Group, pp. 1-20.
"RadioShack and Trumpet Mobile launch prepaid mobile phone service nationwide with unique mobile money transfer capabilities", Apr. 1, 2008, Source: Trumpet Mobile, pp. 1-3.
Sultana, "Mobile banking: overview of regulatory framework in emerging markets", Grameenphone Ltd, Celebration Point, Bangladesh, electronic copy available at <http://ssrn.com/abstract=1554160>, pp. 1-17.
Ivatury et al., "The early experience with branchless banking", CGAP, No. 46, Apr. 2008, electronic copy available at <http://ssrn.com/abstract=1655257>, pp. 1-16.
Porteous, "The enabling environment for mobile banking in Africa", version 3.1, report commissioned by Department for International Development (DFID), Bankable Frontier Associates, May 2006, pp. 1-57.
Jack et al., "Mobile money: the economics of M-PESA", working paper 16721, National Bureau of Economic Research (NBER) working paper series, Jan. 2011, accessible at <http://www.nber.org/papers/w16721>, pp. 1-30.
Rice, "Kenya sets world first with money transers by mobile", The Guardian, Mar. 20, 2007. pp. 1-3, accessed via <https://www.theguardian.com/money/2007/mar/20/kenya.mobilephones> Mar. 25, 2019.
PYMNTS, "Mobile payments go viral: M-PESA in Kenya", Aug. 4, 2010, Business Wire, from 'Yes Africa can: success stories from a dynamic continent, world bank' —May 2010, pp. 1-30, accessed via <https://www.pymnts.com/business-wire/2010/mobile-payments-go-viral-m-pesa-in-kenya/> on Mar. 25, 2019.
Youtube video, "M-PESA: send money home tv commerical", accessed via <https://www.youtube.com/watch?v=nEZ30K5dBWU> on Mar. 25, 2019.
Graham, "M-PESA: Kenya's mobile wallet revolution", technology of business reporter, BBC news, Nov. 22, 2010, pp. 1-18, accessed via <https://www.bbc.com/news/business-11793290> on Mar. 25, 2019.
Starita, "Mobile cash transfers pose threat to banks", Feb. 26, 2009, News & Commentary, Philanthropy Action, pp. 1-4, accessed via <philanthropyaction.com/nc/mobile_cash_transfers_pose_threat_to_banks/> on Mar. 25, 2019.
Anonymous Staff Writer, "Portuguese firm flourishing in Mozambique", Africa Business Insight, How We Made It in Africa, pp. 1-2, accessed via <https://howwemadeitinafrica.com/portugese-firm-flourishing-in-mozambique/3599/> on Mar. 25, 2019.
Njihia, "What you dont now about Mpesa . . . ", The Mind of Mbugua Njihia, Jul. 15, 2009, adapted from an article by Olga Morawczynski from CGAP dated Jul. 14, 2009, pp. 1-3, accessed via <www.mbuguanjihia.com/business/what-you-dont-now-about-mpesa.html> on Mar. 25, 2019.
McKinley, "Trumpet Mobile Wallet Takes-Off", May 6, 2008, CardFlash, pp. 1-5, accessed via <https://cardweb.com/news/2008/05/trumpet-mobile-wallet-takes-off> on Mar. 25, 2019.
Anonymous, "Radioshack, Trumpet launch prepaid-mobile-money", Apr. 1, 2008, FierceWireless, pp. 1-3, accessed via <https://www.fiercewireless.com/wireless/radioshack-trumpet-launch-prepaid-mobile-money> on Mar. 25, 2019.
Anonymous, "RadioShack to offer Trumpet Mobile service—plan includes mobile money transfer capabilities", Apr. 1, 2008, The Prepaid Press—Where Prepaid Converges, pp. 1-2, accessed via <www.prepaidpress.com/features/radioshack-to-offer-trumpet-mobile-servies.html> on Mar. 25, 2019.
Lugmayr, "RadioShack and Trumpet Mobile launch prepaid mobile phone service", posted Apr. 1, 2008, updated Aug. 11, 2010, I4U News, pp. 1-5, accessed via <https://www.i4u.com/19814/radioshack-and-trumpet-mobile-launch-prepaid-mobile-phone-service> on Mar. 25, 2019.
Labrou, Yannis et al, Wireless Wallet. Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services [Online] 2004, pp. 1-10.
Motorola, Motorola M-Wallet Solution. [Online] 2006 http://www.motorola.com/networkoperators/pdfs/M-Wallet-Brochure.pdf (Accessed Oct. 4, 2012).
Valcourt, E. et al., "Investigating Mobile Payment," Wireless and Mobile Computing, Networking and Communications, 2005. (WiMob'2005), IEEE International Conference on Aug. 22-24, 2005, Aug. 2005, vol. 4, pp. 29-36.
Gao, Jerry, et al., "P2P-Paid: A Peer-to-Peer Wireless Payment System," Proceedings of the 205 Second IEEE International Workshop on Mobile Commerce and Services (WMCS'05) Jul. 2005, 10 pages.
Edwin, et al., "Technobiography," Oct. 2004, 29 pages.
International Search Report and Written Opinion for PCT/US2012/066013 dated Jan. 29, 2013.
International Search Report and Written Opinion for PCT/US2012/040131 dated Jan. 29, 2013.
International Search Report and Written Opinion for PCT/US2012/043321 dated Sep. 6, 2012.
International Search Report and Written Opinion for PCT/US2012/058849 dated Jan. 4, 2013.

(56) **References Cited**

OTHER PUBLICATIONS

International Search Report and Written Opinion for PCT/US2013/039100 dated Aug. 23, 2013.
European Search Report for EP12824344 dated Sep. 29, 2014.
Sykes, et al. "Securing Mobile Banking," Credit Union Management, Nov. 2010, vol. 33 No. 11; ISSN 0273-9267.
Clarke, Irvine III, "Emerging Value Propositions for M-commerce," *Journal of Business Strategies*, vol. 25, Issue 2, Fall 2008, p. 41-57; ISSN: 0887-2058.
Wei, et al., "Development of a Web-Based Mobile Airline Ticketing Model with Usability Features," 2005, Industrial Management + Data Systems; vol. 105 No. 9, ISSN: 0263-5577.
International Search Report and Written Opinion for PCT/US2012/43458 dated Aug. 17, 2012.
International Search Report and Written Opinion for PCT/US2015/58886 dated Feb. 4, 2016.
European Search Report for EP12851211 dated Feb. 18, 2016.
Ron White, How Computers Work, Oct. 15, 2003, Paul Boger, Illustrated by Timothy Edward Dwons, 7th Edition (Year: 2003).
U.S. Appl. No. 13/484,199, dated Jun. 7, 2013, Notice of Allowance.
U.S. Appl. No. 13/527,466, dated Apr. 15, 2013, Office Action.
U.S. Appl. No. 13/527,466, dated Dec. 4, 2013, Final Office Action.
U.S. Appl. No. 13/527,466, dated Aug. 1, 2014, Office Action.
U.S. Appl. No. 13/527,466, dated Jul. 16, 2015, Office Action.
U.S. Appl. No. 13/527,466, dated Apr. 1, 2016, Office Action.
U.S. Appl. No. 13/527,466, dated Dec. 14, 2016, Office Action.
U.S. Appl. No. 13/527,466, dated Aug. 9, 2017, Office Action.
U.S. Appl. No. 13/528,720, dated Jun. 25, 2014, Office Action.
U.S. Appl. No. 13/528,720, dated Dec. 10, 2014, Final Office Action.
U.S. Appl. No. 13/528,720, dated Jul. 22, 2015, Office Action.
U.S. Appl. No. 13/528,720, dated Mar. 2, 2016, Final Office Action.
U.S. Appl. No. 13/680,824, dated Jun. 16, 2014, Office Action.
U.S. Appl. No. 13/680,824, dated Feb. 6, 2015, Final Office Action.
U.S. Appl. No. 13/680,824, dated Sep. 18, 2015, Notice of Allowance.
U.S. Appl. No. 13/874,192, dated Jul. 14, 2015, Office Action.
U.S. Appl. No. 13/874,192, dated Apr. 18, 2016, Final Office Action.
U.S. Appl. No. 13/964,707, dated Feb. 24, 2014, Office Action.
U.S. Appl. No. 13/964,707, dated Jul. 10, 2014, Office Action.
U.S. Appl. No. 13/964,707, dated Mar. 16, 2015, Final Office Action.
U.S. Appl. No. 14/012,822, dated Aug. 7, 2014, Office Action.
U.S. Appl. No. 14/012,822, dated Jan. 7, 2015, Final Office Action.
U.S. Appl. No. 14/012,822, dated Sep. 11, 2015, Office Action.
U.S. Appl. No. 14/012,822, dated May 6, 2016, Final Office Action.
U.S. Appl. No. 14/213,543, dated May 6, 2014, Office Action.
U.S. Appl. No. 14/213,543, dated Apr. 8, 2015, Office Action.
U.S. Appl. No. 14/213,543, dated Jan. 6, 2016, Final Office Action.
U.S. Appl. No. 14/341,605, dated Nov. 27, 2017, Office Action.
U.S. Appl. No. 14/928,105, dated Aug. 27, 2018, Office Action.
U.S. Appl. No. 14/928,521, dated Apr. 2, 2018, Office Action.
U.S. Appl. No. 14/928,521, dated Oct. 5, 2018, Office Action.
U.S. Appl. No. 15/201,152, dated Oct. 25, 2016, Office Action.
U.S. Appl. No. 15/201,152, dated Jun. 15, 2017, Final Office Action.
U.S. Appl. No. 15/201,152, dated Aug. 8, 2017, Notice of Allowance.
U.S. Appl. No. 14/928,105, dated Mar. 7. 2019, Final Office Action.
U.S. Appl. No. 14/928,521, dated May 23, 2019, Notice of Allowance.
U.S. Appl. No. 15/809,872, dated Apr. 23, 2020, Office Action.
Final Office Action received for U.S. Appl. No. 15/809,872, dated Jan. 7, 2021, 9 pages.
Non-Final Office Action received for U.S. Appl. No. 16/550,029, dated Jun. 4, 2021, 8 pages.
Non-Final Office Action received for U.S. Appl. No. 15/809,872, dated Jun. 24, 2021, 9 pages.

* cited by examiner

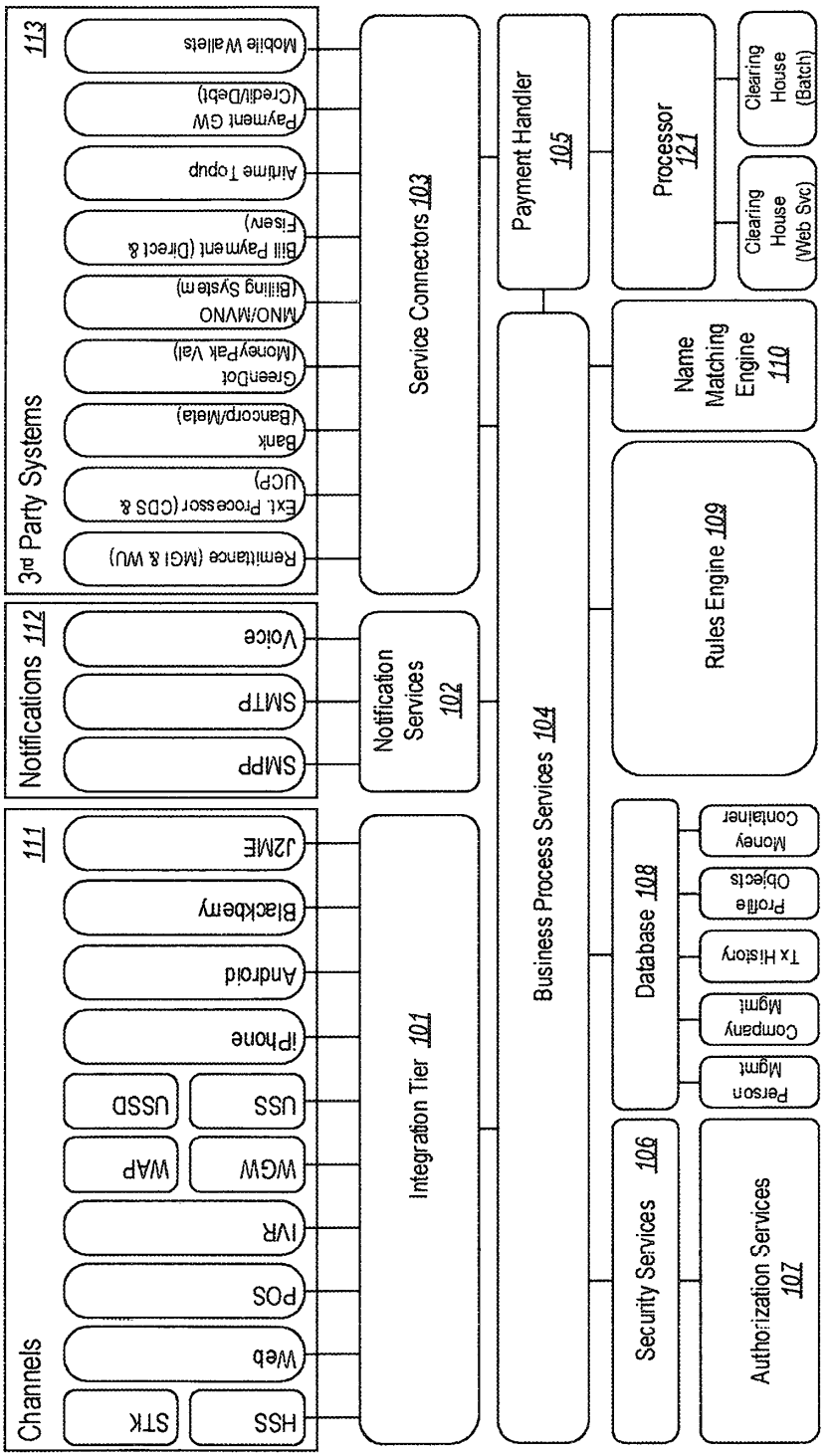


Figure 1

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 192 of 381

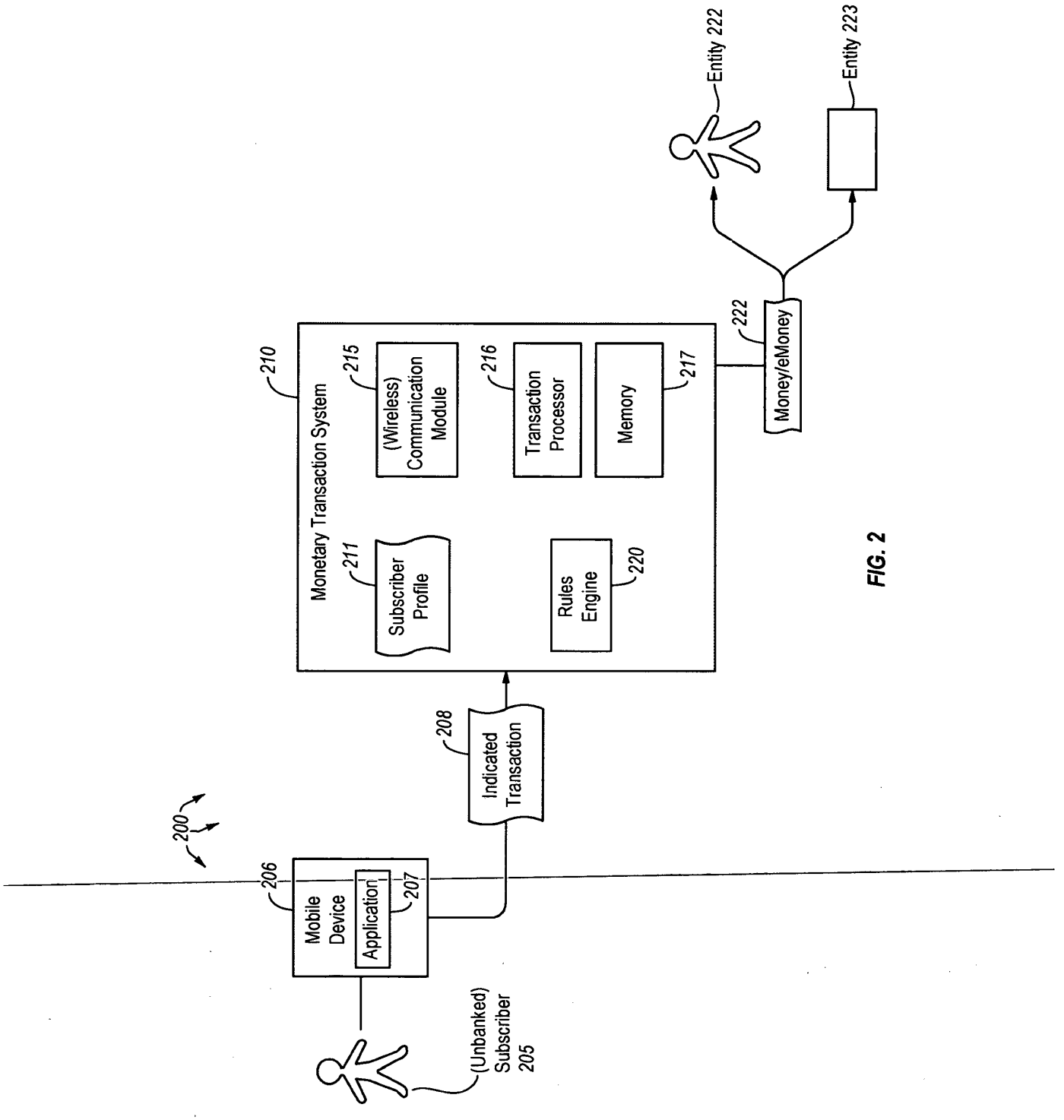
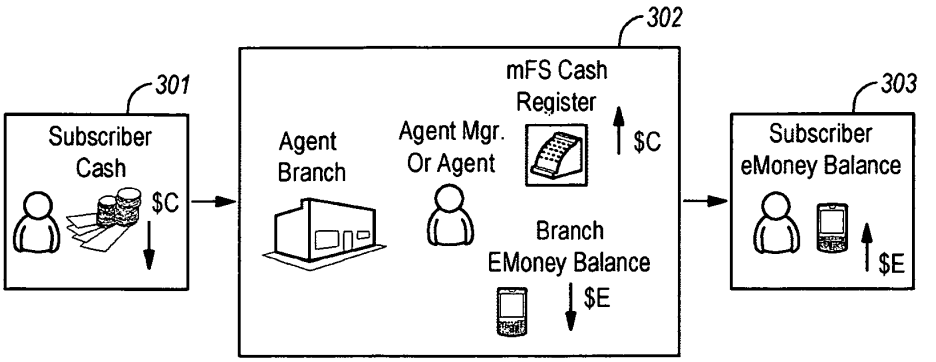


FIG. 2

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 193 of 381


302
301
303
Subscriber
Cash
$C
Agent
Branch
Agent Mgr.
Or Agent
mFS Cash
Register
$C
Branch
EMoney Balance
$E
Subscriber
eMoney Balance
$E
Subscriber Deposit

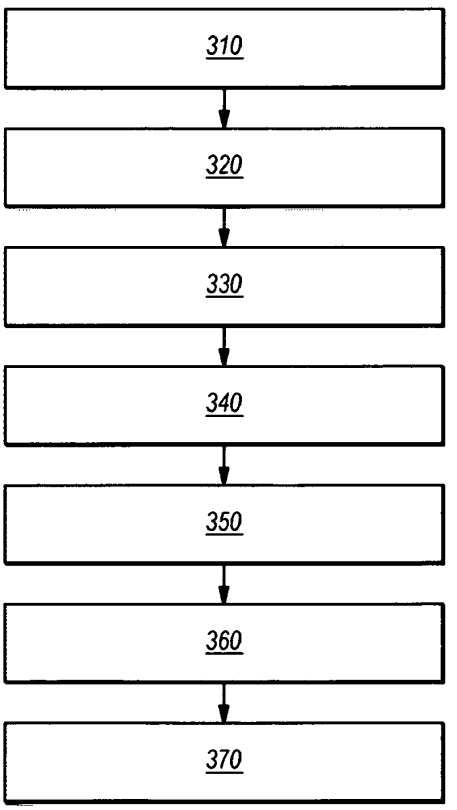
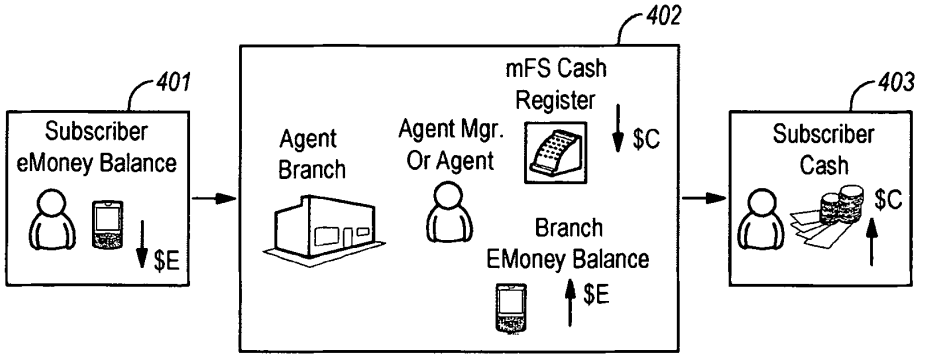

310
320
330
340
350
360
370

FIG. 3



Subscriber Withdrawal

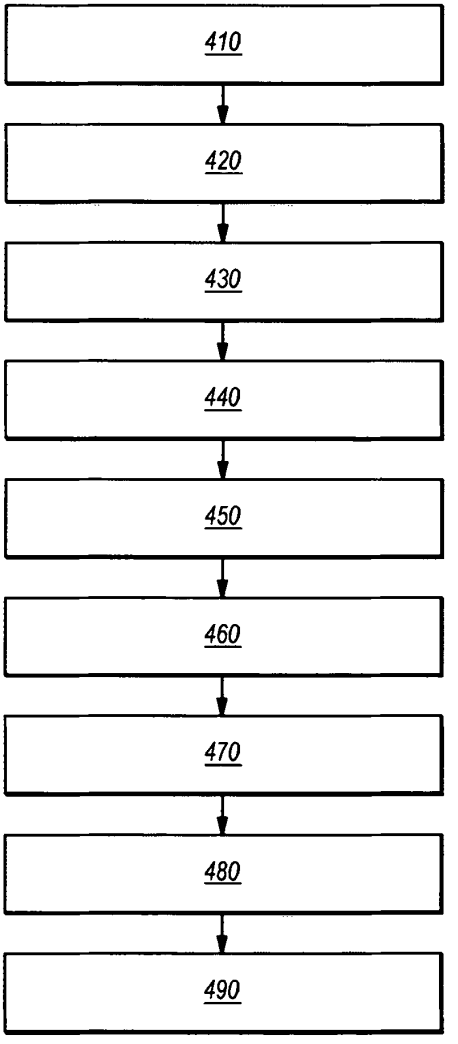
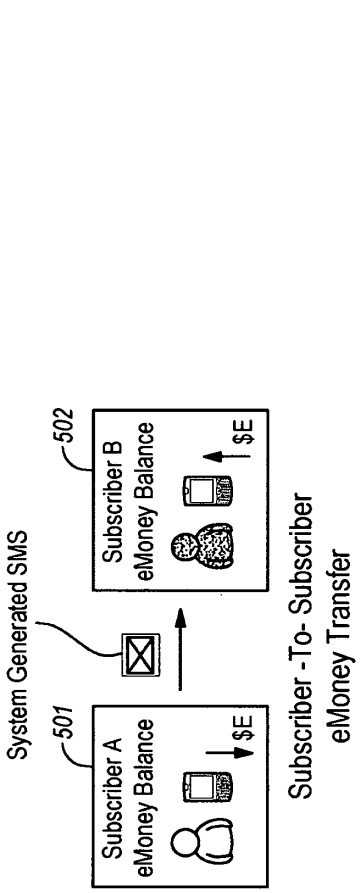
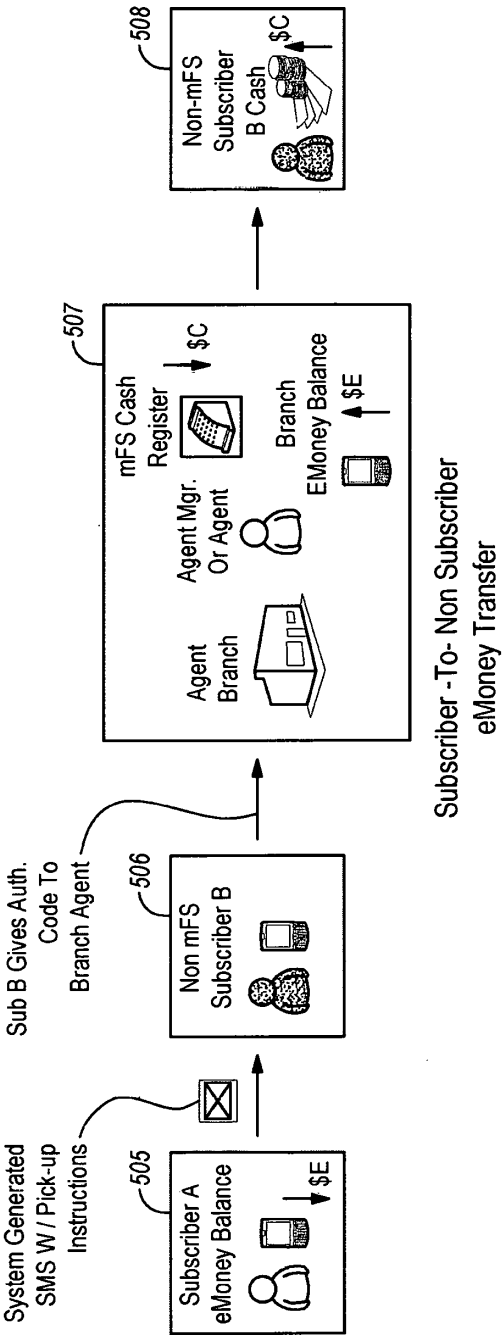


FIG. 4



Subscriber -To- Subscriber eMoney Transfer

FIG. 5A



Subscriber -To- Non Subscriber eMoney Transfer

FIG. 5B

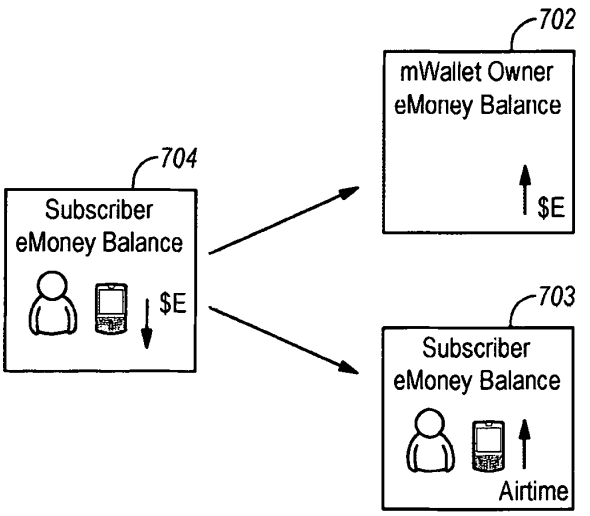
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 196 of 381

Subscriber -To- Subscriber
International eMoney Transfer

FIG. 6A

Subscriber -To- Non Subscriber
International eMoney Transfer

FIG. 6B



Subscriber Buys Airtime

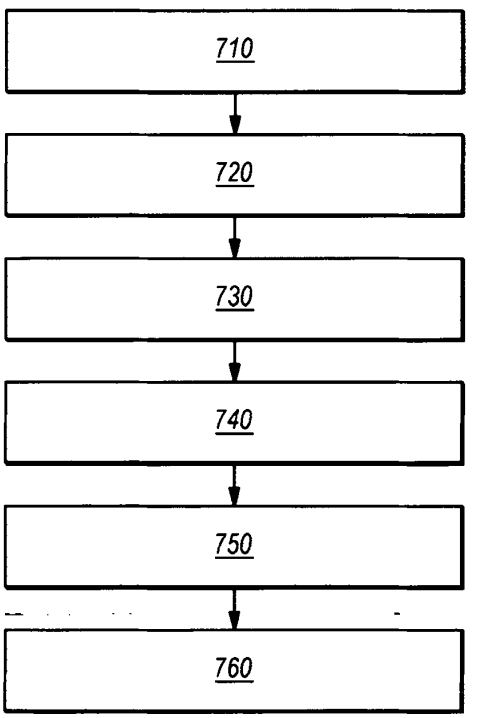
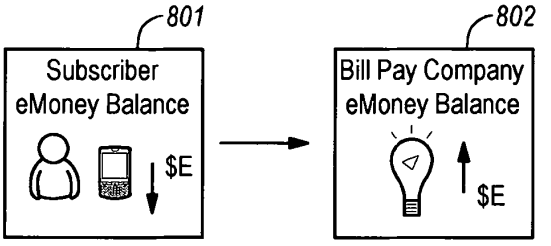


FIG. 7



Subscriber Pays Bill

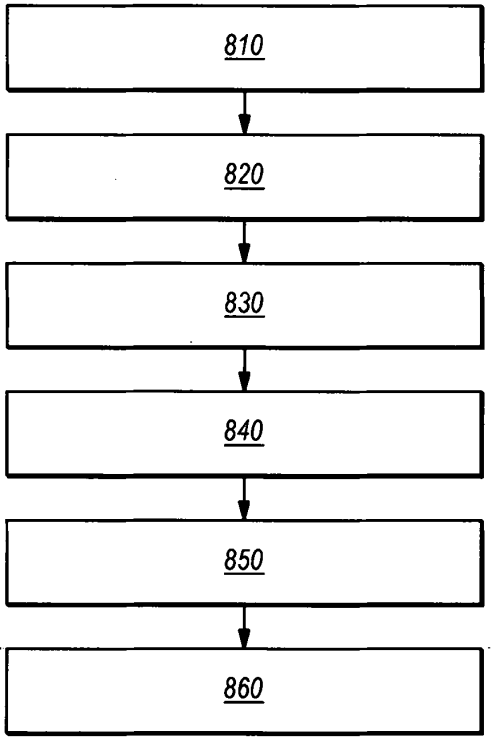
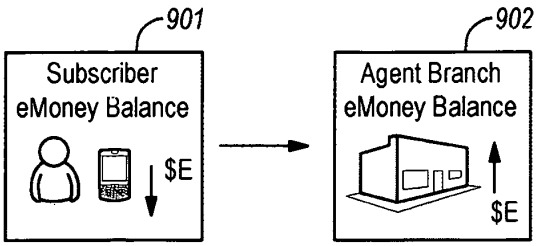


FIG. 8



Subscriber Makes Retail Purchase

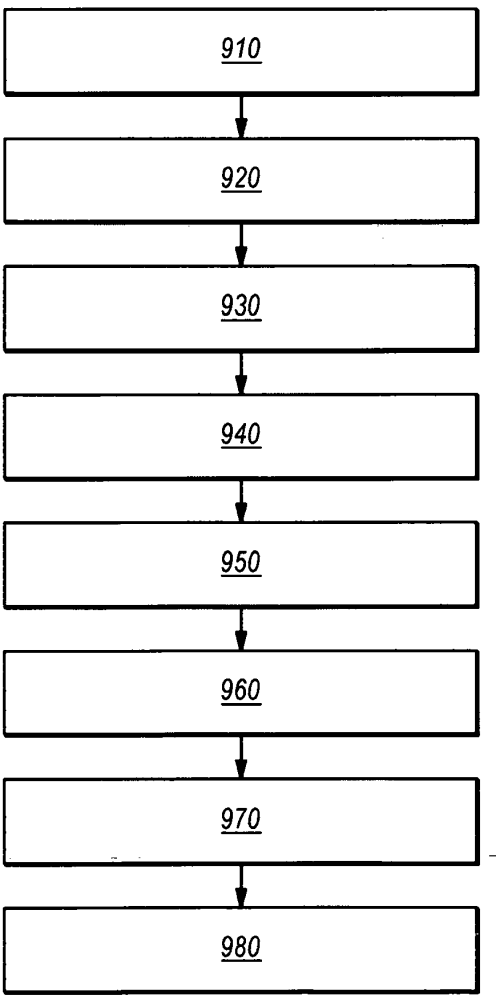
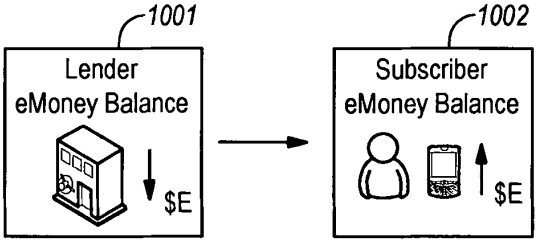
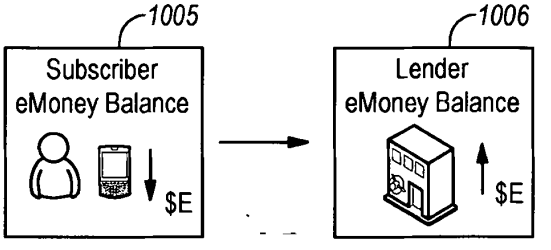


FIG. 9



Subscriber Requests Micro-Loan

FIG. 10A



Subscriber Repays Micro-Loan

FIG. 10B

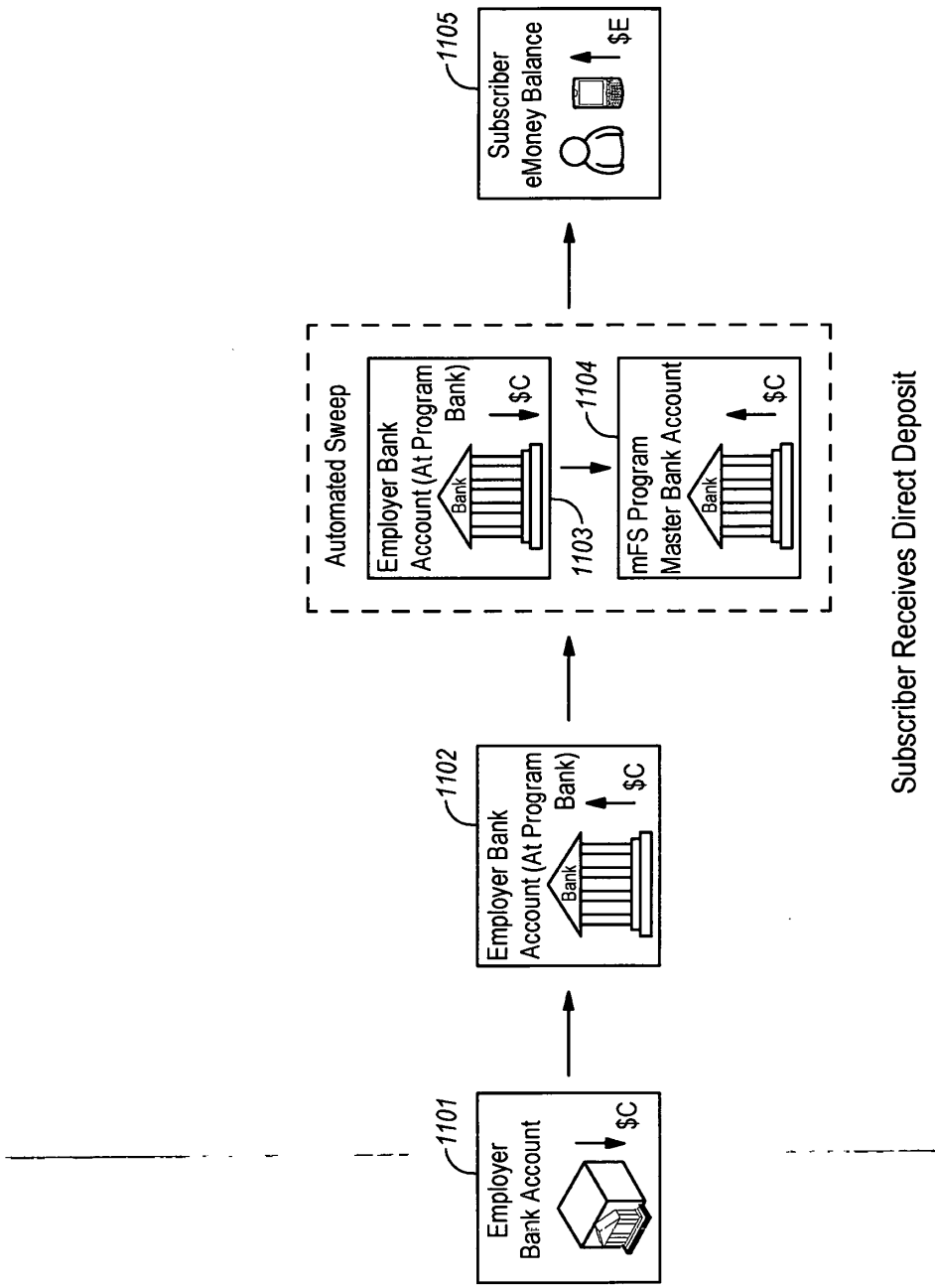
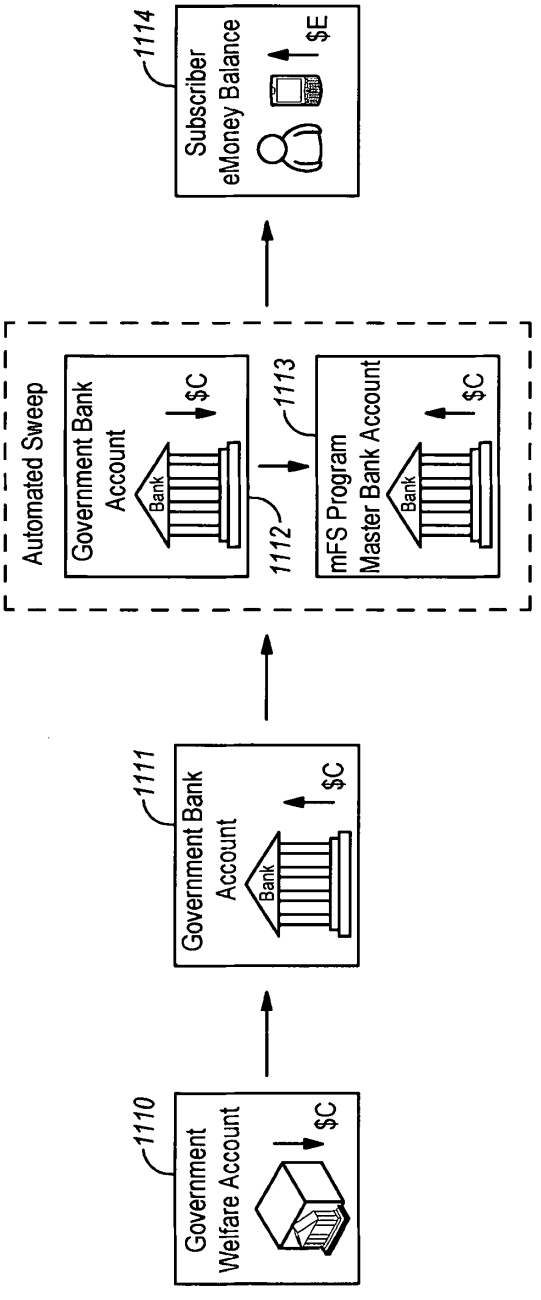


FIG. 11A

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 202 of 381



Subscriber Receives Government Welfare Payment

FIG. 11B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 203 of 381

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 204 of 381

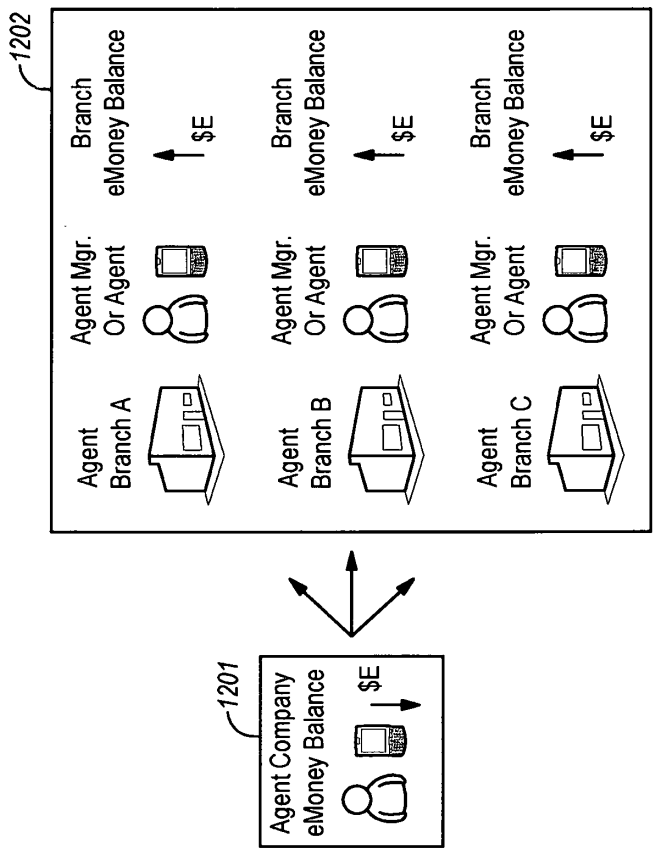
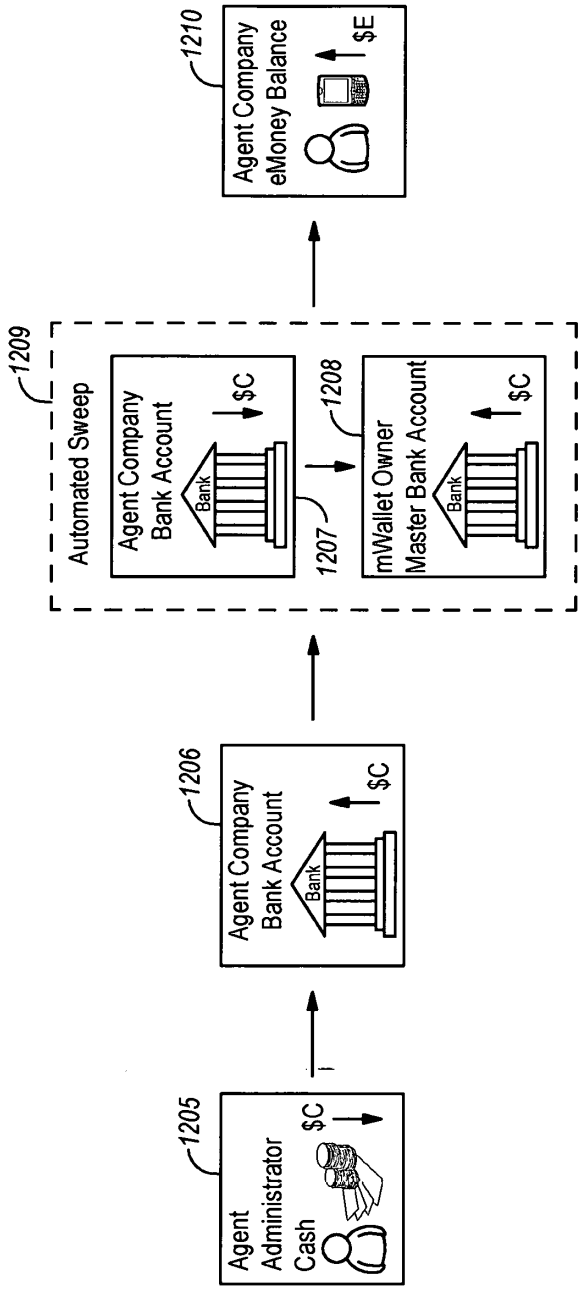


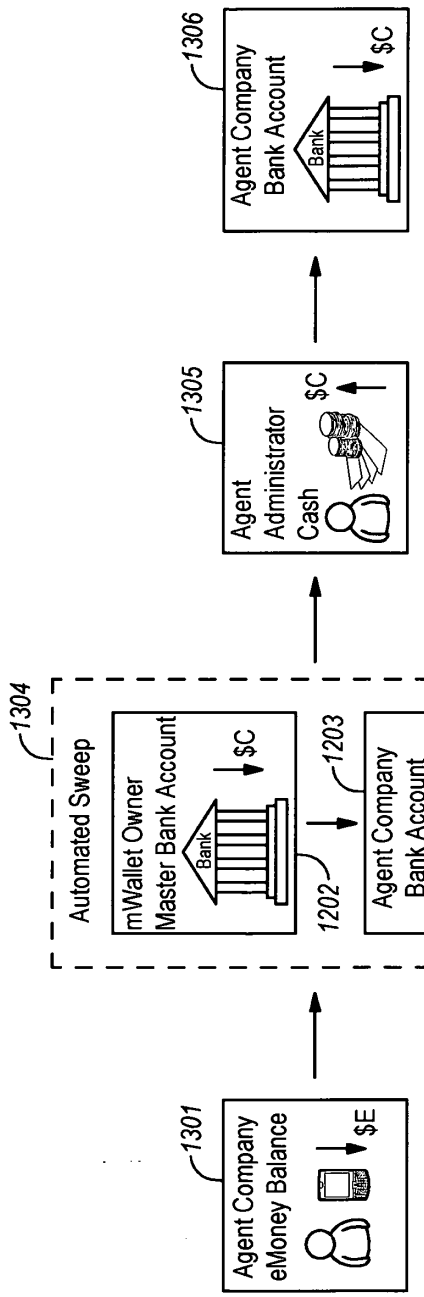
FIG. 12A



Agent Company Deposit

FIG. 12B

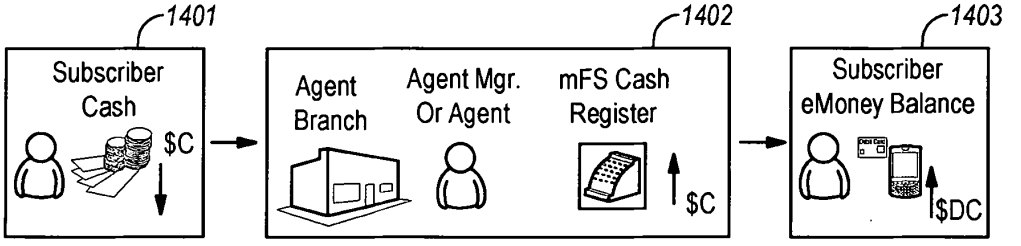
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 205 of 381



Agent Company Withdrawal

FIG. 13

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 206 of 381



Subscriber Deposit At Agent Branch

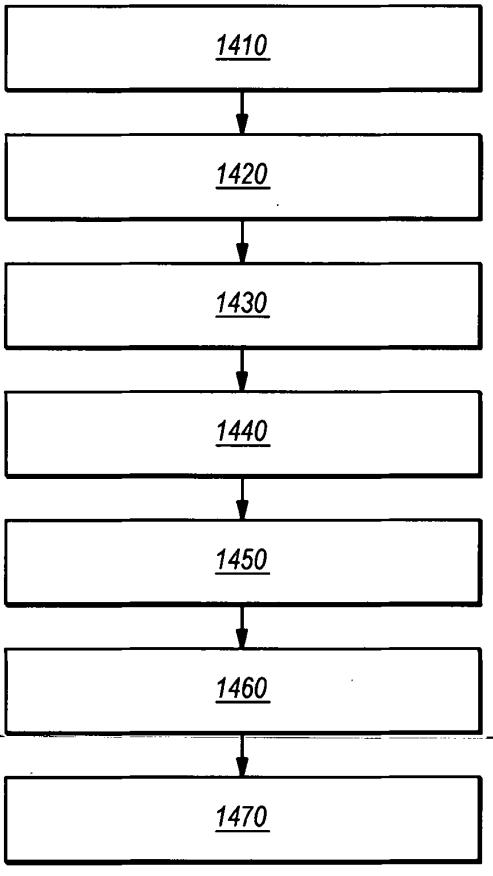


FIG. 14

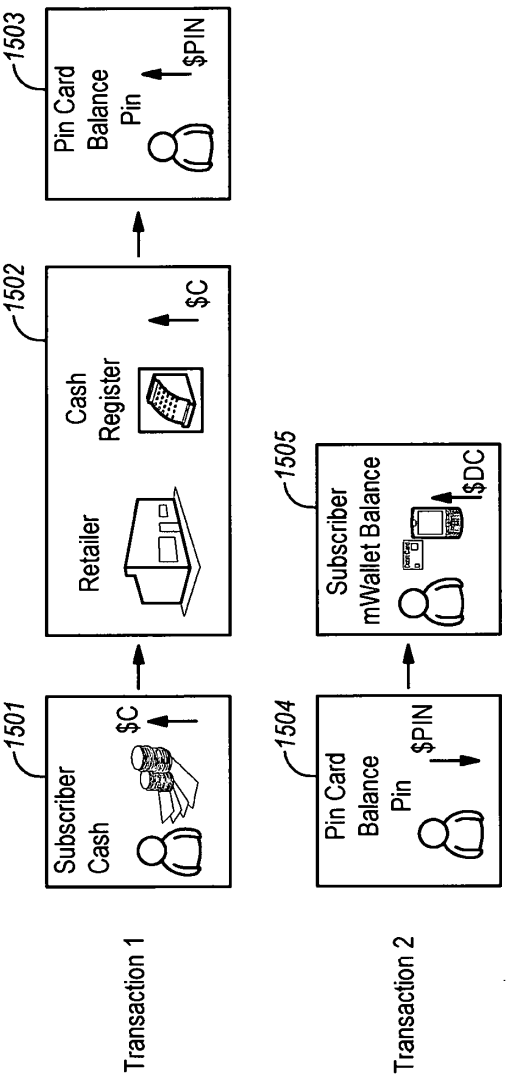
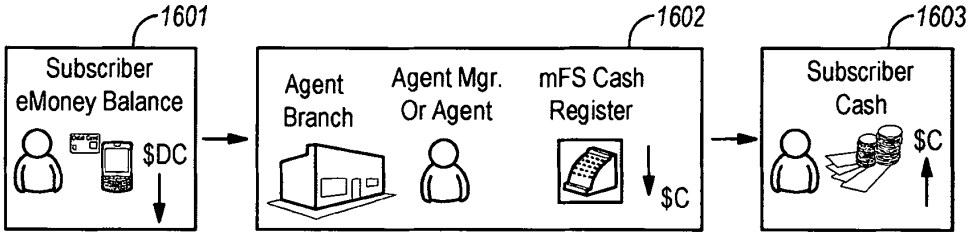


FIG. 15

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 208 of 381



Subscriber Withdrawal (Agent)

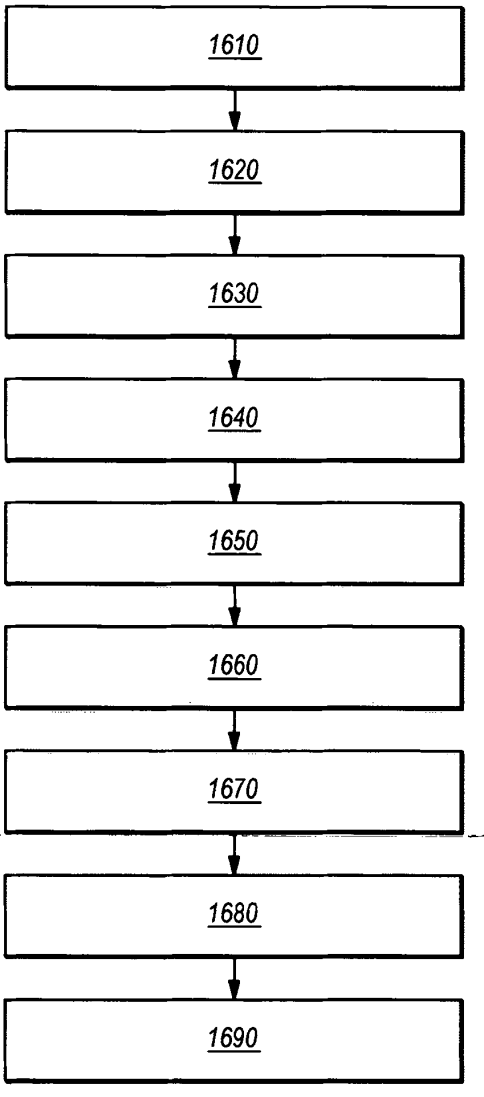
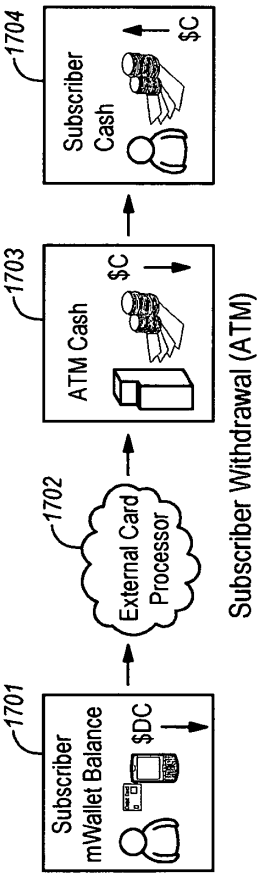
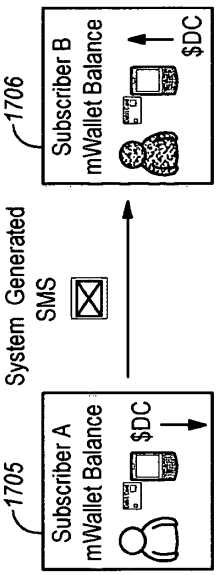


FIG. 16



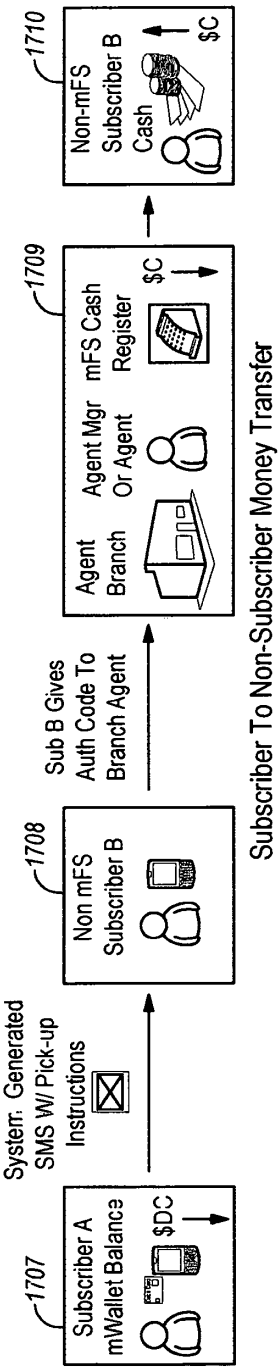
Subscriber Withdrawal (ATM)

FIG. 17A



Subscriber To Subscriber Money Transfer

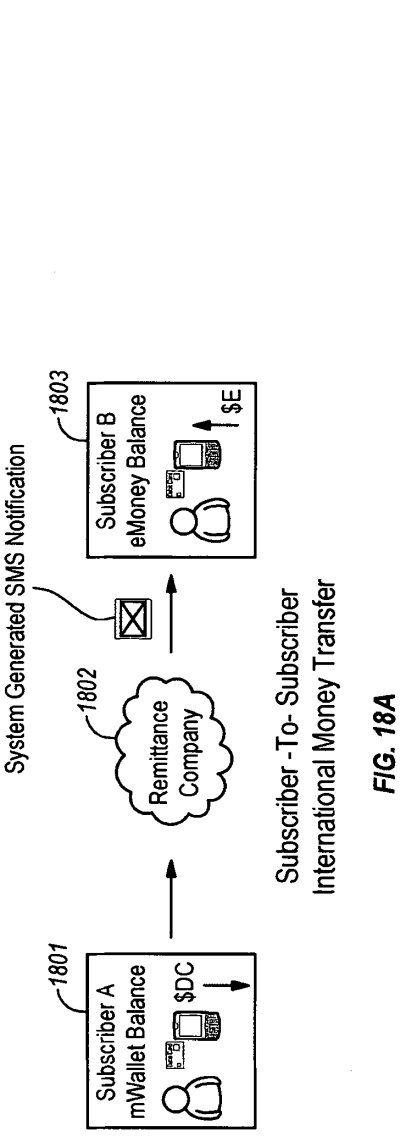
FIG. 17B



Subscriber To Non-Subscriber Money Transfer

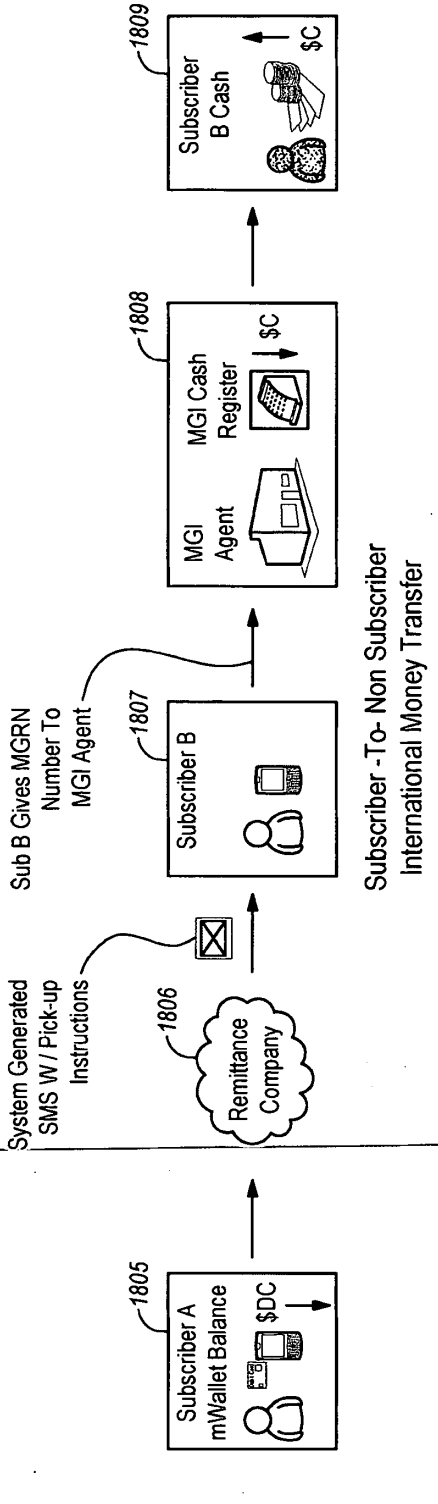
FIG. 17C

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 210 of 381



Subscriber -To- Subscriber International Money Transfer

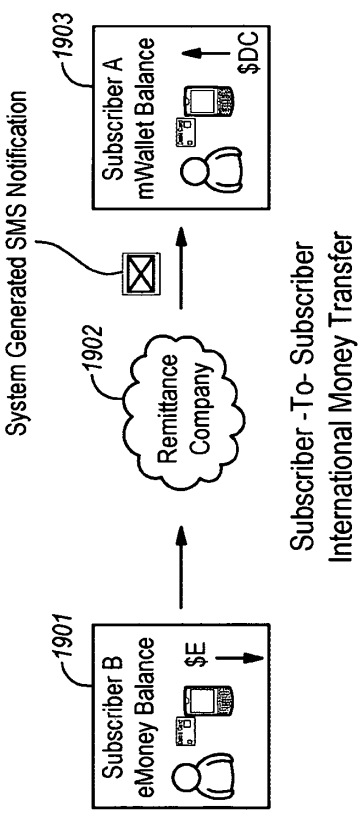
FIG. 18A



Subscriber -To- Non Subscriber International Money Transfer

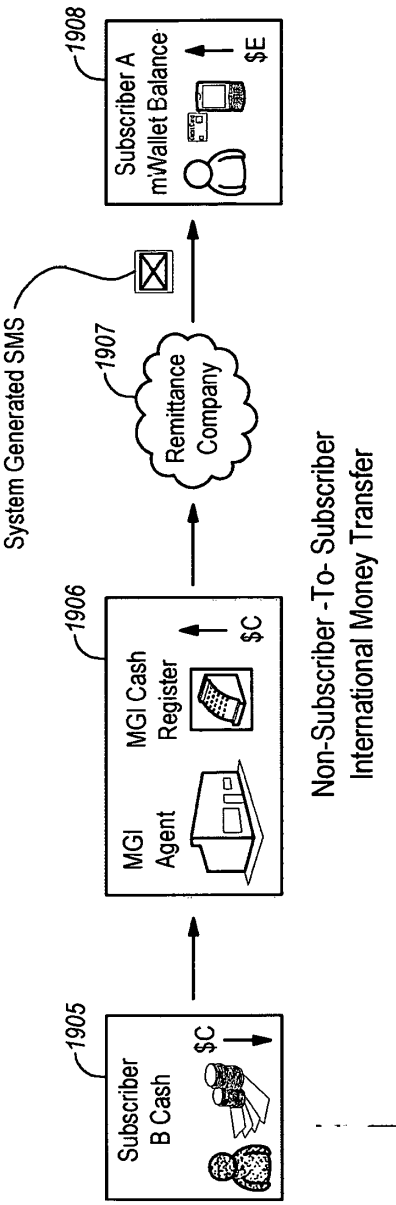
FIG. 18B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 211 of 381



Subscriber -To- Subscriber
International Money Transfer

FIG. 19A



Non-Subscriber -To- Subscriber
International Money Transfer

FIG. 19B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 212 of 381

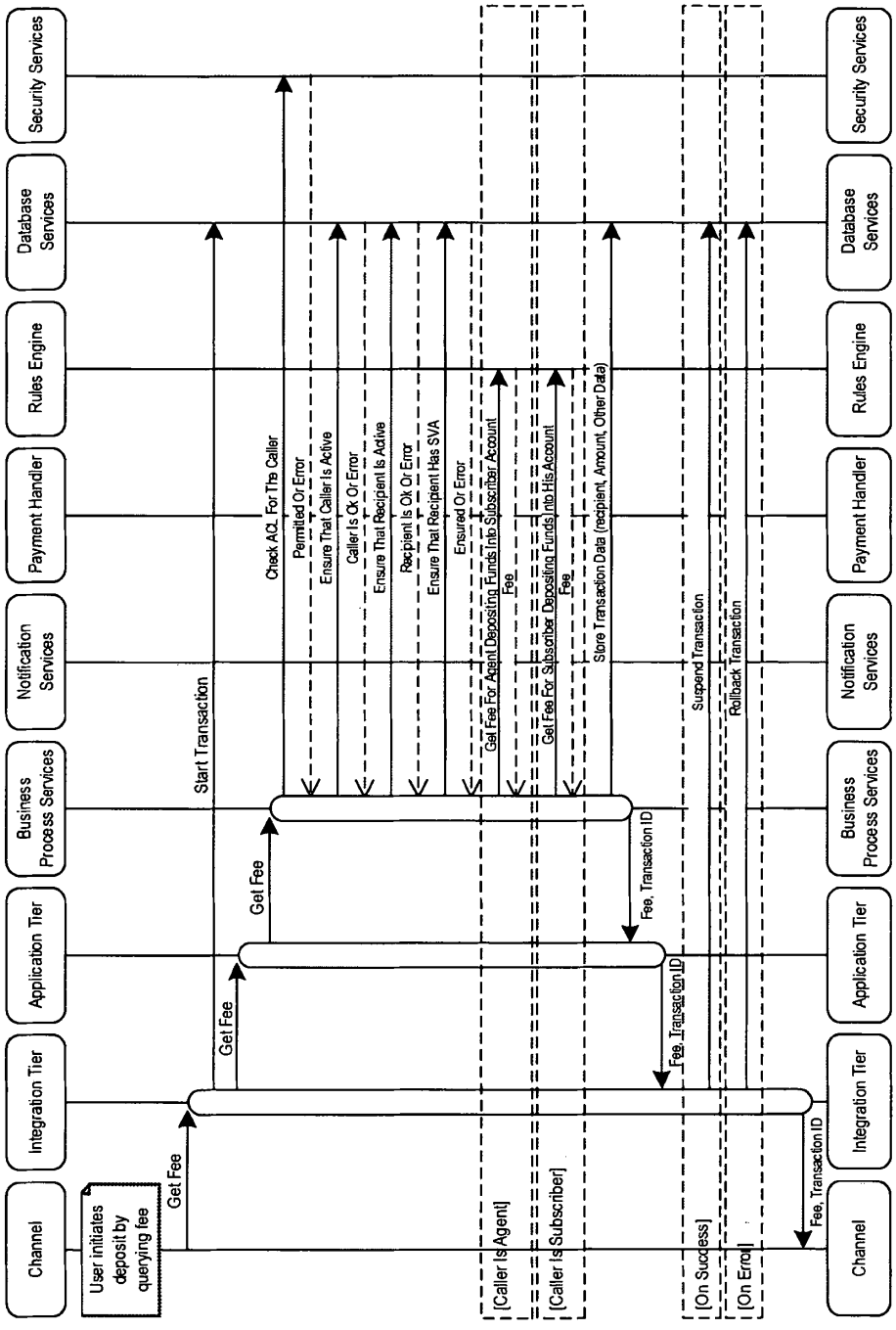


Figure 20A

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 213 of 381

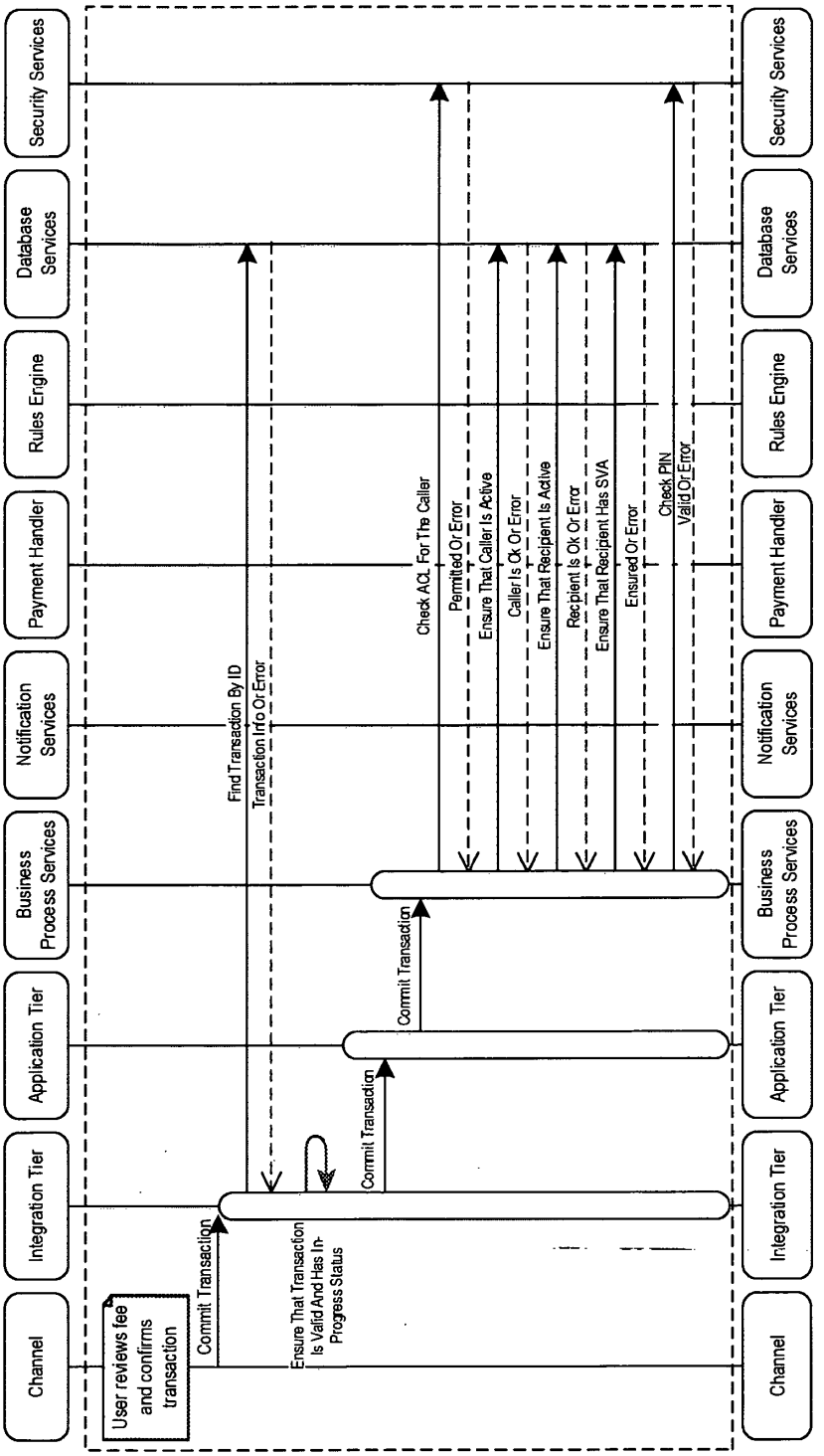


Figure 20B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 214 of 381

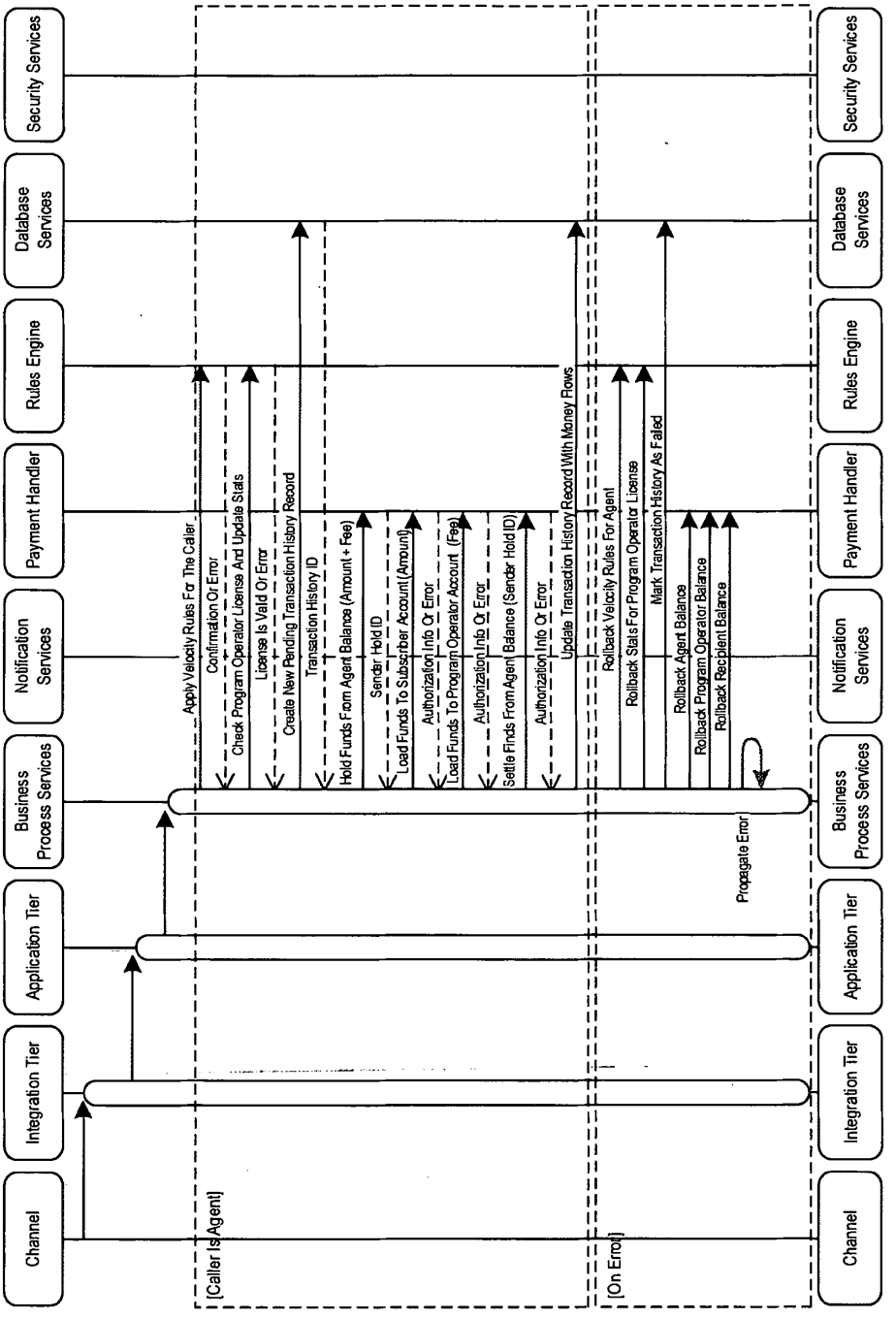


Figure 20C

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 215 of 381

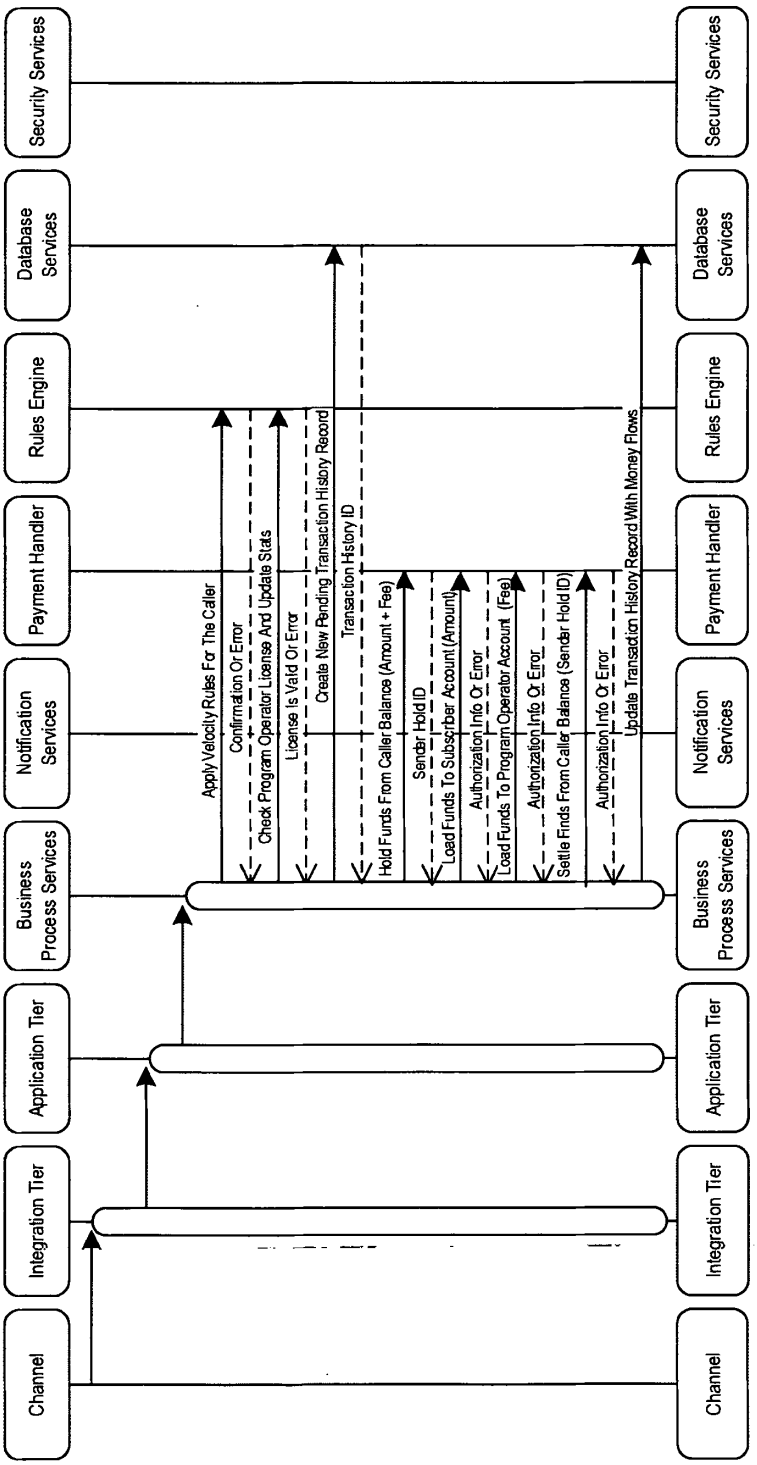


Figure 20D

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 216 of 381

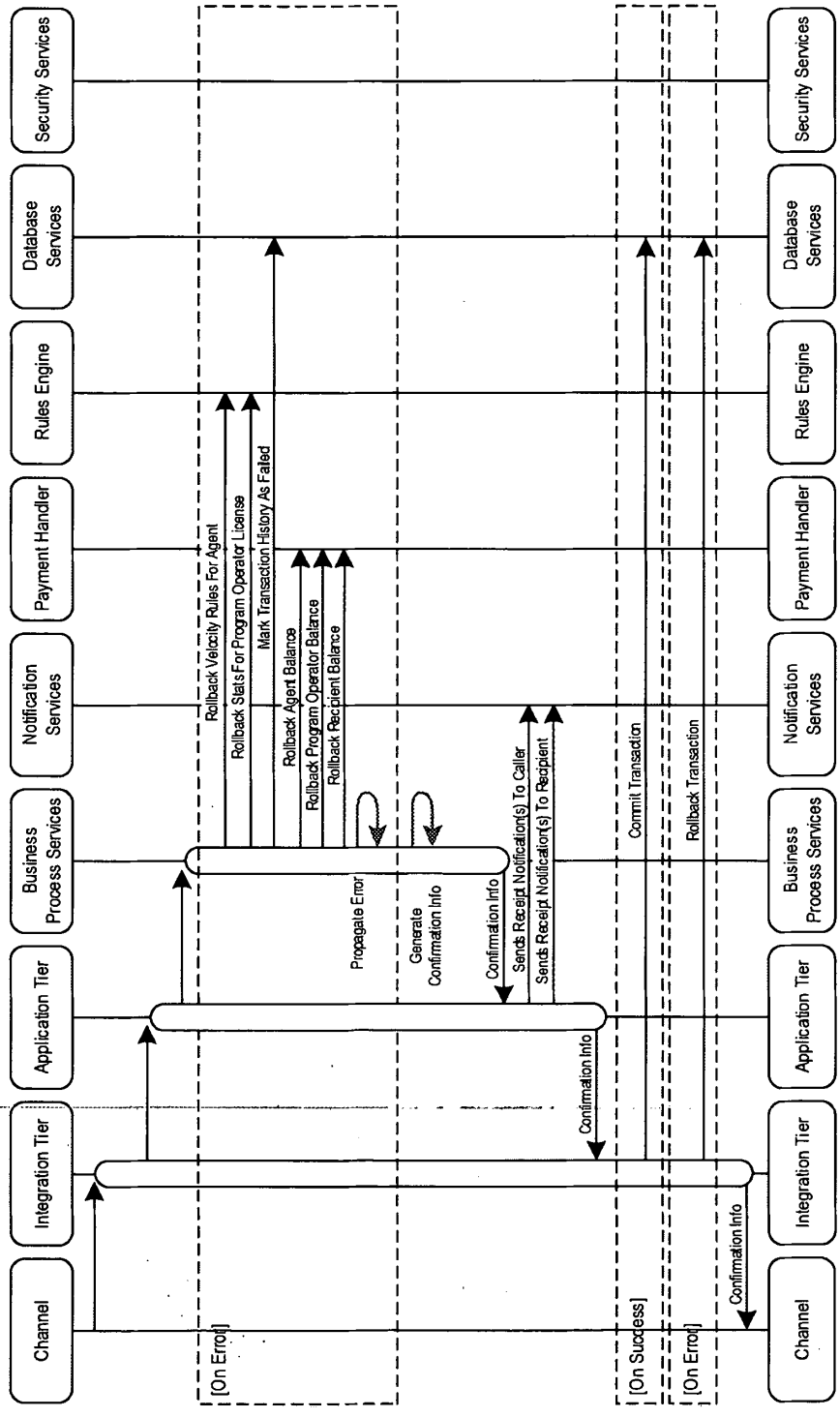


Figure 20E

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 217 of 381

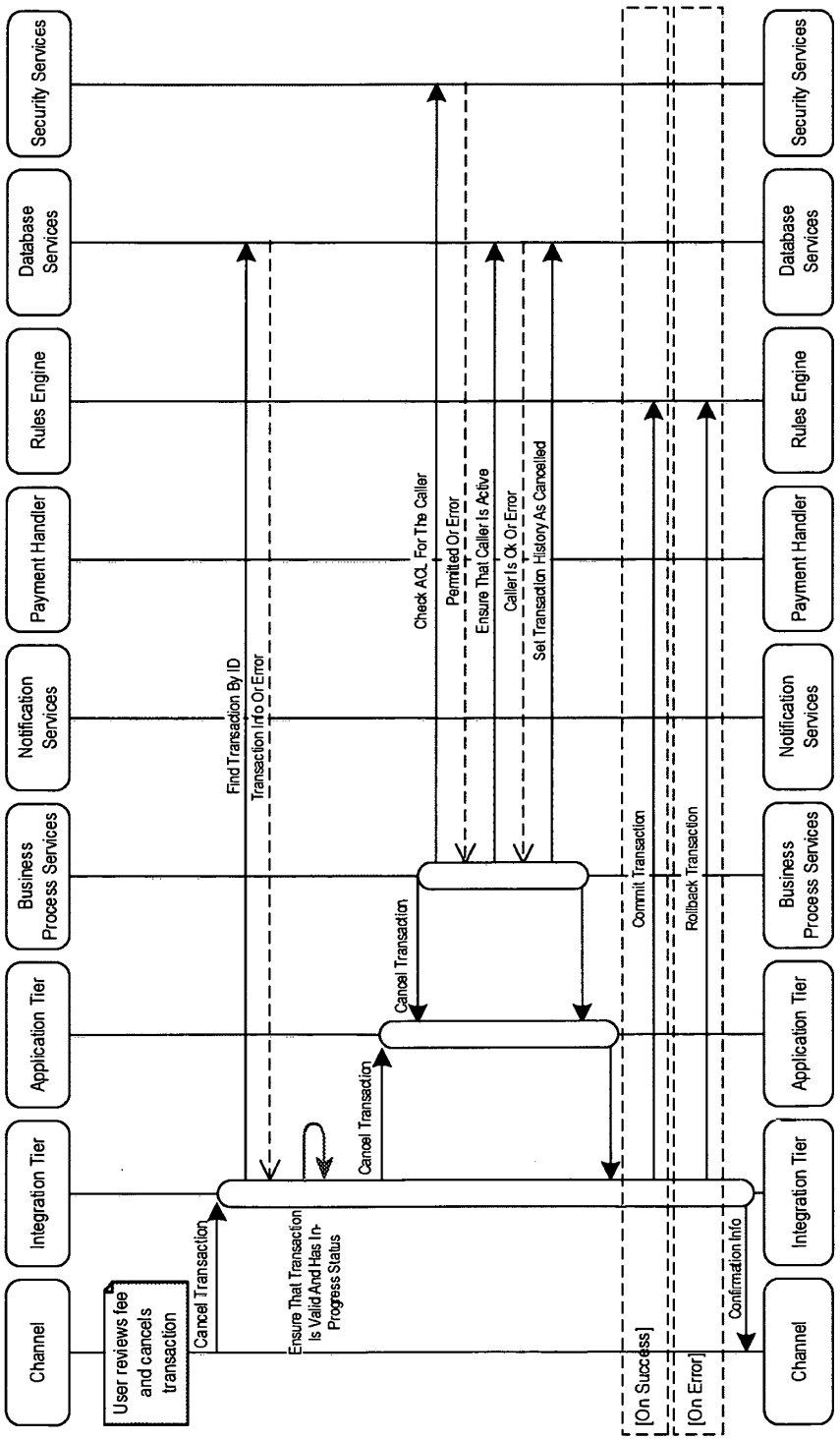


Figure 20F

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 218 of 381

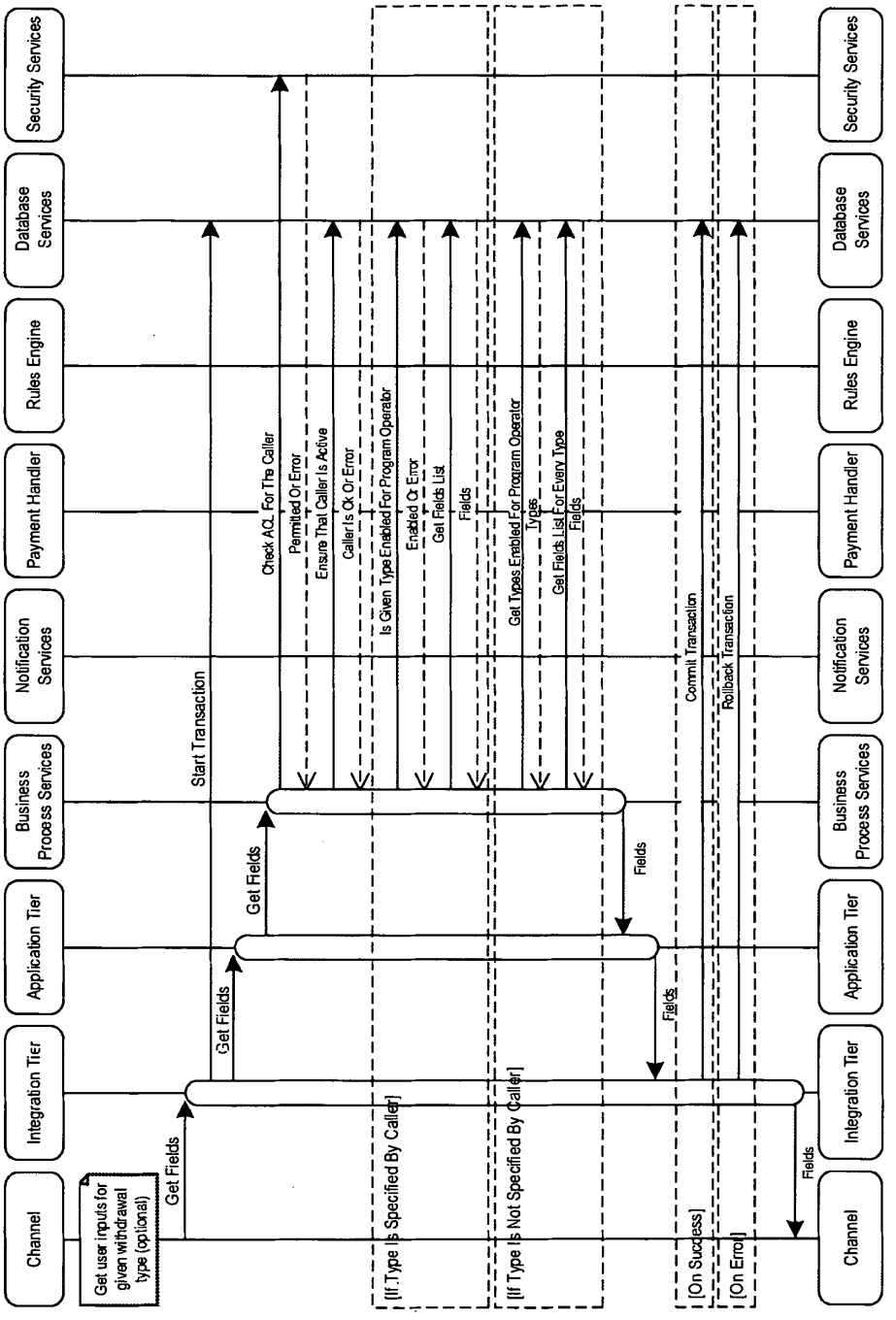


Figure 21A

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 219 of 381

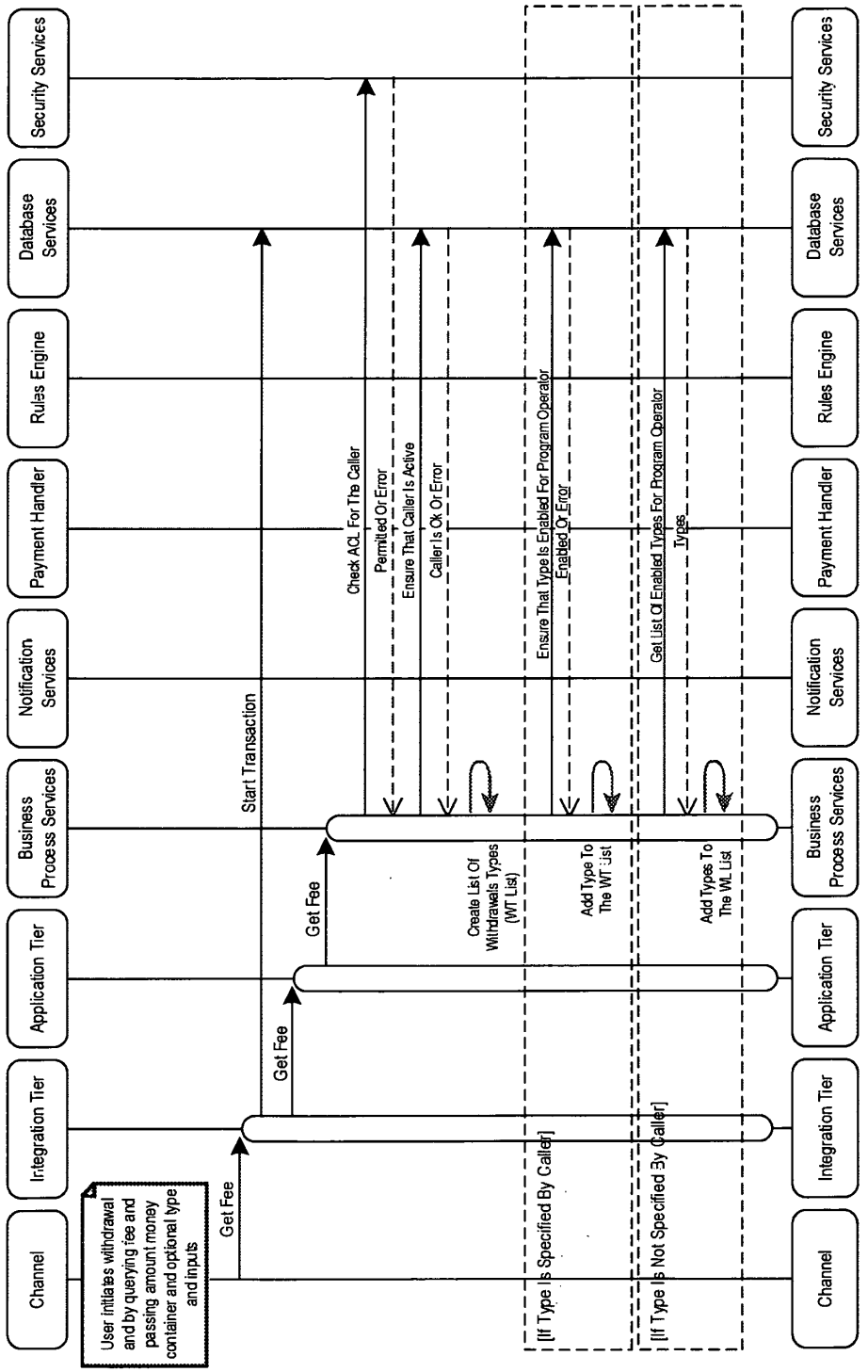


Figure 21B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 220 of 381

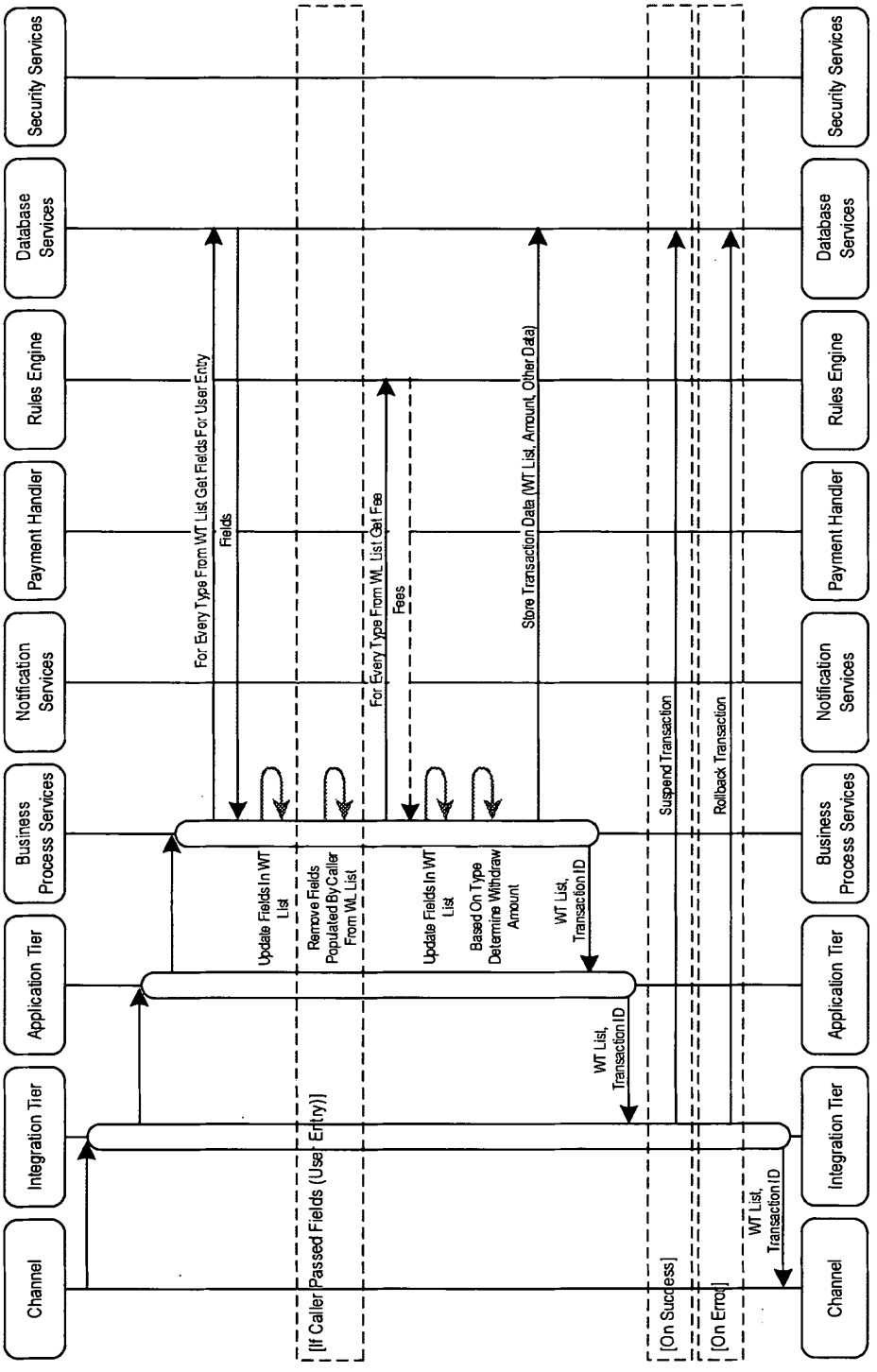


Figure 21C

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 221 of 381

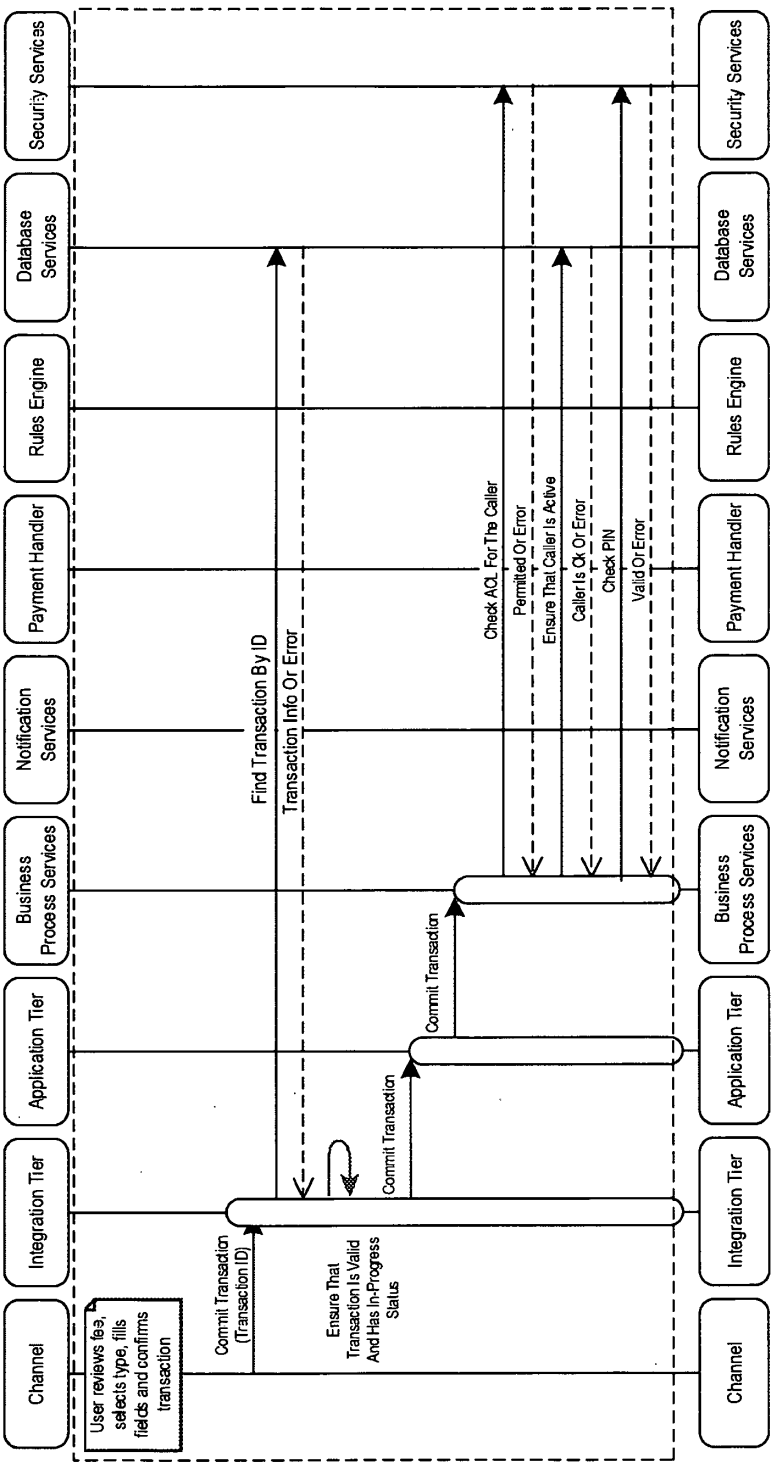


Figure 21D

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 222 of 381

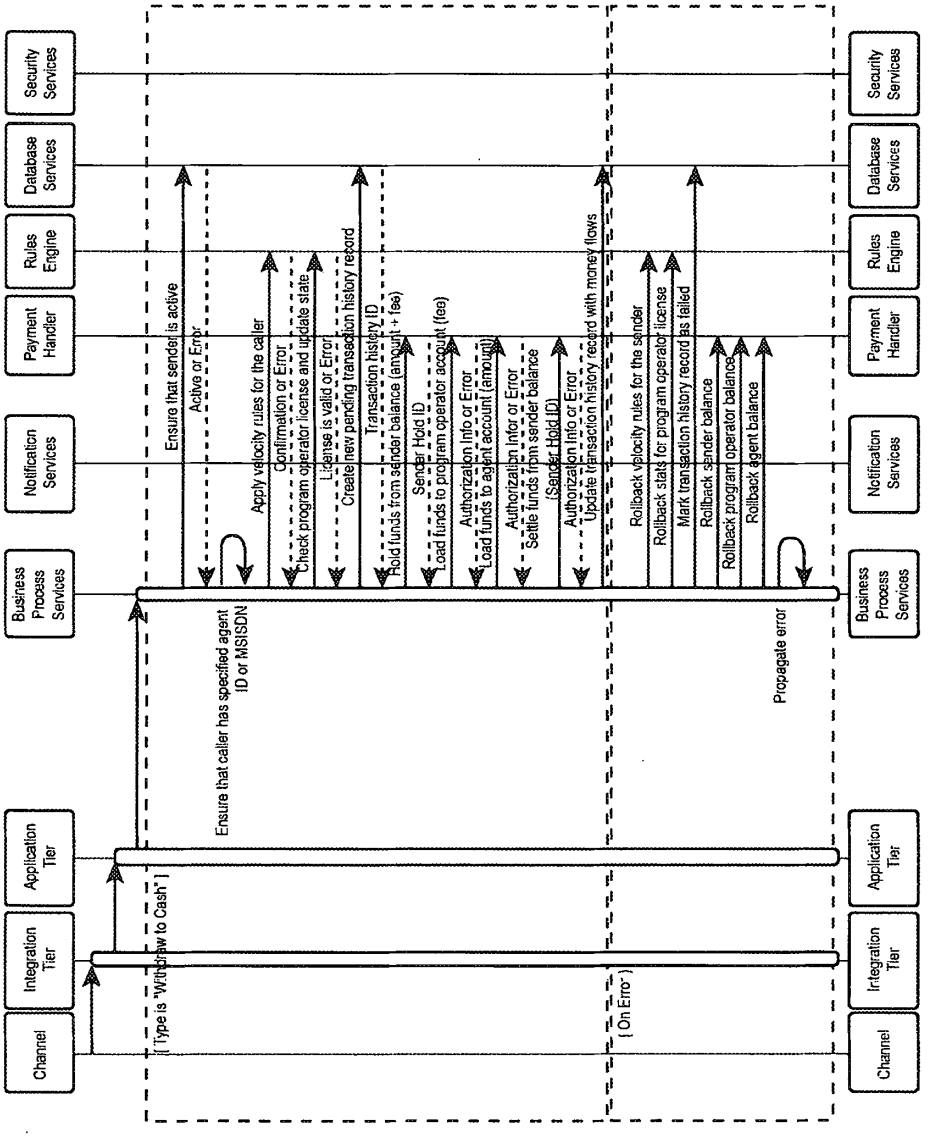


Figure 21E

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 223 of 381

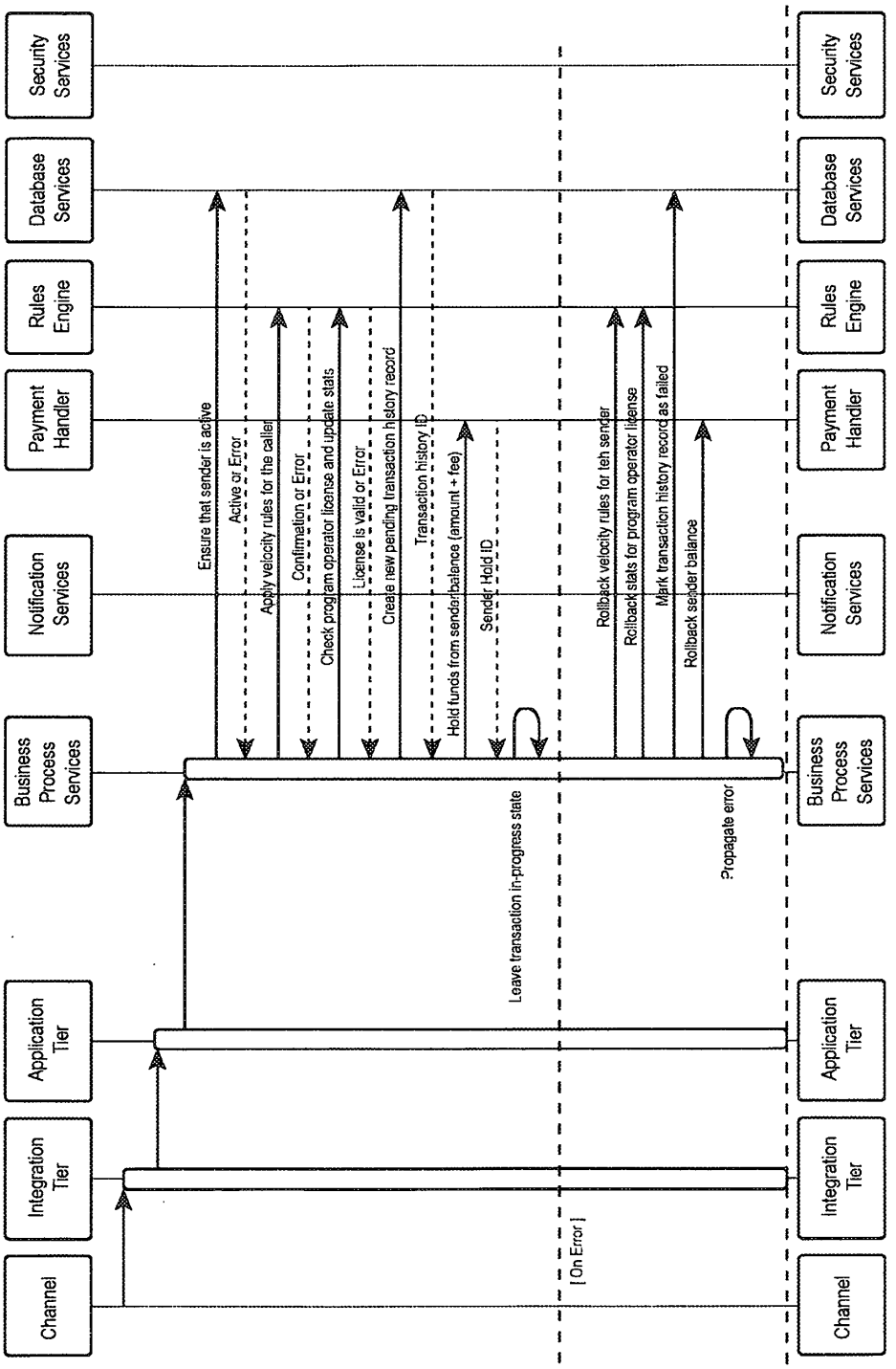


Figure 21F

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 224 of 381

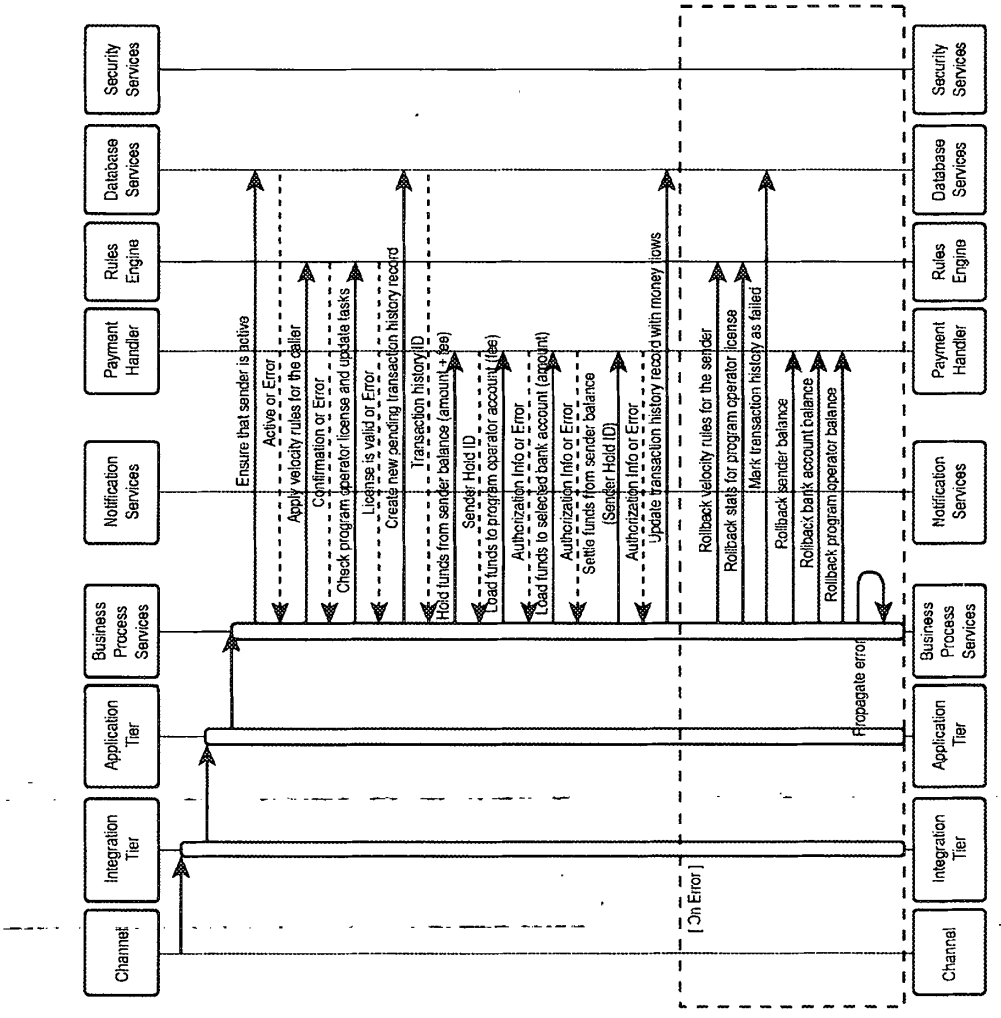


Figure 21G

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 225 of 381

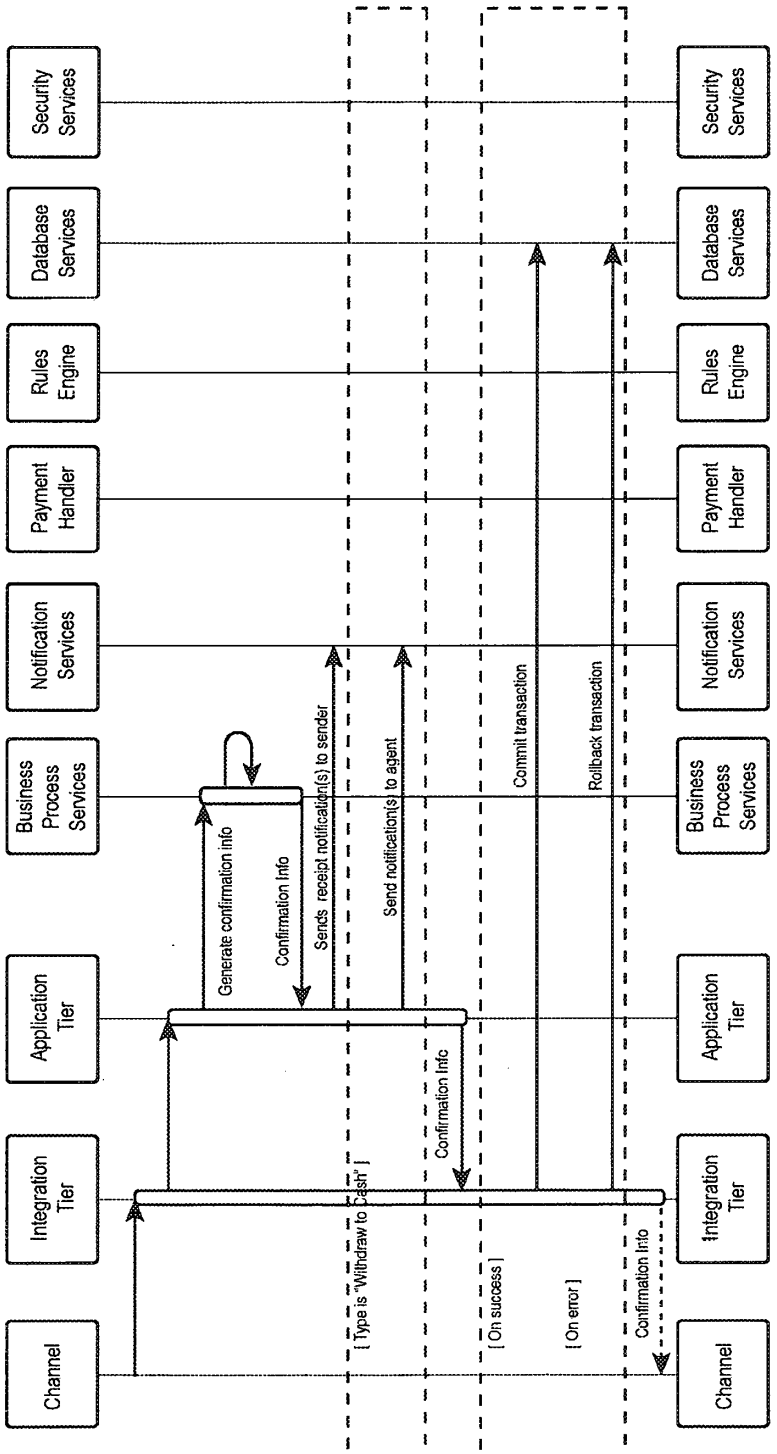


Figure 21H

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 226 of 381

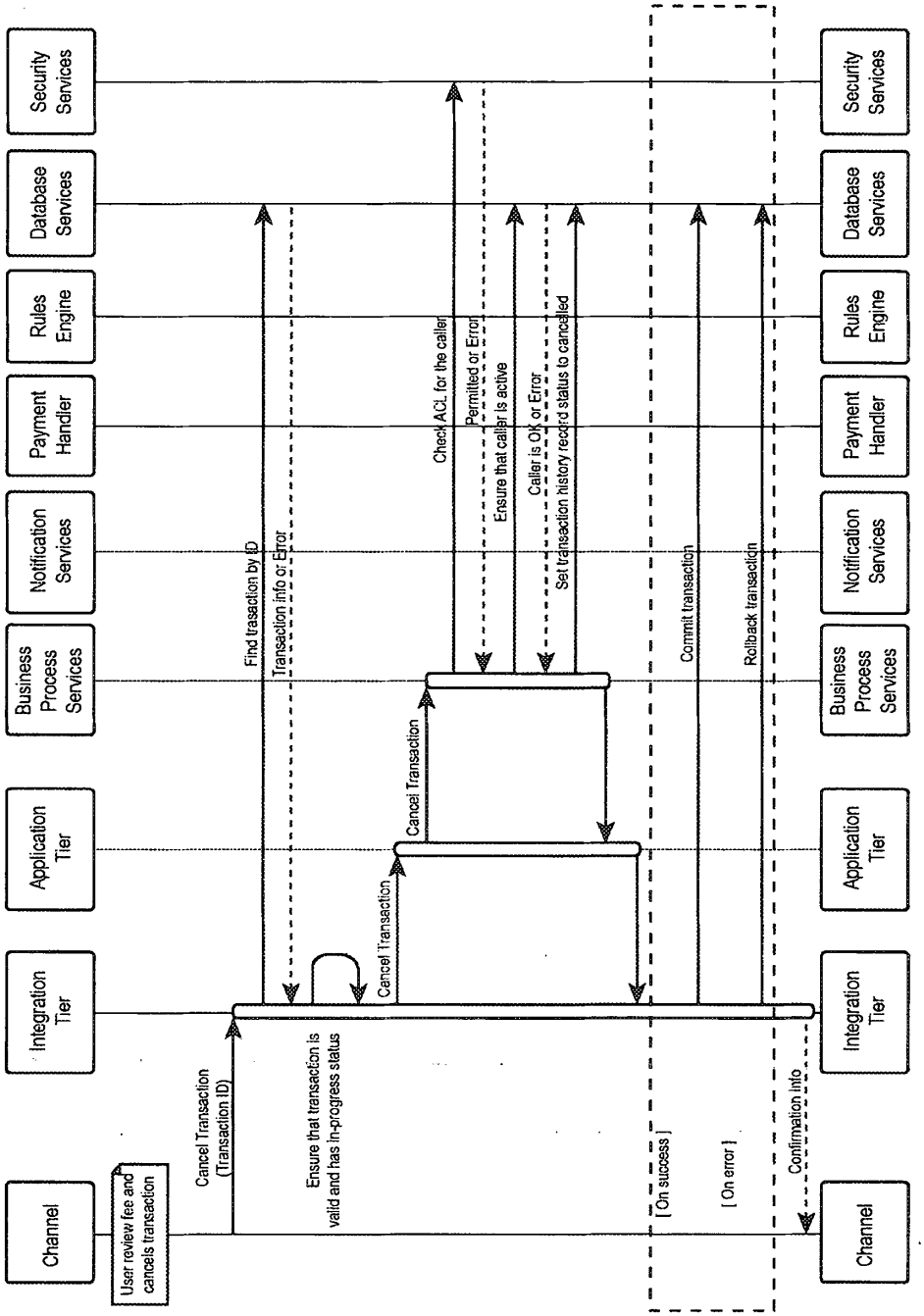


Figure 21I

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 227 of 381

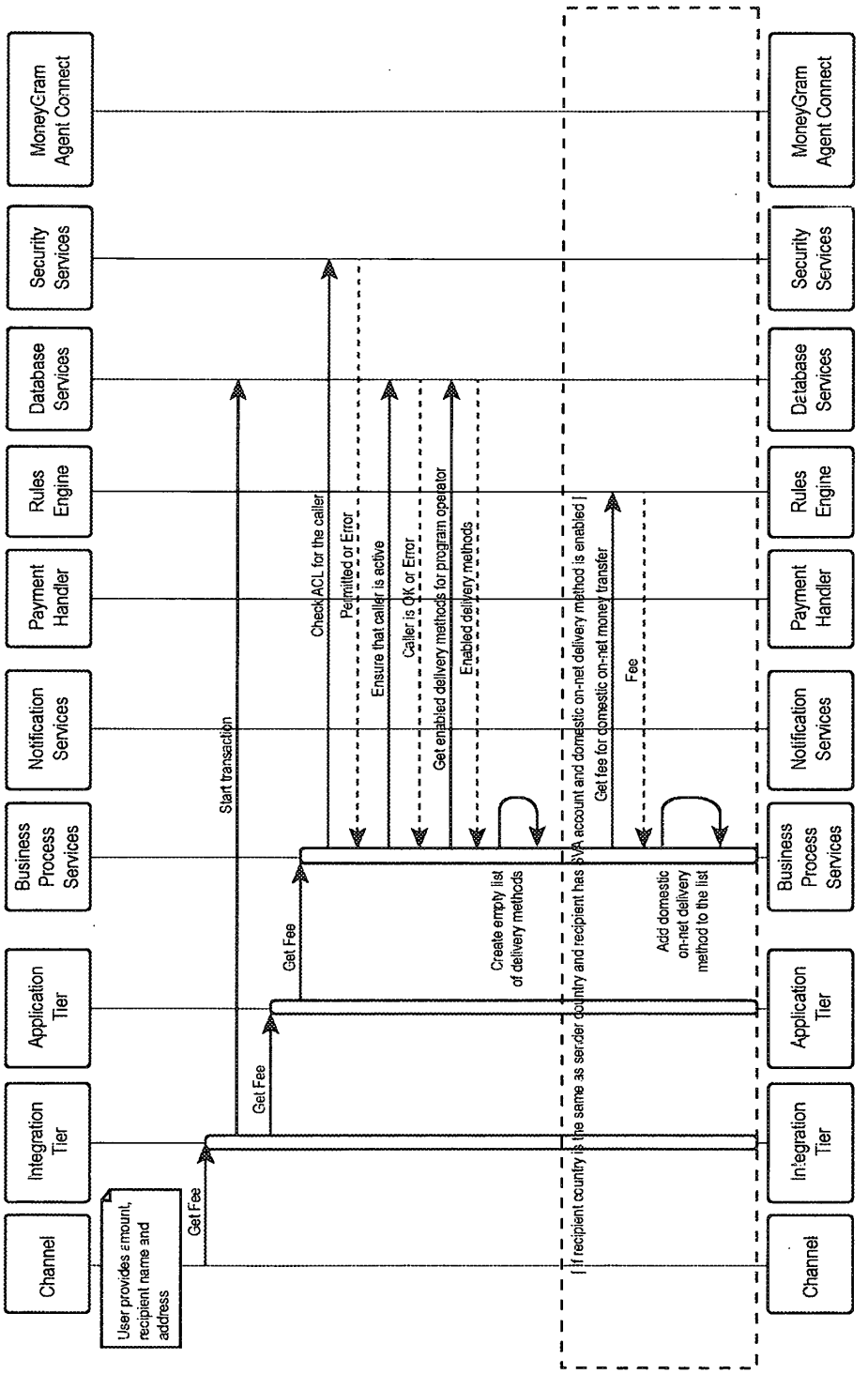


Figure 22A

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 228 of 381

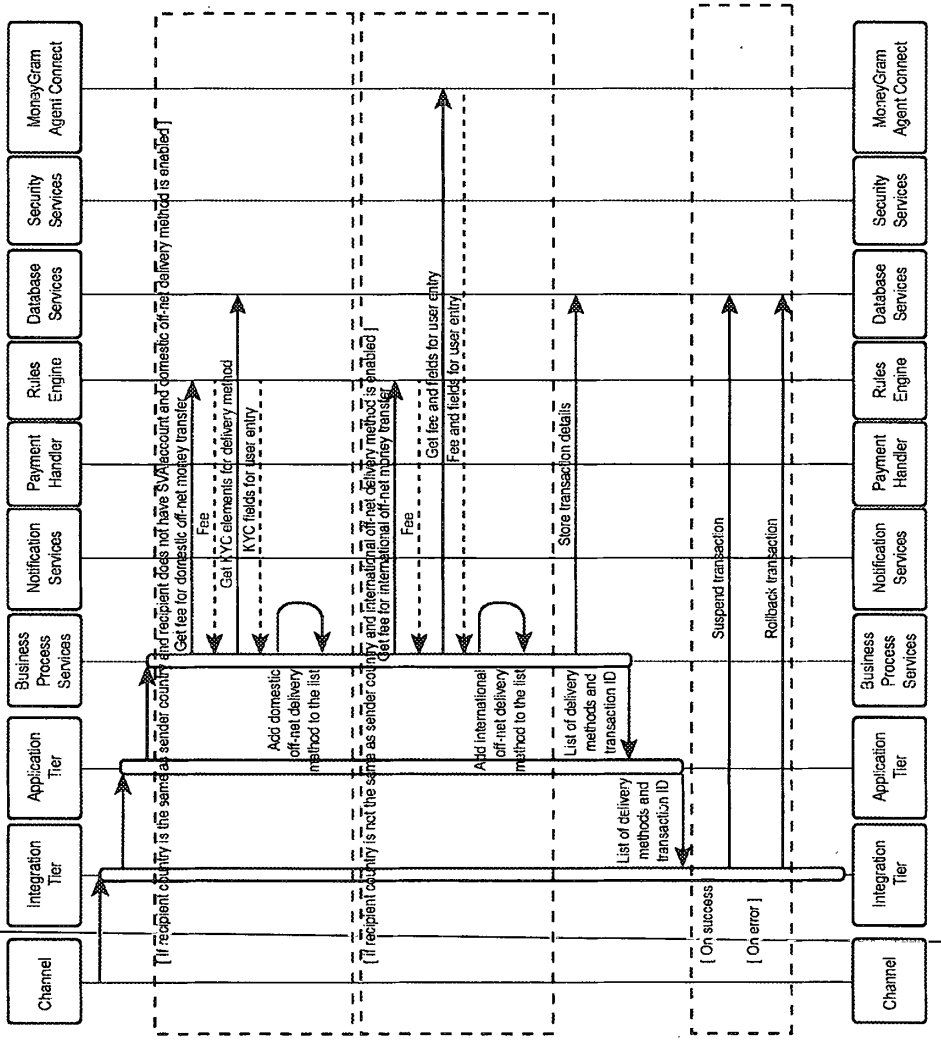


Figure 22B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 229 of 381

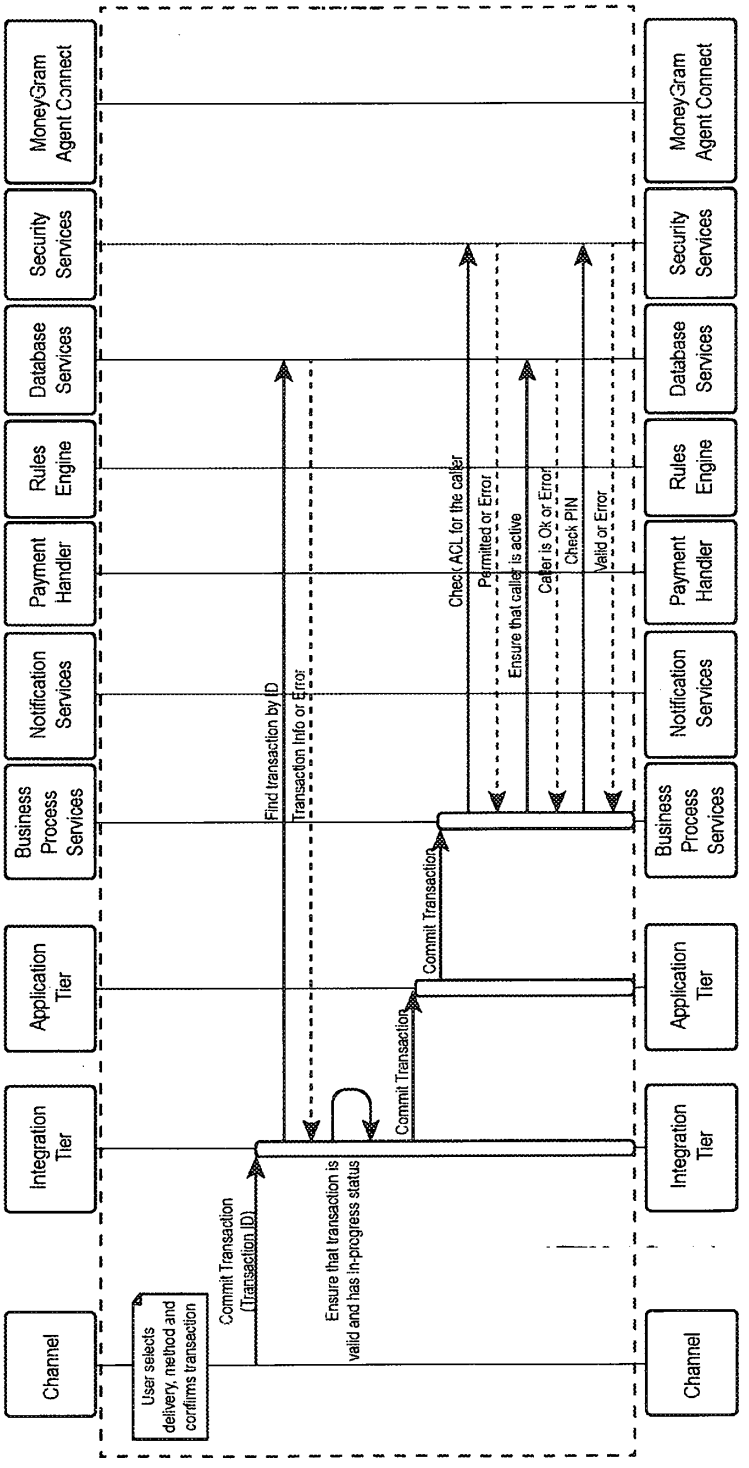


Figure 22C

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 230 of 381

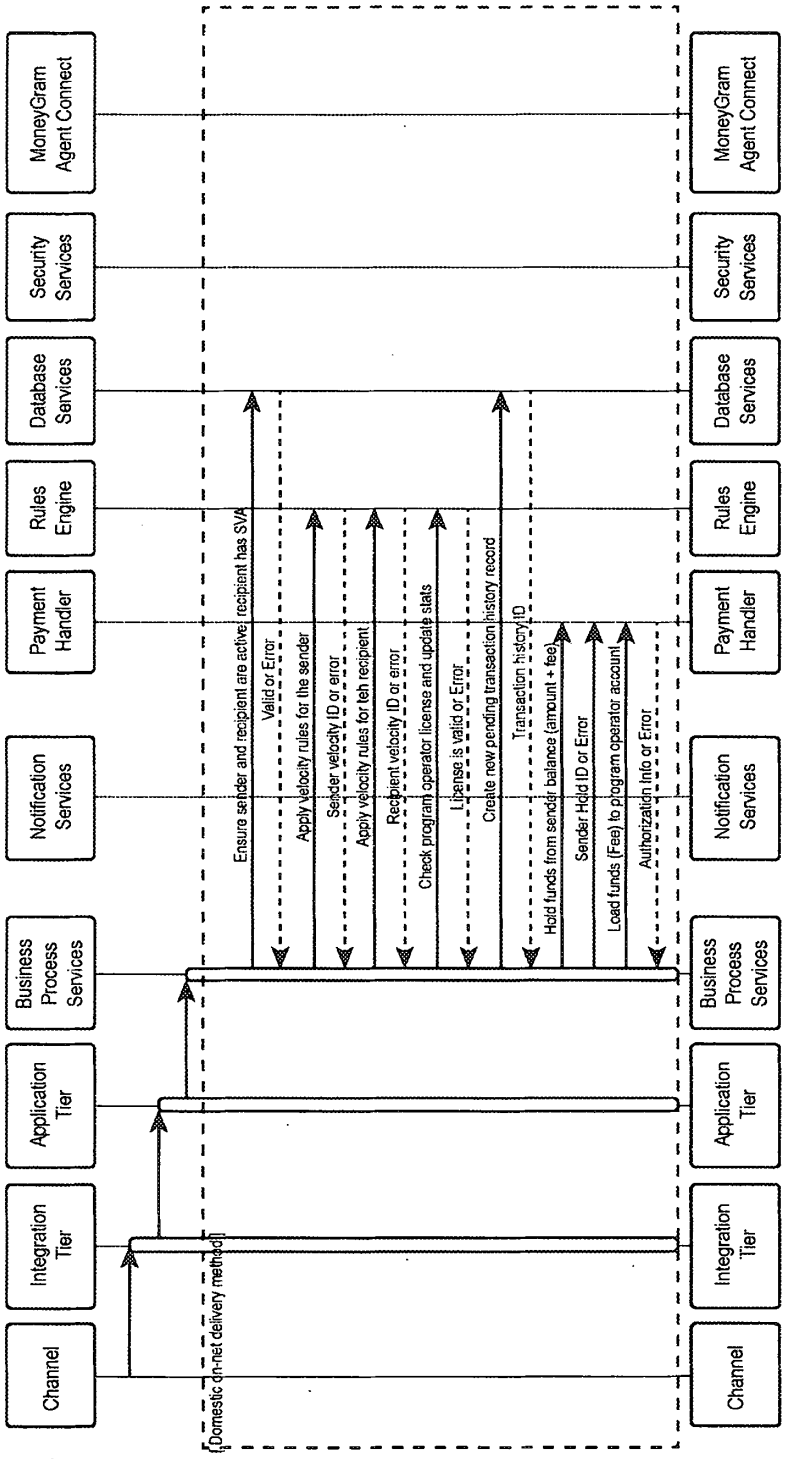


Figure 22D

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 231 of 381

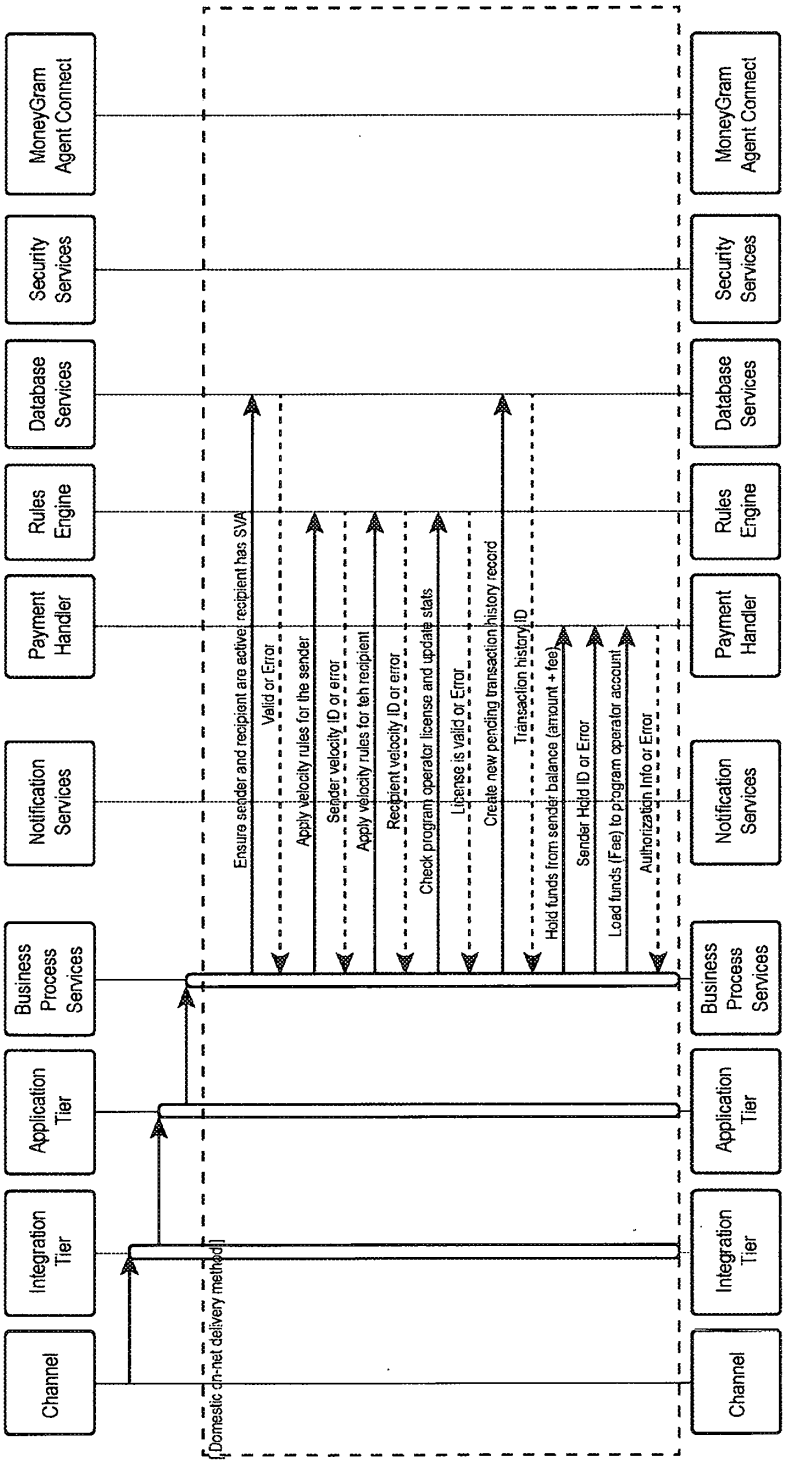


Figure 22E

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 232 of 381

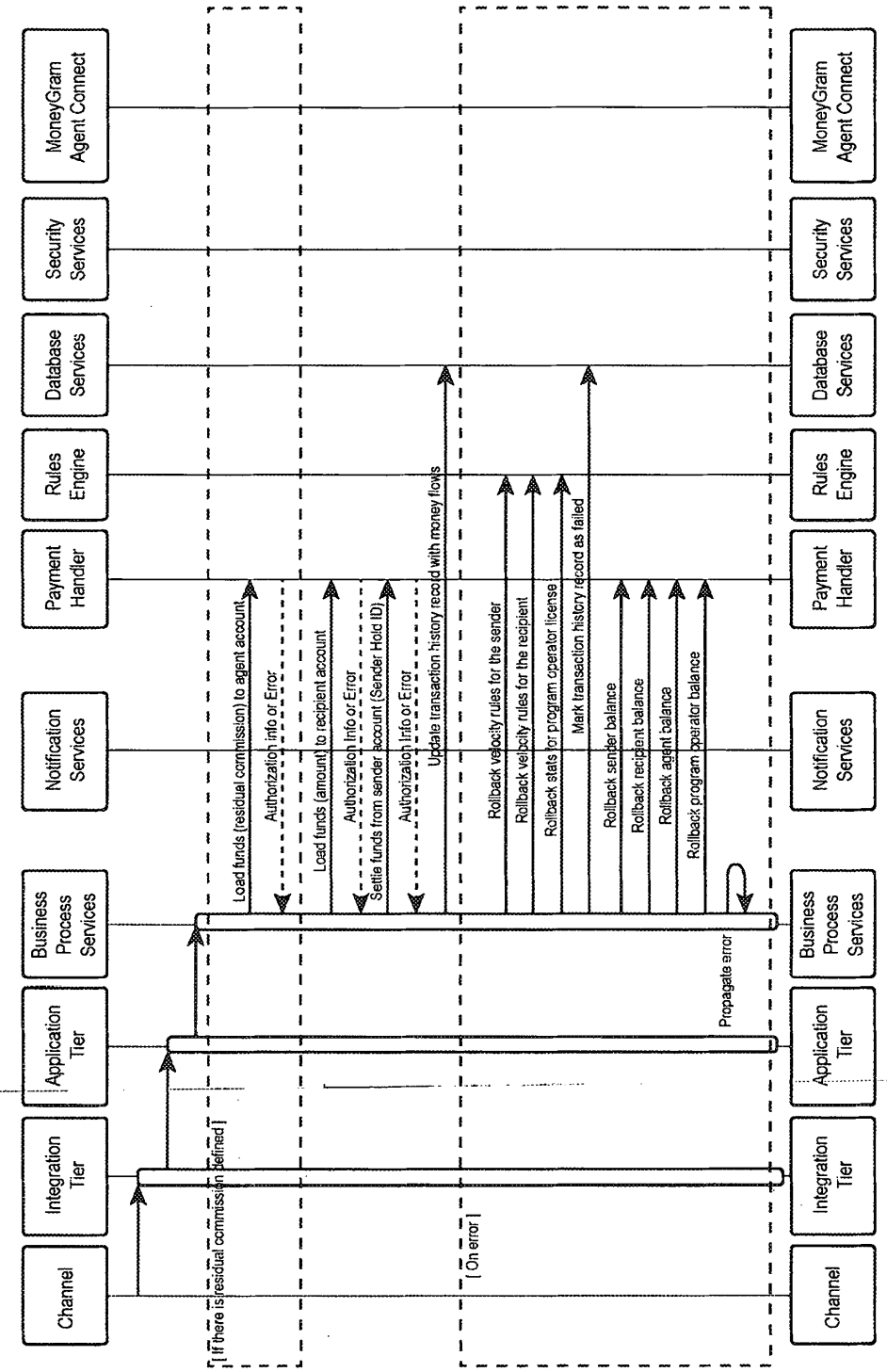


Figure 22F

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 233 of 381

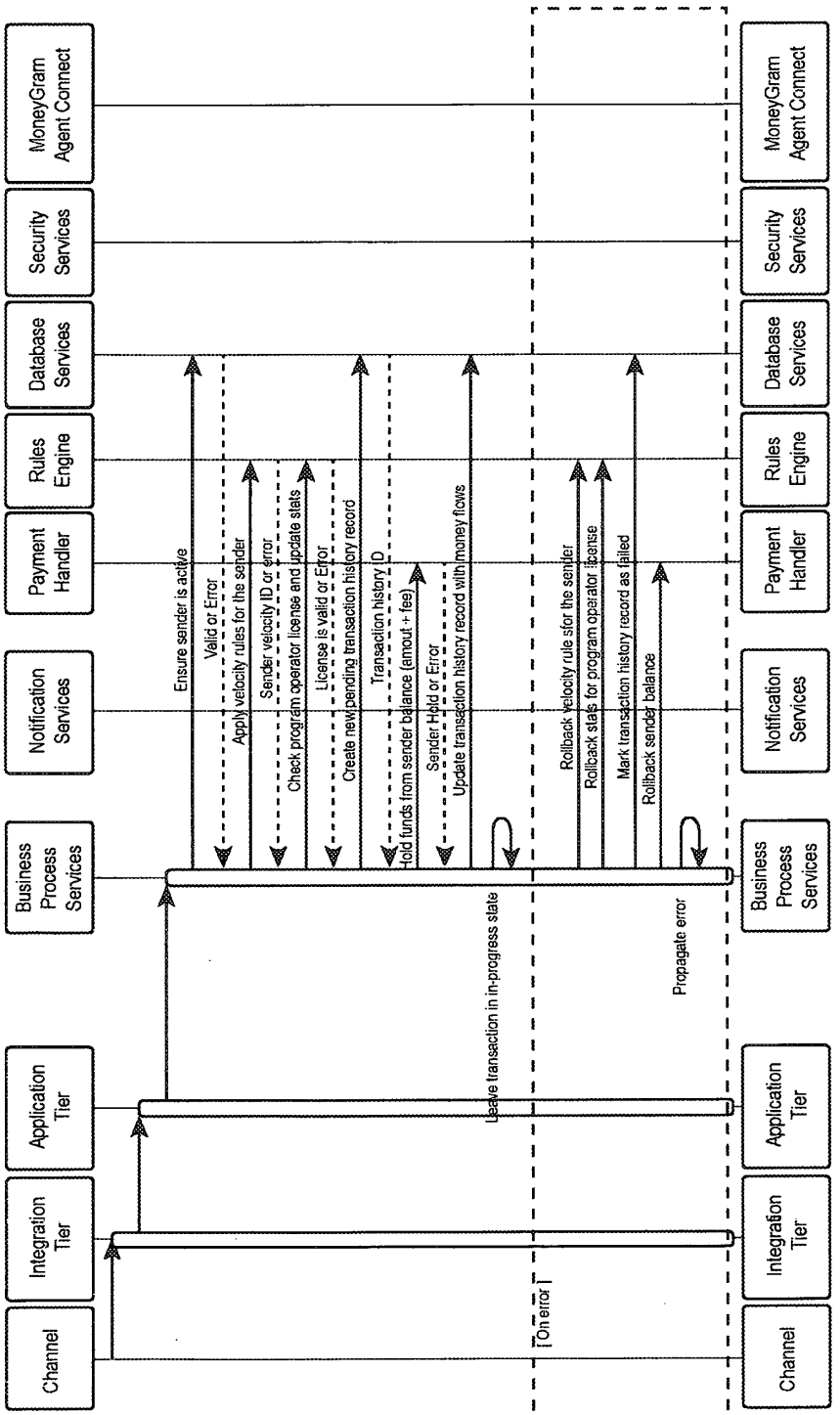


Figure 22G

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 234 of 381

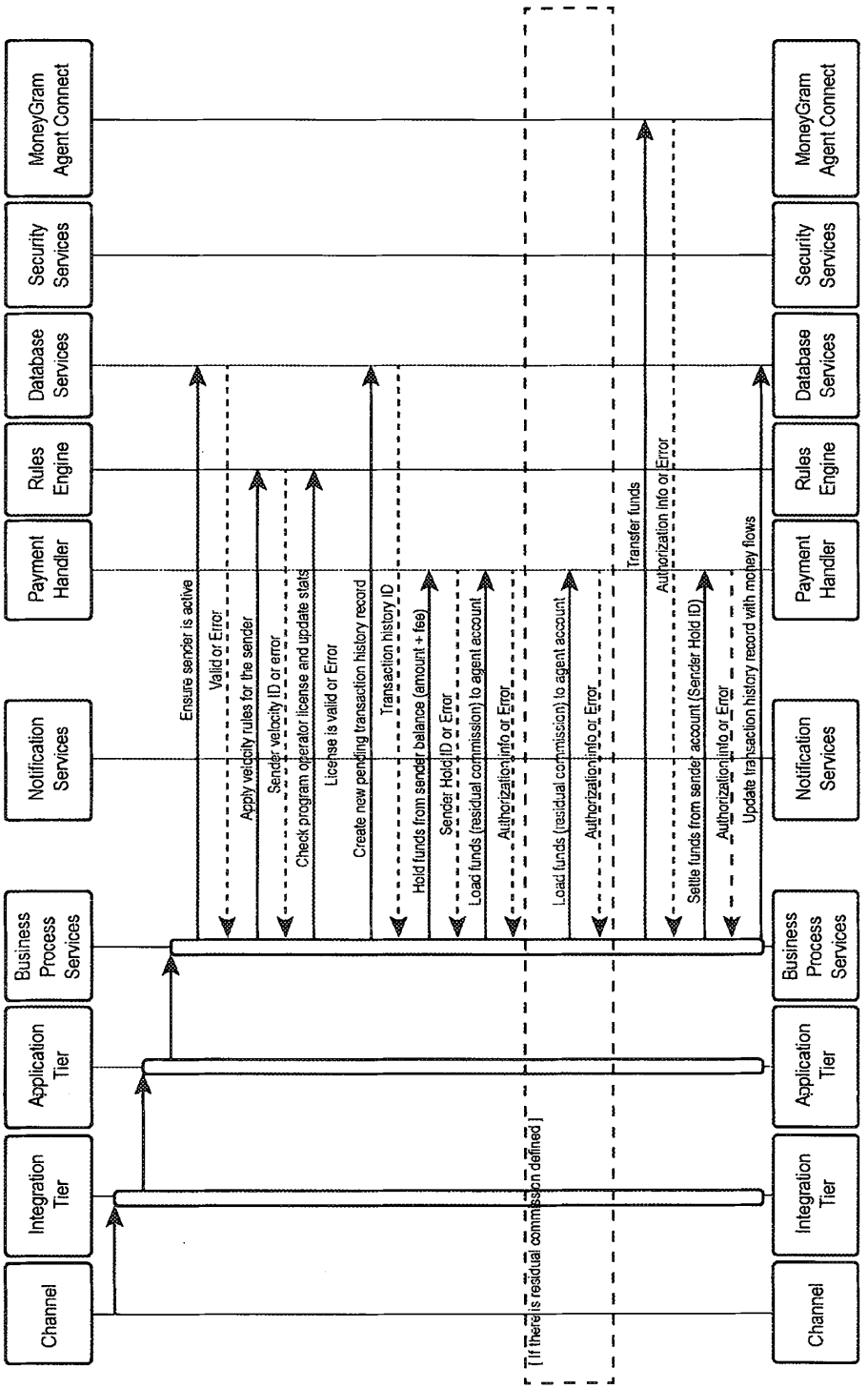


Figure 22H

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 235 of 381

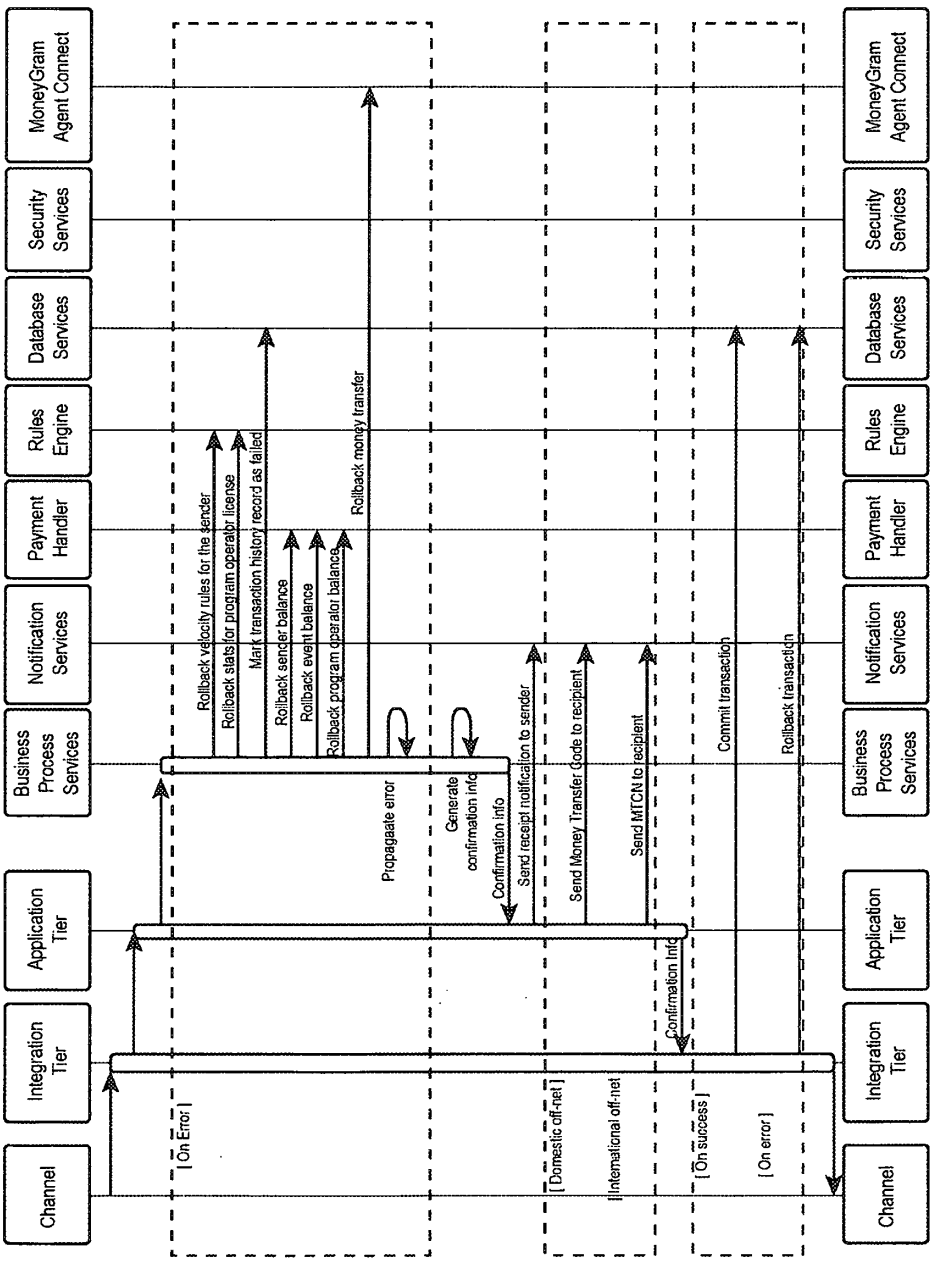


Figure 22I

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 236 of 381

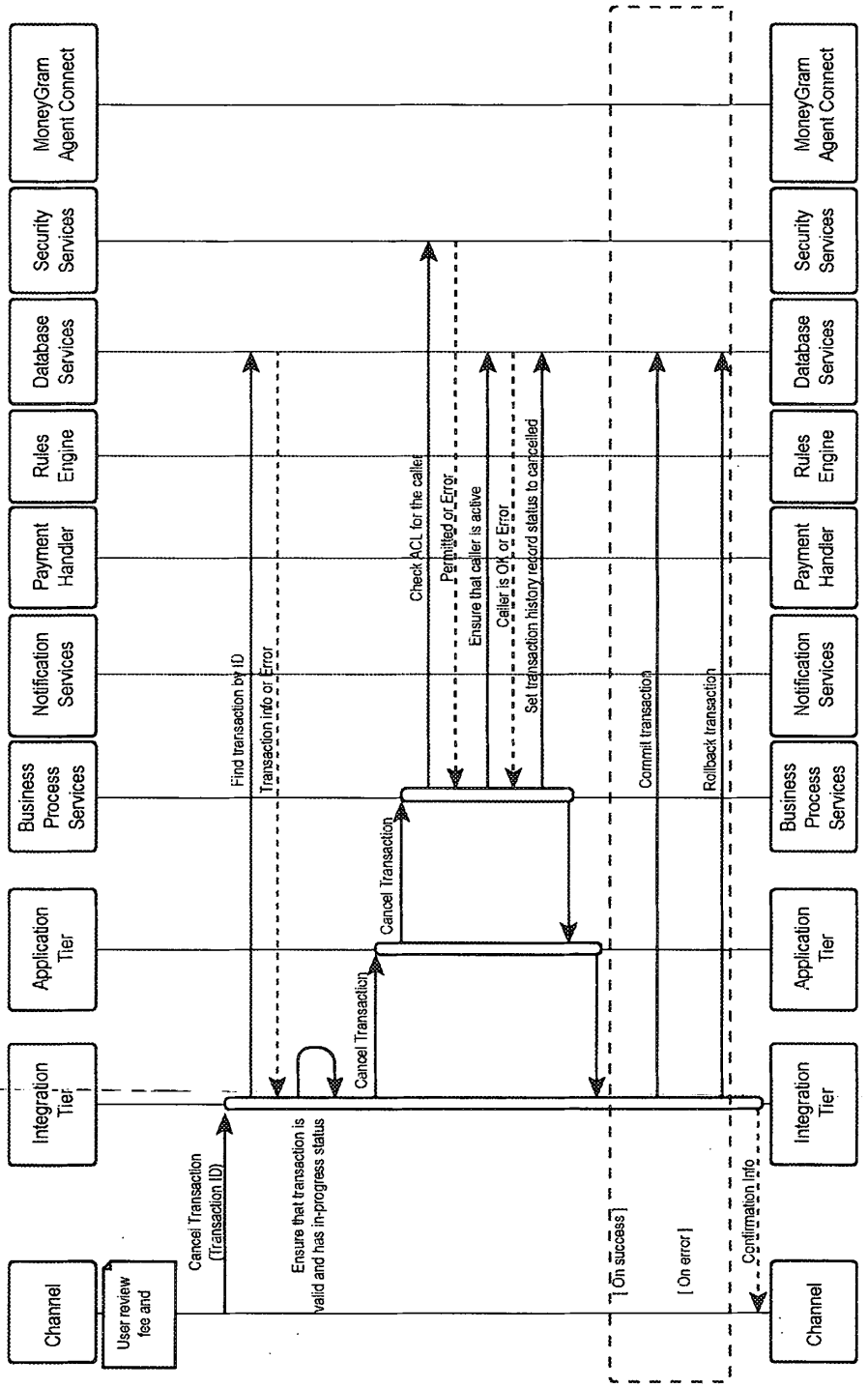


Figure 22J

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 237 of 381

MONETARY TRANSACTION SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 15/809,872, filed Nov. 10, 2017, entitled "Monetary Transaction System", which is a continuation of U.S. patent application Ser. No. 15/201,152, now issued as U.S. Pat. No. 9,892,386, filed Jul. 1, 2016, entitled "Monetary Transaction System", which is a continuation of U.S. patent application Ser. No. 14/213,543, filed Mar. 14, 2014, entitled "Monetary Transaction System", which is a continuation of U.S. patent application Ser. No. 13/964,707, filed Aug. 12, 2013, entitled "Monetary Transaction system", which application is a continuation of U.S. patent application Ser. No. 13/484,199 now issued as U.S. Pat. No. 8,538,845, filed May 30, 2012, entitled "Monetary Transaction System", which application claims priority to and the benefit of U.S. Provisional Application Ser. No. 61/522,099, filed on Aug. 10, 2011, entitled "Mobile Wallet Platform", and U.S. Provisional Application Ser. No. 61/493,064, filed on Jun. 3, 2011, entitled "Mobile Wallet Platform". All of the aforementioned applications are incorporated by reference herein in their entirety.

BACKGROUND

Mobile phones and other digital devices have become increasingly popular in recent years. Many mobile device users use their devices to perform countless different daily tasks. For instance, mobile devices allow users to check email, send and receive instant messages, check calendar items, take notes, set up reminders, browse the internet, play games or perform any number of different things using specialized applications or "apps". These applications allow mobile devices to communicate with other computer systems and perform a wide variety of network-connected tasks previously not possible with a mobile device.

BRIEF SUMMARY

Embodiments described herein are directed to monetary transaction system for conducting monetary transactions between transaction system subscribers and other entities. In one embodiment, the monetary transaction system includes a mobile device configured to run a monetary transaction system application. The monetary transaction system also includes a monetary transaction system subscriber that has a profile with the system. The subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system. The system further includes a monetary transaction system processor that performs the transactions specified by the subscriber. Performing these transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile.

The monetary transaction system also includes at least one entity that is to be involved in the specified transaction, where the entity has a profile with the monetary transaction system. This entity may be a person, a retail store, an agent or other entity. The subscriber may have access to a bank account, or may be an "unbanked user" that does not have access to a bank account. Each of the terms included above will be described in greater detail below in conjunction with the drawings.

The monetary transaction system may be used for many different tasks including enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a mobile wallet, adding a debit or credit card account to a mobile wallet, depositing funds in a mobile wallet, withdrawing funds from a mobile wallet, paying bills from a mobile wallet, topping up a prepaid mobile account through a mobile wallet, transferring funds through a mobile wallet (nationally or internationally), making in-store purchases using a mobile wallet, and various other tasks as described herein below.

This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

Additional features and advantages will be set forth in the description which follows, and in part will be apparent to one of ordinary skill in the art from the description, or may be learned by the practice of the teachings herein. Features and advantages of embodiments described herein may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. Features of the embodiments described herein will become more fully apparent from the following description and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

To further clarify the above and other features of the embodiments described herein, a more particular description will be rendered by reference to the appended drawings. It is appreciated that these drawings depict only examples of the embodiments described herein and are therefore not to be considered limiting of its scope. The embodiments will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

FIG. **1** illustrates a monetary transaction system architecture in which embodiments described herein may operate.

FIG. **2** illustrates an alternate example embodiment of a monetary transaction system.

FIG. **3** illustrates an example data flow for performing a subscriber deposit via a mobile wallet.

FIG. **4** illustrates an example data flow for performing a subscriber withdrawal via a mobile wallet.

FIGS. **5**A and **5**B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber eMoney transfers via a mobile wallet, respectively.

FIGS. **6**A and **6**B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber international eMoney transfers via a mobile wallet, respectively.

FIG. **7** illustrates an example data flow for performing a subscriber airtime purchase via a mobile wallet.

FIG. **8** illustrates an example data flow for performing a subscriber-initiated bill pay via a mobile wallet.

FIG. **9** illustrates an example data flow for performing a subscriber-initiated retail purchase via a mobile wallet.

FIGS. **10**A and **10**B illustrate example data flows for requesting and repaying micro-loans via a mobile wallet, respectively.

FIG. **11**A illustrates an example data flow of a subscriber receiving a direct deposit via a mobile wallet.

FIG. **11**B illustrates an example data flow of a subscriber receiving a governmental welfare payment via a mobile wallet.

FIG. **12**A illustrates an example data flow of an agent administrator distributing eMoney via a mobile wallet.

FIG. **12**B illustrates an example data flow of an agent company making a deposit using a mobile wallet.

FIG. **13** illustrates an example data flow of an agent company making a withdrawal using a mobile wallet.

FIG. **14** illustrates an example data flow of a subscriber making a deposit at an agent branch using a mobile wallet.

FIG. **15** illustrates an example data flow of a subscriber making a deposit with a non-agent using a mobile wallet.

FIG. **16** illustrates an example data flow of a subscriber making a withdrawal with an agent using a mobile wallet.

FIG. **17**A illustrates an example data flow of a subscriber making a withdrawal from an ATM using a mobile wallet.

FIG. **17**B illustrates an example data flow of a subscriber-to-subscriber money transfer using a mobile wallet.

FIG. **17**C illustrates an example data flow of a subscriber-to-non-subscriber money transfer using a mobile wallet.

FIG. **18**A illustrates an example data flow of a subscriber-to-subscriber international money transfer using a mobile wallet.

FIG. **18**B illustrates an example data flow of a subscriber-to-non-subscriber international money transfer using a mobile wallet.

FIG. **19**A illustrates an example data flow of a subscriber-to-subscriber international money transfer using a mobile wallet.

FIG. **19**B illustrates an example data flow of a non-subscriber-to-subscriber international money transfer using a mobile wallet.

FIG. **20**A illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **20**B illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **20**C illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **20**D illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **20**E illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **20**F illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **21**A illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **21**B illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **21**C illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **21**D illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **21**E illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **21**F illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **21**G illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **21**H illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **21**I illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **22**A illustrates a flow chart of actions in accordance with disclosed embodiments. FIG. **22**B illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **22**C illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **22**D illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **22**E illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **22**F illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **22**G illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **22**H illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **22**I illustrates a flow chart of actions in accordance with disclosed embodiments.

FIG. **22**J illustrates a flow chart of actions in accordance with disclosed embodiments.

DETAILED DESCRIPTION

Embodiments described herein are directed to monetary transaction system for conducting monetary transactions between transaction system subscribers and other entities. In one embodiment, the monetary transaction system includes a mobile device configured to run a monetary transaction system application. The monetary transaction system also includes a monetary transaction system subscriber that has a profile with the system. The subscriber indicates, via the monetary transaction system application, one or more specified transactions that are to be performed using the monetary transaction system. The system further includes a monetary transaction system processor that performs the transactions specified by the subscriber. Performing these transactions includes communicating with a monetary transaction database to determine whether the transaction is permissible based on data indicated in the subscriber's profile.

The monetary transaction system also includes at least one entity that is to be involved in the specified transaction, where the entity has a profile with the monetary transaction system. This entity may be a person, a retail store, an agent or other entity. The subscriber may have access to a bank account, or may be an "unbanked user" that does not have access to a bank account. Each of the terms included above will be described in greater detail below in conjunction with the drawings.

The monetary transaction system may be used for many different tasks including enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a mobile wallet, adding a debit or credit card account to a mobile wallet, depositing funds in a mobile wallet, withdrawing funds from a mobile wallet, paying bills from a mobile wallet, topping up a prepaid mobile account through a mobile wallet, transferring funds through a mobile wallet (nationally or internationally), making in-store purchases using a mobile wallet, and various other tasks as described herein below.

The following discussion now refers to a number of methods and method steps or acts that may be performed. It should be noted, that although the method steps may be discussed in a certain order or illustrated in a flow chart as occurring in a particular order, no particular ordering is necessarily required unless specifically stated, or required because a step is dependent on another step being completed prior to the step being performed.

Embodiments of the mobile transaction system or "mobile wallet platform" described herein may comprise or utilize a special purpose or general-purpose computer including

computer hardware, such as, for example, one or more processors and system memory, as discussed in greater detail below. Embodiments described herein also include physical and other computer-readable media for carrying or storing computer-executable instructions and/or data structures. Such computer-readable media can be any available media that can be accessed by a general purpose or special purpose computer system. Computer-readable media that store computer-executable instructions in the form of data are computer storage media. Computer-readable media that carry computer-executable instructions are transmission media. Thus, by way of example, and not limitation, embodiments described herein can comprise at least two distinctly different kinds of computer-readable media: computer storage media and transmission media.

Computer storage media includes RAM, ROM, EEPROM, CD-ROM, solid state drives (SSDs) that are based on RAM, Flash memory, phase-change memory (PCM), or other types of memory, or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store desired program code means in the form of computer-executable instructions, data or data structures and which can be accessed by a general purpose or special purpose computer.

A "network" is defined as one or more data links and/or data switches that enable the transport of electronic data between computer systems and/or modules and/or other electronic devices. When information is transferred or provided over a network (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a transmission medium. Transmission media can include a network which can be used to carry data or desired program code means in the form of computer-executable instructions or in the form of data structures and which can be accessed by a general purpose or special purpose computer. Combinations of the above should also be included within the scope of computer-readable media.

Further, upon reaching various computer system components, program code means in the form of computer-executable instructions or data structures can be transferred automatically from transmission media to computer storage media (or vice versa). For example, computer-executable instructions or data structures received over a network or data link can be buffered in RAM within a network interface module (e.g., a network interface card or "NIC"), and then eventually transferred to computer system RAM and/or to less volatile computer storage media at a computer system. Thus, it should be understood that computer storage media can be included in computer system components that also (or even primarily) utilize transmission media.

Computer-executable (or computer-interpretable) instructions comprise, for example, instructions which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. The computer executable instructions may be, for example, binaries, intermediate format instructions such as assembly language, or even source code. Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the described features or acts described above. Rather, the described features and acts are disclosed as example forms of implementing the claims.

Those skilled in the art will appreciate that various embodiments may be practiced in network computing environments with many types of computer system configurations, including personal computers, desktop computers, laptop computers, message processors, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, mobile telephones, PDAs, tablets, pagers, routers, switches, and the like. Embodiments described herein may also be practiced in distributed system environments where local and remote computer systems that are linked (either by hardwired data links, wireless data links, or by a combination of hardwired and wireless data links) through a network, each perform tasks (e.g. cloud computing, cloud services and the like). In a distributed system environment, program modules may be located in both local and remote memory storage devices.

In this description and the following claims, "cloud computing" is defined as a model for enabling on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). The definition of "cloud computing" is not limited to any of the other numerous advantages that can be obtained from such a model when properly deployed.

For instance, cloud computing is currently employed in the marketplace so as to offer ubiquitous and convenient on-demand access to the shared pool of configurable computing resources. Furthermore, the shared pool of configurable computing resources can be rapidly provisioned via virtualization and released with low management effort or service provider interaction, and then scaled accordingly.

A cloud computing model can be composed of various characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service, and so forth. A cloud computing model may also come in the form of various service models such as, for example, Software as a Service ("SaaS"), Platform as a Service ("PaaS"), and Infrastructure as a Service ("IaaS"). The cloud computing model may also be deployed using different deployment models such as private cloud, community cloud, public cloud, hybrid cloud, and so forth. In this description and in the claims, a "cloud computing environment" is an environment in which cloud computing is employed.

Additionally or alternatively, the functionally described herein can be performed, at least in part, by one or more hardware logic components. For example, and without limitation, illustrative types of hardware logic components that can be used include Field-programmable Gate Arrays (FPGAs), Program-specific Integrated Circuits (ASICs), Program-specific Standard Products (ASSPs), System-on-a-chip systems (SOCs), Complex Programmable Logic Devices (CPLDs), and other types of programmable hardware.

Still further, system architectures described herein can include a plurality of independent components that each contribute to the functionality of the system as a whole. This modularity allows for increased flexibility when approaching issues of platform scalability and, to this end, provides a variety of advantages. System complexity and growth can be managed more easily through the use of smaller-scale parts with limited functional scope. Platform fault tolerance is enhanced through the use of these loosely coupled modules. Individual components can be grown incrementally as business needs dictate. Modular development also translates

to decreased time to market for new functionality. New functionality can be added or subtracted without impacting the core system.

Various terminology will be used herein to describe the monetary transaction system (also referred to as a "mobile wallet platform", "mobile wallet program" or "mobile wallet transaction system"). The term "agent" is used to refer to an individual with mobile financial services (mFS) transaction system tools and training to support specific mFS functions. These mFS functions include subscriber registration and activation, and the deposit and withdrawal of funds from the mFS transaction system. Agents are representatives of the mFS transaction system or "program". Agents can be employees or contractors of the program provider, or other companies and organizations that partner with the program provider to provide these services themselves. Agents may be found in every facet of a typical economy, and may include large retailers, mobile network operators (MNO) airtime sales agents, gas stations, kiosks, or other places of business.

The mobile wallet platform includes a mobile wallet application, web interface or some other type of functionality that allows the user to interact with the mFS platform using their mobile device. The mobile wallet application may include a subscriber identity module (SIM) application, an Unstructured Supplementary Service Data (USSD) application, a smartphone application, a web application, a mobile web application, a Wireless Application Protocol (WAP) application, a Java 2 Platform, Micro Edition (J2ME) application, a tablet application or any other type of application or interface that provides tools for the agent to register, activate, and offer other services to the mFS subscriber.

As used herein, a mobile wallet application is a mobile wallet application installed on a SIM card. A USSD application is an application that implements USSD for various functionality including prepaid callback service, location-based content services, menu-based information services and other mobile wallet platform services. A web application is one that implements or uses the internet to provide mobile wallet platform functionality. A mobile web application is similar to a web application, but is tailored for mobile devices. A WAP application is one that uses the wireless application protocol to communicate with the mobile wallet platform to provide the platform's functionality. A J2ME application is an application developed in Java and is designed to provide mobile wallet functionality on a variety of different hardware. A tablet application is an application specifically designed for a touchscreen-based tablet that provides mobile wallet platform functionality for tablet devices, and as part of configuring the phone on the network. Any of these applications (or any combination thereof) may be provided on the user's mobile device. This functionality can also be made available on a retail point of sale (POS) system or web site.

The term "agent administrator" refers to an individual with mFS program tools and training to administrate the allocation of funds to agent branches (e.g. retail locations). As agents perform mFS transactions with subscribers, such as depositing and withdrawing money, the agents are adding and removing money from their own accounts. If there are insufficient funds in the agent's account to complete a transaction, additional money will need to be transferred from the agent company's master account to that agent branch account to cover that transaction. An agent administrator is responsible for these funds transfers. Any of the applications referred to above may be configured to provide tools used by the agent administrator to view the agent company balance, view the agent branch balances, and transfer funds into and out of agent branch mobile wallets. This functionality can also be made available on a website for easier access.

The term "agent administrator mobile wallet application" refers to a software program or application installed on the agent administrator's terminal in the agent administrator's mobile device (such as a mobile phone or tablet). This software application provides the agent administrator the ability to securely perform agent administrator functions such as querying the agent company account balance or transferring funds into and out of agent branch accounts. The agent administrator's mobile wallet application may be installed on a global system for mobile communications (GSM) SIM card (or on any other type of SIM card), and may be accessed using a GSM mobile phone. The agent administrator's application may also be installed on a code division multiple access (CDMA) mobile phone, a 3G, 4G, 4G LTE (Long Term Evolution) or other wireless carrier standard. The application may, additionally or alternatively, be installed directly on the agent administrator's mobile device. The application communicates with the mFS transaction system using binary and/or text short message service (SMS) messages. A wireless service provider or MNO provides the GSM SMS network infrastructure on which the mFS platform operates.

In some embodiments, the mFS platform application may utilize triple data encryption standard (3DES) encryption (or some other type of encryption), encrypted message signing, and password security on some or all of its communications with the mFS transaction system in order to ensure that the transactions are properly secured and authenticated.

The term "agent branch" refers to any location where an agent provides support for subscriber services of the mFS platform. Funds are allocated by the agent administrator from the agent company's main account to each agent branch to fund the subscriber mFS functions such as depositing or withdrawing cash, in-store purchases, bill payments, prepaid airtime top-ups and money transfers. In some cases, multiple agents may work in a single branch. However, at least in some cases, monetary funds are allocated to from the agent company's main account on a per branch basis.

The term "agent branch account balance" refers to the amount of money residing in a particular agent branch account at a given time. Funds can be deposited into the branch account by the agent administrator, or the funds can come from participating in subscriber mFS transactions such as depositing or withdrawing cash from the subscriber's mobile wallet accounts, or making retail purchases with the mobile wallet.

Each agent branch is to maintain a balance in their branch account. This applies more strongly in countries where mFS program and financial services infrastructure is still developing. In cases where real-time processing of financial transactions including card processing is not practical, subscribers leverage the applications on their mobile phones to submit transactions and conduct business with retailers, businesses, and other subscribers. The mFS platform manages the balance of mobile wallet accounts for each subscriber as value is transferred from one mobile wallet to another (e.g. from a subscriber's mobile wallet to an agent's mobile wallet in payment for goods or services). This value is referred to herein as "eMoney".

As subscribers conduct business with mFS agents, they deposit or withdraw cash from their mobile wallet accounts. Virtual or eMoney credits are transferred between the sub-

scriber's mobile wallet account and the agent branch's account as a form of currency to support the transaction. As agents accept cash into their cash register by mFS subscribers, they transfer the equivalent amount of eMoney credits into the mFS subscriber's mobile wallet account. For instance, if an mFS subscriber gives an mFS agent $10 to deposit into the subscriber's mobile wallet account, the agent would place the cash into his register and transfer $10 from the agent branch's eMoney account into the subscriber's mobile wallet account. While the agent acquired $10 in his register, he transferred out $10 of eMoney credits from his branch eMoney account.

In some embodiments, in countries with more developed economies, it may be beneficial to use program-issued pre-paid debit cards, pre-paid access accounts, stored value accounts or gift cards to conduct business along with the added convenience of card processing networks such as Cirrus, STAR, or Visa for POS and automated teller machine (ATM) functionality. Agents, particularly those in retail outlets and kiosks, can still support subscribers with deposits, withdrawals, and other transfers, but in this case bank external card processors manage the mobile wallet and branch account balances and provide the real-time transfer of funds.

The term "agent branch ledger" refers to a written (or electronic) ledger maintained by the mFS platform. Agent branch transactions are performed on the agent's and subscriber's mobile phones where an electronic record of the transaction is generated and stored on the mFS platform. These electronic transactions are then reconciled with agent branch ledgers to ensure the security and integrity of the transaction. Agent branch ledgers are printed or electronic transaction logs that are distributed to the agent branch locations in hard copy form to serve as a backup record to the electronic transactions.

The term "agent company" refers to a business that registers to participate in the mFS program as a partner of the mFS program provider or owner. The agent company has one or more agent branches which conduct mFS business with mFS program subscribers. In some cases, the agent company may be referred to as a distributor or retailer.

The term "agent company account balance" refers to the sum of the funds deposited at a "partner bank" (defined below) by the agent company to fund the agent company's daily transactions. The funds in the agent company account are then distributed to agent branches by the agent company's agent administrator to conduct everyday business such as accepting cash deposits and cash withdrawals from mFS subscribers. This balance is sometimes referred to as the "agent company float".

An "agent manager" is a supervisor of company agents for a given company. The agent manager has the training and tools to create, delete or modify agent accounts for a company, as well as monitor the transactions performed by agents. The agent manager may have a special application or an increased level of rights to access applications features not available to other users. The special application is a program installed on the agent manager's terminal. This application provides the agent manager the ability to securely perform agent manager functions such as registering and activating new agent accounts.

The mFS agent manager application may be installed on any terminal or device. It communicates with the mFS platform using binary and/or text SMS messages. A wireless service provider or MNO provides the GSM SMS network infrastructure on which the mFS platform operates. The mFS platform mobile wallet applications may utilize 3DES encryption (or any other type of encryption), encrypted message signing, and password security on some or all of its communications with the mFS platform in order to ensure that the transactions are properly secured and authenticated.

The term "agent application" refers to an application that provides all the tools necessary for an agent to register, activate, and offer other services to the mFS subscriber. The agent application is a program installed on the agent's SIM card or otherwise installed in the agent's mobile device's memory. This application provides the agent the ability to securely perform agent functions such as registering and activating new subscribers and depositing and withdrawing funds from mobile wallet accounts. The mFS agent application may be installed on a GSM SIM card or mobile phone and may be accessed using a GSM or CDMA mobile phone. A wireless service provider or MNO provides the data and SMS network infrastructure on which the mFS platform operates.

The terms "mFS platform", "mobile wallet platform" and "monetary transaction system" refer to an overall platform or ecosystem of different components that work together to provide the various functions described herein on a global scale. At least some of the various logic components include the following: the application. The "mobile wallet application" or "mFS application" manages the processing of incoming transactions regardless of their source. The application handles end-user authentication, transaction processing, subscriber profile management, and further manages interactions between the various platform components.

The mFS platform further includes a transaction processor. This component is used when the mFS application is implemented in a country where real-time processing of financial transactions is not practical (or not possible). The transaction processor manages the balance of mobile wallet accounts, agent accounts, and the accounts of any other program participant. The transaction processor handles balance inquiries, credits, debits, and transaction roll-backs.

The mFS platform further includes a rules engine that manages and applies the rules and policy that are defined for transactions as they are processed on the mFS platform. Rules impact transaction fees, limits, velocity limits, and commissions as well as program actor roles and permissions. Rules can be customized for each implementation. The mFS platform also includes an integration interface that manages the integration and interaction between external systems (i.e. external to the mFS platform) and the mFS platform. Connectivity to the wireless service provider's pre-paid airtime billing platform and the program partner bank, for example, are managed by the integration interface.

The mFS platform further includes a transaction database that stores the data that supports the mFS platform. This includes subscriber profiles and subscription data, transaction data and logs, and application configuration and runtime data, among other types of data. Another component of the mFS platform is a handset support service that interfaces with the wireless service provider's SMS network to allow communication between the mobile wallet applications and the back-office systems via SMS messaging or some other form of data transfer. Still further, another component of the mFS platform is a web component that provides a web interface to the mFS program participants that allows the subscriber to perform the same functions in the web interface that they would have available through their applications.

The term "bill pay company" refers to a business that signs-up to participate in the mFS transaction system. As a participant in the mFS transaction system, the company

accepts payment from mFS mobile wallet accounts, either in the form of eMoney or through periodic settlements.

At least in some embodiments, financial transactions that take place in the mFS mobile wallet platform are funded through pre-paid mobile wallet accounts. Mobile wallet platform subscribers can deposit cash into their mobile wallet account through a process referred to herein as 'cash-in'. The cash-in process is supported by mFS agents at agent branch locations. The agent accepts the cash from the subscriber and transfers the equivalent amount of eMoney to the subscriber's mobile wallet account. This process is similar to withdrawing cash from a bank account.

As mentioned above, in some embodiments, financial transactions that take place in the mobile wallet platform are funded through pre-paid mobile wallet accounts. Mobile wallet platform subscribers can withdraw cash from their mobile wallet account through a process known as "cash-out". The cash-out process is supported by mFS agents at agent branch locations. The subscriber transfers eMoney from their mobile wallet account to the agent's eMoney account. Upon receiving the eMoney, the agent gives the subscriber cash from their branch cash register.

Accounts managed on the mFS platform by the mFS eMoney transaction processor maintain the mobile wallet balance of mFS program participants including subscribers, agent branches, agent companies, and non-agent companies. eMoney is moved between Mobile Wallet accounts by the transaction processor based on mFS transaction processing. Only when transactions involving cash (i.e. depositing or withdrawing funds from the mFS program) or the movement of money from mFS participants to non-mFS program participants are funds moved from the master bank accounts.

As subscribers, agents, and other mFS program participants conduct business in the mFS program, value is transferred from one account to the next as payment for services rendered or goods purchased. This value can be in the form of real currency or the electronic representation referred to herein as eMoney.

Among other situations, eMoney is used in mFS implementations where the real-time processing of financial transactions including card processing is not practical. The mFS platform utilizes an internal transaction processor for managing the real-time balance of mobile wallet and agent accounts as value (eMoney) is transferred from one mobile wallet to another in payment for services.

As subscribers conduct business with mFS agents, they deposit or withdraw cash from their mobile wallet accounts. Virtual or eMoney credits are transferred between the subscriber mobile wallet accounts and the agent branch accounts as a form of currency to support the transaction. As agents accept cash into their cash register by mFS subscribers, they transfer the equivalent amount of eMoney credits into the mFS subscriber's mobile wallet account. For example, if an mFS subscriber gives an mFS agent $10 to deposit into the subscriber's mobile wallet account, the agent would place the cash into his or her register, and transfer $10 from the agent branch eMoney account into the subscriber's mobile wallet account. While the agent acquired $10 in his or her register, the agent transferred-out $10 of eMoney credits from his or her branch eMoney account. This will be explained in greater detail below.

In some embodiments, employers may wish to participate in the mFS program by allowing the direct deposit of paychecks into subscribers' mobile wallet accounts. Accordingly, each payday, the user's pay is directly transferred to the subscribers' mobile wallet.

The term "know your customer" or "KYC" refers to information collected about an individual that identifies that individual. Such information is used to establish a mobile wallet account with the mobile wallet platform. Regulatory requirements in some countries require that new bank account creation must be preceded by a display of a valid government ID. These KYC regulations may vary from country to country. Accordingly, different KYC information may be requested from subscribers in different countries in order to establish a mobile wallet account.

The term micro-finance institution (MFI) refers to a lender that issues small loans. MFIs participating in the mFS program lend to mFS program subscribers and accept loan repayment either in the form of eMoney or settlements with the mFS platform provider.

The term "mFS program", like the term "mFS platform" refers to the ecosystem of companies, service providers, and subscribers that participate in providing mobile financial services to their customers. In some embodiments, there may be one mFS program implementation per country. Each program includes a program owner and operator, a program platform, a partner wireless services provider or MNO, and a partner bank.

The term "mFS program master account" refers to a bank account maintained by the mFS program partner bank to provide funds and float for the operation of the mFS platform. Depending on the type of mFS implementation, the master account can include sub-accounts for each of the agent branches and subscriber mobile wallets, giving the bank visibility into all transactions on a per-user basis. The mFS platform can also manage the balance of sub-accounts and interact with the bank's master account when funds need to be deposited or withdrawn from the account.

The term mobile network operator (MNO) refers to a provider of mobile phone service including basic voice, SMS, unstructured supplementary service data (USSD) and data service, and may also be referred to as a "wireless service provider".

The term "mobile wallet" or "mobile wallet account" refers to a stored value account or prepaid access account (PPA) that allows the owner (or "subscriber") to pay for goods and services on the mFS platform from his or her mobile wallet account. When the mFS eMoney transaction processor is used, the mobile wallet balance is maintained by the mFS platform and value is exchanged within the mFS program as eMoney. When the mFS platform is integrated to an external card processor, the mobile wallet utilizes funds from the subscriber's prepaid debit card and bank account to exchange value on the mFS platform.

The term "non-agent company" refers to a mFS program participant who accepts payments from mFS subscribers but does not provide the same services as mFS agent companies. Payment is accepted either in the form of eMoney or through periodic settlements with the mFS platform provider. Examples of non-agent companies include bill pay providers and micro-finance lenders.

The term "non-mFS subscribers" refers to unregistered users that participates in various use cases in the mFS program. Non-mFS subscribers can send money to or receive money from mFS subscribers through interaction with the mFS program agents or with international remittance providers.

The term "partner bank" refers to the primary bank participating in the mFS program. The partner bank is responsible for holding the mFS program master accounts that hold the funds for all mFS services and transactions. A "PIN" refers to a numeric password that may be required to

perform a transaction via the mobile wallet application. A "transaction processor" refers to an application or service that manages the mFS program account balances. The transaction processor determines the amount of funds or eMoney is in a particular account at any given time, and manages account balances. Mobile transaction system requests to credit, debit, or view the balance of a particular mobile wallet or program account are handled by the transaction processor (in conjunction with other components of the mobile wallet platform).

The term "sub-accounts" refers to accounts that are maintained within the mFS platform or by an external card processor. A partner bank may elect to maintain a separate bank account for each subscriber and/or agent branch, or a single master account may be established that contains the funds for all of the subscriber mobile wallet and agent branch accounts (at least within a country or other geographical region). The balance of each individual user may be managed by the mFS transaction processor.

When using a master account, the bank is involved only in transactions that require the movement of funds external to the mFS program. For example, subscriber cash-in and cash-out transactions involve the addition and removal of cash from the mFS program and would consequently include a deposit or withdrawal from the master account. Retail purchases from participating mFS program retailers or the exchange of funds between mFS subscribers results in no net change in the mFS program balance and thus do not require involvement by the partner bank.

The term "subscriber" refers to a participant of the mFS mobile wallet platform. The subscriber maintains a mobile wallet balance and performs transactions using the mFS application. An "unbanked subscriber" is a subscriber that does not have (or does not have access to) a bank account or credit union account. The application or "mobile wallet application" provides mobile wallet functionality to the (unbanked) subscriber. The mobile wallet application is installed on a mobile device in the device's memory, on a SIM card (such as a GSM SIM card) or is otherwise accessible to the mobile device. The mobile wallet application provides the subscriber the ability to securely perform subscriber functions such as making retail purchases, paying bills, or transferring money to other mFS subscribers and non-subscribers. The mobile wallet application communicates with the mFS platform using binary and text SMS messages, among other forms of wireless communication. A wireless service provider or MNO provides the GSM network infrastructure on which the mFS platform operates.

FIG. **1** illustrates an example system architecture for a mobile wallet platform. Integration tier **101** is configured to manage mobile wallet sessions and maintain integrity of financial transactions. Integration tier **101** can also include a communication (e.g., Web services) API and/or other communication mechanisms to accept messages from channels **111**. Other mechanisms include, but are not limited to: International Standards Organization ("ISO") **8583** for Point of Sale ("POS") and Automated Teller Machines ("ATM") devices and Advanced Message Queuing Protocol ("AMQP") for queue based interfaces. Each of channels **111** can be integrated to one or more mechanisms for sending messages to integration tier **101**. Notification services **102** is configured to send various notifications through different notification channels **112**, such as, for example, Short Message Peer-to-Peer ("SSMP") for Short Messaging Service ("SMS") and Simple Mail Transfer Protocol ("SMTP") for emails. Notification services **102** can be configured through a web services API.

Service connectors **103** are a set of connectors configure to connect to 3rd party systems **113**. Each connector can be a separate module intended to integrate an external service to the system architecture. Business process services **104** are configured to implement business workflows, including executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects. Payment handler **105** is configured to wrap APIs of different payment processors, such as, for example, banking accounts, credit/debit cards or processor **121**. Payment handler **105** exposes a common API to facilitate interactions with many different kinds of payment processors.

Security services **106** are configured to perform subscriber authentication. Authorization services **107** are configured to perform client authorization, such as, for example, using a database-based Access Control List ("ACL") table.

Database **108** is configured to manage customer accounts (e.g., storing customer accounts and properties), manage company accounts (e.g., storing company accounts and properties), manage transaction histories (e.g., storing financial transaction details), store customer profiles, storing dictionaries used by the mobile wallet platform, such as, for example, countries, currencies, etc., and managing money containers. Rules engine **109** is configured to gather financial transaction statistics and uses the statistics to provide transaction properties, such as, for example, fees and bonuses. Rules engine **109** is also configured to enforce business constraints, such as, for example, transactions and platform license constraints.

Name matching engine **110** is configured to match different objects according to specified configuration rules. Matching engine **110** can be use to find similarities between names, addresses, etc. Transaction processor **121** is configured to manage financial accounts and transactions. The transaction processor **121** can be used to hold, load, withdraw and deposit funds to mobile wallet accounts. Transaction processor **121** can also be used as a common interface to a third party processor system. When used as a common interface, financial operations may be delegated to the external processor. A Clearing House subsystem of transaction processor **121** can be used to exchange the financial information with a bank.

Components of a mobile wallet platform can be connected to one another over (or be part of) a system bus and/or a network. Networks can include a Local Area Network ("LAN"), a Wide Area Network ("WAN"), and even the Internet. Accordingly, components of the mobile wallet platform can be "in the cloud". As such, mobile wallet platform components as well as any other connected computer systems and their components, can create message related data and exchange message related data (e.g., Internet Protocol ("IP") datagrams and other higher layer protocols that utilize IP datagrams, such as, Transmission Control Protocol ("TCP"), Hypertext Transfer Protocol ("HTTP"), Simple Mail Transfer Protocol ("SMTP"), etc.) over the system bus and/or network.

The components depicted in FIG. **1** can interoperate to provide a number of financial and other services including but not limited to enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a mobile wallet, adding a debit or credit card account to a mobile wallet, depositing funds in a mobile wallet, withdrawing funds from a mobile wallet, paying bills from a mobile wallet, topping up a prepaid mobile account through a mobile wallet, transferring funds through a mobile

wallet (nationally or internationally), making in-store purchases using a mobile wallet, and various other tasks as described herein below. These services will be described in greater detail below with regard to system FIGS. **1** and **2**, as well as FIGS. **3-19B**.

FIG. **2** depicts a monetary transaction system **200** similar to that described in FIG. **1**. The monetary transaction system **200** may provide a more simplified system structure in which each of the above services may be provided. The system includes a subscriber **205**. The subscriber may have access to a bank account, or may be an unbanked subscriber. The subscriber has a profile **211** with the monetary transaction system **210**. The profile includes the subscriber's KYC information, as well as any associated bank accounts, credit union accounts, bill pay accounts or other accounts. The subscriber has (or has access to) a mobile device **206** such as a phone or tablet. The mobile device runs the mobile wallet application (or mobile wallet application) **207**.

The subscriber can indicate, using the mobile application **207** which transaction or other action he or she would like to perform. The indicated transaction **208** is sent to the mobile wallet platform **210** to be carried out by the platform. The transaction processor **216** (which may be similar to or the same as transaction processor **121** of FIG. **1**) performs the transaction(s) specified by the (unbanked) subscriber **205**. The transaction processor may implement various other components to perform the transaction including memory **217**, (wireless) communication module **215**, rules engine **210** and/or transaction database **225**.

Performing the specified transactions may include communicating with the monetary transaction database **225** to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile (for instance, whether the subscriber has enough eMoney in his or her stored value account, or has enough money in his or her bank account). Rules engine **220** may also be consulted to determine whether the subscriber has exceeded a specified number of allowed transactions. Then, if funds are available, and the transaction is otherwise permissible, the monetary transaction system can transfer money or eMoney **221** to or from an entity such as a user or agent (e.g. entity **222**) to or from an establishment such as a retail store or agent company (e.g. entity **223**).

In some cases, the monetary transaction system **210** application provides a web interface that allows subscribers to perform the same functions provided by the monetary transaction system application. For instance, mobile wallet application **207** may provide a web interface that allows a user to enroll for a mobile wallet. The web interface (or the mobile wallet application itself) receives a subscriber-initiated transaction over one of a plurality of channels (**111** from FIG. **1**) connected to the monetary transaction system **210**. The web interface or mobile wallet application may prompt for and receive enrollment information (e.g. KYC information) for the (unbanked) subscriber **205** over at least one of the plurality of channels (e.g. web, point-of-sale (POS), interactive voice response (IVR, etc.). The web interface or mobile wallet application may then send activation instructions over the same or a different channel to activate the (unbanked) subscriber **205** and create a subscriber account for the (unbanked) subscriber.

Once the subscriber has an account, the monetary transaction system generates a corresponding mobile wallet for the unbanked subscriber (available via the web interface and/or the mobile wallet application. The system then presents the (unbanked) subscriber's account data associated with the mobile wallet and/or a notification indicating that enrollment was successful to the subscriber. Accordingly, the mobile wallet application or the web interface may be used to provide user enrollment functionality. It should also be understood that either the mobile wallet application or the web interface may be used to provide substantially all of the mobile wallet functionality described herein.

It should also be noted that the mobile device **206** may be any type of plan-based phone or tablet, or prepaid phone or tablet. Many subscribers, such as unbanked subscribers, may primarily use prepaid phones. The mobile wallet application **207** may be installed on both plan-based phones and prepaid phones. The mobile wallet application may be installed on the device's SIM card, or on the device's main memory. Accordingly, the monetary transaction system **200** may be accessed and used via substantially any type of plan-based or prepaid mobile device.

FIG. **3** shows three different graphics (**301-303**) and corresponding method steps (**310-370**) that illustrate an unbanked subscriber making a deposit using a mobile wallet (and, by extension, using the mobile wallet transaction system **210**). In at least some of the embodiments described below, the actions of each participant are shown and described. This will also, at least in some embodiments, include an illustration of money flow throughout the mobile wallet transaction system. In the graphics, various terms are used as follows: $C=Cash Balance and $E=Electronic Money (eMoney) Balance.

At graphic **301**, it is assumed that the unbanked subscriber (e.g. **205**) has already registered and activated an eMoney account at an agent branch location (e.g. a retail store, gas station, or other location that has registered to be an agent branch). To deposit cash in order to get eMoney credit, the subscriber informs the agent manager or agent that they want to deposit a certain amount of cash (in **301**). The agent manager/agent takes the cash and notifies the mobile wallet transaction system of the deposit using their agent manager or agent application (**302**). The transaction system **210** then credits the subscriber's eMoney account (**303**). Accordingly, any location that has registered to accept eMoney payments from subscribers' mobile wallets can also accept cash deposits. The agent branch's eMoney balance is reduced because their actual money balance was increased by the amount of the deposit. The subscriber's mobile wallet account is credited with eMoney in the amount of the deposit. In this manner, a subscriber can deposit cash into their mobile wallet account (in the form of eMoney) at any retail location or other agent branch location.

Thus, the agent manager receives the physical cash deposit into the subscriber's eMoney account via the agent manager or agent's application. The subscriber gives cash to agent manager or agent, and the mFS platform processes the request, updates the agent branch and subscriber's eMoney balances, logs the transaction, and sends details (such as eMoney account balances, transaction logs, etc.) to bank specified by the mobile wallet platform. These details may be sent instantaneously as transactions occur, or in batches at pre-determined intervals.

In one embodiment, the monetary transaction system **210** of FIG. **2** is implemented to deposit funds at an agent branch using a mobile wallet. The monetary transaction system **210** receives communication from an agent branch over one of a plurality of channels (e.g. **111**) connected to the monetary transaction system (step **310**). The agent communication indicates that the unbanked subscriber **205** desires to deposit a specified amount of funds into the unbanked subscriber's mobile wallet account. The transaction processor **216** then validates the status of the unbanked subscriber's mobile

wallet account (step **320**) and determines if the agent branch is authorized to receive deposited money (i.e. determine if it has pre-registered as an official agent branch) (step **330**).

The monetary transaction system may then use rules engine **220** to perform a limit check (to determine whether sufficient funds are available) and/or a velocity check (to determine whether the user has exceeded a specified number of (hourly, daily, or weekly) transactions) on the unbanked subscriber's mobile wallet account (step **340**). The transaction system then credits the unbanked subscriber's mobile wallet account with the specified amount of funds (step **350**) and returns a notification to the agent branch confirming the deposit (step **360**) and returns another notification to the subscriber notifying the subscriber that the specified amount of funds was deposited in the their mobile wallet account (step **370**). Any of channels **111** may be used to perform these communications.

FIG. **4** shows three different graphics (**401-403**) and corresponding method steps (**410-490**) that illustrate an unbanked subscriber making a withdrawal using a mobile wallet (and, by extension, using the mobile wallet transaction system **210**). As above, the terms in the graphics include "$C" representing cash balance and "$E" representing eMoney balance.

To withdraw cash at an agent branch, a subscriber submits a withdrawal request using their application (**401**). The subscriber may also enter information about the agent branch (e.g. name of establishment, name of agent, location or other information) that allows the monetary transaction system **210** to identify the agent branch. The transaction processor **216** may then determine whether the unbanked subscriber has enough eMoney to withdraw the requested amount. If he or she does have enough eMoney, then the subscriber's eMoney is deducted and that amount is transferred to the agent branch's eMoney account (**402**). Then, the agent branch gives the subscriber the requested amount of cash (**403**). In this manner, any entity that has established itself as an agent branch (including retail stores, gas stations, service providers, etc.) can provide cash withdrawal to a mobile wallet subscriber (whether banked or unbanked). The agent's or agent manager's role is to verify the withdrawal request (e.g. via SMS on the agent's or agent manager's phone) and gives the cash to subscriber. The subscriber requests cash withdrawal from agent branch's eMoney account via the application, and receives physical cash from agent manager/agent. The mobile wallet platform processes the request, updates the agent branch's and subscriber's eMoney balances, logs the transaction, and sends transaction details to a specified bank at pre-determined intervals.

In one embodiment, the monetary transaction system **210** is implemented to withdraw funds at an agent branch using a mobile wallet. The communication module **215** receives a communication from an unbanked subscriber over one of a plurality of channels **111** connected to the monetary transaction system **210** (step **410**). The communication indicates that the unbanked subscriber **205** desires to withdraw a specified amount of funds from the unbanked subscriber's mobile wallet account at the agent branch. The monetary transaction system **210** validates the status of the unbanked subscriber's mobile wallet account (step **420**) and determines if the balance of the unbanked subscriber's mobile wallet account is sufficient to accommodate the requested withdrawal for the specified amount of funds (step **430**).

The transaction processor **216** performs one or more of a limit check (to verify sufficient funds) and a velocity check (to verify the subscriber hasn't exceeded specified transfer limits) on the unbanked subscriber's mobile wallet account (step **440**). The monetary transaction system **210** then returns a secure, perishable withdrawal code to the subscriber **205** over at least one of the plurality of channels **111** connected to the monetary transaction system (step **450**). The monetary transaction system **210** receives subsequent agent branch communication over at least one of the plurality of channels connected to the monetary transaction system indicating that the withdrawal code has been presented to the agent branch (step **460**). The monetary transaction system **210** then debits the unbanked subscriber's mobile wallet account by the specified amount of funds (step **470**), returns a notification to the agent branch confirming the withdrawal (step **480**) and notifies the subscriber that the specified amount of funds was withdrawn from the unbanked subscriber's mobile wallet account over at least one of the channels **111** connected to the monetary transaction system (step **490**). Accordingly, the monetary transaction system **210** may be used to allow subscribers to withdraw cash using their mobile wallet applications at any store or other entity registered as an agent branch.

FIG. **5**A depicts a subscriber-to-subscriber eMoney transfer. To perform such a transfer, subscriber A (**501**) enters some type of identification information identifying subscriber B (e.g. subscriber B's phone number) and an amount of money he or she wishes to transfer. The transaction processor **216** of the monetary transaction system **210** determines if there are sufficient funds to complete the transfer. If sufficient funds are available, the monetary transaction system **210** decrements subscriber A's account and credits subscriber B's account (**502**). The system then sends some kind of notification (e.g. SMS) to subscriber B indicating that a certain amount of money was transferred to their account. Subscriber A may also receive a notification that the transfer was successful. Accordingly, eMoney may be transferred between two mFS platform subscribers, one or both of which may be unbanked. The monetary transaction system **210** processes the subscribers' requests, updates the subscribers' eMoney balances, logs the transactions, and sends transaction information to a specified bank when needed.

FIG. **5**B illustrates a subscriber-to-non-subscriber eMoney transfer. In graphic **505**, subscriber A wishes to send eMoney to another individual that is not a subscriber to the mFS platform. The transaction is initiated in the same fashion as the subscriber-to-subscriber transfer scenario. However, since non-subscriber B does not have a mobile wallet account, the monetary transaction system **210** cannot credit them with eMoney. Instead, the monetary transaction system **210** sends a notification (e.g. via SMS) to non-subscriber B with instructions for how to pick-up the transferred money, along with an authorization code (**506**). The monetary transaction system **210** puts a hold on subscriber A's account for the amount transferred. Subscriber B then has a specified number of days to pick up the cash before the hold expires and the amount is credited back to subscriber A's eMoney account by the monetary transaction system **210**.

When non-subscriber B goes to pick up the money at an agent branch, the agent branch's manager or agent verifies the authorization code via an agent manager or agent mobile wallet application (that, in turn, accesses the mFS platform). Once the transfer has been validated, the agent gives the cash to non-subscriber B. The agent branch's mFS account is credited with the transfer amount (**507**) and the user leaves with the cash in hand (**508**). The mFS platform processes the

transfer request, updates subscriber A's eMoney balance, logs the transaction, and sends transaction details to a platform-specified bank.

FIG. **6**A illustrates a subscriber-to-subscriber international eMoney transfer. This embodiment is, at least in some respects, similar to sending eMoney to an mFS subscriber domestically. In this case the monetary transaction system **210** leverages one or more existing international money transfer organizations or "remittance companies" such as MoneyGram®. In some embodiments, MoneyGram® is pre-integrated to the monetary transaction system **210**, but other international money transfer organizations may also be used. Still further, at least in some embodiments, subscriber B may need to have an eMoney account with a foreign mFS program that is also affiliated with MoneyGram® or another international money transfer organization.

In FIG. **6**A, subscriber A initiates the international eMoney transfer at **601**, the international money transfer organization (e.g. MoneyGram®) transfers the eMoney to subscriber B at **602** and subscriber B's eMoney balance is increased by the transferred amount. Thus, subscriber A requests to send eMoney from his or her eMoney account via the mobile wallet application. The eMoney is transferred using an international money transfer organization, and subscriber B receives a notification (that may, for example, include a reference number, among other information) that their eMoney balance has increased by the transfer amount. The monetary transfer system **210** processes subscriber A's request, updates subscriber A's and subscriber B's eMoney balances, logs the transaction, and send transaction details to a mFS platform-specified bank.

FIG. **6**B illustrates a subscriber-to-non-subscriber international eMoney transfer. In this illustration, subscriber A wishes to send cash to subscriber B who is not an mFS program subscriber. Similar to the scenario described in FIG. **6**A, the monetary transaction system **210** leverages various international money transfer organizations or remittance companies such as MoneyGram® to transfer the eMoney. Subscriber A initiates a typical eMoney transfer at **605** by providing non-subscriber B's identification information, as well as the amount to be transferred. The Monetary transaction system **210** recognizes the eMoney transfer is not destined for a domestic phone number and routes the request to the international money transfer organization (e.g. MoneyGram®) (**606**).

The international money transfer organization sends non-subscriber B a notification (e.g. via SMS) with instructions for how and where to pick up the money (in embodiments where MoneyGram® transfers the eMoney, the notification may include a MoneyGram® reference number (MGRN)) (**607**). Non-subscriber B can then show the MGRN to an agent at an agent branch (**608**) and then receive the cash (**609**). The monetary transaction system **210** then decrements subscriber A's eMoney account for the transferred amount. The monetary transfer system **210** thus processes subscriber A's transfer request, updates subscriber A's eMoney balance, logs the transaction, and sends transaction detail to a platform-specified bank. It should also be noted that an mFS subscriber may also receive money in a foreign country from either a subscriber or a non-subscriber in a similar manner.

FIG. **7** illustrates a subscriber purchasing airtime using a mobile wallet. Mobile wallet platform subscribers may buy airtime by using their mobile wallet application **207**. The monetary transaction system **210** will reload their airtime account within the mobile network operator's (MNO's) systems. The subscriber requests to purchase airtime by entering the request via the mobile wallet application or via a mobile wallet web interface. The monetary transaction system **210** then decrements the subscriber's eMoney account (**701**), while crediting the mFS platform's eMoney account (**702**). The purchased airtime is then added to the subscriber's airtime balance (**703**). The monetary transaction system **210** processes the subscriber's request, updates the subscriber's eMoney balances as well as its own eMoney balance, logs the transaction, and sends transaction detail to a mFS platform-specified bank.

In one embodiment, the monetary transaction system **210** is implemented to top up a prepaid mobile account from a mobile wallet. The communication module **215** of the monetary transaction system **210** receives a subscriber communication over one of a plurality of channels **111** connected to the monetary transaction system (step **710**). The subscriber communication indicates that an unbanked subscriber **205** desires to top up a prepaid mobile account by a specified amount using a specified payment method from the unbanked subscriber's mobile wallet. The transaction processor **216** validates the status of the selected payment method (step **720**) and performs a limit check and/or a velocity check on the selected payment method (step **730**). The monetary transaction system **210** then debits the specified payment method by the specified amount of funds (step **740**) and processes the mobile top-up via a billing system integrator and/or an aggregator (step **750**), and notifies the subscriber that the prepaid mobile account was topped up over at least one of the channels connected to the monetary transaction system (step **760**).

FIG. **8** illustrates an embodiment where a mFS subscriber pays a bill using a mobile wallet. At least in some embodiments, the company that the subscriber wishes to pay needs to have signed-up to be part of the mFS platform. The mFS platform may publish a list of company names that have registered to be part of the mFS platform. This list of companies may include company IDs so that subscribers can know which company ID to enter in their mobile wallet application. Once the company ID is known, the subscriber can pay a bill by entering the company ID and the amount to be paid. The monetary transaction system **210** then decrements the subscriber's eMoney account (**801**) and credits the identified company's eMoney account (**802**). Accordingly, in response to the subscriber's request to pay bill via their mobile wallet application, the monetary transaction system **210** processes the request, updates the bill pay company's and the subscriber's eMoney balances, logs the transaction, and sends transaction details to the mFS platform-specified bank.

In one embodiment, the monetary transaction system **210** is implemented to pay a bill from a mobile wallet. The communications module **215** of the monetary transaction system **215** receives a subscriber communication over a communication channel **111** connected to the monetary transaction system (step **810**). The subscriber communication indicates that unbanked subscriber **205** desires to pay a bill for a specified amount using a specified payment method from the unbanked subscriber's mobile wallet (e.g. eMoney). The monetary transaction system **210** validates the status of the selected payment method (step **820**) and performs a limit check and/or a velocity check on the selected payment method to ensure the eMoney transfer is permissible (step **830**). The monetary transaction system then debits the specified payment method by the specified amount of funds (step **840**), processes the bill payment via a direct biller connection or a bill pay aggregator (step **850**), and notifies the unbanked subscriber that the bill was paid

using a communication channel (e.g. SMS) connected to the monetary transaction system (step **860**). Thus, in this manner, a subscriber may use a mobile wallet to pay various bills including rent, utility, mortgage, phone, cable, medical and other bills.

FIG. **9** illustrates a mobile wallet subscriber making a retail purchase. Mobile wallet subscribers can make retail purchases at agent branches directly from their mobile device. Agent branches, as explained above, are retail stores or other entities that have registered with the mFS system and are able to accept mobile wallet payments. Accordingly, a subscriber can select the items they wish to purchase, and indicate (via the mobile wallet application) to the agent branch that they wish to pay for the items. The mobile wallet application then communicates with the agent branch and the monetary transaction system to indicate the price of the transaction. The monetary transaction system **210** then debits the subscriber's eMoney account (**901**) and credits the agent branch's eMoney account (**902**). The agent branch (and/or the agent manager or agent) receives confirmation that subscriber paid for the purchase. The subscriber may also receive a summary of the retail purchase and may be asked to confirm the purchase by entering a PIN. The monetary transaction system processes the purchase request, updates the agent branch and subscriber's eMoney balances, logs the transaction, and sends transaction details to a mFS platform-specified bank.

In one embodiment, the monetary transaction system **210** is implemented to make a purchase from a mobile wallet. The communications module **215** of the monetary transaction system **210** receives a communication from a subscriber over a communication channels **111** (step **910**). The subscriber communication indicates that an unbanked subscriber **205** desires to purchase an item for a specified amount of funds using a specified payment method from the unbanked subscriber's mobile wallet.

The monetary transaction system **210** then returns a secure, perishable purchase code to the unbanked subscriber over at least one of the channels connected to the monetary transaction system (step **920**) and receives a subsequent agent branch communication over a channel indicating that the purchase code has been presented to an agent (branch) (step **930**). The monetary transaction system **210** validates the status of the specified payment method (step **940**), determines if the specified payment method can accommodate a purchase for the specified amount (step **950**), performs a limit check and/or a velocity check on the selected payment method (**960**), debits the specified payment method by the specified amount of funds (**970**), returns a notification to the agent branch authorizing the purchase (**980**) and sends a receipt to the unbanked subscriber over a communication channel. The monetary transaction system **210** may thus be used to make a retail purchase using a mobile wallet.

FIG. **10**A illustrates a subscriber requesting a micro-loan. Financial institutions and potentially other mFS program participants may sign up to become money or eMoney lenders. Mobile wallet subscribers may be able to use their mobile wallets to request micro-loans from these approved lenders. The micro-loans are tracked by the monetary transaction system **210**, and repayment reminders, interest and commissions are managed by the monetary transaction system. The subscriber requests a micro-loan from a lender, indicating the amount in the request, as well as other information such as the repayment date and the commission (i.e. interest rate). Potential lenders then have a chance to counter the loan request with their own terms. Once the lender approves the subscriber's request, the lender's eMoney account balance is debited for the specified amount (**1001**) and the subscriber's eMoney account is credited with the requested amount (**1002**). The monetary transaction system **210** processes the micro-loan requests, update the lender and subscriber's eMoney balances, sets up repayment schedules and reminders, logs the transaction, and sends transaction detail to a mFS bank. It should also be noted that while the term "micro-loan" is used herein, the loan may be for substantially any amount of money.

Following on the embodiment described in FIG. **10**A, FIG. **10**B illustrates a subscriber repaying a micro-loan. The subscriber may repay the loan using functionality provided in the mobile wallet application or in a similar web interface. Repayments can be made in installments or in full depending on the rules of the micro-loan. The subscriber enters the amount they wish to repay and the loan ID. The subscriber's eMoney account is then debited for the specified amount (**1005**), while the lender's eMoney account is credited the specified amount (**1006**). Both the lender and the subscriber may receive confirmation that the loan has been repaid via SMS or some other communication channel. The mFS platform thus processes the subscriber's micro-loan repayment request, updates lender and subscriber's eMoney balances, updates repayment schedule and reminders, logs the transaction, and sends transaction details to a specified mFS platform bank.

FIG. **11**A illustrates a subscriber receiving a direct deposit from an employer or other entity. Subscribers to the mFS platform have the ability to receive any direct deposit into their eMoney account. Subscribers may be asked by their employers to provide account information in order to set up direct deposit. The employer then submits a direct deposit request using their existing processes (i.e the processes they use for a normal checking or savings bank account). Once the direct deposit is set up and a payday arrives, the employer's bank account is debited for the proper amount (**1101**) and the employer's mFS account is credited with that amount (**1102**). Then, once the funds have been received at the mFS platform bank, the mFS platform bank sweeps the employers direct deposit balance (**1103**) into a mFS platform master account (**1104**) and notifies the mFS platform of each account to be incremented (including the subscriber's mobile wallet (eMoney) account). The subscriber's eMoney account is then credited with the paycheck amount (**1105**) upon which the eMoney may be used to pay for goods, pay bills, top up airtime, transfer to other entities or for cash withdrawal.

The subscriber does not need to have a bank account to participate in direct deposit. The employer's bank can communicate with the mFS platform's bank to perform the necessary steps in directly depositing the subscriber's paycheck in his or her eMoney mobile wallet account. The bank facilitates monetary deposit into the employer's bank account for direct deposit and performs an automated sweep of recent deposits from the employer's bank account into the mFS platform's master bank account. The bank also sends transaction details to the monetary transaction system **210** including transaction logs. The monetary transaction system receives a list of eMoney accounts that are to be credited directly from the employer (or bank), processes the list and requests to establish a direct deposit, updates subscriber's eMoney balance, log the transaction, and sends transaction details to the mFS platform bank.

In a similar manner, a subscriber may receive a government welfare payment directly on their mobile device. FIG. **11**B illustrates a subscriber receiving a government social welfare payment directly into their eMoney account. In

some embodiments, subscribers may need to opt-in and register with the government program for which they choose to receive the payment via their mobile wallet. Once the funds have been received, the subscriber can use that eMoney for any goods or services, as described above. Once the direct deposit has been established and a payout has been initiated, the government's welfare account deposits the money (**1110**) into the government's bank account for welfare payments (**1111**) and performs an automated sweep of recent deposits from the government's bank account (**1112**) into the mFS program's master bank account (**1113**). The bank then sends transaction details to the monetary transaction system **210** regarding the deposit. The subscriber receives a notification that the welfare payment has been credited to their eMoney account (**1114**). The mFS platform receives an indication of eMoney accounts that are to be credited from the government, processes the welfare payments, updates the subscriber's eMoney balance, logs the transactions, and sends transaction details to the mFS platform bank.

FIG. **12**A illustrates an agent administrator distributing eMoney to various recipients. An agent administrator, as explained above, is a person who acts as an agent company's representative. The agent administrator deposits, withdraws, and distributes funds into and out of the agent company's bank account. When an agent administrator deposits cash into an agent company's bank account, it is credited as eMoney to the agent company's account. In order to provide the agent branches with eMoney, the agent administrator first moves the eMoney from the agent company's account (**1201**) to the branch accounts (**1202**). This is performed using the agent administrator's mobile wallet application or portal. In an agent administrator money transfer, the monetary transaction system **210** processes the administrator's eMoney transfer request, updates the agent company and agent branch eMoney balances, logs the transaction, and sends transaction details to the mFS platform bank.

FIG. **12**B illustrates an agent company deposit. The agent company has an eMoney account in the monetary transaction system **210** that may also include a corresponding bank account (that may be created automatically upon creation of the agent company's eMoney account). After the agent company's bank account has been set up, the agent administrator can make deposits into that account. As FIG. **12**B shows, once cash (**1205**) has been deposited into the bank account (**1206**), it is transferred to a mFS platform master account (**1208**) that includes all or a part of the mFS platform's funds. The agent company's bank account is decreased by the deposit amount (**1207**), while the agent company's eMoney account balance is correspondingly increased (**1210**). At this time, the agent company account is credited with eMoney. The agent company's bank facilitates a physical cash deposit into the agent company's bank account and performs an automated sweep (**1209**) of recent deposits from the agent company's bank account into the mFS platform's master bank account. The agent company's bank then sends transaction details to the monetary transaction system **210**. The agent administrator physically delivers the cash (or form of money such as a check or money order) to a bank branch for deposit. The monetary transfer system receives transaction details from the agent company's bank about recent transactions (including deposits, as shown in FIG. **12**B.

FIG. **13** illustrates an agent company withdrawal. To make a cash withdrawal for an agent company, the agent administrator requests a withdrawal using the agent administrator mobile wallet application. The monetary transaction system **210** then notifies the bank that a certain amount of eMoney is to be transferred from the master mFS account (**1302**) to the agent company bank account (**1303**). When the money is in the agent company bank account, the agent administrator can withdraw the cash by traditional withdrawal means. The mFS master bank receives transaction details from the monetary transaction system **210** about recent transactions (recent withdrawals in this case). The mFS master bank performs an automated sweep (**1304**) of the mFS platform's master bank account to reflect the recent withdrawal request from agent the agent company (**1301**). The agent company's eMoney account is reduced by the amount of the withdrawal. The agent company also sends transaction details to the monetary transaction system **210**. The agent administrator can request withdrawal via the agent administrator mobile wallet application and physically withdrawal cash (**1305**) from the agent company's bank branch (**1306**). The mFS platform processes the agent company's withdrawal request, updates agent company and agent branch eMoney balances, logs the transaction, and sends transaction details to an mFS platform-specified bank.

Attention will now be turned to embodiments in which subscribers have bank accounts associated with their mobile wallets. The monetary transaction system **210** provides similar functionality to consumers that have bank or credit union accounts. Although many different transactions are presented herein, many more and varied types of transactions may be processed by the monetary transaction system. In the following figures, "$C" refers to cash balance, "$DC" refers to a debit card (prepaid) balance and "$PIN" refers to a recharge PIN value.

FIG. **14** describes a subscriber deposit at an agent branch. The subscriber has a registered and activated (prepaid) debit card at an agent branch location. The prepaid debit card is associated with the mobile wallet application in the subscriber's mobile device. As such, the debit card is linked to the subscriber's account in the monetary transaction system **210**. To deposit cash onto the mobile wallet, the subscriber informs the agent that they want to deposit a specified amount of cash (**1401**). The agent takes the cash and notifies the monetary transaction system **210** of the deposit using their point of sale (POS) system or the agent mobile wallet application (**1402**), and the monetary transaction system **210** credits the subscriber's mobile wallet account (**1403**). The funds collected at the cash register typically do not reach a bank account until the reconciliation and settlement of funds occurs between the agent and the mFS owner's bank.

The subscriber's bank then receives a settlement report from the card processor and receives funds from the agent's bank. The agent or agent manager physically deposits the cash into the subscriber's mobile wallet account via their POS system or agent manager/agent mobile wallet application. The monetary transaction system processes the deposit request, increments the subscriber's mobile wallet balance within the card processor and logs the transaction. An external card processor increments the subscriber's mobile wallet balance and sends reports to the bank for settlement on a regular (e.g. nightly) basis.

In one embodiment, the monetary transaction system **210** is implemented to deposit funds into a bank or credit union account using a mobile wallet. The communications module **215** of the monetary transaction system **210** receives communication from an agent branch over a communication channel (step **1410**). The agent communication indicates that a subscriber **205** desires to deposit a specified amount of funds into a bank or credit union account. The transaction processor **216** validates the status of the bank or credit union

account (step **1420**), determines if the agent branch is authorized to deposit money (step **1430**), and performs a limit check and/or a velocity check on the bank or credit union account (step **1440**). The monetary transaction system then credits the bank or credit union account with the specified amount of funds (step **1450**), returns a notification to the agent branch confirming the deposit (step **1460**) and notifies the subscriber that the specified amount of funds was deposited in the bank or credit union account using at least one of the communication channels connected to the monetary transaction system (step **1470**). Accordingly, cash may be deposited into a bank or credit union account associated with a subscriber's mobile wallet.

FIG. **15** illustrates a subscriber deposit that is performed with a non-agent. In some economies, subscribers may have the ability to leverage other channels outside of agents to deposit funds onto their card. One deposit method is a PIN-based recharge that allows a subscriber to purchase a PIN worth the deposit value. The PIN can then be redeemed via an interactive voice response (IVR) system or via the subscriber's mobile wallet application. The mobile wallet application will allow the monetary transaction system **210** to deposit the funds onto the subscriber's card. The retailer's bank settles with the PIN card provider's bank and the PIN card provider's bank settles with the mFS platform's bank for the deposit. The subscriber gives cash to the agent (**1501**) which increases the agent company's physical cash (**1502**). The subscriber uses IVR or their SIM Application to recharge mobile wallet account using a PIN card (**1503**). In some cases, an agent may provide the PIN card (i.e. the prepaid debit card) to the subscriber. The monetary transaction system **210** processes the subscriber deposit request, increments the subscriber's mobile wallet balance within the card processor and logs the transaction. An external card processor decreases the subscriber's PIN card balance (**1504**), increments the subscriber's mobile wallet balance (**1505**) and send reports to the mFS platform bank for settlement.

FIG. **16** illustrates a subscriber withdrawal at an agent branch. To withdraw cash at an agent branch from a (prepaid) debit card, a subscriber submits a withdrawal request using the mobile wallet application on their mobile device. The subscriber may also need to enter details about the agent branch that allows the monetary transaction system **210** to determine if the subscriber has sufficient funds on their debit card. The mFS platform then notifies the agent branch that it can give cash to the subscriber. If the subscriber has sufficient funds, the monetary transaction system **210** will decrement the subscriber's funds from their card (**1601**) and transfer it to the mobile wallet owner's account within the same card processor or bank. The agent branch (**1602**) then provides the withdrawn cash to the subscriber (**1603**).

Accordingly, the subscriber requests a cash withdrawal from their own mobile wallet account via the mobile wallet application. The agent or agent manager verifies the withdrawal request via POS authorization or SMS received on agent's phone and, once verified, gives cash to the subscriber. The monetary transaction system **210** processes the subscriber's withdrawal request, decrements the subscriber's mobile wallet balance within the card processor and logs the transaction. An external card processor decrements the subscriber's mobile wallet balance and sends reports to the bank for settlement on a periodic basis.

In one embodiment, the monetary transaction system **210** is implemented to withdraw funds from a bank or credit union account using a mobile wallet. The communication module **215** of the monetary transaction system **210** receives a communication from a subscriber **205** over a communication channel **111** (step **1610**). The subscriber communication indicates that subscriber **205** desires to withdraw a specified amount of funds from a bank or credit union account. The transaction processor validates the status of the bank or credit union account (step **1620**), determines if the balance of the bank or credit union account is sufficient to accommodate the requested withdrawal for the specified amount of funds (step **1630**) and performs a limit check and/or a velocity check on the bank or credit union account (step **1640**).

The monetary transaction system **210** then returns a secure, perishable withdrawal code to the subscriber **205** over at least one of the communication channels (step **1650**) and receives a subsequent agent branch communication indicating that the withdrawal code has been presented to an agent (step **1660**). The monetary transaction system **210** then debits the bank or credit union account by the specified amount of funds (step **1670**), returns a notification to the agent branch confirming the withdrawal (**1680**) and notifies the subscriber that the specified amount of funds were withdrawn from the bank or credit union account using at least one of the communication channels connected to the monetary transaction system (step **1690**). Accordingly, a subscriber can withdraw cash stored on their mobile wallet from an agent branch or a non-agent branch.

FIG. **17**A illustrates a subscriber withdrawal using an automated teller machine (ATM). Subscribers in many countries have access to ATM machines and can use their mobile wallets to perform withdrawals using their (prepaid) debit card at most ATMs. Banks provide ATMs to their customers (typically at no charge) and to non-customers (typically for a small charge). The subscriber requests a cash withdrawal from the subscriber's mobile wallet via the subscriber's debit card that is associated with the mobile wallet. The bank providing the debit card may receive settlement reports from the card processor and may transfer and/or settle funds from subscriber's account to the ATM network bank. An extern card processor decrements the subscriber's mobile wallet balance (**1701**) and sends transaction reports to the bank for settlement. Accordingly, once the withdrawal request has been received and the external card processor (e.g. Visa® or MasterCard®) (**1702**) has debited the debit card account, the ATM (**1703**) dispenses the withdrawn cash to the subscriber (**1704**).

FIG. **17**B illustrates a subscriber-to-subscriber money transfer. An mFS subscriber (**1705**) may send money to another mFS subscriber (**1706**). To do so, subscriber A enters information identifying subscriber B (e.g. a phone number, email address or other identifier). The monetary transaction system **210** determines if there are enough funds to complete the transaction, and if so, the monetary transaction system **210** decrements subscriber A's debit card and credits subscriber B's debit card. The subscriber, accordingly, may request to send money from their own mobile wallet (i.e. money stored on a (prepaid) debit card) account via the subscriber mobile wallet application. The other subscriber receives a notification that the balance of the debit card associated with their mobile wallet has increased. The bank receives a settlement report from the debit card processor and transfers or settles funds from subscriber A's account to subscriber B's account (if necessary). The monetary transaction system **210** processes the transfer request, updates subscriber A's and subscriber B's debit cards that are associated with their mobile wallets and logs the transaction. The external card processor decrements subscriber A's debit

card balance, increments subscriber B's debit card balance and sends transaction reports to the mFS platform bank for settlement.

FIG. **17**C illustrates subscriber-to-non-subscriber money transfers. In this embodiment, subscriber A (an mFS subscriber) wishes to send money to another subscriber (a non-mFS subscriber). The transaction is initiated in the same fashion as described above in FIG. **17**B. However, since subscriber B does not have an mFS account, the monetary transaction system **210** cannot credit them with money. Instead, the monetary transaction system **210** sends a communication (e.g. a SMS) to subscriber B (**1708**) with an authorization code and instructions for how to pick up the cash. The monetary transaction system **210** puts a hold on subscriber A's debit card for the amount transferred (**1707**). Subscriber B has a specified time period in which to pick up the cash before the hold expires and the amount is credited back to the debit card associated with subscriber A's mobile wallet account. The agent branch verifies the authorization code via POS or their agent mobile wallet application (**1709**) and gives the cash to the non-subscriber (**1710**). (In some countries, an agent network needs to be capable of giving cash to a subscriber based on the money transfer reference number).

The mFS bank receives a settlement report from the card processor and transfer and settle funds from subscriber A's debit card to the agent's bank (if necessary). The monetary transaction system **210** processes the money transfer request, decrements subscriber A's mobile wallet balance within the card processor, generates a money transfer reference number, authorizes the reference number to be paid out by the agent and logs the transaction. An external card processor decrements subscriber A's mobile wallet balance and sends periodic transaction reports to the bank for settlement. Thus, as seen in FIGS. **17**B and **17**C, money may be transferred from subscriber to subscriber and from subscriber to non-subscriber.

Subscribers may similarly send money internationally to both subscribers and non-subscribers. FIG. **18**A illustrates a subscriber-to-subscriber international money transfer. In this embodiment, subscriber A wishes to send cash to subscriber B who resides in another country. As in the embodiments described above where money was transferred internationally, the monetary transaction system **210** may use one or more international money transfer organizations or remittance companies such as MoneyGram® to transfer the money. Subscriber A initiates the international money transfer using his or her phone. Subscriber A's debit card account is decremented by the transfer amount (**1801**). The money is transferred between countries using an international money transfer organization (**1802**). In this case, subscriber B has an mFS eMoney account with a foreign mFS platform that is also affiliated with the selected international money transfer organization. That organization can then credit subscriber B's eMoney account directly (**1803**).

Thus, subscriber A requests to send money from their debit card account via the subscriber mobile wallet application. Subscriber B receives a notification (including a MoneyGram® Reference Number (MGRN) (or other reference number when other international money transfer organizations are used) and instructions on how to access the eMoney) that their eMoney balance has increased. The mFS bank receives settlement reports from the debit card processor and transfers and/or settles funds from subscriber's account to the international organization's bank. The monetary transfer system **210** processes the transfer request, update subscriber A's and subscriber B's eMoney balances and logs the transaction. An external card processor decrements subscriber A's mobile wallet balance and sends periodic transaction reports to the bank for settlement.

FIG. **18**B illustrates a subscriber-to-non-subscriber international money transfer. In this embodiment, subscriber A wishes to send cash to subscriber B who resides in another country. As above, the monetary transaction system **210** uses an international money transfer organization (**1806**) to transfer the money between countries. Once the transfer has been initiated by subscriber A, the international money transfer organization debits subscriber A's debit card account (**1805**) and transfers that money to subscriber B. Subscriber B (**1807**) receives a notification (e.g. via SMS) with pick up instructions and a transfer ID number. Subscriber B can then go to an agent company (**1808**), show them the notification (including, perhaps an authorization code), and receive the transferred money (**1809**).

Similar to the transaction described in FIG. **18**A, the embodiment of **19**A illustrates a transaction where a subscriber receives an international money transfer. Subscriber B (**1901**) initiates a money transfer using their mobile wallet application. The international money transfer organization (**1902**) debits subscriber B's eMoney account balance. This money is then transferred by the international money transfer organization to subscriber A. Subscriber A receives a notification along with a transfer ID number indicating that their debit card account has been credited with the transferred money (**1903**).

FIG. **19**B illustrates a non-subscriber-to-subscriber international money transfer. This scenario is very similar to that described in FIG. **19**A from the mFS subscriber's perspective, except that their eMoney account is credited here, and their debit card account was credited in **19**A. The initiator, subscriber B (**1905**), does not have an mFS account and, as a result, takes their cash to an international money transfer organization (e.g. MoneyGram®) or other remittance company's agent (**1906**) to send it to subscriber A's mobile wallet eMoney account. The international money transfer organization (**1907**) then transfers the specified amount to subscriber A (**1908**) and subscriber A's mobile wallet eMoney account is credited with the amount of the transfer. Subscriber A may receive a transaction ID number, along with an indication that the transfer has occurred. The mFS bank may receive settlement reports from the card processor and settle funds from the international money transfer organization's bank to subscriber A's mobile wallet account. The monetary transaction system processes the money transfer request, updates subscriber A's mobile wallet balance within the card processor and logs the transaction. An external card processor increments subscriber A's mobile wallet balance and sends periodic transaction reports to the mFS bank for settlement.

Other functionality described above in relation to using an eMoney mobile wallet account may also apply to banked subscribers using a debit card associated with their mobile wallet. Such subscribers may buy airtime for their mobile device, pay bills, make retail purchases, receive direct deposits, and perform other functionality.

In one embodiment, the monetary transaction system **210** is implemented to add a mobile wallet platform stored value account to a mobile wallet. The stored value account may include eMoney or other monetary credits. In the embodiment, communication module **215** of monetary transaction system **210** may receive subscriber data for an unbanked subscriber **205** over a communication channel. The transaction processor may perform validation checks on the unbanked subscriber to validate that the unbanked sub-

scriber is not exceeding a specified allowable number of accounts per subscriber. The monetary transaction system **210** may then send subscriber data to another entity (such as a third party verification system) for identification of the unbanked subscriber. The monetary transaction system **210** receives results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber, creates a stored value account for the unbanked subscriber that maintains a recorded balance for the created stored value account, adds the stored value account to the unbanked subscriber's mobile wallet and notifies the unbanked subscriber of the addition of the stored value account over at least one communication channel connected to the mobile wallet platform.

In another embodiment, the monetary transaction system **210** is implemented to add a third party stored value account to a mobile wallet. The monetary transaction system **210** receives unbanked subscriber data, including account details, over a communication channel. The transaction processor **216** performs a validation check on the unbanked subscriber to validate that the unbanked subscriber is not exceeding a specified allowable number of accounts per subscriber. If the validation check is ok, the monetary transaction system **210** sends subscriber data to a third party verification system for identification of the unbanked subscriber. In some cases, validating the status of the sender or the recipient includes performing a check on the specified sender or recipient to comply with the office of foreign assets control. The monetary transaction system **210** then receives results from the third party verification system indicating that the subscriber data appropriately identifies the unbanked subscriber, and submits the unbanked subscriber's account details to a third party account processor. The monetary transaction system **210** receives an indication from the third party account processor that third party account processor created a third party stored value account for the subscriber. The transaction processor maintains a link between the subscriber data and the third party stored value account and adds the third party stored value account to the unbanked subscriber's mobile wallet. The monetary transaction system **210** then notifies the unbanked subscriber of the addition of the third party stored value account over a communication channels connected to the monetary transaction system.

In another embodiment, the monetary transaction system **210** is implemented to add a bank or credit union account to a mobile wallet. The communication module **215** receives subscriber data, including bank or credit union account details, over a communication channel **111**. The transaction processor **216** performs validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber and sends subscriber data to a third party verification system for identification of the subscriber. The communication module then receives results from the third party verification system indicating that the subscriber data appropriately identifies the subscriber. Upon receiving these results, the monetary transaction system **210** submits bank or credit union account details for validation by the transaction processor, receives an indication that the bank or credit union account details correspond to a valid bank or credit union account, maintains a link between the subscriber data and the bank or credit union account and notifies the subscriber of the bank or credit union account validation over a communication channel.

In still another embodiment, the monetary transaction system is implemented to add a debit or credit card account to a mobile wallet. The communication module **215** receives subscriber data, including a debit or credit card account number, over a communication channel **111** connected to the monetary transaction system. The transaction processor performs validation checks on the subscriber to validate that the subscriber is not exceeding a specified allowable number of accounts per subscriber. The communication module sends subscriber data to a third party verification system for identification of the subscriber and receives results from the third party system indicating that the subscriber data appropriately identifies the subscriber. The monetary transaction system **210** securely stores the debit or credit card account number for access by the mobile wallet (e.g. in memory **217** or transaction database **225**), adds the debit or credit card account number to the subscriber's mobile wallet, and notifies the subscriber of the addition of the debit or credit card account number. It should be noted that many other transactions can take place over the monetary transaction system, and that the embodiments described herein should not be read as limiting.

Embodiments of the invention can adhere to Know Your Customer (KYC) rules in the US by performing Customer Identification Program (CIP) checks as required by the Bank Secrecy Act and US PATRIOT Act. A minimum amount of information can be gathered about a customer, such as, for example, first name, last name, date of birth, government ID Type, government ID number and address. The CIP processes are designed to validate customer identity against government blacklists and assists in the prevention of money laundering and terrorist financing. A combination of non-documentary and documentary verification can be used to ensure beyond a reasonable doubt the identity of the customer.

Non-documentary verification can occur through the presentment of the information that was collected from the user to an external third party, such as, for example, Lexis Nexis®. Documentary verification can occur if non-documentary verification fails, then the user is asked to present an unexpired government ID. Various differ forms of identification including driver's license, passport, alien identification (e.g., green card or work visa), and Mexican Consular identification card, can be accepted.

Embodiments of the invention can perform Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) checks. AML and CFT checks can be performed using transaction monitoring methods to flag names and suspicious transactions for further investigation. The mobile wallet platform can perform AML and CFT checks on all electronic financial transactions to ensure that electronic funds are not being used for money laundering or terrorism. Transaction limits can be placed on user accounts. The transaction limits are fully configurable for each particular use case, channel and payment method that allows maximum flexibility to restrict higher risk use cases. Velocity checks can also be performed. Velocity Checks ensure that subscribers are not abusing the mobile wallet platform within the allowable limits.

FIGS. **20**A through **20**F depicts relationships between embodiments of various components within the monetary transaction system depicted in FIG. **1**. In particular, FIGS. **20**A through **20**F depict communications between the specific components within the monetary transaction system during an operation to deposit of funds within a financial account. The depicted interactions are representative of computer executed functions that enable the deposit of money through a mobile transaction system that is capable of functioning without an associated bank account.

FIGS. **21**A through **21**I depicts relationships between embodiments of various components within the monetary transaction system depicted in FIG. **1**. In particular, FIGS. **21**A through **21**I depict communications between the specific components within the monetary transaction system during an operation to withdraw funds from a financial account. The depicted interactions are representative of computer executed functions that enable the withdrawal of money through a mobile transaction system that is capable of functioning without an associated bank account.

FIGS. **22**A through **22**J depicts relationships between embodiments of various components within the monetary transaction system depicted in FIG. **1**. In particular, FIGS. **22**A through **22**J depict communications between the specific components within the monetary transaction system during an operation to transfer funds between financial accounts. The depicted interactions are representative of computer executed functions that enable the transfer of money through a mobile transaction system that is capable of functioning without an associated bank account.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed is:

1. A monetary transaction system for conducting monetary transactions between subscribers and other entities, the system comprising:

one or more processors;

a storage system configured to store financial transaction details, customer profiles and money containers;

an integration tier configured to manage mobile wallet sessions, the integration tier also including a communication application programming interface (API) and other communication mechanisms to accept messages from channels;

notification services configured to send notifications through different notification channels including one or more of short message peer-to-peer, short-message services, and simple mail transfer protocol emails;

business process services configured to implement business workflows, including at least one of executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects;

a payment handler configured to use APIs of different payment processors including one or more APIs of banks, credit and debit cards processors, and bill payment processors;

a rules engine configured to gather financial transaction statistics and use the gathered financial transaction statistics to enforce constraints including transaction constraints;

a security service configured to perform subscriber authentication;

an entity profile saved with the monetary transaction system, the entity profile associated with an entity that is to be involved in a specified transaction; and

one or more computer-readable media having stored thereon executable instructions that when executed by the one or more processors configure the system to perform at least the following:

receiving a communication message from a mobile device over one of a plurality of channels connected to the monetary transaction system, the communication message being received by an API associated with the integration tier of the monetary transaction system, the communication message indicating that a subscriber desires to deposit a specified amount of funds into a subscriber's account;

validating a status of the subscriber's account, wherein validating the status of the subscriber's account comprises communicating from the integration tier to the storage system to query attributes of the subscriber's account;

saving a pending transaction through the business process services, wherein the integration tier communicates a transaction save request to the business process services;

receiving confirmation from the business process services that the pending transaction has been saved;

sending, through the notification services, a receipt notification to the mobile device; and

wherein saving the pending transaction further comprises the following steps as orchestrated by the business process services:

ensuring, via the storage system, that the subscriber has an active account;

validating, through communication with the security service, one or more of a PIN number and an access control list;

applying with the rules engine, velocity rules;

creating with the storage system a new pending transaction history record;

holding funds from an agent account using the payment handler;

loading the funds to the subscriber's account using the payment handler; and

updating, using the storage system, a pending transaction history record to reflect the funds.

2. A method for conducting monetary transactions between subscribers and other entities within a monetary transaction system, the method executed on a computer system comprising one or more processors, the method comprising:

initiating a storage system for storing financial transaction details, customer profiles, and money containers;

initiating an integration tier configured to manage mobile wallet sessions, the integration tier also including a communication application programming interface (API) and other communication mechanisms to accept messages from channels;

initiating notification services configured to send notifications through different notification channels including one or more of short message peer-to-peer, short-message services, simple mail transfer protocol emails, and web services API;

initiating business process services configured to implement business workflows, including at least one of executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects;

initiating a payment handler configured to use APIs of different payment processors including one or more APIs of banks, credit and debit cards processors, bill payment processors;

initiating a rules engine configured to gather financial transaction statistics and use the gathered financial transaction statistics to enforce constraints including transaction constraints;

initiating a security service configured to perform subscriber authentication;

initiating an entity profile saved with the monetary transaction system, the entity profile associated with an entity that is to be involved in a specified transaction;

receiving a communication message from a mobile device over one of a plurality of channels connected to the monetary transaction system, the communication message being received by an API associated with the integration tier of the monetary transaction system, the communication message indicating that a subscriber desires to deposit a specified amount of stored value into a subscriber's account;

validating a status of the subscriber's account by querying attributes of the subscriber's account;

ensuring that the subscriber has an active account;

applying, with the rules engine, velocity rules;

holding stored value from an agent account using the payment handler;

loading the stored value to the subscriber's account using the payment handler;

updating, using the storage system, a pending transaction to reflect the stored value;

sending, through the notification services, a receipt notification to the mobile device; and

saving the pending transaction to the storage system.

3. A monetary transaction system for conducting monetary transactions between subscribers and other entities, the system comprising:

one or more processors; and

(i) a storage system for storing financial transaction details, customer profiles and money containers, the storage system configured to:

validate a status of a subscriber's account, wherein validating the status of the subscriber's account comprises communicating from an integration tier to the storage system to query attributes of the subscriber's account;

(ii) the integration tier comprising a communication application programming interface (API) and other communication mechanisms to accept messages from channels, the integration tier configured to:

manage mobile wallet sessions, and

receive a communication message from a mobile device over one of a plurality of channels connected to the monetary transaction system, the communication message being received by an API associated with the integration tier of a monetary transaction system, the communication message indicating that the subscriber desires to deposit a specified amount of funds into a subscriber's account,

(iii) notification services configured to:

send notifications through different notification channels including one or more of short message peer-to-peer, short-message services, simple mail transfer protocol emails, and web services API, and

send a receipt notification to the mobile device;

(iv) business process services configured to:

implement business workflows, including at least one of executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects,

ensure, via the storage system, that the subscriber has an active account,

apply with a rules engine, velocity rules,

hold funds from an agent account using a payment handler,

load the funds to the subscriber's account using the payment handler, and

update, using the storage system, a pending transaction to reflect the funds;

(v) the payment handler configured to:

use APIs of different payment processors including one or more APIs of banks, credit and debit cards processors, bill payment processors;

(vi) the rules engine configured to:

gather financial transaction statistics and use the gathered financial transaction statistics to enforce constraints including transaction constraints;

(vii) a security service configured to perform subscriber authentication; and

(viii) an entity profile saved with the monetary transaction system, the entity profile associated with an entity that is to be involved in a specified transaction.

4. A method for conducting monetary transactions between subscribers and other entities in a monetary transaction system, the method executed on a computer system comprising one or more processors, the method comprising:

initiating an integration tier configured to manage mobile wallet sessions and maintain the integrity of financial transactions, the integration tier also including a communication application programming interface (API) and other communication mechanisms to accept messages from channels;

initiating notification services configured to send notifications through different notification channels including one or more of short message peer-to-peer, short-message services, and simple mail transfer protocol emails;

initiating business process services configured to implement business workflows, including at least one of executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects;

initiating a security service configured to perform subscriber authentication;

initiating a storage system configured to store financial transaction details, store customer profiles, and money containers;

initiating a mobile device configured to run a monetary transaction system;

initiating a payment handler configured to use APIs of different payment processors including one or more APIs of banks, credit and debit cards processors, bill payment processors;

initiating a rules engine configured to gather financial transaction statistics and use the gathered financial transaction statistics to enforce business constraints including transaction constraints;

initiating a security service configured to perform subscriber authentication;

initiating an entity profile saved with the monetary transaction system, the entity profile associated with an entity that is to be involved in a specified transaction;

initiating a monetary transaction system subscriber profile with the monetary transaction system the monetary transaction system subscriber profile stored in the storage system of the monetary transaction system, wherein the subscriber indicates, via the monetary

transaction system, one or more specified transactions that are to be performed using the monetary transaction system;

receiving a communication message from the mobile device over one of a plurality of channels connected to the monetary transaction system, the communication message being received by an API associated with the integration tier of the monetary transaction system, the communication message comprising a pending transaction indicating that the subscriber desires to withdraw a specified amount of funds from a subscriber's account;

determining that the pending transaction is valid and in progress;

ensuring that the subscriber has an active account;

applying with the rules engine, velocity rules;

holding funds from an agent account using the payment handler;

loading the funds to the subscriber account using the payment handler;

updating, using the storage system, a pending transaction history record to reflect the funds;

sending, through the notification services, a receipt notification to the mobile device; and

saving the pending transaction to the storage system.

5. A monetary transaction system for conducting monetary transactions between subscribers and other entities, the system comprising:

one or more processors;

(i) a storage system for storing financial transaction details, store customer profiles, and money containers, the storage system configured to:

store a monetary transaction system subscriber profile, wherein the subscriber profile indicates, via the monetary transaction system, one or more specified transactions that are to be performed using the monetary transaction system,

validate a status of a subscriber's account, wherein validating the status of the subscriber's account comprises communicating from an integration tier to the storage system to query attributes of the subscriber's account,

save a pending transaction to the storage system, and

create a new pending transaction history record;

(ii) the integration tier comprising a communication application programming interface (API) and other communication mechanisms to accept messages from channels, the integration tier configured to:

manage mobile wallet sessions and maintain the integrity of financial transactions, and

receive a communication message from a mobile device over one of a plurality of channels connected to the monetary transaction system, the communication message being received by an API associated with the integration tier of the monetary transaction system, the communication message comprising a pending transaction indicating that a subscriber desires to withdraw a specified amount of funds from the subscriber's account;

(iii) notification services configured to:

send notifications through different notification channels including one or more of short message peer-to-peer, short-message services, and simple mail transfer protocol emails, and web services API,

send a receipt notification to the mobile device, and

communicate a transaction save request to a business process services;

(iv) the business process services configured to:

implement business workflows, including at least one of executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects;

(v) a payment handler configured to:

use APIs of different payment processors including one or more APIs of banks, credit and debit cards processors, and bill payment processors,

hold funds from an agent account,

load the funds to the subscriber account using the payment handler, and

updating, using the storage system, a pending transaction history record to reflect the funds;

(vi) a rules engine configured to:

gather financial transaction statistics and use the gathered financial transaction statistics to enforce business constraints including transaction constraints, and applying velocity rules;

(vii) a security service configured to perform subscriber authentication;

(viii) an entity profile saved with the monetary transaction system, the entity profile associated with an entity that is to be involved in a specified transaction; and

wherein the monetary transaction system is implemented to withdraw funds from an account associated with the subscriber using a mobile device.

6. A method for conducting monetary transactions between subscribers and other entities in a monetary transaction system, the method executed on a computer system comprising one or more processors, the system comprising:

managing mobile wallet sessions and maintaining the integrity of financial transactions, an integration tier also including a communication application programming interface (API) and other communication mechanisms to accept messages from channels;

sending notifications through different notification channels including one or more of short message peer-to-peer, short-message services and simple mail transfer protocol emails;

implementing business workflows, including at least one of executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects;

storing financial transaction details, store customer profiles, and money containers;

storing a subscriber profile in a storage system of the monetary transaction system, wherein the subscriber profile indicates, via the monetary transaction system, one or more specified transactions that are to be performed using the monetary transaction system;

using APIs of different payment processors including one or more APIs of banks, credit and debit cards processors, bill payment processors;

gathering financial transaction statistics and using the gathered financial transaction statistics to enforce business constraints including transaction constraints;

performing subscriber authentication;

associating at least one entity profile with an entity involved in a specified transaction;

receiving a communication message from a mobile device over one of a plurality of channels connected to the monetary transaction system, the communication message being received by an API associated with the integration tier of the monetary transaction system, the communication message indicating that a subscriber

desires to transfer a specified amount of funds from a subscriber's account to a recipient;

validating a status of the subscriber's account, wherein validating the status of the subscriber's account comprises communicating from the integration tier to the storage system to query attributes of the subscriber's account;

saving a pending transaction through a business process services, wherein the integration tier communicates a transaction save request to the business process services;

receiving confirmation from the business process services that a pending transaction has been saved;

sending, through a notification services, a receipt notification to the mobile device;

saving the pending transaction to the storage system;

ensuring, via the storage system, that the subscriber has an active account;

applying with a rules engine, velocity rules;

loading funds to a subscriber account using a payment handler; and

updating, using the storage system, a pending transaction history record to reflect the funds.

7. A monetary transaction system for conducting monetary transactions between subscribers and other entities, the system comprising one or more of:

one or more processors;

(i) a storage system configured to:

store financial transaction details, store customer profiles, and money containers,

store a monetary transaction system subscriber profile, wherein the monetary transaction system subscriber profile indicates, via the monetary transaction system, one or more specified transactions that are to be performed using the monetary transaction system,

validate a status of a subscriber's account, wherein validating the status of the subscriber's account comprises communicating from an integration tier to the storage system to query attributes of the subscriber's account,

save a pending transaction to the storage system,

ensure that a subscriber has an active account,

create a new pending transaction history record, and

update a pending transaction history record to reflect a specified amount of funds;

(ii) an integration tier configured to:

manage mobile wallet sessions and maintain the integrity of financial transactions,

receive a communication message from a mobile device over one of a plurality of channels connected to the monetary transaction system, the communication message being received by an API associated with the integration tier of the monetary transaction system, the communication message indicating that the subscriber desires to transfer the specified amount of funds from a subscriber's account to a recipient, and

receive confirmation from a business process services that a pending transaction has been saved;

(iii) notification services configured to:

send notifications through different notification channels including one or more of short message peer-to-peer, short-message services and simple mail transfer protocol emails, and

send a receipt notification to the mobile device;

(iv) business process services configured to:

implement business workflows, including at least one of executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects;

(v) a payment handler configured to:

use APIs of different payment processors including one or more APIs of banks, credit and debit cards processors, bill payment processors, and

load the funds to a subscriber account using the payment handler;

(vi) a rules engine configured to:

gather financial transaction statistics and use the gathered financial transaction statistics to enforce business constraints including transaction constraints, and

apply velocity rules;

(vii) a security service configured to perform subscriber authentication;

(viii) at least one entity profile saved within the monetary transaction system, the at least one entity profile being associated with an entity involved in specified transaction; and

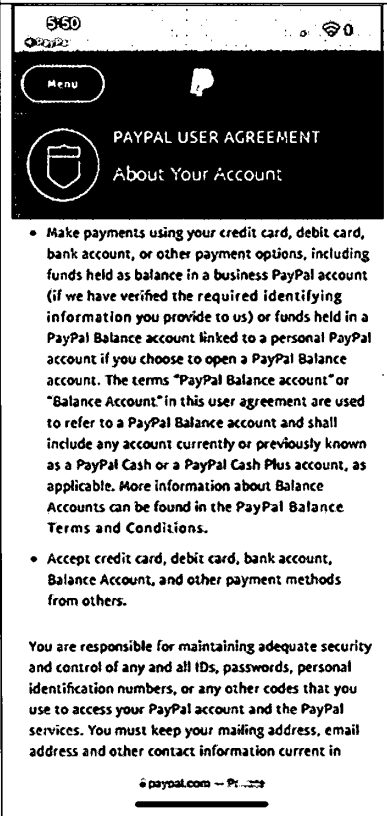
wherein the monetary transaction system is implemented to transfer funds using a mobile device configured to run a monetary transaction system.

* * * * *

Exhibit F
PayPal Infringement Chart for
U.S. Patent No. 11,120,413

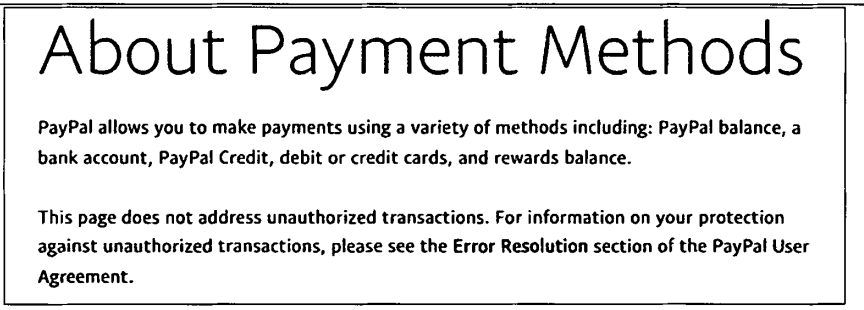
U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
1. A monetary transaction system for conducting monetary transactions between subscribers and other entities, the system comprising:	Upon information and belief, the PayPal System manages a transaction system and payment application that allows users to make monetary transactions between subscribers and other entities. SEND AND REQUEST MONEY FOR FREE • When funded by a bank account or with your PayPal balance, it's free and secure to send money or ask for it back from friends and family in the US. • Just type a name, email or phone number and PayPal will find the right person for you if they have an account. • Request money quickly and securely from friends or family and personalize your payments with animations, stickers, emojis and more. See https://apps.apple.com/app/id283646709?mt=8 (last accessed on February 25, 2022).

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 See PayPal User Agreement on PayPal Mobile App.

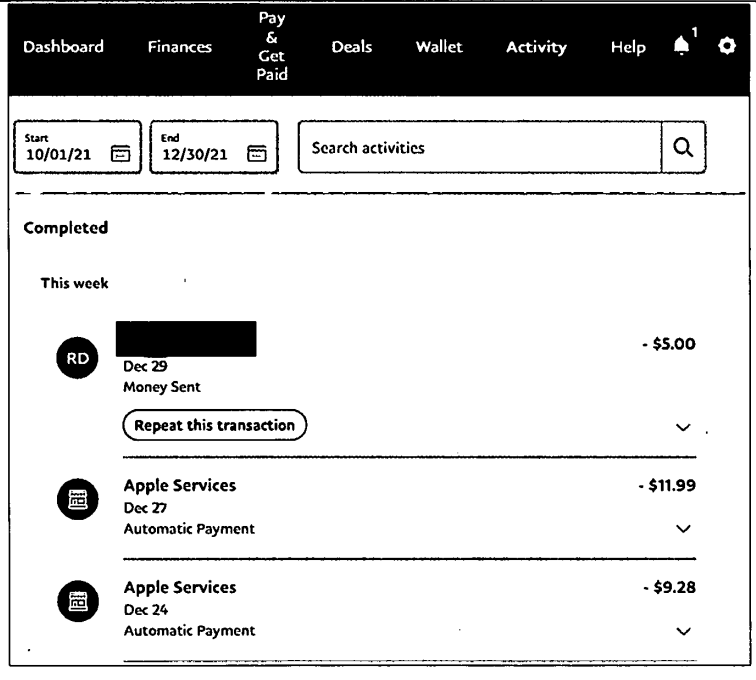
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 259 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 See https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022).
1[a] One or more processors.	See Preamble.
1[b] a storage system configured to store financial transaction details, customer profiles and money containers	Upon information and belief, the PayPal System includes a storage system configured to store financial transaction details, customer profiles and money containers. For example, financial transactions are stored and can be accessed via the PayPal website and the user login. The user profile and money containers can also be accessed.

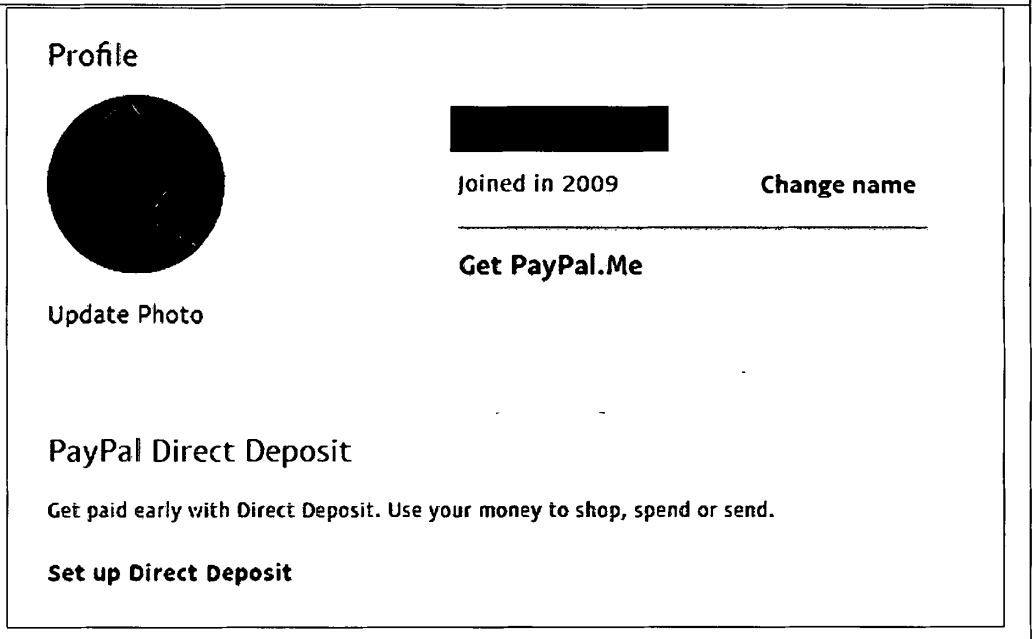
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 260 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 261 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* Screenshots of PayPal website accessing stored information. Upon information and belief, the PayPal System allows a user to make payments using a variety of methods including: PayPal balance, a bank account, PayPal Credit, debit or credit cards, and rewards balance.

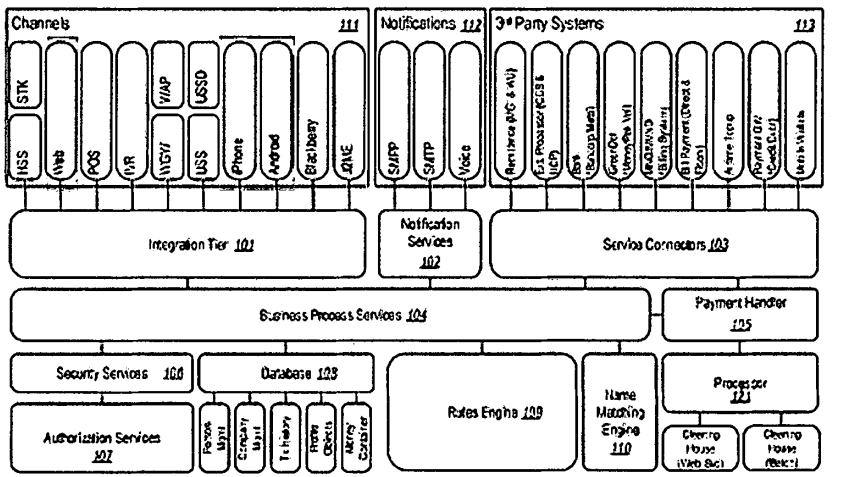
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 262 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
1[c] an integration tier configured to manage mobile wallet sessions, the integration tier also including a communication application programming interface (API) and other communication mechanisms to accept messages from channels;	Upon information and belief, the PayPal System includes an integration tier. The integration tier is configured to manage mobile wallet sessions. The integration tier, for example, handles communications from different mobile phones (e.g. Apple and/or Android) and uses API and other communication mechanisms to communicate.  We have versions of our app for iOS, Android, and Windows. In a few moments you can log on to PayPal, check your balance, pay bills, and more. It is easy, fast, and secure. With PayPal there are no borders. Download Now: iPhone | Android https://www.paypal.com/bs/webapps/mpp/shop/apps (last accessed on February 25, 2022).

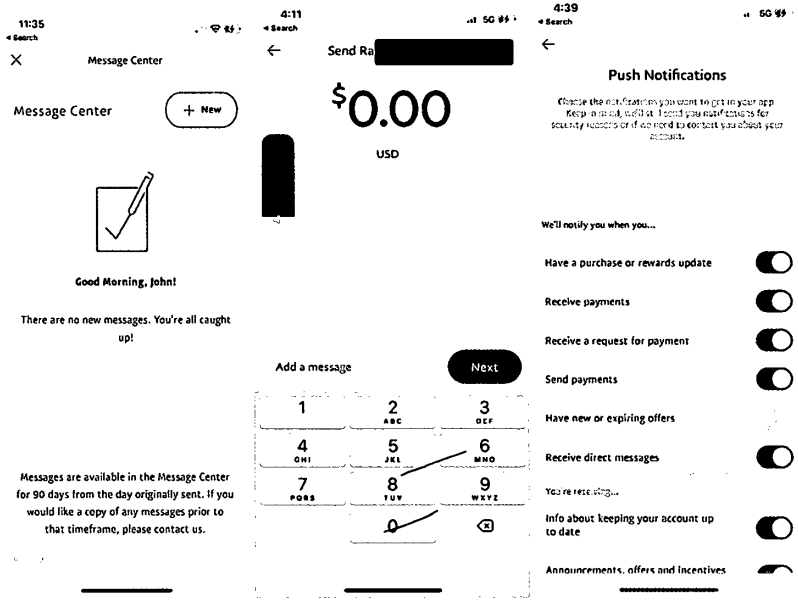
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 263 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *Figure 1* *See e.g.* '386 Patent Figure 1. Upon information and belief, the PayPal System provides REST APIs for new integrations. These APIs use HTTP methods, a RESTful endpoint structure, the OAuth 2.0 protocol, and JSON-formatted payloads. The REST APIs can be used to incorporate the PayPal System's functionality

U.S. Patent Feb. 13, 2018 Sheet 1 of 46 US 9,892,386 B2

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	into a user's web and mobile apps. Standard PayPal APIs can be accessed via the PayPal Developer Portal (*see* http://developer.paypal.com (last accessed on February 25, 2022)).
1[d] notification services configured to send notifications through different notification channels including one or more of short message peer-to-peer, short-message services, and simple mail transfer protocol emails;	Upon information and belief, the PayPal system includes notification services that are capable of sending notifications though various communication channels including short message peer-to-peer, short-message services and simple mail transfer protocol emails. 

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	See Screenshots of PayPal Mobile app showing ability to send/receive messages.
1[e] business process services configured to implement business workflows, including at least one of executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects;	Upon information and belief, the PayPal system includes business process services which include at least executing financial transactions as well as other business services. About Payment Methods PayPal allows you to make payments using a variety of methods including: PayPal balance, a bank account, PayPal Credit, debit or credit cards, and rewards balance. This page does not address unauthorized transactions. For information on your protection against unauthorized transactions, please see the Error Resolution section of the PayPal User Agreement. *See* https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022).

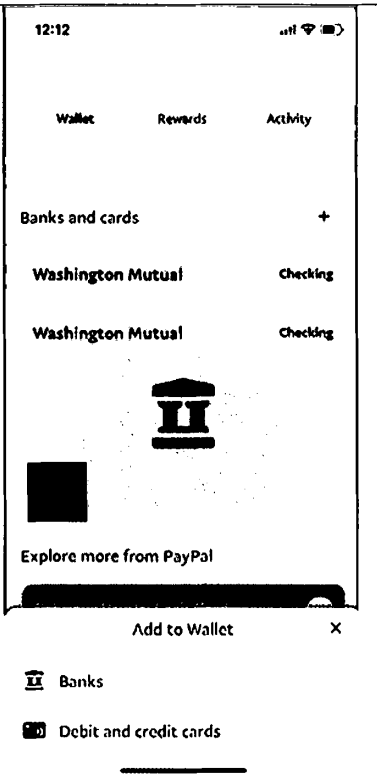
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 266 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	Why are limitations placed on an account? There can be several reasons for an account limitation: • *An unauthorized person may be using your account.* If PayPal believes someone is using your account without your knowledge, the account could be limited to protect you from fraudulent charges while PayPal investigates the suspicious transactions. Similar steps may be taken if your debit or credit card issuer or bank notifies PayPal that someone has used your card or bank account without permission. • *The account is out of compliance with regulatory requirements.* Limitations can also be placed on an account that has been found to be out of compliance with regulatory requirements. For example, if you receive donations, you're required to provide documents confirming you're a registered nonprofit organization. PayPal may limit your account while you gather those documents or while we're working with you to satisfy any other regulatory requirements. The same is true if you don't follow PayPal's **Acceptable Use Policy**—selling banned items, such as prescription drugs or guns, for example. • *Your account has a high number of claims and chargebacks.* When there's a high number of **buyer claims and chargebacks** to your account, we may review your account. While we're reviewing, you may experience an account limitation. • *Sudden, rapid changes in what or how much you sell.* If you start to sell an entirely new type of product, specifically higher-end items like jewelry; or there's a rapid increase in sales volume, your account may be limited while PayPal reviews it. *See* https://www.paypal.com/us/brc/article/understanding-account-limitations (last accessed on February 25, 2022).
1 [f] a payment handler configured to use APIs of different payment processors including one or more	Upon information and belief, the PayPal System, includes a payment handler which can interface with APIs of payment processors for banks, credit card, debit card, and bill payment processors.

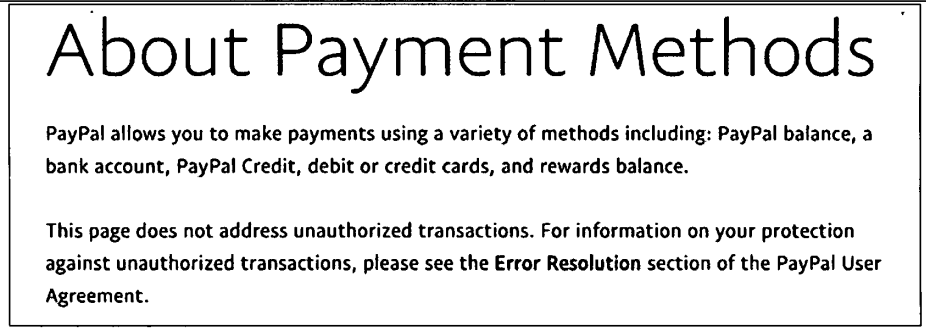
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 267 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
APIs of banks, credit and debit cards processors, and bill payment processors;	 *See* Screenshot of PayPal Mobile Application identifying bank account with option to add credit and debit cards.

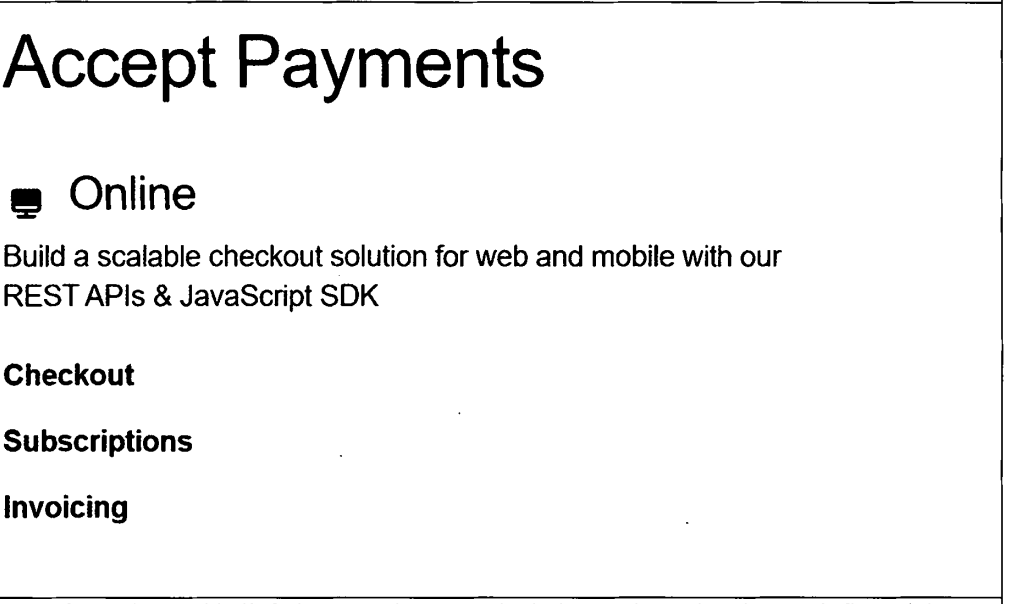
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 268 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022). Upon information and belief, the PayPal System provides REST APIs for new integrations. These APIs use HTTP methods, a RESTful endpoint structure, the OAuth 2.0 protocol, and JSON-formatted payloads. The REST APIs can be used to incorporate the PayPal System's functionality into a user's web and mobile apps. Standard PayPal APIs can be accessed via the PayPal Developer Portal (*see* http://developer.paypal.com (last accessed on February 25, 2022)).

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 269 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	
1[g] and 1[h] a rules engine configured to gather financial transaction statistics and use the gathered financial transaction statistics to enforce constraints including transaction constraints; a security service configured to perform subscriber authentication;	Upon information and belief, the PayPal System, includes a rule engine that track financial transactions and enforce constraints including transaction constraints. Upon information and belief, the PayPal System also discloses a security service that performs subscriber authentication.

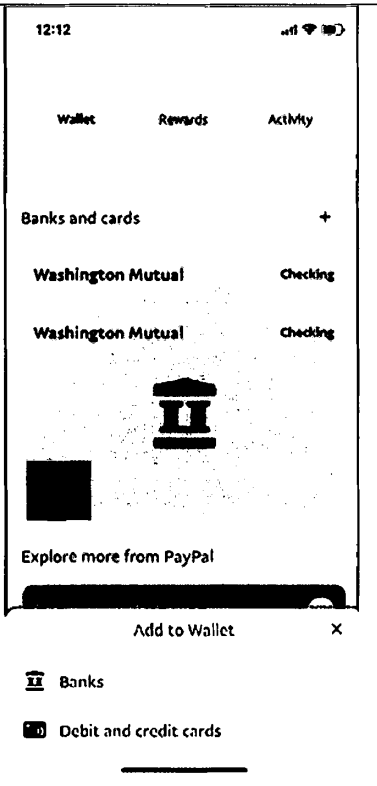
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 270 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	Why are limitations placed on an account? There can be several reasons for an account limitation: • *An unauthorized person may be using your account.* If PayPal believes someone is using your account without your knowledge, the account could be limited to protect you from fraudulent charges while PayPal investigates the suspicious transactions. Similar steps may be taken if your debit or credit card issuer or bank notifies PayPal that someone has used your card or bank account without permission. • *The account is out of compliance with regulatory requirements.* Limitations can also be placed on an account that has been found to be out of compliance with regulatory requirements. For example, if you receive donations, you're required to provide documents confirming you're a registered nonprofit organization. PayPal may limit your account while you gather those documents or while we're working with you to satisfy any other regulatory requirements. The same is true if you don't follow PayPal's **Acceptable Use Policy**—selling banned items, such as prescription drugs or guns, for example. • *Your account has a high number of claims and chargebacks.* When there's a high number of **buyer claims and chargebacks** to your account, we may review your account. While we're reviewing, you may experience an account limitation. • *Sudden, rapid changes in what or how much you sell.* If you start to sell an entirely new type of product, specifically higher-end items like jewelry; or there's a rapid increase in sales volume, your account may be limited while PayPal reviews it. *See* https://www.paypal.com/us/brc/article/understanding-account-limitations (last accessed on February 25, 2022)
1[i] an entity profile saved with the monetary transaction system, the entity profile associated with an entity that is to be involved in a specified transaction; and	Upon information and belief, the PayPal System, includes a payment handler which can interface with APIs of payment processors for banks, credit card, debit card, and bill payment processors.

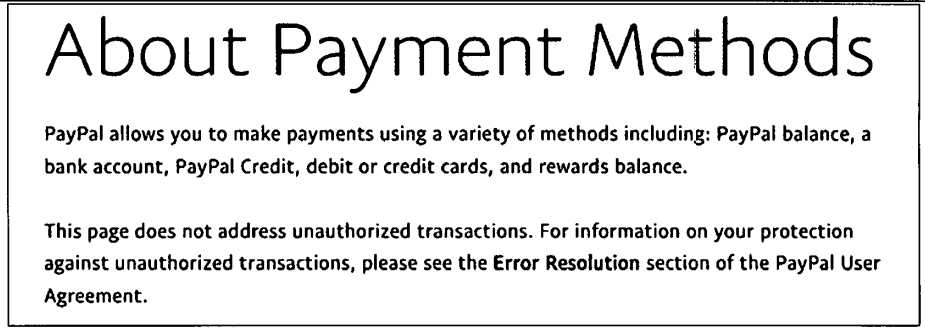
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 271 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* Screenshot of PayPal Mobile Application identifying bank account with option to add credit and debit cards.

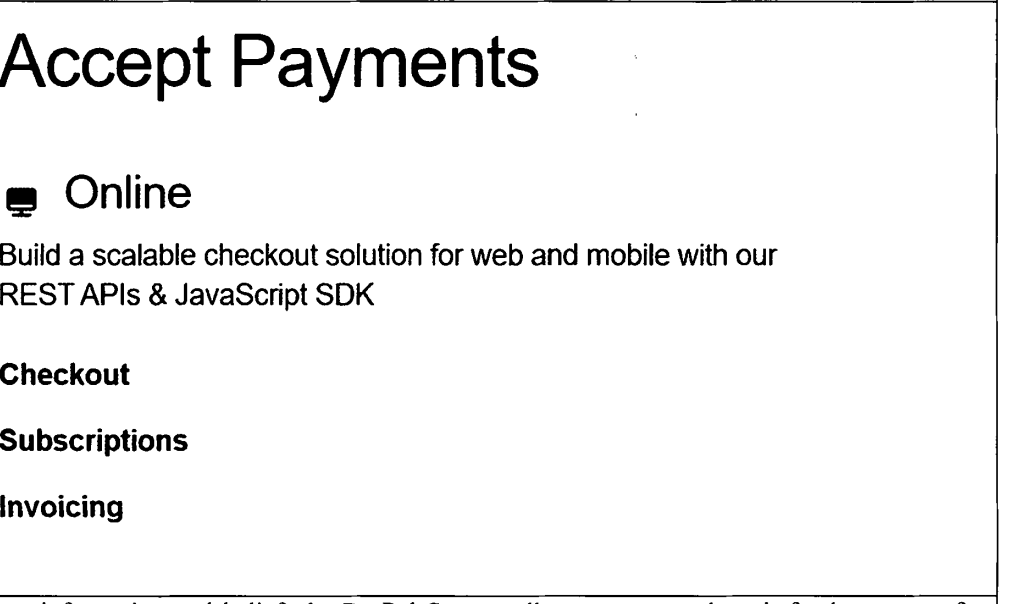
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 272 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

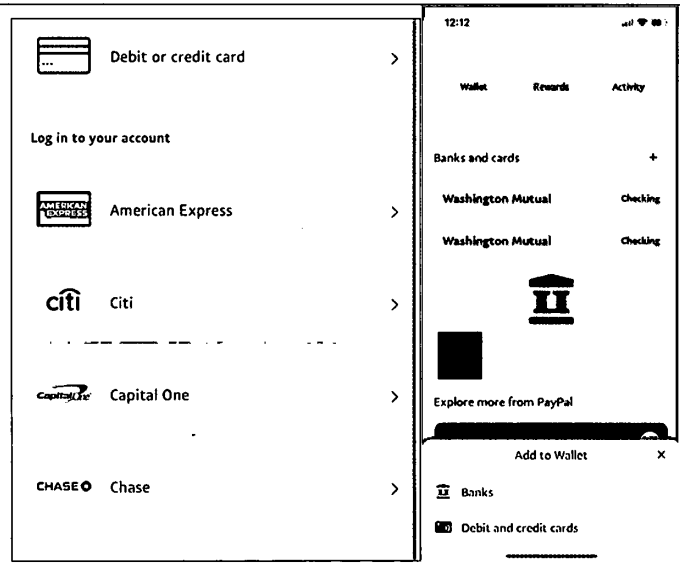
U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022). Upon information and belief, the PayPal System provides REST APIs for new integrations. These APIs use HTTP methods, a RESTful endpoint structure, the OAuth 2.0 protocol, and JSON-formatted payloads. The REST APIs can be used to incorporate the PayPal System's functionality into a user's web and mobile apps. Standard PayPal APIs can be accessed via the PayPal Developer Portal (*see* http://developer.paypal.com (last accessed on February 25, 2022)).

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 273 of 381

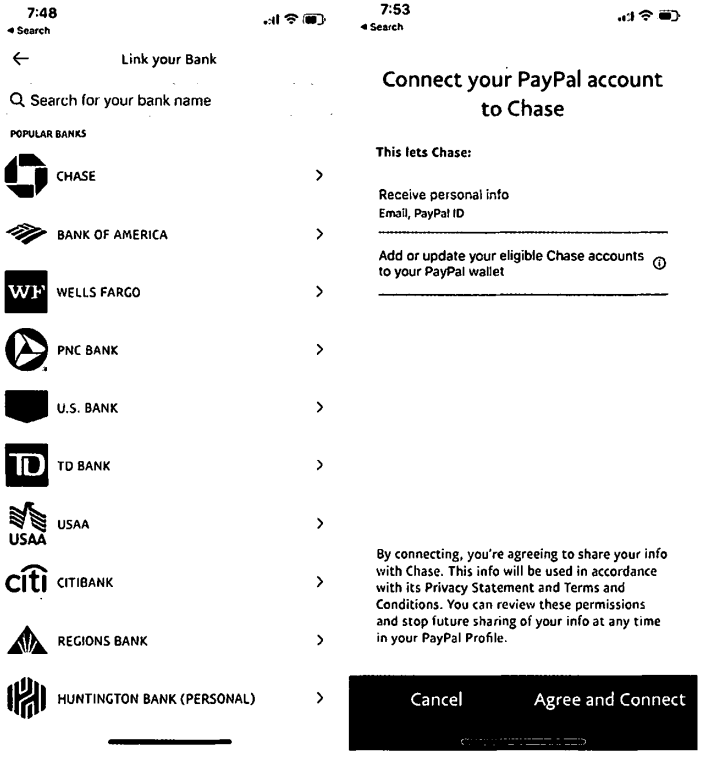
PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	
1[m] [n] [o] [p] [q] one or more computer-readable media having stored thereon executable instructions that when executed by the one or more processors configure the system to perform at least the following: receiving a communication message from a mobile device over	Upon information and belief, the PayPal System allows a user to deposit funds as part of a transaction with an entity that can be involved in a specified transaction, including for example, accessing a Chase bank account that is linked to the PayPal account.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

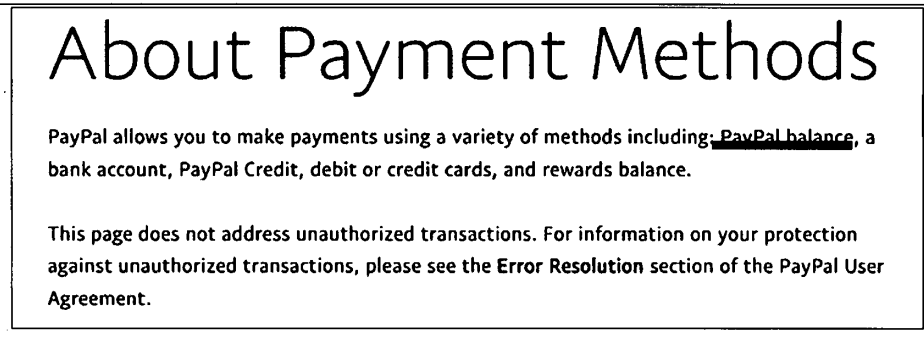
U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
one of a plurality of channels connected to the monetary transaction system, the communication message being received by an API associated with the integration tier of the monetary transaction system, the communication message indicating that a subscriber desires to deposit a specified amount of funds into a subscriber's account; validating a status of the subscriber's account, wherein validating the status of the subscriber's account comprises communicating from the integration tier to the storage system to query attributes of the subscriber's account; saving a pending transaction through the business process services, wherein the integration tier communicates a transaction save request to the business process services; receiving confirmation from the business process services that the pending transaction has been saved;	

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
sending, through the notification services, a receipt notification to the mobile device; and	 *See* Screenshot of PayPal Mobile Application allowing users to link credit card and/or bank accounts to the PayPal System with bank specific privacy statement and showing an active legacy Washington Mutual account.

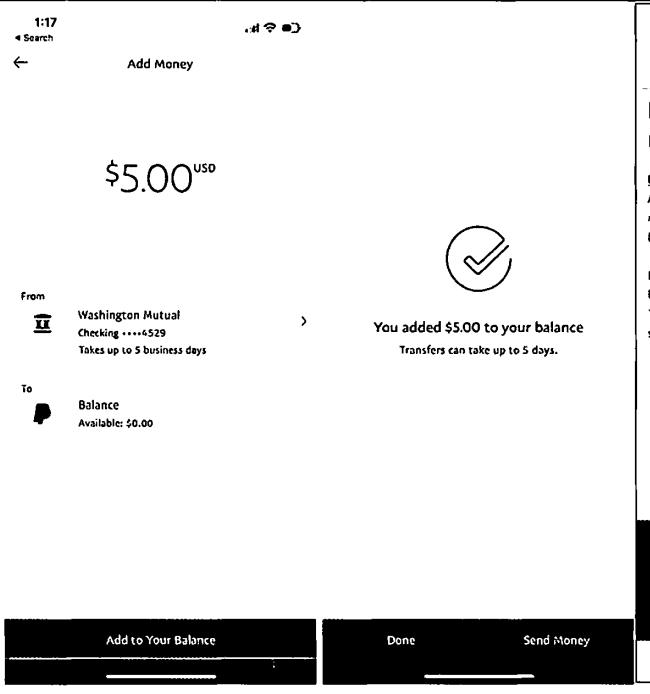
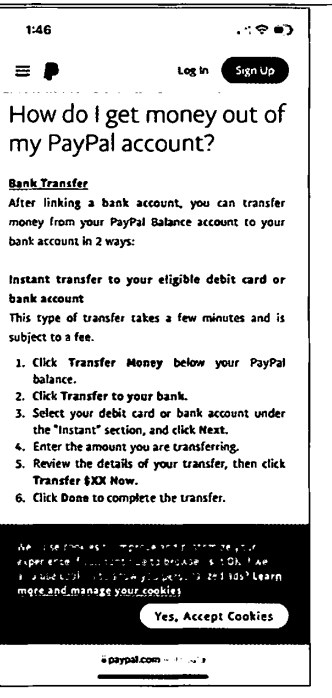
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 276 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022). Upon information and belief, the PayPal System meets the following limitations and is capable of facilitating a deposit of funds to and from a PayPal account linked to a bank, for example chase Bank. Discovery and review of PayPal internal documents are needed for this limitation.

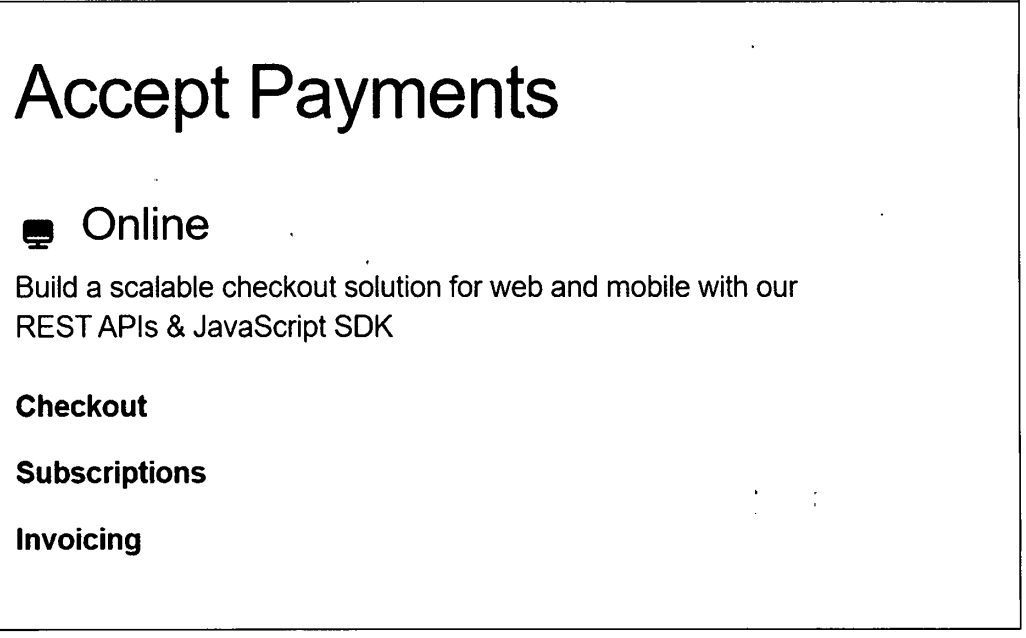
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 277 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	  Upon information and belief, the PayPal System provides REST APIs for new integrations. These APIs use HTTP methods, a RESTful endpoint structure, the OAuth 2.0 protocol, and JSON-formatted payloads. The REST APIs can be used to incorporate the PayPal System's functionality into a user's web and mobile apps. Standard PayPal APIs can be accessed via the PayPal Developer Portal (*see* http://developer.paypal.com (last accessed on February 25, 2022)).

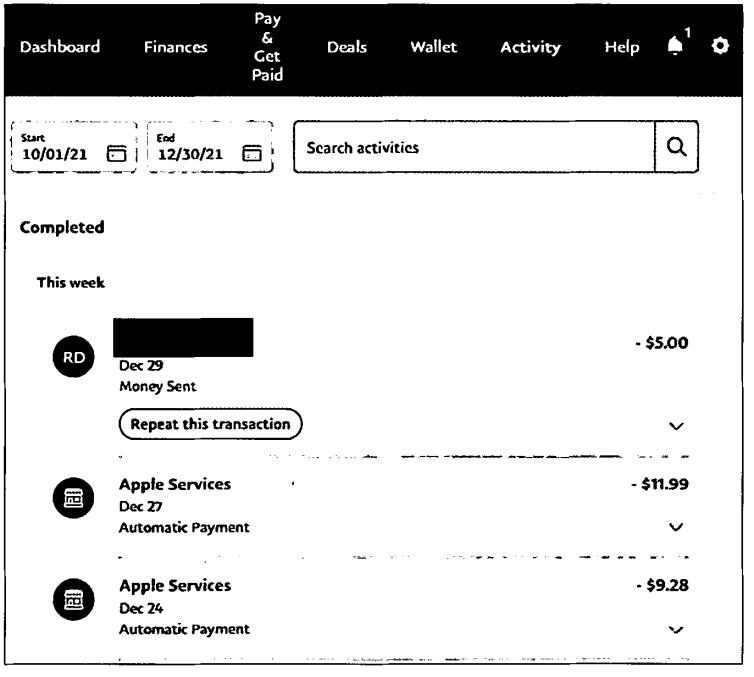
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 278 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 279 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
1[r][s][t][u][v][w] wherein saving the pending transaction further comprises the following steps as orchestrated by the business process services: ensuring, via the storage system, that the subscriber has an active account; validating, through communication with the security service, one or more of a PIN number and an access control list; applying with the rules engine, velocity rules; creating with the storage system a new pending transaction history record; holding funds from an agent account using the payment handler; loading the funds to the subscriber's account using the payment handler; and	Upon information and belief, the PayPal System meets the following limitations and is capable of facilitating a deposit of funds to and from a PayPal account linked to a bank, for example chase Bank. Discovery and review of PayPal internal documents are needed for this limitation. 

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
updating, using the storage system, a pending transaction history record to reflect the funds.	**Why are limitations placed on an account?** There can be several reasons for an account limitation: • *An unauthorized person may be using your account.* If PayPal believes someone is using your account without your knowledge, the account could be limited to protect you from fraudulent charges while PayPal investigates the suspicious transactions. Similar steps may be taken if your debit or credit card issuer or bank notifies PayPal that someone has used your card or bank account without permission. • *The account is out of compliance with regulatory requirements.* Limitations can also be placed on an account that has been found to be out of compliance with regulatory requirements. For example, if you receive donations, you're required to provide documents confirming you're a registered nonprofit organization. PayPal may limit your account while you gather those documents or while we're working with you to satisfy any other regulatory requirements. The same is true if you don't follow PayPal's **Acceptable Use Policy**—selling banned items, such as prescription drugs or guns, for example. • *Your account has a high number of claims and chargebacks.* When there's a high number of **buyer claims and chargebacks** to your account, we may review your account. While we're reviewing, you may experience an account limitation. • *Sudden, rapid changes in what or how much you sell.* If you start to sell an entirely new type of product, specifically higher-end items like jewelry; or there's a rapid increase in sales volume, your account may be limited while PayPal reviews it. *See* https://www.paypal.com/us/brc/article/understanding-account-limitations (last accessed on February 25, 2022). Upon information and belief, the PayPal system also performs velocity check, including to identify fraud, to address regulatory requirements, or filter for transaction issues. Upon information and belief, the PayPal System includes velocity checks. These checks for example, monitor the number of transactions the user receive by minute, hour, etc. and the IP addresses of the user's customers. PayPal's Fraud Protection Services in the PayPal System include velocity checks along with many other filters to help assist in preventing fraud.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 281 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	Account number velocity filter The account number velocity filter is triggered for excessive use of a card within a short period of time. What does the filter do? The account number velocity filter triggers when any credit card account number is used five times within a three-day (72-hour) period. *See e.g.* https://developer.paypal.com/api/nvp-soap/payflow/fraud-protection/ (showing velocity functionality) (last accessed on February 25, 2022). Upon information and belief, the PayPal System utilizes a PayPal Security Key, which is an additional layer of security at login. In addition to the user's password, the user can enter a One-Time PIN (OTP) that's unique for each login attempt.  **PayPal Security Key** This is your free additional layer of security at login. In addition to your password, you'll enter a One-Time PIN (OTP) that's unique for each login attempt. Register your mobile phone to use PayPal Security Key

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 282 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 11,120,413 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	Upon information and belief, the PayPal System includes an access-control list (ACL) such as a list of permissions associated with system resources. A user can manually grant the PayPal System permissions to a third party to access specific information in the user's account at the PayPal system and perform PayPal API operations on the user's behalf. For example, if the user is integrating with a third-party shopping cart, the cart owner needs permission to the user's PayPal account to perform specific operations on behalf of the user. Upon information and belief, by way of example, the PayPal systems utilizes OAuth 2.0 protocol to provide authenticated and/or authorized access to various protected resources. In particular, OAuth 2.0 scopes are used to specify or limit the type of access (i.e., ACL) that is associated with a granted access token. *See* https://oauth.net/2/scope/ (last accessed on February 25, 2022); https://developer.paypal.com/api/rest/ (last accessed on February 25, 2022).

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 283 of 381

Exhibit G
U.S. Patent No. 9,208,488

US009208488B2

(12) **United States Patent**
Liberty

(10) **Patent No.: US 9,208,488 B2**
(45) **Date of Patent: Dec. 8, 2015**

(54) **USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS**

(71) Applicant: **MOZIDO, INC.**, Austin, TX (US)

(72) Inventor: **Michael A. Liberty**, Orlando, FL (US)

(73) Assignee: **MOZIDO, INC.**, Austin, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **13/680,824**

(22) Filed: **Nov. 19, 2012**

(65) **Prior Publication Data**

US 2013/0132219 A1 May 23, 2013

Related U.S. Application Data

(60) Provisional application No. 61/562,301, filed on Nov. 21, 2011.

(51) **Int. Cl.**

G06Q 20/00	(2012.01)
G06G 1/12	(2006.01)
G06Q 20/36	(2012.01)
G06Q 20/20	(2012.01)
G06Q 20/06	(2012.01)

(52) **U.S. Cl.**

CPC ***G06Q 20/36*** (2013.01); ***G06Q 20/065*** (2013.01); ***G06Q 20/202*** (2013.01)

(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,717,374	A	2/1998	Smith
5,828,739	A	10/1998	Nakanishi
5,991,749	A	11/1999	Morrill, Jr.
6,021,397	A	2/2000	Jones et al.
6,175,823	B1	1/2001	Van Dusen
6,185,545	B1	2/2001	Resnick et al.

(Continued)

FOREIGN PATENT DOCUMENTS

AU	2007312879	4/2008
CA	2666616	4/2008

(Continued)

OTHER PUBLICATIONS

International Search Report for PCT/US2012/066013 dated Jan. 29, 2013.

(Continued)

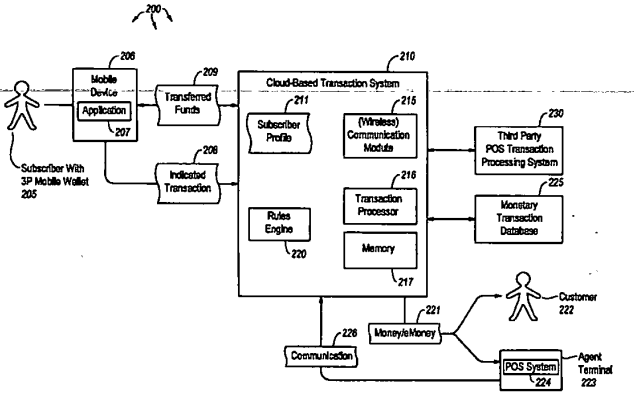
Primary Examiner — Paul Danneman

(74) *Attorney, Agent, or Firm* — Workman Nydegger

(57) **ABSTRACT**

Embodiments are directed to performing a transaction using a third party mobile wallet, performing a transaction using a third party point of sale (POS) system and to making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. In one scenario, a cloud-based transaction platform is provided, which receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that a customer desires to perform a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the agent communication to a third party mobile wallet platform, receives communication from the third party mobile wallet platform confirming processing of the transaction, and sends communication to the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

22 Claims, 9 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

6,250,557 B1 6/2001 Forslund
6,415,156 B1 7/2002 Stadelmann
6,622,015 B1 9/2003 Himmel
6,697,839 B2 2/2004 Sini
6,714,797 B1 3/2004 Rautila
6,736,322 B2 5/2004 Gobburu
6,819,219 B1 11/2004 Bolle
6,840,448 B2 1/2005 Fukushima
6,862,575 B1 3/2005 Antilla et al.
6,873,974 B1 3/2005 Schutzer
6,957,342 B2 10/2005 Vantanen
7,016,532 B2 3/2006 Boncyk
7,024,174 B2 4/2006 Nagy et al.
7,054,430 B2 5/2006 Lynam
7,069,001 B2 6/2006 Rupp et al.
7,089,208 B1 8/2006 Levchin et al.
7,099,850 B1 8/2006 Mann, II et al.
7,100,821 B2 9/2006 Rasti
7,107,247 B2 9/2006 Kinoshita et al.
7,110,972 B1 9/2006 Handa et al.
7,221,939 B2 5/2007 Ylitalo
7,240,836 B2 7/2007 Vrotsos et al.
7,248,855 B2 7/2007 Joyce et al.
7,255,264 B2 8/2007 De Leon
7,275,685 B2 10/2007 Gray et al.
7,322,043 B2 1/2008 Letsinger
7,325,132 B2 1/2008 Takayama
7,334,720 B2 2/2008 Hulst et al.
7,347,361 B2 3/2008 Lovett
7,349,871 B2 3/2008 Labrou et al.
7,353,382 B2 4/2008 Labrou et al.
7,363,261 B2 4/2008 Whitehead, Jr. et al.
7,403,652 B2 7/2008 Boncyk
7,461,010 B2 12/2008 Kwan
7,461,028 B2 12/2008 Wronski, Jr.
7,477,780 B2 1/2009 Boncyk
7,494,055 B2 2/2009 Fernandes et al.
7,512,098 B2 3/2009 Jiang
7,527,194 B2 5/2009 Truitt
7,548,915 B2 6/2009 Ramer
7,562,818 B1 7/2009 Bierbaum
7,564,469 B2 7/2009 Cohen
7,565,008 B2 7/2009 Boncyk
7,606,560 B2 10/2009 Labrou
7,657,489 B2 2/2010 Stambaugh
7,677,973 B2 3/2010 Van Luchene
7,680,324 B2 3/2010 Boncyk
7,689,506 B2 3/2010 Fei et al.
7,694,876 B2 4/2010 Barnes et al.
7,699,218 B2 4/2010 Garcia et al.
7,708,194 B2 5/2010 Vawter
7,729,963 B1 6/2010 Lego et al.
7,729,987 B1 6/2010 Wakim et al.
7,748,618 B2 7/2010 Vawter
7,774,076 B2 8/2010 Skowronek
7,774,231 B2 8/2010 Pond et al.
7,775,437 B2 8/2010 Cohen
7,784,684 B2 8/2010 Labrou et al.
7,801,826 B2 9/2010 Labrou et al.
7,819,307 B2 10/2010 Lyons
7,822,688 B2 10/2010 Labrou
7,823,772 B2 11/2010 Vawter
7,848,500 B2 12/2010 Lynam
7,848,504 B2 12/2010 Lynam
7,865,414 B2 1/2011 Fung et al.
7,865,431 B2 1/2011 Takayama
7,877,605 B2 1/2011 Labrou et al.
7,881,529 B2 2/2011 Boncyk
7,886,962 B2 2/2011 Vawter
7,890,424 B1 2/2011 Wakim et al.
7,899,243 B2 3/2011 Boncyk
7,899,252 B2 3/2011 Boncyk
7,937,302 B1 5/2011 Lego et al.
7,937,305 B1 5/2011 Lego et al.
7,942,317 B2 5/2011 Racz et al.
7,958,052 B2 6/2011 Powell
7,967,196 B1 6/2011 Bierbaum
7,979,026 B2 7/2011 Hulvey
7,988,060 B2 8/2011 Killian et al.
8,016,185 B2 9/2011 Modi
8,019,365 B2 9/2011 Fisher
8,033,458 B2 10/2011 Hulst et al.
8,041,338 B2 10/2011 Chen
8,052,042 B2 11/2011 Kolinski-Schultz et al.
8,060,012 B2 11/2011 Sklovsky
8,061,598 B2 11/2011 Racz et al.
8,073,783 B2 12/2011 Felsted et al.
8,077,042 B2 12/2011 Peeters
8,090,945 B2 1/2012 Singhal
8,095,113 B2 1/2012 Kean
8,116,734 B2 2/2012 Vawter
8,116,773 B2 2/2012 Chitrapu
8,118,221 B2 2/2012 Racz et al.
8,121,945 B2 2/2012 Rackley
8,130,242 B2 3/2012 Cohen
8,145,568 B2 3/2012 Rackley
8,160,959 B2 4/2012 Rackley
8,170,485 B2 5/2012 Hulvey
8,190,087 B2 5/2012 Fisher
8,195,576 B1 6/2012 Grigg
8,196,131 B1 6/2012 von Behren
8,213,470 B2 7/2012 Gu et al.
8,218,873 B2 7/2012 Boncyk
8,229,354 B2 7/2012 Sklovsky
8,239,325 B2 8/2012 Schwarz
8,275,312 B2 9/2012 Fisher
8,290,433 B2 10/2012 Fisher
8,332,272 B2 12/2012 Fisher
8,333,319 B2 12/2012 Roth
8,336,772 B2 12/2012 Racz et al.
8,352,323 B2 1/2013 Fisher
8,355,670 B2 1/2013 White
8,359,265 B2 1/2013 Van Rensburg
8,360,329 B2 1/2013 Grigg
8,374,916 B2 2/2013 White
8,380,177 B2 2/2013 Laracey
8,396,793 B2 3/2013 Hill
8,487,771 B2 7/2013 Hsieh et al.
8,577,803 B2 11/2013 Chatterjee et al.
8,612,325 B2 11/2013 Laracey
8,632,000 B2 1/2014 Laracey
2001/0011248 A1 8/2001 Himmel
2001/0037264 A1 11/2001 Husemann
2001/0042785 A1 11/2001 Walker et al.
2002/0042776 A1 4/2002 Woo et al.
2002/0052754 A1 5/2002 Joyce et al.
2002/0060246 A1 5/2002 Gobburu
2002/0065774 A1 5/2002 Young et al.
2002/0069123 A1 6/2002 Soderlind et al.
2002/0131404 A1 9/2002 Mehta et al.
2002/0141586 A1 10/2002 Margalit
2002/0152177 A1 10/2002 Wolf
2002/0161708 A1 10/2002 Offer
2003/0001010 A1 1/2003 Schmidt et al.
2003/0055735 A1 3/2003 Cameron
2003/0071115 A1 4/2003 Horn et al.
2003/0154165 A1 8/2003 Horn et al.
2003/0195842 A1 10/2003 Reece
2004/0117302 A1 6/2004 Weichert et al.
2004/0181531 A1 9/2004 Becker
2004/0205618 A1 10/2004 Sini
2004/0235450 A1 11/2004 Rosenberg
2004/0248554 A1 12/2004 Khan et al.
2005/0070265 A1 3/2005 Korpinen
2005/0080697 A1 4/2005 Foss, Jr. et al.
2005/0187873 A1 8/2005 Labrou
2005/0199709 A1 9/2005 Linlor
2005/0222961 A1 10/2005 Staib
2006/0116892 A1 6/2006 Grimes
2006/0136901 A1 6/2006 Nichols
2006/0165060 A1 7/2006 Dua
2006/0179452 A1 8/2006 Amodeo et al.
2006/0200427 A1 9/2006 Morrison et al.
2006/0253335 A1 11/2006 Keena et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2006/0287004 A1 12/2006 Fuqua
2007/0033285 A1 2/2007 Shiigi
2007/0106564 A1 5/2007 Matotek et al.
2007/0123305 A1 5/2007 Chen
2007/0125838 A1 6/2007 Law et al.
2007/0125840 A1 6/2007 Law et al.
2007/0162471 A1 7/2007 Samuelsson
2007/0179885 A1 8/2007 Bird et al.
2007/0198432 A1 8/2007 Pitroda
2007/0203850 A1 8/2007 Singh et al.
2007/0241189 A1 10/2007 Slavin
2007/0244811 A1 10/2007 Tumminaro
2007/0255620 A1 11/2007 Tumminaro et al.
2007/0255652 A1 11/2007 Tumminaro et al.
2007/0255653 A1 11/2007 Tumminaro et al.
2007/0265984 A1 11/2007 Santhana
2008/0006685 A1 1/2008 Rackley
2008/0010191 A1 1/2008 Rackley
2008/0010196 A1 1/2008 Rackley
2008/0010204 A1 1/2008 Rackley
2008/0010215 A1 1/2008 Rackley
2008/0011825 A1 1/2008 Giordano et al.
2008/0017704 A1 1/2008 VanDeburg et al.
2008/0040265 A1 2/2008 Rackley
2008/0040285 A1 2/2008 Wankmueller
2008/0052192 A1 2/2008 Fisher
2008/0065490 A1 3/2008 Novick et al.
2008/0097851 A1 4/2008 Bemmel
2008/0126145 A1 5/2008 Rackley
2008/0126929 A1 5/2008 Bykov
2008/0143487 A1 6/2008 Hulvey
2008/0197190 A1 8/2008 Fujita
2008/0204358 A1 8/2008 Sato
2008/0208743 A1 8/2008 Arthur et al.
2008/0208744 A1 8/2008 Arthur et al.
2008/0208762 A1 8/2008 Arthur et al.
2008/0210751 A1 9/2008 Kim
2008/0249927 A1 10/2008 Rethorn
2008/0249928 A1 10/2008 Hill et al.
2008/0249930 A1 10/2008 Hill
2008/0249933 A1 10/2008 Rethorn
2008/0255947 A1 10/2008 Friedman
2008/0275779 A1 11/2008 Lakshminarayanan
2008/0281737 A1 11/2008 Fajardo
2009/0037326 A1 2/2009 Chitti
2009/0055322 A1 2/2009 Bykov
2009/0063312 A1 3/2009 Hurst
2009/0081989 A1 3/2009 Wuhrer
2009/0098854 A1 4/2009 Park
2009/0104888 A1 4/2009 Cox
2009/0106148 A1 4/2009 Prada
2009/0108015 A1 4/2009 Kreamer
2009/0119190 A1 5/2009 Realini
2009/0132362 A1 5/2009 Fisher
2009/0132392 A1 5/2009 Davis
2009/0138366 A1 5/2009 Bemmel et al.
2009/0144161 A1 6/2009 Fisher
2009/0156190 A1 6/2009 Fisher
2009/0157546 A1 6/2009 Garcia et al.
2009/0177578 A1 7/2009 Garcia et al.
2009/0177581 A1 7/2009 Garcia et al.
2009/0210308 A1 8/2009 Toomer
2009/0222353 A1 9/2009 Guest et al.
2009/0222358 A1 9/2009 Bednarek
2009/0234751 A1 9/2009 Chan et al.
2009/0248537 A1 10/2009 Sarkeshik
2009/0254440 A1 10/2009 Pharris
2009/0254479 A1 10/2009 Pharris
2009/0265272 A1 10/2009 Dill et al.
2009/0281904 A1 11/2009 Pharris
2009/0288012 A1 11/2009 Hertel
2009/0299844 A1 12/2009 Reilly
2009/0307132 A1 12/2009 Phillips
2010/0010964 A1 1/2010 Skowronek
2010/0023449 A1 1/2010 Skowronek
2010/0030651 A1 2/2010 Matotek et al.
2010/0044430 A1 2/2010 Song et al.
2010/0048226 A1 2/2010 Owen
2010/0049599 A1 2/2010 Owen
2010/0051685 A1 3/2010 Royyuru
2010/0057614 A1 3/2010 Rainey
2010/0057619 A1 3/2010 Weller et al.
2010/0057624 A1 3/2010 Hurt
2010/0063895 A1 3/2010 Dominguez et al.
2010/0088188 A1 4/2010 Kumar
2010/0125495 A1 5/2010 Smith
2010/0125510 A1 5/2010 Smith
2010/0151790 A1 6/2010 Hoeksel et al.
2010/0197326 A1 8/2010 Ngo
2010/0223110 A1 9/2010 Slavin
2010/0235283 A1 9/2010 Gerson
2010/0248710 A1 9/2010 Sklovsky
2010/0250356 A1 9/2010 Gillenson
2010/0250436 A1 9/2010 Loevenguth
2010/0260388 A1 10/2010 Garrett
2010/0333129 A1 12/2010 Alhadeff et al.
2011/0047016 A1 2/2011 Cook
2011/0057025 A1 3/2011 Denzer
2011/0087529 A1 4/2011 Angell
2011/0087610 A1 4/2011 Batada
2011/0105022 A1 5/2011 Vawter
2011/0113473 A1 5/2011 Corda
2011/0145049 A1 6/2011 Hertel
2011/0145149 A1 6/2011 Valdes
2011/0179113 A1 7/2011 Thomas
2011/0196788 A1 8/2011 Lu et al.
2011/0218911 A1 9/2011 Spodak
2011/0246284 A1 10/2011 Chaikin
2011/0250866 A1 10/2011 Fisher
2011/0251941 A1 10/2011 Dunwoody
2011/0258024 A1 10/2011 Prince
2011/0258115 A1 10/2011 Mulhim
2011/0276417 A1 11/2011 Campbell
2011/0295750 A1 12/2011 Rammal
2011/0302016 A1 12/2011 Haddad
2011/0302406 A1 12/2011 Machani
2011/0313924 A1 12/2011 Carell et al.
2011/0320243 A1 12/2011 Khan
2011/0320293 A1 12/2011 Khan
2011/0320294 A1 12/2011 Votaw
2011/0320345 A1 12/2011 Taveau
2012/0005076 A1 1/2012 Dessert
2012/0011058 A1 1/2012 Pitroda et al.
2012/0011063 A1 1/2012 Killian
2012/0028612 A1 2/2012 Hurst
2012/0029990 A1 2/2012 Fisher
2012/0047070 A1 2/2012 Pharris
2012/0074232 A1 3/2012 Spodak
2012/0078735 A1 3/2012 Bauer
2012/0079521 A1 3/2012 Garg et al.
2012/0084203 A1 4/2012 Mehew
2012/0095855 A1 4/2012 Sterling
2012/0095856 A1 4/2012 Sanjeev
2012/0122447 A1 5/2012 Craft
2012/0123841 A1 5/2012 Taveau
2012/0123868 A1 5/2012 Brudnicki
2012/0123880 A1 5/2012 Craft
2012/0123935 A1 5/2012 Brudnicki
2012/0123937 A1 5/2012 Spodak
2012/0143752 A1 6/2012 Wong
2012/0150669 A1 6/2012 Langley
2012/0158589 A1 6/2012 Katzin
2012/0171992 A1 7/2012 Cheong
2012/0172026 A1 7/2012 Kwon
2012/0172089 A1 7/2012 Bae
2012/0174189 A1 7/2012 Lim
2012/0191557 A1 7/2012 Fisher
2012/0191612 A1 7/2012 Spodak
2012/0196586 A1 8/2012 Grigg
2012/0197691 A1 8/2012 Grigg
2012/0197740 A1 8/2012 Grigg
2012/0197743 A1 8/2012 Grigg
2012/0197745 A1 8/2012 Fisher
2012/0197787 A1 8/2012 Grigg

(56) **References Cited**

U.S. PATENT DOCUMENTS

2012/0203610 A1 8/2012 Grigg et al.
2012/0203632 A1 8/2012 Blum
2012/0209688 A1 8/2012 Lamothe
2012/0209749 A1 8/2012 Hammad
2012/0215701 A1 8/2012 Mehta
2012/0221421 A1 8/2012 Hammad
2012/0221475 A1 8/2012 Grigg
2012/0226610 A1 9/2012 Gill
2012/0229647 A1 9/2012 Calman
2012/0229657 A1 9/2012 Calman
2012/0231424 A1 9/2012 Calman
2012/0231425 A1 9/2012 Calman
2012/0232937 A1 9/2012 Calman
2012/0232977 A1 9/2012 Calman
2012/0232983 A1 9/2012 Bertha
2012/0245986 A1 9/2012 Regan et al.
2012/0253852 A1 10/2012 Pourfallah
2012/0259686 A1 10/2012 Yurrow
2012/0259698 A1 10/2012 Yurrow
2012/0259732 A1 10/2012 Sasankan
2012/0265677 A1 10/2012 Rackley
2012/0265685 A1 10/2012 Brudnicki
2012/0271712 A1 10/2012 Katzin
2012/0284131 A1 11/2012 Soffer
2012/0286928 A1 11/2012 Mullen
2012/0290376 A1 11/2012 Dryer
2012/0290449 A1 11/2012 Mullen
2012/0290478 A1* 11/2012 Crofts G06Q 20/322 705/44
2012/0293303 A1 11/2012 Khan
2012/0296708 A1 11/2012 Bachmann
2012/0296720 A1 11/2012 Pirillo
2012/0296722 A1 11/2012 Gosavi
2012/0296741 A1 11/2012 Dykes
2012/0297204 A1 11/2012 Buer
2012/0302204 A1 11/2012 Gupta
2012/0303425 A1 11/2012 Katzin
2012/0310720 A1 12/2012 Balsan
2012/0310760 A1 12/2012 Phillips
2012/0310824 A1 12/2012 Liberty
2012/0310826 A1 12/2012 Chatterjee
2012/0316950 A1 12/2012 LaPorte
2012/0316951 A1 12/2012 Fisher
2012/0316992 A1 12/2012 Oborne
2012/0317019 A1 12/2012 Carnes
2012/0323653 A1 12/2012 Fisher
2012/0323664 A1 12/2012 Klems
2012/0323670 A1 12/2012 Fisher
2012/0323777 A1 12/2012 Liberty
2012/0329394 A1 12/2012 Fisher
2012/0330737 A1 12/2012 Liberty
2012/0330792 A1 12/2012 Kashanian
2013/0012125 A1 1/2013 Fisher
2013/0012126 A1 1/2013 Fisher
2013/0012131 A1 1/2013 Fisher
2013/0013352 A1 1/2013 Fisher
2013/0013353 A1 1/2013 Fisher
2013/0013355 A1 1/2013 Fisher
2013/0013432 A1 1/2013 Fisher
2013/0013434 A1 1/2013 Fisher
2013/0013490 A1 1/2013 Keller
2013/0013498 A1 1/2013 Fisher
2013/0013499 A1 1/2013 Kalgi
2013/0013501 A1 1/2013 Rackley
2013/0017784 A1 1/2013 Fisher
2013/0018738 A1 1/2013 Faires
2013/0018740 A1 1/2013 Fisher
2013/0018742 A1 1/2013 Fisher
2013/0018793 A1 1/2013 Wong
2013/0023209 A1 1/2013 Fisher
2013/0023294 A1 1/2013 Singh
2013/0024220 A1 1/2013 Fisher
2013/0024221 A1 1/2013 Fisher
2013/0024223 A1 1/2013 Thomas
2013/0024280 A1 1/2013 Fisher
2013/0024364 A1 1/2013 Shrivastava et al.
2013/0024371 A1 1/2013 Hariramani
2013/0024372 A1 1/2013 Spodak
2013/0024377 A1 1/2013 Stong
2013/0029646 A1 1/2013 Chowdhury
2013/0030828 A1 1/2013 Pourfallah
2013/0030960 A1 1/2013 Kashanian
2013/0030997 A1 1/2013 Spodak
2013/0035035 A1 2/2013 Fisher
2013/0035036 A1 2/2013 Fisher
2013/0035037 A1 2/2013 Fisher
2013/0035068 A1 2/2013 Fisher
2013/0035069 A1 2/2013 Fisher
2013/0035070 A1 2/2013 Fisher
2013/0035071 A1 2/2013 Fisher
2013/0035072 A1 2/2013 Fisher
2013/0035087 A1 2/2013 Fisher
2013/0035967 A1 2/2013 Fisher
2013/0035968 A1 2/2013 Fisher
2013/0035969 A1 2/2013 Fisher
2013/0035970 A1 2/2013 Fisher
2013/0040568 A1 2/2013 Fisher
2013/0040569 A1 2/2013 Fisher
2013/0041699 A1 2/2013 Fisher
2013/0041700 A1 2/2013 Fisher
2013/0041701 A1 2/2013 Roth
2013/0041736 A1 2/2013 Coppinger
2013/0041743 A1 2/2013 Coppinger
2013/0041744 A1 2/2013 Coppinger
2013/0041745 A1 2/2013 Coppinger
2013/0041769 A1 2/2013 Fisher
2013/0046608 A1 2/2013 Coppinger
2013/0046634 A1 2/2013 Grigg
2013/0046645 A1 2/2013 Grigg
2013/0048723 A1 2/2013 King
2013/0052952 A1 2/2013 Fisher
2013/0054336 A1 2/2013 Graylin
2013/0054337 A1 2/2013 Brendell
2013/0054412 A1 2/2013 Brendell
2013/0054441 A1 2/2013 Kamdar
2013/0057392 A1 3/2013 Bullock
2013/0060618 A1 3/2013 Barton
2013/0073373 A1 3/2013 Fisher
2013/0073458 A1 3/2013 Sherwin
2013/0080228 A1 3/2013 Fisher
2013/0080229 A1 3/2013 Fisher
2013/0080230 A1 3/2013 Fisher
2013/0080231 A1 3/2013 Fisher
2013/0080232 A1 3/2013 Fisher
2013/0080233 A1 3/2013 Fisher
2013/0080240 A1 3/2013 Fisher
2013/0080241 A1 3/2013 Fisher
2013/0080329 A1 3/2013 Royyuru
2013/0091012 A1 4/2013 Liberty
2013/0238455 A1 9/2013 Laracey
2013/0246141 A1 9/2013 Liberty
2013/0246203 A1 9/2013 Laracey
2013/0317928 A1 11/2013 Laracey
2013/0332347 A1 12/2013 Liberty
2014/0006048 A1 1/2014 Liberty
2014/0201070 A1 7/2014 Liberty

FOREIGN PATENT DOCUMENTS

CN	101606400	12/2009
CN	102073958	5/2011
DE	10119808	9/2002
EP	1280115	1/2003
EP	2084921	4/2008
JP	2001297198	10/2001
JP	2001357164	12/2001
JP	2002-99716	4/2002
KR	10-2002-0065989	8/2002
KR	10-2003-0068603	8/2003
KR	10-2007-0092400	9/2007
WO	9834203	8/1998
WO	9913636	3/1999
WO	0171627	9/2001
WO	0197118	12/2001

(56) **References Cited**

FOREIGN PATENT DOCUMENTS

WO	02071354	9/2002
WO	03012717	2/2003
WO	2004010393	1/2004
WO	2004023353	3/2004
WO	2004053640	6/2004
WO	2004088641	10/2004
WO	2005079254	9/2005
WO	2005086593	9/2005
WO	2007145500	12/2007
WO	2008008735	1/2008
WO	2012025824	3/2012
WO	WO 2013009444	1/2013
WO	WO 2013009446	1/2013
WO	WO 2013025273	2/2013
WO	WO 2013078176	5/2013
WO	WO 2013166174	7/2013

OTHER PUBLICATIONS

Written Opinion for PCT/US2012/066013 dated Jan. 29, 2013.
Chen, Jiajun Jim et al. Short-range Wireless Technologies with Mobile Payments Systems. Proceedings of the 6th international conference on Electronic commerce [Online] 2004, pp. 649-656.
Labrou, Yannis et al. Wireless Wallet. Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services [Online] 2004, pp. 1-10.
Motorola, Motorola M-Wallet Solution. [Online] 2006 http://www.motorola.com/networkoperators/pdfs/M-Wallet-Brochure.pdf (accessed Oct. 4, 2012).
Valcourt, E. et al., "Investigating Mobile Payment", Wireless and Mobile Computing, Networking and Communications, 2005. (WiMob'2005), IEEE International Conference on Aug. 22-24, 2005, vol. 4, pp. 29-36 vol. 4.
Gao, Jerry, et al., "P2P-Paid: A Peer-to-Peer Wireless Payment System", Proceedings of the 2005 Second IEEE International Workshop on Mobile Commerce and Services (WMCS'05) Jul. 2005, 10 pages.
Edwin, et al., "Technobiography", Oct. 2004, 29 pages.
U.S. Appl. No. 13/527,466, Dec. 4, 2013, Final Office Action.
U.S. Appl. No. 13/964,707, Feb. 24, 2014, Office Action.
International Search Report for PCT/US2012/040131 Dated Jan. 29, 2013.
Written Opinion for PCT/US2012/040131 dated Jan. 29, 2013.
U.S. Appl. No. 13/527,466, Apr. 15, 2013, Office Action.
U.S. Appl. No. 13/484,199, Jun. 7, 2013, Notice of Allowance.
U.S. Appl. No. 14/213,543, May 6, 2014, Office Action.
U.S. Appl. No. 14/341,605, filed Jul. 25, 2014, Liberty, Michael A.
European Search Report for EP12824344 dated Sep. 29, 2014.
Sykes, et al. "Securing Mobile Banking," Credit Union Management, Novemer 2010, vol. 33 No. 11; ISSN 0273-9267.
Clarke, Irvine III, "Emerging Value Propositions for M-commerce," *Journal of Business Strategies*, vol. 25, Issue 2, Fall 2008, p. 41-57; ISSN: 0887-2058.
Wei, et al., "Development of a Web-Based Mobile Airline Ticketing Model with Usability Features," 2005, Industrial Management + Data Systems; vol. 105 No. 9, ISSN: 0263-5577.
International Search Report and Written Opinion for PCT/US2012/43458 dated Aug. 17, 2012.
U.S. Appl. No. 13/528,720, Jun. 25, 2014, Office Action.
U.S. Appl. No. 13/964,707, Jul. 10, 2014, Office Action.
U.S. Appl. No. 13/527,466, Aug. 1, 2014, Office Action.
U.S. Appl. No. 13/528,720, Dec. 10, 2014, Final Office Action.
Liberty, Michael A. , International Search Report for PCT/US2012/043321 dated Sep. 6, 2012.
Liberty, Michael A., International Search Report for PCT/US2012/058849 dated Jan. 4, 2013.
Liberty, Michael A., Written Opinion for PCT/US2012/043321 dated Sep. 6, 2012.
Liberty, Michael A., Written Opinion for PCT/US2012/058849 dated Jan. 4, 2013.
International Search Report for PCT/US2013/039100 dated Aug. 23, 2013.
Written Opinion for PCT/US2013/039100 dated Aug. 23, 2013.
U.S. Appl. No. 14/012,822, Jan. 7, 2015, Final Office Action.
U.S. Appl. No. 14/012,822, Aug. 7, 2014, Office Action.
U.S. Appl. No. 13/964,707, Mar. 16, 2015, Final Office Action.
U.S. Appl. No. 14/213,543, Apr. 8, 2015, Office Action.
U.S. Appl. No. 13/874,192, Jul. 14, 2015, Office Action.
U.S. Appl. No. 13/527,466, Jul. 16, 2015, Office Action.
U.S. Appl. No. 13/528,720, Jul. 22, 2015, Office Action.

* cited by examiner

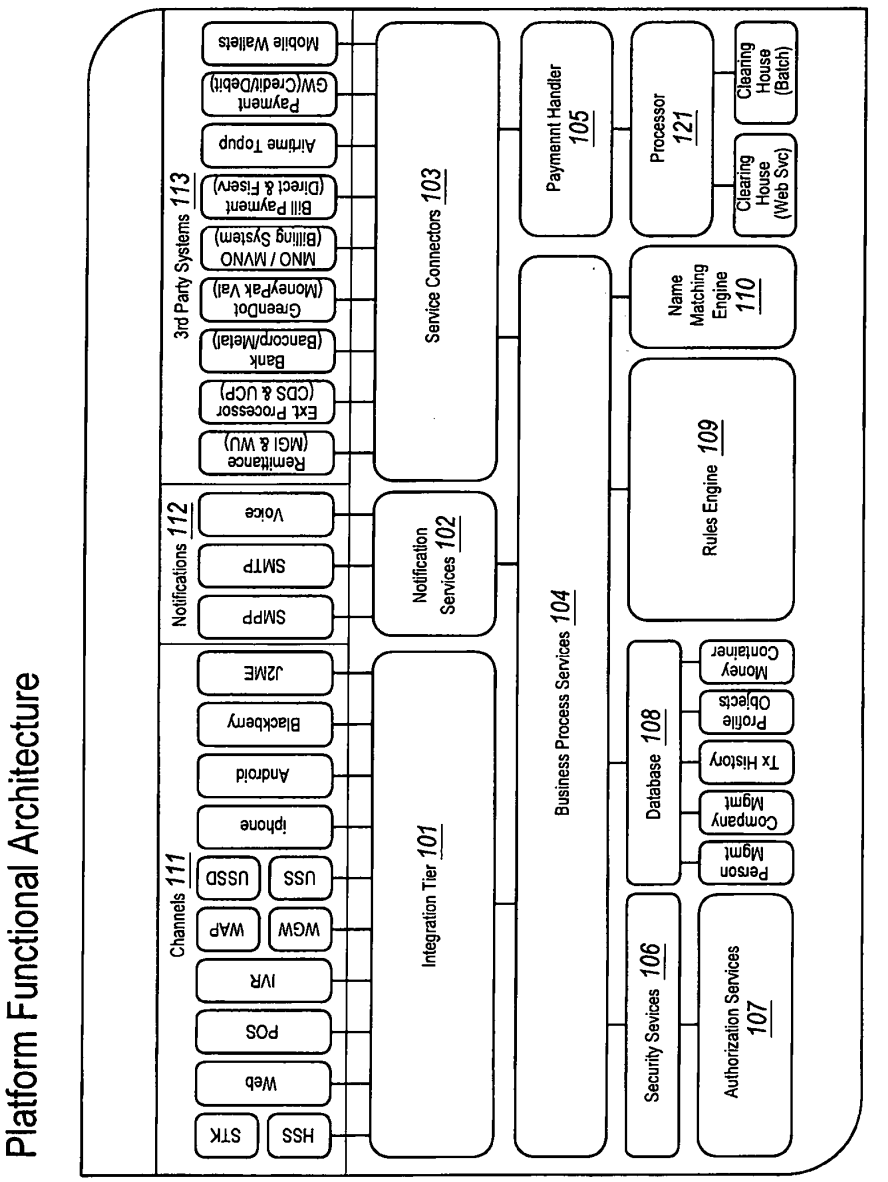

Platform Functional Architecture
Channels 111
HSS
STK
Web
POS
IVR
WGW
WAP
USS
USSD
iphone
Android
Blackberry
J2ME
Notifications 112
SMPP
SMTP
Voice
3rd Party Systems 113
Remittance (MGI & WU)
Ext. Processor (CDS & UCP)
Bank (Bancorp/Metal)
GreenDot (MoneyPak Val)
MNO / MVNO (Billing System)
Bill Payment (Direct & Fiserv)
Airtime Topup
Payment GW(Credit/Debit)
Mobile Wallets
Integration Tier 101
Notification Services 102
Service Connectors 103
Business Process Services 104
Paymennt Handler 105
Security Sevices 106
Database 108
Person Mgmt
Company Mgmt
Tx History
Profile Objects
Money Container
Authorization Services 107
Rules Engine 109
Name Matching Engine 110
Processor 121
Clearing House (Web Svc)
Clearing House (Batch)

FIG. 1

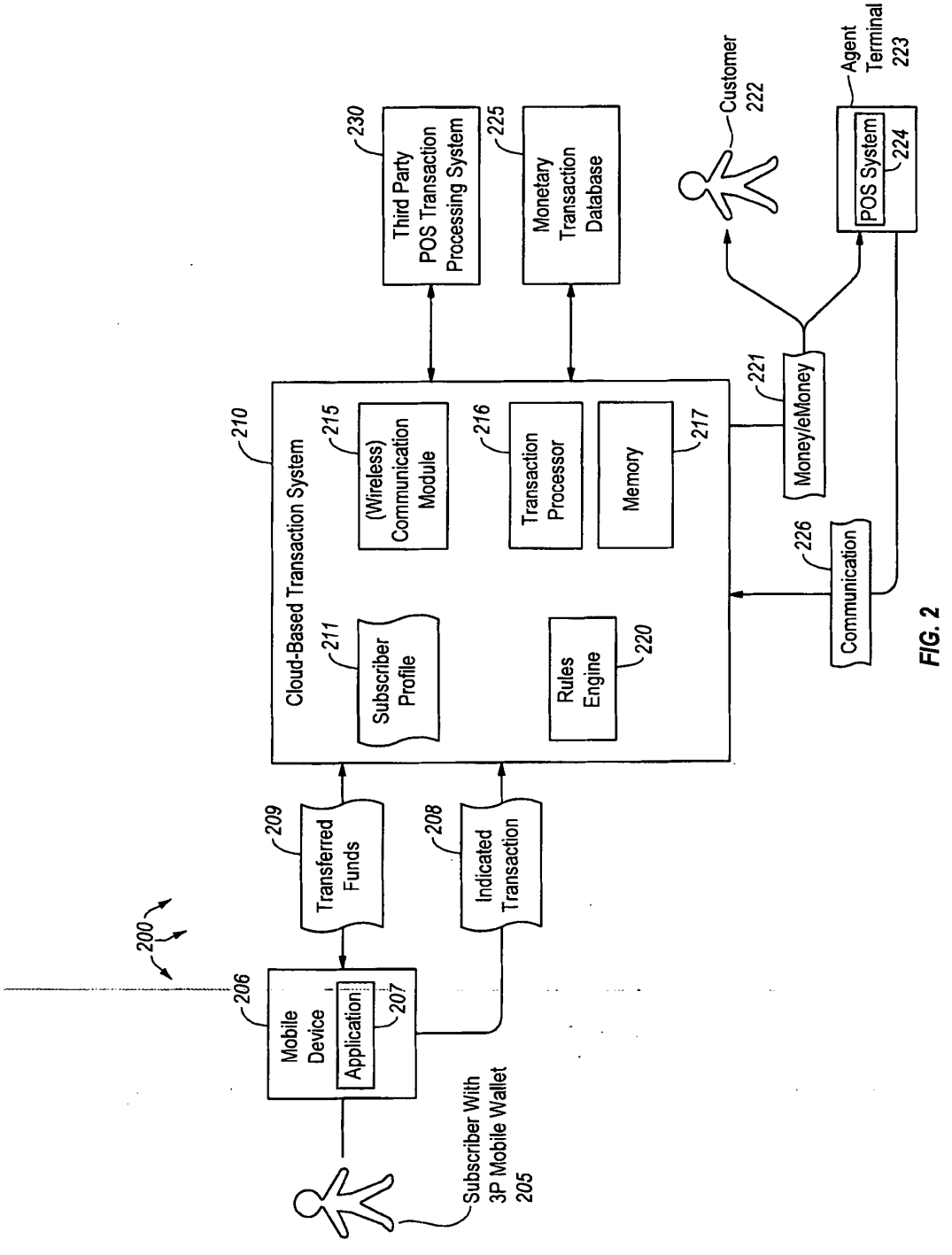
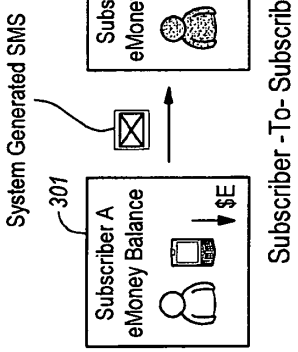


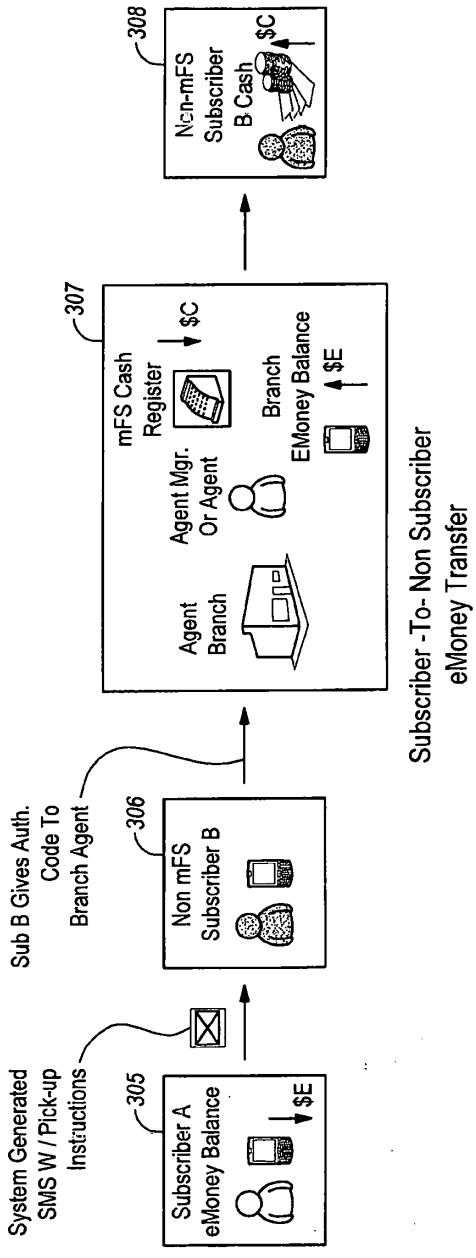
FIG. 2

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 291 of 381



Subscriber -To- Subscriber eMoney Transfer

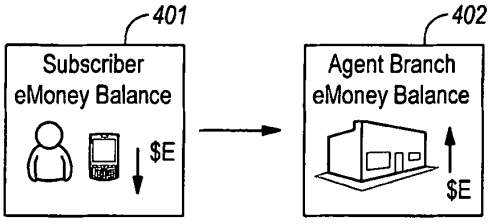
FIG. 3A



Subscriber -To- Non Subscriber eMoney Transfer

FIG. 3B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 292 of 381



Subscriber Makes Retail Purchase

FIG. 4

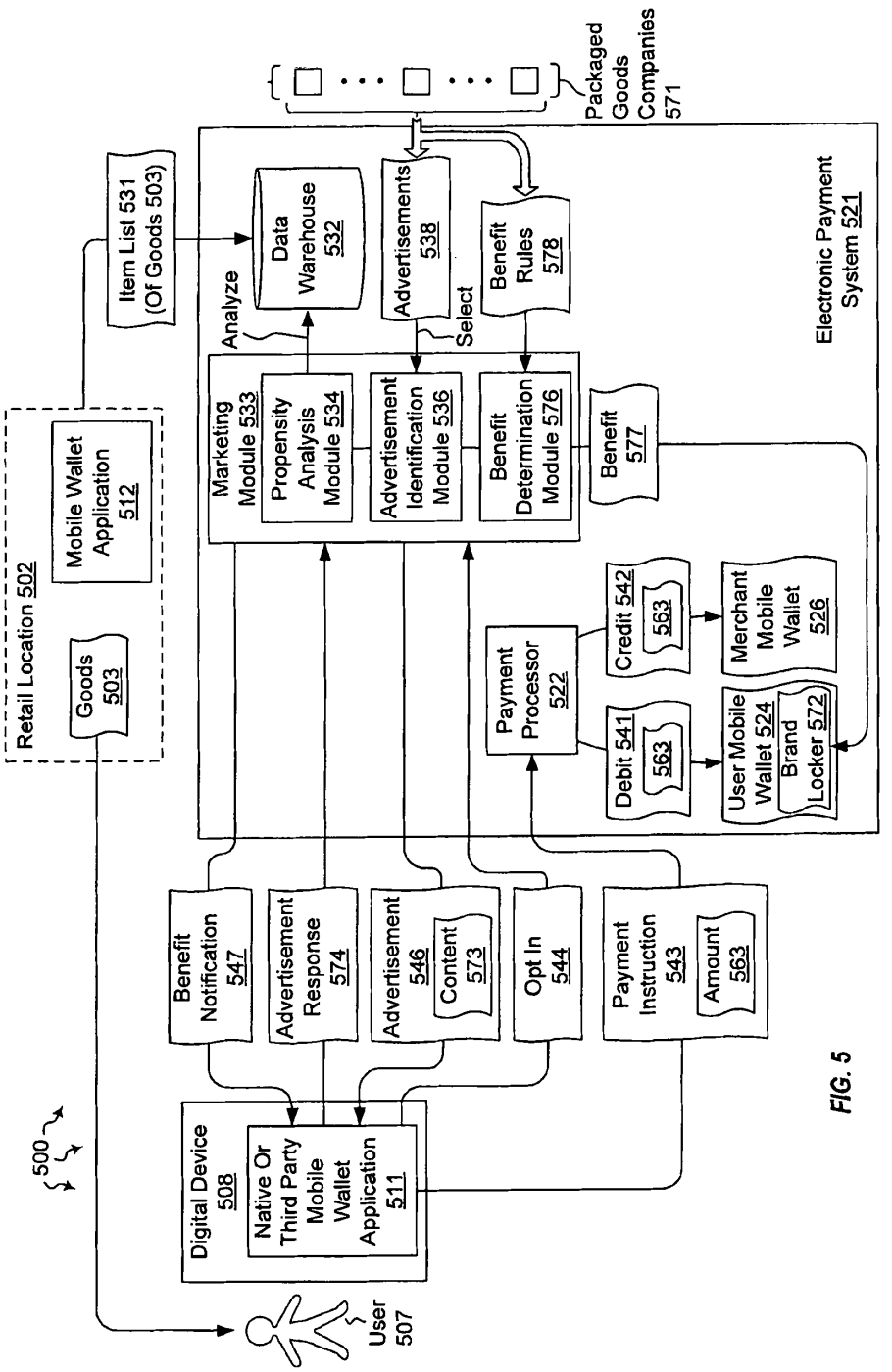


FIG. 5

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 294 of 381

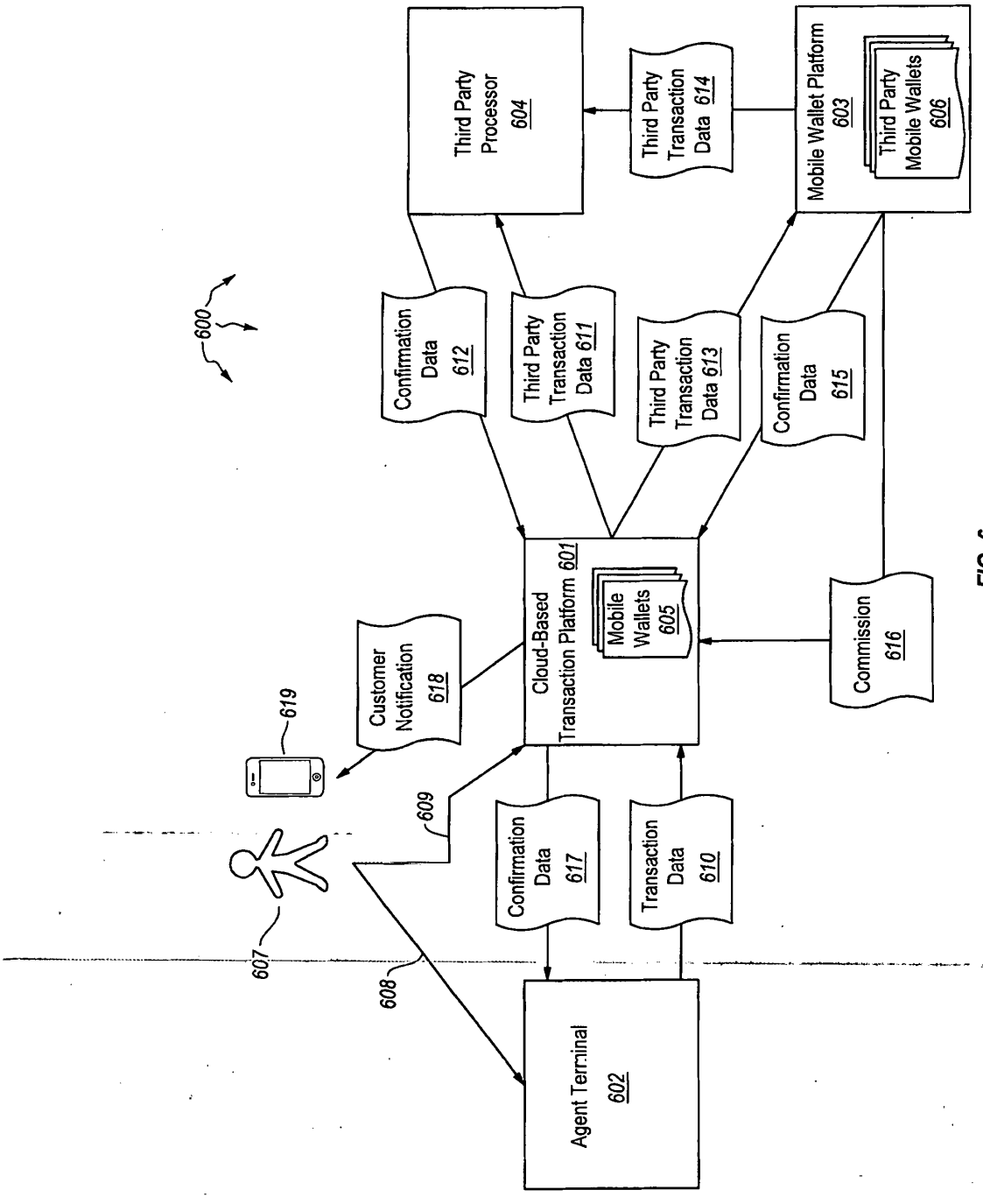


FIG. 6

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 295 of 381

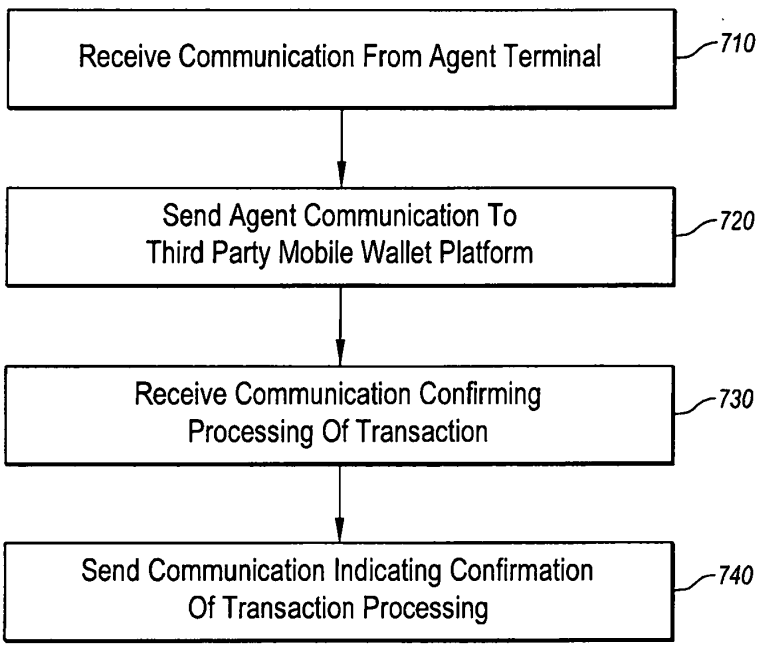

Receive Communication From Agent Terminal
710
Send Agent Communication To Third Party Mobile Wallet Platform
720
Receive Communication Confirming Processing Of Transaction
730
Send Communication Indicating Confirmation Of Transaction Processing
740

FIG. 7

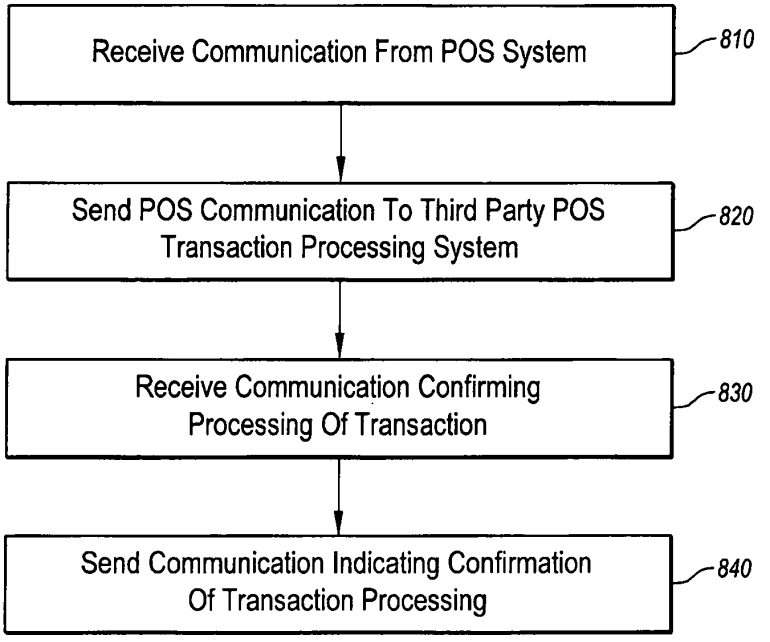

Receive Communication From POS System
810
Send POS Communication To Third Party POS Transaction Processing System
820
Receive Communication Confirming Processing Of Transaction
830
Send Communication Indicating Confirmation Of Transaction Processing
840

FIG. 8

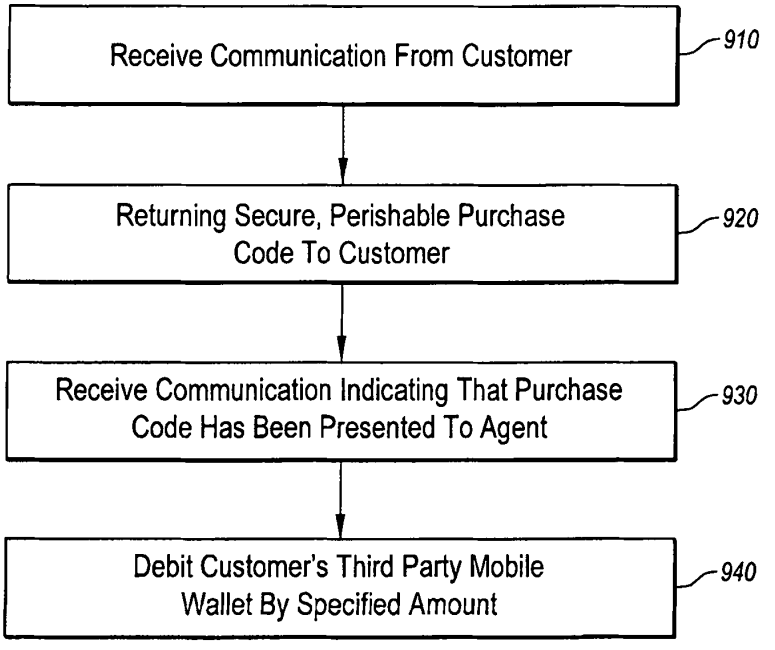

Receive Communication From Customer
910
Returning Secure, Perishable Purchase Code To Customer
920
Receive Communication Indicating That Purchase Code Has Been Presented To Agent
930
Debit Customer's Third Party Mobile Wallet By Specified Amount
940

FIG. 9

USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to and the benefit of U.S. Provisional Application Ser. No. 61/562,301, entitled "Using a Mobile Wallet Infrastructure to Support Multiple Mobile Wallet Providers", filed on Nov. 21, 2011, which is herein incorporated by reference in its entirety.

BACKGROUND

Mobile phones and other digital devices have become increasingly popular in recent years. Many mobile device users use their devices to perform countless different daily tasks. For instance, mobile devices allow users to check email, send and receive instant messages, check calendar items, take notes, set up reminders, browse the internet, play games or perform any number of different things using specialized applications or "apps". These applications allow mobile devices to communicate with other computer systems and perform a wide variety of network-connected tasks previously not possible with a mobile device.

BRIEF SUMMARY

Embodiments described herein extend to methods, systems, and computer program products for a cloud-based transaction platform. Embodiments include an infrastructure that can be used with third party mobile wallets provided by third party mobile wallet providers. Users with native or third party mobile wallets can use the cloud-based transaction platform to enroll a customer for a third party mobile wallet, add a stored value account (either hosted by the cloud-based transaction platform or a third party), add a bank/credit union account to a third party mobile wallet, add a debit/credit card account to a third party mobile wallet, deposit funds in a third party mobile wallet, withdraw funds from a third party mobile wallet, pay bills from a third party mobile wallet, top up a prepaid mobile account through a third party mobile wallet, transfer funds through a third party mobile wallet, and make in store purchases from a third party mobile wallet.

Embodiments described herein are directed to performing a transaction using a third party mobile wallet, performing a transaction using a third party point of sale (POS) system and to making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. In one embodiment, a cloud-based transaction platform is provided, which receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that a customer desires to perform a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the agent communication to a third party mobile wallet platform, receives communication from the third party mobile wallet platform confirming processing of the transaction, and sends communication to the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

In another embodiment, a cloud-based transaction platform performs a transaction using a third party point of sale (POS) system. The cloud-based transaction platform receives communication from a specified POS system implemented at an agent terminal over a communication channel connected to the cloud-based transaction platform. The POS communication indicates that a customer has initiated a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the POS communication to a corresponding third party POS transaction processing system that has been established to process POS transactions from the specified POS system, receives communication from the third party POS transaction processing system confirming processing of the transaction, and sends communication to the specified POS system implemented at the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

In yet another embodiment, a cloud-based transaction platform is provided which allows users to make purchases from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform receives communication from a customer over a communication channel connected to the cloud-based transaction platform. The customer communication indicates that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's third party mobile wallet. The cloud-based transaction platform returns a secure, perishable purchase code to the customer over at least one the communication channels connected to the cloud-based transaction platform and receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent terminal communication indicates that the purchase code has been presented to an agent. The cloud-based transaction platform then debits the customer's third party mobile wallet by the specified amount of funds to complete the purchase.

This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

Additional features and advantages will be set forth in the description which follows, and in part will be apparent to one of ordinary skill in the art from the description, or may be learned by the practice of the teachings herein. Features and advantages of embodiments described herein may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. Features of the embodiments described herein will become more fully apparent from the following description and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

To further clarify the above and other features of the embodiments described herein, a more particular description will be rendered by reference to the appended drawings. It is appreciated that these drawings depict only examples of the embodiments described herein and are therefore not to be considered limiting of its scope. The embodiments will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

FIG. 1 illustrates a monetary transaction system architecture in which embodiments described herein may operate.

FIG. 2 illustrates an example embodiment of a cloud-based transaction platform.

FIGS. 3A and 3B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber eMoney transfers via a mobile wallet, respectively.

FIG. 4 illustrates an example data flow for making a retail purchase using a mobile wallet.

FIG. 5 illustrates an example embodiment of a monetary transaction system architecture.

FIG. 6 illustrates an alternate example embodiment of a cloud-based transaction platform.

FIG. 7 illustrates an example embodiment data flow for performing a transaction using a third party mobile wallet.

FIG. 8 illustrates an example embodiment data flow for performing a transaction using a third party point of sale (POS) system.

FIG. 9 illustrates an example embodiment data flow for making a purchase from a third party mobile wallet provided by a third party mobile wallet provider.

DETAILED DESCRIPTION

Embodiments described herein extend to methods, systems, and computer program products for a cloud-based transaction platform. Embodiments include an infrastructure that can be used with third party mobile wallets provided by third party mobile wallet providers. Users with native or third party mobile wallets can use the cloud-based transaction platform to enroll a customer for a third party mobile wallet, add a stored value account (either hosted by the cloud-based transaction platform or a third party), add a bank/credit union account to a third party mobile wallet, add a debit/credit card account to a third party mobile wallet, deposit funds in a third party mobile wallet, withdraw funds from a third party mobile wallet, pay bills from a third party mobile wallet, top up a prepaid mobile account through a third party mobile wallet, transfer funds through a third party mobile wallet, and make in store purchases from a third party mobile wallet.

Embodiments described herein are directed to performing a transaction using a third party mobile wallet, performing a transaction using a third party point of sale (POS) system and to making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. In one embodiment, a cloud-based transaction platform is provided, which receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that a customer desires to perform a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the agent communication to a third party mobile wallet platform, receives communication from the third party mobile wallet platform confirming processing of the transaction, and sends communication to the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

In another embodiment, a cloud-based transaction platform performs a transaction using a third party point of sale (POS) system. The cloud-based transaction platform receives communication from a specified POS system implemented at an agent terminal over a communication channel connected to the cloud-based transaction platform. The POS communication indicates that a customer has initiated a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the POS communication to a corresponding third party POS transaction processing system that has been established to process POS transactions from the specified POS system, receives communication from the third party POS transaction processing system confirming processing of the transaction, and sends communication to the specified POS system implemented at the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

In yet another embodiment, a cloud-based transaction platform is provided which allows users to make purchases from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform receives communication from a customer over a communication channel connected to the cloud-based transaction platform. The customer communication indicates that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's third party mobile wallet. The cloud-based transaction platform returns a secure, perishable purchase code to the customer over at least one the communication channels connected to the cloud-based transaction platform and receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent terminal communication indicates that the purchase code has been presented to an agent. The cloud-based transaction platform then debits the customer's third party mobile wallet by the specified amount of funds to complete the purchase. Such purchases may be for items that are provided by the cloud-based transaction platform, either directly or via a third-party provider. These items may include music, movies, games and other downloadable content, physical items that can be shipped to the user and other items such as health care services.

Embodiments described herein may comprise or utilize a special purpose or general-purpose computer including computer hardware, such as, for example, one or more processors and system memory, as discussed in greater detail below. Embodiments described herein also include physical and other computer-readable media for carrying or storing computer-executable instructions and/or data structures. Such computer-readable media can be any available media that can be accessed by a general purpose or special purpose computer system. Computer-readable media that store computer-executable instructions in the form of data are computer storage media. Computer-readable media that carry computer-executable instructions are transmission media. Thus, by way of example, and not limitation, embodiments described herein can comprise at least two distinctly different kinds of computer-readable media: computer storage media and transmission media.

Computer storage media includes RAM, ROM, EEPROM, CD-ROM, solid state drives (SSDs) that are based on RAM, Flash memory, phase-change memory (PCM), or other types of memory, or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store desired program code means in the form of computer-executable instructions, data or data structures and which can be accessed by a general purpose or special purpose computer.

A "network" is defined as one or more data links and/or data switches that enable the transport of electronic data between computer systems and/or modules and/or other electronic devices. When information is transferred or provided over a network (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a transmission medium. Transmission media can include a network which can be used to carry data or desired program code means in the form of computer-executable instructions or in the form of data structures and which can be accessed by a general purpose or

special purpose computer. Combinations of the above should also be included within the scope of computer-readable media.

Further, upon reaching various computer system components, program code means in the form of computer-executable instructions or data structures can be transferred automatically from transmission media to computer storage media (or vice versa). For example, computer-executable instructions or data structures received over a network or data link can be buffered in RAM within a network interface module (e.g., a network interface card or "NIC"), and then eventually transferred to computer system RAM and/or to less volatile computer storage media at a computer system. Thus, it should be understood that computer storage media can be included in computer system components that also (or even primarily) utilize transmission media.

Computer-executable (or computer-interpretable) instructions comprise, for example, instructions which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. The computer executable instructions may be, for example, binaries, intermediate format instructions such as assembly language, or even source code. Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the described features or acts described above. Rather, the described features and acts are disclosed as example forms of implementing the claims.

Those skilled in the art will appreciate that various embodiments may be practiced in network computing environments with many types of computer system configurations, including personal computers, desktop computers, laptop computers, message processors, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, mobile telephones, PDAs, tablets, pagers, routers, switches, and the like. Embodiments described herein may also be practiced in distributed system environments where local and remote computer systems that are linked (either by hardwired data links, wireless data links, or by a combination of hardwired and wireless data links) through a network, each perform tasks (e.g. cloud computing, cloud services and the like). In a distributed system environment, program modules may be located in both local and remote memory storage devices.

In this description and the following claims, "cloud computing" is defined as a model for enabling on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). The definition of "cloud computing" is not limited to any of the other numerous advantages that can be obtained from such a model when properly deployed.

For instance, cloud computing is currently employed in the marketplace so as to offer ubiquitous and convenient on-demand access to the shared pool of configurable computing resources. Furthermore, the shared pool of configurable computing resources can be rapidly provisioned via virtualization and released with low management effort or service provider interaction, and then scaled accordingly.

A cloud computing model can be composed of various characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service, and so forth. A cloud computing model may also come in the form of various service models such as, for example, Software as a Service ("SaaS"), Platform as a Service ("PaaS"), and Infrastructure as a Service ("IaaS"). The cloud computing model may also be deployed using different deployment models such as private cloud, community cloud, public cloud, hybrid cloud, and so forth. In this description and in the claims, a "cloud computing environment" is an environment in which cloud computing is employed.

Additionally or alternatively, the functionally described herein can be performed, at least in part, by one or more hardware logic components. For example, and without limitation, illustrative types of hardware logic components that can be used include Field-programmable Gate Arrays (FPGAs), Program-specific Integrated Circuits (ASICs), Program-specific Standard Products (ASSPs), System-on-a-chip systems (SOCs), Complex Programmable Logic Devices (CPLDs), and other types of programmable hardware.

Still further, system architectures described herein can include a plurality of independent components that each contribute to the functionality of the system as a whole. This modularity allows for increased flexibility when approaching issues of platform scalability and, to this end, provides a variety of advantages. System complexity and growth can be managed more easily through the use of smaller-scale parts with limited functional scope. Platform fault tolerance is enhanced through the use of these loosely coupled modules. Individual components can be grown incrementally as business needs dictate. Modular development also translates to decreased time to market for new functionality. New functionality can be added or subtracted without impacting the core system.

Various terminology will be used herein to describe the cloud-based transaction platform (also referred to as a "monetary transaction system", "mobile wallet platform", "mobile wallet program", "mobile wallet transaction system", "mobile financial services (mFS) platform" or "electronic payment system"). The term "agent" is used to refer to an individual with mFS transaction system tools and training to support specific mFS functions. These mFS functions include subscriber registration and activation, and the deposit and withdrawal of funds from the mFS transaction system. Agents are representatives of the mFS transaction system or "program". Agents can be employees or contractors of the program provider, or other companies and organizations that partner with the program provider to provide these services themselves. Agents may be found in every facet of a typical economy, and may include large retailers, mobile network operators (MNO) airtime sales agents, gas stations, kiosks, or other places of business.

The cloud-based transaction platform includes an infrastructure that allows native mobile wallet application and third party mobile wallet applications to interact both with the transaction system and with each other. This allows the user of a native or a third party mobile wallet to make purchases, transfer money or perform any of the other transactions described herein. The cloud-based transaction platform may include a mobile wallet application and a web interface or some other type of functionality that allows the user to interact with the cloud-based transaction platform using their mobile device. The native and third party mobile wallet applications may include a subscriber identity module (SIM) application, an Unstructured Supplementary Service Data (USSD) application, a smartphone application, a web application, a mobile web application, a Wireless Application Protocol (WAP) application, a Java 2 Platform, Micro Edition (J2ME) application, a tablet application or any other type of application or interface that provides tools for the agent to register, activate, and offer other services to the mFS subscriber.

As used herein, a mobile wallet application is a mobile wallet application installed on a SIM card or elsewhere on a mobile device. The mobile wallet application may either be native (i.e. provided by the provider of the cloud-based transaction platform) or third party (i.e. provided by a provider other than the provider of the cloud-based transaction platform).

A USSD application is an application that implements USSD for various functionality including prepaid callback service, location-based content services, menu-based information services and other mobile wallet platform services. A web application is one that implements or uses the internet to provide mobile wallet platform functionality. A mobile web application is similar to a web application, but is tailored for mobile devices. A WAP application is one that uses the wireless application protocol to communicate with the mobile wallet platform to provide the platform's functionality. A J2ME application is an application developed in Java and is designed to provide mobile wallet functionality on a variety of different hardware. A tablet application is an application specifically designed for a touchscreen-based tablet that provides mobile wallet platform functionality for tablet devices. Any of these applications (or any combination thereof) may be provided on the user's mobile device. This functionality can also be made available on a retail point of sale (POS) system or web site. Indeed, the cloud-based transaction platform allows different POS systems to interact with each other and conduct transactions between themselves.

The term "agent administrator" refers to an individual with mFS program tools and training to administrate the allocation of funds to agent branches (e.g. retail locations). As agents perform mFS transactions with subscribers, such as depositing and withdrawing money, the agents are adding and removing money from their own accounts. Any of the applications referred to above may be configured to provide tools used by the agent administrator to view the agent company balance, view the agent branch balances, and transfer funds into and out of agent branch mobile wallets. This functionality can also be made available on a website for easier access.

In some embodiments, the mFS platform application may utilize triple data encryption standard (3DES) encryption (or some other type of encryption), encrypted message signing, and password security on some or all of its communications with the mFS transaction system in order to ensure that the transactions are properly secured and authenticated.

The term "agent branch" refers to any location where an agent provides support for subscriber services of the mFS platform. Funds are allocated by the agent administrator from the agent company's main account to each agent branch to fund the subscriber mFS functions such as depositing or withdrawing cash, in-store purchases, bill payments, prepaid airtime top-ups and money transfers. In some cases, multiple agents may work in a single branch. However, at least in some cases, monetary funds are allocated to from the agent company's main account on a per branch basis.

The term "agent branch account balance" refers to the amount of money residing in a particular agent branch account at a given time. Funds can be deposited into the branch account by the agent administrator, or the funds can come from participating in subscriber mFS transactions such as depositing or withdrawing cash from the subscriber's mobile wallet accounts, or making retail purchases with the mobile wallet.

In some embodiments, in countries with more developed economies, it may be beneficial to use program-issued prepaid debit cards, pre-paid access accounts, stored value accounts or gift cards to conduct business along with the added convenience of card processing networks such as Cirrus, STAR, or Visa for POS and automated teller machine (ATM) functionality. Agents, particularly those in retail outlets and kiosks, can still support subscribers with deposits, withdrawals, and other transfers, but in this case bank external card processors manage the mobile wallet and branch account balances and provide the real-time transfer of funds.

The term "agent branch ledger" refers to a written (or electronic) ledger maintained by the mFS platform. Agent branch transactions are performed on the agent's and subscriber's mobile phones where an electronic record of the transaction is generated and stored on the mFS platform. These electronic transactions are then reconciled with agent branch ledgers to ensure the security and integrity of the transaction. Agent branch ledgers are printed or electronic transaction logs that are distributed to the agent branch locations in hard copy form to serve as a backup record to the electronic transactions.

The term "agent company" refers to a business that registers to participate in the mFS program as a partner of the mFS program provider or owner. The agent company has one or more agent branches which conduct mFS business with mFS program subscribers. In some cases, the agent company may be referred to as a distributor or retailer.

The term "agent company account balance" refers to the sum of the funds deposited at a "partner bank" (defined below) by the agent company to fund the agent company's daily transactions. The funds in the agent company account are then distributed to agent branches by the agent company's agent administrator to conduct everyday business such as accepting cash deposits and cash withdrawals from mFS subscribers. This balance is sometimes referred to as the "agent company float".

An "agent manager" is a supervisor of company agents for a given company. The agent manager has the training and tools to create, delete or modify agent accounts for a company, as well as monitor the transactions performed by agents. The agent manager may have a special application or an increased level of rights to access applications features not available to other users. The special application is a program installed on the agent manager's terminal. This application provides the agent manager the ability to securely perform agent manager functions such as registering and activating new agent accounts. The mFS agent manager application may be installed on any terminal or device. It communicates with the mFS platform using binary and/or text SMS messages. A wireless service provider or MNO provides the GSM SMS network infrastructure on which the mFS platform operates.

As subscribers, agents, and other mFS program participants conduct business in the mFS program, value is transferred from one account to the next as payment for services rendered or goods purchased. This value can be in the form of real currency or the electronic representation referred to herein as eMoney. Among other situations, eMoney is used in mFS implementations where the real-time processing of financial transactions including card processing is not practical. The mFS platform utilizes an internal transaction processor for managing the real-time balance of mobile wallet and agent accounts as value (eMoney) is transferred from one mobile wallet to another in payment for services.

The term "mFS program master account" refers to a bank account maintained by the mFS program partner bank to provide funds and float for the operation of the mFS platform. Depending on the type of mFS implementation, the master account can include sub-accounts for each of the agent branches and subscriber mobile wallets, giving the bank visibility into all transactions on a per-user basis. The mFS

platform can also manage the balance of sub-accounts and interact with the bank's master account when funds need to be deposited or withdrawn from the account.

The term mobile network operator (MNO) refers to a provider of mobile phone service including basic voice, SMS, unstructured supplementary service data (USSD) and data service, and may also be referred to as a "wireless service provider".

The term "mobile wallet" or "mobile wallet account" refers to a stored value account or prepaid access account (PPA) that allows the owner (or "subscriber") to pay for goods and services on the mFS platform from his or her mobile wallet account. When the mFS eMoney transaction processor is used, the mobile wallet balance is maintained by the mFS platform and value is exchanged within the mFS program as eMoney. When the mFS platform is integrated to an external card processor, the mobile wallet utilizes funds from the subscriber's prepaid debit card and bank account to exchange value on the mFS platform.

The term "partner bank" refers to the primary bank participating in the mFS program. The partner bank is responsible for holding the mFS program master accounts that hold the funds for all mFS services and transactions. A "PIN" refers to a numeric password that may be required to perform a transaction via the mobile wallet application.

The term "subscriber" refers to a participant of the mFS mobile wallet platform. The subscriber maintains a mobile wallet balance and performs transactions using the mFS application. An "unbanked subscriber" is a subscriber that does not have (or does not have access to) a bank account or credit union account. The application or "mobile wallet application" provides mobile wallet functionality to the (unbanked) subscriber. The mobile wallet application is installed on a mobile device in the device's memory, on a SIM card (such as a GSM SIM card) or is otherwise accessible to the mobile device. The mobile wallet application provides the subscriber the ability to securely perform subscriber functions such as making retail purchases, paying bills, or transferring money to other mFS subscribers and non-subscribers. The mobile wallet application communicates with the mFS platform using binary and text SMS messages, among other forms of wireless communication. A wireless service provider or MNO provides the GSM network infrastructure on which the mFS platform operates.

FIG. **1** illustrates an example system architecture for a cloud-based transaction platform. Integration tier **101** is configured to manage mobile wallet sessions and maintain integrity of financial transactions. Integration tier **101** can also include a communication (e.g., Web services) API and/or other communication mechanisms to accept messages from channels **111**. Other mechanisms include, but are not limited to: International Standards Organization ("ISO") 8583 for Point-of-Sale-("POS")-and-Automated-Teller-Machines ("ATM") devices and Advanced Message Queuing Protocol ("AMQP") for queue based interfaces. Each of channels **111** can be integrated to one or more mechanisms for sending messages to integration tier **101**. Notification services **102** is configured to send various notifications through different notification channels **112**, such as, for example, Short Message Peer-to-Peer ("SSMP") for Short Messaging Service ("SMS") and Simple Mail Transfer Protocol ("SMTP") for emails. Notification services **102** can be configured through a web services API.

Service connectors **103** are a set of connectors configure to connect to 3rd party systems **113**. Each connector can be a separate module intended to integrate an external service to the system architecture. Business process services **104** are configured to implement business workflows, including executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects. Payment handler **105** is configured to wrap APIs of different payment processors, such as, for example, banking accounts, credit/debit cards or processor **121**. Payment handler **105** exposes a common API to facilitate interactions with many different kinds of payment processors.

Security services **106** are configured to perform subscriber authentication. Authorization services **107** are configured to perform client authorization, such as, for example, using a database-based Access Control List ("ACL") table.

Database **108** is configured to manage customer accounts (e.g., storing customer accounts and properties), manage company accounts (e.g., storing company accounts and properties), manage transaction histories (e.g., storing financial transaction details), store customer profiles, storing dictionaries used by the mobile wallet platform, such as, for example, countries, currencies, etc., and managing money containers. Rules engine **109** is configured to gather financial transaction statistics and uses the statistics to provide transaction properties, such as, for example, fees and bonuses. Rules engine **109** is also configured to enforce business constraints, such as, for example, transactions and platform license constraints.

Name matching engine **110** is configured to match different objects according to specified configuration rules. Matching engine **110** can be used to find similarities between names, addresses, etc. Transaction processor **121** is configured to manage financial accounts and transactions. The transaction processor **121** can be used to hold, load, withdraw and deposit funds to mobile wallet accounts. Transaction processor **121** can also be used as a common interface to a third party processor system. When used as a common interface, financial operations may be delegated to the external processor. A Clearing House subsystem of transaction processor **121** can be used to exchange the financial information with a bank.

Components of a mobile wallet platform can be connected to one another over (or be part of) a system bus and/or a network. Networks can include a Local Area Network ("LAN"), a Wide Area Network ("WAN"), and even the Internet. Accordingly, components of the mobile wallet platform can be "in the cloud". As such, mobile wallet platform components as well as any other connected computer systems and their components, can create message related data and exchange message related data (e.g., Internet Protocol ("IP") datagrams and other higher layer protocols that utilize IP datagrams, such as, Transmission Control Protocol ("TCP"), Hypertext Transfer Protocol ("HTTP"), Simple Mail Transfer Protocol ("SMTP"), etc.) over the system bus and/or network.

The components depicted in FIG. **1** can interoperate to provide a number of financial and other services including but not limited to enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a third party mobile wallet, adding a debit or credit card account to a third party mobile wallet, depositing funds in a third party mobile wallet, withdrawing funds from a third party mobile wallet, paying bills from a third party mobile wallet, topping up a prepaid mobile account through a third party mobile wallet, transferring funds through a third party mobile wallet (nationally or internationally), making in-store purchases using a third party mobile wallet, selecting health care providers and paying for health care services, paying for music, games, movies or other downloadable provided by a

third party provider and made available over the cloud-based transaction system, and various other tasks as described herein below.

FIG. **2** depicts a monetary transaction architecture **200** similar to that described in FIG. **1**. The monetary transaction architecture **200** may provide a more simplified system structure in which each of the above services may be provided. The system includes a subscriber **205**. The subscriber may have access to a bank account, or may be an unbanked subscriber. The subscriber has a profile **211** with the cloud-based transaction system **210**. The profile includes the subscriber's know your customer (KYC) information, as well as any associated bank accounts, credit union accounts, bill pay accounts or other accounts. The subscriber has (or has access to) a mobile device **206** such as a phone or tablet. The mobile device runs the native or third party mobile wallet application **207**.

The subscriber can indicate, using the mobile wallet application **207**, which transaction or other action he or she would like to perform. The indicated transaction **208** is sent to the mobile wallet platform **210** to be carried out by the platform. The transaction processor **216** (which may be similar to or the same as transaction processor **121** of FIG. **1**) performs the transaction(s) specified by the (unbanked) subscriber **205**. The transaction processor may implement various other components to perform the transaction including memory **217**, (wireless) communication module **215**, rules engine **220** and/or a transaction database **225**.

Performing the specified transactions may include communicating with the monetary transaction database **225** to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile (for instance, whether the subscriber has enough eMoney **221** in his or her stored value account, or has enough money in his or her bank account). Rules engine **220** may also be consulted to determine whether the subscriber has exceeded a specified number of allowed transactions. Then, if funds are available, and the transaction is otherwise permissible, the monetary transaction system can transfer money or eMoney **221** to or from an entity such as a user or agent (e.g. customer **222**) to or from an establishment such as an agent terminal (i.e. a retail store or agent company) **223**.

In some cases, the cloud-based transaction system **210** provides a web interface that allows subscribers of third party mobile wallet applications to perform the same functions provided for native subscribers. For instance, mobile wallet application **207** may provide a web interface that allows a user to enroll for a native or third party mobile wallet. The web interface (or the mobile wallet application itself) receives a subscriber-initiated transaction over one of a plurality of communication channels (**111** from FIG. **1**) connected to the cloud-based transaction system **210**. The web interface or mobile wallet application may prompt for and receive enrollment information (e.g. KYC information) for the (unbanked) subscriber **205** over at least one of the plurality of communication channels (e.g. web, point-of-sale (POS), interactive voice response (IVR, etc.). The web interface or mobile wallet application may then send activation instructions over the same or a different channel to activate the (unbanked) subscriber **205** and create a subscriber account for the (unbanked) subscriber.

Once the subscriber has an account, the cloud-based transaction system generates (or allows the third party provider to generate) a corresponding mobile wallet for the unbanked subscriber (available via the web interface and/or the mobile wallet application). The system then presents the (unbanked) subscriber's account data associated with the mobile wallet and/or a notification indicating that enrollment was successful to the subscriber. Accordingly, the mobile wallet application or the web interface may be used to provide user enrollment functionality. It should also be understood that either the mobile wallet application or the web interface may be used to provide substantially all of the third party or native mobile wallet functionality described herein.

It should also be noted that the mobile device **206** may be any type of plan-based phone or tablet, or prepaid phone or tablet. Many subscribers, such as unbanked subscribers, may primarily use prepaid phones. The mobile wallet application **207** may be installed on both plan-based phones and prepaid phones. The mobile wallet application may be installed on the device's SIM card, or on the device's main memory. Accordingly, the monetary transaction system **200** may be accessed and used via substantially any type of plan-based or prepaid mobile device.

The components depicted in FIG. **1** can interoperate to provide a number of financial and other services including but not limited to enrolling a customer for a third party mobile wallet, adding a stored value account (either hosted by an electronic payment system or a third party), adding a bank/credit union account to a third party mobile wallet, adding a debit/credit card account to a third party mobile wallet, depositing funds in a third party mobile wallet, withdrawing funds from a third party mobile wallet, paying bills from a third party mobile wallet, topping up a prepaid mobile account through a third party mobile wallet, transferring funds through a third party mobile wallet, making in store purchases from a third party mobile wallet, or transferring money or eMoney from one business account to another business account (i.e. from one business's mobile vault to another business's mobile vault, as will be shown in FIG. **4**).

FIG. **3**A depicts a subscriber-to-subscriber eMoney transfer. In a merchant and distributor scenario, either or both of the merchant and the distributor (including any delivery personnel) may be subscribers. To perform such a transfer, subscriber A (**301**) enters some type of identification information identifying subscriber B (e.g. subscriber B's phone number) and an amount of money he or she wishes to transfer. The transaction processor **216** of the monetary transaction system **210** determines if there are sufficient funds to complete the transfer. If sufficient funds are available, the monetary transaction system **210** decrements subscriber A's account and credits subscriber B's account (**302**). The system then sends some kind of notification (e.g. SMS) to subscriber B indicating that a certain amount of money was transferred to their account. Subscriber A may also receive a notification that the transfer was successful. Accordingly, eMoney may be transferred between two cloud-based platform subscribers, one or both of which may be unbanked. The cloud-based transaction system **210** processes the subscribers' requests, updates the subscribers' eMoney balances, logs the transactions, and sends transaction information to a specified bank when needed.

FIG. **3**B illustrates a subscriber-to-non-subscriber eMoney transfer. Accordingly, as mentioned above, either or both of the merchant and the distributor may be non-subscribers. In graphic **305**, subscriber A wishes to send eMoney to another individual that is not a subscriber to the cloud-based transaction platform. The transaction is initiated in the same fashion as the subscriber-to-subscriber transfer scenario. However, since non-subscriber B does not have a mobile wallet account, the cloud-based transaction system **210** cannot credit them with eMoney. Instead, the cloud-based transaction system **210** sends a notification (e.g. via SMS) to non-subscriber B with instructions for how to pick-up the transferred money, along with an authorization code (**306**). The cloud-based

transaction system **210** puts a hold on subscriber A's account for the amount transferred. Subscriber B then has a specified number of days to pick up the cash before the hold expires and the amount is credited back to subscriber A's eMoney account by the monetary transaction system **210**.

When non-subscriber B goes to pick up the money at an agent branch, the agent branch's manager or agent verifies the authorization code via an agent manager or agent mobile wallet application (that, in turn, accesses the cloud-based transaction platform). Once the transfer has been validated, the agent gives the cash to non-subscriber B. The agent branch's mFS account is credited with the transfer amount (**307**) and the user leaves with the cash in hand (**308**). The cloud-based transaction platform processes the transfer request, updates subscriber A's eMoney balance, logs the transaction, and sends transaction details to a platform-specified bank.

FIG. **4** illustrates a mobile wallet subscriber making a retail purchase. Mobile wallet subscribers can make retail purchases at agent branches directly from their mobile device. Agent branches, as explained above, are retail stores or other entities that have registered with the cloud-based transaction platform and are able to accept native and third party mobile wallet payments. Accordingly, a subscriber can select the items they wish to purchase, and indicate (via the mobile wallet application) to the agent branch that they wish to pay for the items. The mobile wallet application then communicates with the agent branch and the monetary transaction system to indicate the price of the transaction. The monetary transaction system **210** then debits the subscriber's eMoney account (**401**) and credits the agent branch's eMoney account (**402**). The agent branch (and/or the agent manager or agent) receives confirmation that subscriber paid for the purchase. The subscriber may also receive a summary of the retail purchase and may be asked to confirm the purchase by entering a PIN. The monetary transaction system processes the purchase request, updates the agent branch and subscriber's eMoney balances, logs the transaction, and sends transaction details to a cloud-based transaction platform-specified bank.

In one embodiment, the cloud-based transaction system **210** is implemented to make a purchase from a mobile wallet. The communications module **215** of the monetary transaction system **210** receives a communication from a subscriber over a communication channel **111**. The subscriber communication indicates that an unbanked subscriber **205** desires to purchase an item for a specified amount of funds using a specified payment method from the unbanked subscriber's native or third party mobile wallet.

The monetary transaction system **210** then returns a secure, perishable purchase code to the unbanked subscriber over at least one of the channels connected to the monetary transaction system and receives a subsequent agent branch communication over a channel indicating that the purchase code has been presented to an agent (branch). The monetary transaction system **210** validates the status of the specified payment method, determines if the specified payment method can accommodate a purchase for the specified amount, performs a limit check and/or a velocity check on the selected payment method, debits the specified payment method by the specified amount of funds, returns a notification to the agent branch authorizing the purchase and sends a receipt to the unbanked subscriber over a communication channel. The cloud-based transaction system **210** may thus be used in this manner to make a retail purchase using a native or third party mobile wallet.

FIG. **5** depicts a physical environment and corresponding computer system architecture **500** for allowing a user to participate in various services using a native or third party mobile wallet (e.g. **511**). Some of these services include allowing the user **507** to access disruptively priced or free financial services or items in exchange for participation in opt-in advertising. The environment **500**, like the scenarios described in FIGS. **3**A, **3**B and **4**, involves the use of a native or third party mobile wallet application **511**. The mobile wallet application **511** can be used to provide disruptively priced or free financial services or items in exchange for participation in opt-in advertising. The mobile wallet application may be run on any type of digital device including a mobile phone, tablet, laptop or other digital device. Embodiments include providing digital data (e.g., coupons or vouchers) for obtaining disruptively priced or free items (e.g., consumer goods or groceries) to such digital devices.

In some embodiments, a user has an account with a mobile payment system. The cloud-based transaction system (e.g. **210** of FIG. **2** or electronic payment system **521** of FIG. **5**) can provide the user **507** with a variety of functionality including purchasing items (see FIG. **4**), depositing funds, withdrawing funds, transferring funds (see FIGS. **3**A and **3**B), and others all from a third party wallet. Accordingly, the user can use a digital device to interact with the electronic payment system **521** to pay for goods and/or services.

In exchange for some type of financial benefit, the user opts in to receive advertisements. The financial benefits may include coupons, vouchers, promotions, Buy One Get One ("BOGO") offers or any other type of benefit (such as a reduced cost or free financial service or good) from the electronic payment system. The benefit may be targeted to the user based on the user's age, location or other demographic information, or based on the user's past purchases. At least in some embodiments, when the user agrees to participate in opt-in advertising, the electronic payment system **521** is permitted to store (e.g., by capturing purchase orders), track, and analyze items that the user purchases through their account with the electronic payment system. The electronic payment system stores and maintains lists of the users' purchased items in a data warehouse. The electronic payment system may also store information about the user (anonymous or otherwise) including age, income level, an indication of whether kids are in the family, or other information that may be useful in targeting ads or benefits to the user.

The electronic payment system analyzes **534** the users purchasing habits to identify advertisements and/or promotions that may be of interest to the user. The advertisements and/or promotions can be for items the user has purchased **503**. The advertisements and/or promotions can also be for items related to items the user has purchase. For example, if user has purchased a particular brand of razor, advertisements for the brand's shaving cream can be identified. Advertisements for related items can also be used for cross-promotion. From time to time, at specified intervals, or based on location (e.g., having a coupon for a merchant this is with a specified proximity) the electronic payment system sends identified advertisements and/or promotions to the user's digital device. When specified advertising thresholds are satisfied (e.g., a specified number and/or type of advertisements and/or promotions are presented), the electronic payment system confers a financial benefit on the user's account. For example, the electronic payment system can provide the user's account with a low cost (e.g., reduced fee) or free financial service, such as, for example, one reduced cost bill pay or one free bill pay. Alternately, the electronic payment system can provide the user's account with a coupon or voucher for an item (e.g., an item a user has pre-selected or an item the user has purchased in the past).

In some embodiments, a client application for the electronic payment system runs on the user's digital device (e.g. mobile wallet application **511**). The user interacts with the electronic payment system through the client application. From a screen of the client application, the user can agree to accept opt in advertising. Accordingly, embodiments of the invention essentially permit a user to self-monetize themselves through their digital device.

As further depicted in FIG. **5**, computer architecture **500** includes digital device **508**, retail location **502**, and electronic payment system **521**. Digital device **508** further includes mobile wallet application **511**. Retail location **502** further includes its own mobile wallet application **512**. Electronic payment system **521** includes marketing module **533**, data warehouse **532**, advertisements **538**, payment processor **522**, user mobile wallet **524** (user **507**'s mobile wallet), and merchant mobile wallet **526** (retail location **502**'s mobile wallet).

Generally, each company in packaged goods companies **571** (or retailers that sell the packaged goods or other goods or services) can send advertisement data to electronic payment system **521**. Advertisements **538** represent the collection of advertisement data sent from packaged goods companies **571**. Each company in packaged goods companies **571** can also submit benefit rules to electronic payment system **521**. Benefit rules **578** represent the collection of benefit rules sent from packaged goods companies **571**. Benefit rules **578** define when a benefit, such as, for example, a free financial service, a coupon, a promotion, etc, is to be granted to a user of electronic payment system **521**. For example, in response to completing a questionnaire linked to a product advertisement, a user can be given a coupon for the product or for a related product.

In general, user **507** can use native or third party mobile wallet application **511** to pay for goods purchased at retail location **502** (as shown in FIG. **4**). For example, user **507** can use mobile wallet application **511** to purchase goods **503**. To pay for goods **503**, mobile wallet application **511** can send payment instruction **543** in amount **563** to electronic payment system **521**. Payment processor **522** can receive payment instruction **543**. In response, payment processor **522** can debit **541** user mobile wallet **524** by amount **563**. Payment processor **522** can also credit **542** merchant mobile wallet **526** by amount **563**.

User **507** can use mobile wallet application **511** to participate in opt-in advertising. For example, user **507** can use mobile wallet application **511** to send opt-in **544** to electronic payment system **521**. Advertising module **536** can receive opt-in **544** and record that mobile wallet application **511** has opted in for advertising. As such, when user **507** makes a purchase using mobile wallet application **511**, a list of purchased items is sent to electronic payment system **521**. For example, upon purchasing goods **503**, item list **531** is sent to electronic payment system **521** and stored in data warehouse **532**.

Propensity analysis module **534** can analyze user **507**'s purchases, including item list **531**. From the analysis, propensity analysis module **534** can identify items or categories of items user **507** may be interested in. The items can be items user **507** has purchased in the past (e.g., an item in goods **503**) or items related to items user **507** has purchases in the past. Propensity analysis module **534** can indicate identified items or categories of items to advertisement identification module **536**. These identified items or categories are items that the user is likely interested in and, as such, may have a propensity toward buying these items. The propensity analysis module may use past purchases, personal preferences, lifestyle or demographic information or other data in the propensity analysis.

Advertisement identification module **536** can then select advertisements from advertisements **538** that correspond to the identified items or categories of items. For example, advertisement identification module **536** can select advertisement **546** for presentation at mobile wallet application **511**. Advertisement **546** can be an advertisement for a product made by a company in packaged goods companies **571**. Additionally or alternatively, the advertisement **546** may be created by the merchant and may advertise products or services sold by that merchant.

Advertising module **533** can send selected advertisements to mobile wallet application **511**. For example, advertising module **533** can send advertisement **546** (e.g., related to an item in goods **503**) to mobile wallet application **511**. In general, advertisements can include interactive content. For example, advertisement **546** includes content **573**. Content **573** can be a video, a link to a company website (e.g., for a company in packaged goods companies **571**), a call to action (such as a questionnaire), or some other content user **507** can interact with through digital device **508**. User **507** can interact with content **573**, for example, responding to questions in content **573**. Advertisement response **574** can indicate how user **507** has interacted with content **573**. In one embodiment, a call to action may be to post an update on Facebook® or some other website such as a retail establishment ranking website. If the user makes such a post or performs some other call to action, the user may be rewarded with a benefit. That benefit may be related to the product about which the user posted on the various websites.

Based on advertisement response **574**, benefit determination module **576** can determine if a benefit is to be conferred upon user **507**. Benefit determination module **576** can refer to benefit rules **578** when making a determination whether or not to confer a benefit. Thus, when user **507** interacts with advertisement **546** in a specified way (e.g., completes a survey, watches a video, etc.), benefit rules **578** can indicate that a company benefit (e.g., benefit **577**) is to be conferred upon user **507**. For example, benefit determination module **576** can confer benefit **577** on user **507**. When user **507** receives an advertisement for a razor, for instance, and answers a questionnaire on how often they shave, a razor manufacture can give user **507** a coupon for reduced cost or free razor blades.

When a benefit is to be conferred on a user, the benefit can be stored in the user's brand locker. For example, benefit determination module **576** can store benefit **577** in brand locker **572** (part of user mobile wallet **524**). Benefit **577** can be a coupon, a reduced cost or free financial service, a voucher, a promotion, a free bill pay, etc.

Benefit determination module **576** can also track aggregate statistics, such as, for example, specified number and/or type of advertisements received, for advertisements presented at native or third party mobile wallet application **511**. Benefits can also be conferred upon users based on the aggregate statistics. For example, benefit determination module **576** can confer a benefit upon user **507** in response to twenty advertisements being presented at mobile wallet application **511**. Thus, conferred benefits can be company-specified benefits or can be electronic payment system-specified benefits. Electronic payment system **521** can notify a user when a benefit is conferred. For example, electronic payment system **521** can send benefit notification **547** to mobile wallet application **511** to indicate benefit **577** being stored in brand locker **572**.

When user **507** makes subsequent purchases through user mobile wallet **524**, electronic payment system **521** can auto-

matically check brand locker **572** for benefits related to any purchases items. If benefits for an item are identified, user **507** can be notified through mobile wallet application **511**. In some cases, if benefits are identified, those benefits can be applied automatically when the user purchases that item or service. Thus, if the benefit is a coupon or a buy one get one free offer, that benefit may be applied automatically when the user uses his or her mobile wallet application **511** to purchase that item. Accordingly, embodiments of the invention permit user **507** to self monetize digital device **508** through agreeing to participate in opt-in advertising.

Although not depicted, various other modules from the architecture of FIG. **1** or **2** can also be included electronic payment system **521**. The modules expressly depicted in FIG. **5** can interoperate with these other modules as appropriate to facilitate desired functionality.

FIGS. **7-9** will now be described in conjunction with the computer architecture **600** illustrated in FIG. **6**. FIG. **6** depicts a mobile wallet platform **601** that may have an architecture as shown in FIG. **1**. As further depicted in FIG. **6**, mobile wallet platform **601** communicates with an agent terminal **602** or a customer **607** to process transactions using a native or third party mobile wallet **605**. Mobile wallet platform **601** may also communicate with a third party processor **604** to process transactions using a mobile wallet or third party mobile wallet. Mobile wallet platform **601** may also communicate with a third party mobile wallet platform **603** to process transactions using a mobile wallet owned or managed by a third party mobile wallet provider.

Mobile wallet platform **601** may also process the mobile wallet transaction or third party mobile wallet transaction internally, without the use of third party processors or third party mobile wallet platforms. In particular, mobile wallet platform **601** may process transactions using third party mobile wallets in the same or similar manner that transactions are processed as shown in FIGS. **2-5**. Accordingly, the physical environment and corresponding computer system architecture **600** shown in FIG. **6** allows a cloud-based transaction platform **601** to support multiple third party mobile wallet providers.

Mobile wallet platform **601** communicates with agent terminal **602**, third party mobile wallet platform **603**, third party processor **604**, and customer's mobile phone **619** through a variety of communication channels. For example, the communication between mobile wallet platform **601** and any one of these entities may be through communication channels **111**, notification channels **112**, or third party systems **113**, as shown in FIG. **1**. Communication between mobile wallet platform **601** and any one of these entities may also be through processor **121** shown in FIG. **1**.

With respect to the entire description of FIG. **6**, and as explained above, the term "mobile wallet" encompasses not only mobile wallets owned or managed by the mobile wallet platform, but also third party mobile wallets owned by third party mobile wallet providers or managed by third party mobile wallet platforms. In contrast, the term "third party mobile wallet" refers only to third party mobile wallets owned by third party mobile wallet providers or managed by third party mobile wallet platforms. Accordingly, cloud-based transaction platform **601** may manage and process transactions using mobile wallets **605**, which may be mobile wallets owned by cloud-based transaction platform **601** or mobile wallets owned by a third party mobile wallet provider.

As shown in FIG. **6**, customer **607** initiates a mobile wallet transaction **608** at agent terminal **602**. Agent terminal **602** may be part of an agent network consisting of one or more agent terminals that communicate with cloud-based transaction platform **601**. Examples of agent terminals are stores and other commercial establishments. Alternatively, customer **607** may initiate a mobile wallet transaction **609** by communicating with cloud-based transaction platform **601** through a channel selected by the customer.

Mobile wallet transactions **608** and **609** may be one or more of any type of transaction that can be performed using a mobile wallet, including but not limited to, a deposit, withdrawal, transfer, purchase, bill payment, topping up of a prepaid mobile account, or any other transaction described herein. Customer **607** may initiate transactions **608** and **609** in a variety of ways. For example, customer **607** can initiate a deposit into a mobile wallet, a withdrawal from a mobile wallet, a bill payment from a mobile wallet, topping up of a prepaid mobile account using a mobile wallet, a transfer from a mobile wallet, a remittance transaction, a selection of health care provider or payment of health services, a purchase of music, movies, games or other downloadable content, or other purchases using a mobile wallet.

After customer **607** initiates transaction **609** through agent terminal **602**, agent terminal **602** then communicates with cloud-based transaction platform **601** by sending transaction data **610** to cloud-based transaction platform **601**. Once cloud-based transaction platform **601** has received the transaction either through transaction data **610** from agent terminal **602** or from transaction **609** initiated by customer **607**, cloud-based transaction platform **601** may then process the transaction in a variety of ways.

For example, cloud-based transaction platform **601** may process the transaction by communicating with third party processor **604** by sending third party transaction data **611**, which may include some or all of the information in transaction data **610**. Third party processor can then perform the requested transactional processing and respond by sending confirmation data **612** to cloud-based transaction platform **601**. Confirmation data **612** can indicate whether the requested mobile wallet transaction was processed successfully or unsuccessfully.

In another example, cloud-based transaction platform **601** may process the transaction by communicating with third party mobile wallet platform **603** by sending third party transaction data **613**, which may include some or all of the information in transaction data **610**. Third party mobile wallet platform **603** may have any architecture which is suitable for processing mobile wallet transactions. Third party mobile wallet platform **603** may have an architecture that is the same or similar to the architecture shown in FIG. **1**.

Alternatively, third party mobile wallet platform **603** may have a different architecture. In addition, any aspects of cloud-based transaction platform **601** or functionality provided by that platform may also be present in third party mobile wallet platform **603**. After receiving third party transaction data **613**, third party mobile wallet platform **603** may process the transaction itself or forward the transaction to third party processor **604** by sending third party transaction data **614**.

Once processing of the transaction is complete, third party mobile wallet platform **603** may respond to cloud-based transaction platform **601** by sending confirmation data **615**. Confirmation data **615** can indicate whether the requested mobile wallet transaction was processed successfully or unsuccessfully. In addition, following the processing performed by third party mobile wallet platform **603** after receiving third party transaction data **613**, the third party mobile wallet platform **603** may provide a commission or transaction fee **616** to cloud-based transaction platform **601**.

In a further example, mobile wallet platform **601** may process the transaction internally within cloud-based transaction platform **601**. Specifically, cloud-based transaction platform **601** may process a transaction using a third party mobile wallet entirely within cloud-based transaction platform **601**.

Once processing of the transaction is complete, cloud-based transaction platform **601** may communicate with agent terminal **602** by sending confirmation data **617** indicating information such as whether the transaction was successful or not. Also following processing of the transaction, mobile wallet platform may send customer notification **618** through an appropriate channel such as to the customer's mobile phone **619**. For example, customer notification **618** may be sent using the notification services **102** and notification channels **112** (e.g. SMPP, SMTP, voice) of FIG. **1**.

With reference now to FIGS. **2**, **6** and **7**, the cloud-based transaction system **210** receives communication **226** from an agent terminal **223** over a communication channel connected to the cloud-based transaction platform **210/601** (act **710**). The agent communication indicates that a customer **222/205** desires to perform a mobile wallet transaction using their third party mobile wallet **207**. The cloud-based transaction system **210** sends the agent communication to a third party mobile wallet platform **603** (act **720**). The cloud-based transaction system **210** then receives communication **611** from the third party mobile wallet platform confirming processing of the transaction **612** (act **730**) and sends communication **617** to the agent terminal **602** over communication channels **111** connected to the cloud-based transaction platform indicating confirmation of the processing of the transaction (act **740**).

As mentioned above, multiple different types of transactions may be performed using the infrastructure provided by the cloud-based transaction system. The transactions may be a performed not only by a first customer that uses a first mobile wallet provider, but also by a second, different customer using a second, different third party mobile wallet provider. The third party mobile wallet platform may use a third party processor to perform (at least parts of) the transaction. The customer may be notified of confirmation of the processing of the transaction using the third party mobile wallet over various communication channels connected to the cloud-based transaction platform. In some cases, each third party mobile wallet provider has their own point of sale (POS) processing system **230**. The third party mobile wallet providers' POS processing systems may communicate with each other using the cloud-based transaction platform to process the transaction.

One of the transactions made possible by the cloud-based transaction platform **601** is depositing funds into a third party mobile wallet owned by an entity different than the customer. The cloud-based transaction system may receive a communication **226** from the agent terminal **223** over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that the customer desires to deposit a specified amount of funds into their third party mobile wallet **605**. The cloud-based transaction system may then credit the third party mobile wallet with the specified amount of funds.

Another transaction provided by the cloud-based transaction platform **601** is withdrawing funds from a third party mobile wallet owned by an entity different than the customer. The cloud-based transaction platform receives communication **208** from the customer **205** indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet. The cloud-based transaction platform **601** returns a secure, perishable withdrawal code to the customer over at least one of the communication channels connected to the cloud-based transaction platform. It also receives communication from the agent terminal **223** indicating that the withdrawal code has been presented to an agent and debits the third party mobile wallet by the specified amount of funds.

Another transaction provided by the cloud-based transaction platform **601** is transferring money from a third party mobile wallet within the cloud-based transaction platform to a recipient at a second third party mobile wallet provided by a second mobile wallet provider. In this transaction, the platform **601** receives a customer communication **208** indicating that a customer **205** desires to transfer a specified amount of funds to a specified recipient using a specified payment method from the third party mobile wallet **606**. The cloud-based transaction platform debits the third party mobile wallet by the specified amount of funds and transfers the specified amount of funds from the cloud-based transaction platform to the second different third party mobile wallet platform for delivery to the specified recipient. The specified amount of funds is then transferred to the second third party mobile wallet platform.

Yet another transaction provided by the cloud-based transaction platform **601** is making a purchase from a third party mobile wallet managed by a third party mobile wallet platform. In this transaction, the cloud-based transaction platform receives communication **208** from the customer **205** indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from the customer's third party mobile wallet **606**. The cloud-based transaction platform returns a secure, perishable purchase code to the customer, receives communication **226** from the agent terminal **223** indicating that the purchase code has been presented to an agent, and debits the customer's third party mobile wallet by the specified amount of funds.

In another embodiment, as shown in FIG. **8**, a cloud-based transaction system performs or facilitates a transaction using a third party point of sale (POS) system. The cloud-based transaction system receives communication **226** from a specified POS system **224** implemented at an agent terminal **223** over a communication channels **111** connected to the cloud-based transaction platform **210** (act **810**). The POS communication indicates that a customer **205** has initiated a mobile wallet transaction using their third party mobile wallet **207**. The cloud-based transaction system sends the POS communication to a corresponding third party POS transaction processing system **230** that has been established to process POS transactions from the specified POS system (act **820**). The cloud-based transaction system then receives communication from the third party POS transaction processing system **230** confirming processing of the transaction (act **830**) and sends communication to the specified POS system **224** implemented at the agent terminal **223** indicating confirmation of the processing of the transaction (act **840**).

In some cases, transaction fees or commissions **616** may be paid by the third party mobile wallet platform to the cloud-based transaction platform for facilitating the transaction. One of the transactions allowed by the cloud-based transaction system is depositing funds into a third party mobile wallet provided by a third party mobile wallet provider. In this transaction, the cloud-based transaction platform **210** receives communication **226** from a specified POS system **224** implemented at the agent terminal **223** over a communication channels **111** connected to the cloud-based transaction platform. The POS communication indicates that the customer **205/222** desires to deposit a specified amount of funds into the third party mobile wallet **606** provided by the third

party mobile wallet provider. The cloud-based transaction system validates the status of the third party mobile wallet provided by the third party mobile wallet provider, determines if the specified POS system implemented at the agent terminal is authorized to deposit money, performs a limit check or a velocity check on the third party mobile wallet provided by the third party mobile wallet provider, credits the third party mobile wallet provided by the third party mobile wallet provider with the specified amount of funds, returns a notification to the specified POS system implemented at the agent terminal confirming the deposit and notifies the customer that the specified amount of funds were deposited in the third party mobile wallet provided by the third party mobile wallet provider over a communication channel connected to the cloud-based transaction platform **210**.

Another transaction provided by the cloud-based transaction platform **210** is withdrawing funds from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform **210** receives communication **208** from a customer **205** indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet **606** provided by the third party mobile wallet provider. The cloud-based transaction platform **210** validates the status of the third party mobile wallet provided by the third party mobile wallet provider, determines if the balance of the third party mobile wallet provided by the third party mobile wallet provider is sufficient to accommodate the requested withdrawal for the specified amount of funds, performs a limit check and/or a velocity check on the third party mobile wallet, returns a secure, perishable withdrawal code to the customer over a communication channel **111** connected to the cloud-based transaction platform, receives subsequent POS communication **226** indicating that the withdrawal code has been presented to an agent (e.g. at agent terminal **223**), debits the third party mobile wallet provided by the third party mobile wallet provider by the specified amount of funds, returns a notification to the POS system at the agent terminal confirming the withdrawal and notifies the customer **205** (e.g. in confirmation **617**) that the specified amount of funds were withdrawn from the third party mobile wallet.

In yet another transaction provided by the cloud-based transaction platform, money is transferred using a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform **210** receives customer communication **208** indicating that the customer **205** desires to transfer a specified amount of funds to a specified recipient having a third party mobile wallet **606**, where the transfer uses a specified payment method from the customer's third party mobile wallet at the cloud-based transaction platform **210**. The cloud-based transaction platform validates the status of the specified payment method, performs a limit check and/or a velocity check on the specified payment method, performs a check on the specified recipient having a third party mobile wallet to comply with the office of foreign assets control, debits the customer's mobile wallet at the cloud-based transaction platform by the specified amount of funds, transfers the specified amount of funds to third party mobile wallet provider for delivery to the third party mobile wallet of the specified recipient over a communication channel connected between the cloud-based transaction platform and the third party mobile wallet provider, and notifies the customer that the specified amount of funds was transferred to the specified recipient.

In another transaction provided by the cloud-based transaction platform **210**, a purchase is made from a third party mobile wallet provided by a third party mobile wallet provider. In this transaction, the cloud-based transaction system receives communication **208** from the customer **205** indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from the customer's third party mobile wallet **606**. The cloud-based transaction system returns a secure, perishable purchase code to the customer, receives subsequent agent terminal communication indicating that the purchase code has been presented to an agent, validates the status of the specified payment method, determines if the specified payment method can accommodate a purchase for the specified amount, performs a limit check and/or a velocity check on the specified payment method, debits the customer's third party mobile wallet by the specified amount of funds by sending communication to the third party mobile wallet provider, returns a notification to the POS system at the agent terminal authorizing the purchase and sends a receipt to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform.

FIG. **9** describes a further embodiment in which a cloud-based transaction platform facilitates making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction system **210** receives communication **208** from a customer **205** over a communication channel connected to the cloud-based transaction platform (act **910**). The customer communication indicating that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's third party mobile wallet **606**. The cloud-based transaction system returns a secure, perishable purchase code to the customer (act **920**) and receives communication from an agent terminal **223** over at least one of the communication channels connected to the cloud-based transaction platform indicating that the purchase code has been presented to an agent (act **930**). The cloud-based transaction system **210** then debits the customer's third party mobile wallet **606** by the specified amount of funds (act **940**).

Substantially any item may be purchased using this transaction technique including items provided directly by the cloud-based transaction system, or items provided by third party retailers through the cloud-based transaction system. These items may include health care services, physical, shippable items, music, games, movies or any other digital or downloadable content.

Embodiments of the invention can adhere to Know Your Customer (KYC) rules in the United States by performing Customer Identification Program (CIP) checks as required by the Bank Secrecy Act and U.S. PATRIOT Act. A minimum amount of information can be gathered about a customer, such as, for example, First Name, Last Name, Date of Birth, Government ID Type, Government ID Number, Address. The CIP processes are designed to validate customer identity against government blacklists and assist in the prevention of money laundering and terrorist financing. A combination of non-documentary and documentary verification can be used to ensure beyond a reasonable doubt the identity of the customer.

Non-Documentary Verification can occur through the presentment of the information that was collected from the user to an external third party, such as, for example, Lexis Nexis. Documentary Verification can occur if non-documentary verification fails, then the user is asked to present an unexpired government ID. Various differ forms of identification including Driver's license, Passport, Alien identification (e.g., green card or work visa), and Mexican Consular identification card, can be accepted.

Embodiments of the invention can perform Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) checks. AML and CFT checks can be performed using transaction monitoring methods to flag names and suspicious transactions for further investigation. The mobile wallet platform can perform AML and CFT checks on all electronic financial transactions to ensure that electronic funds are not being used for money laundering or terrorism. Transaction limits can be placed on user accounts. The transaction limits are fully configurable for each particular use case, channel and payment method that allows maximum flexibility to restrict higher risk use cases. Velocity checks can also be performed. Velocity Checks ensure that subscribers are not abusing the mobile wallet platform within the allowable limits.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed:

1. A computing system for facilitating management of a mobile wallet, including:

one or more processors;

system memory;

an integration tier configured to manage mobile wallet sessions with a mobile device and including web services communication mechanisms for interfacing with a mobile wallet application installed on a hardware SIM card as well as with a plurality of different device types over a plurality of different communication channels, the integration tier being configured to receive binary and text messages from the mobile device;

a notification services engine configured to interface with the integration tier and to send Short Message Peer-to-Peer (SSMP) messages, Short Messaging Service (SMS) messages and Simple Mail Transfer Protocol (SMTP) messages over the different communication channels to different devices, including the mobile device, to interface with the mobile wallet application installed on the hardware SIM card;

service connectors that are each configured to connect the computing system to a different third party system, each of the service connectors being configured as a separate module for integrating a corresponding external service to the computing system;

a payment handler that exposes a common API for interacting with different payment processors;

a security services engine that performs subscriber authentication utilizing a database-based Access Control List (ACL);

a rules engine configured to enforce constraints on financial transactions performed with the mobile wallet application, the mobile wallet application being associated with a mobile wallet account; and

one or more computer-readable storage media having stored thereon computer-executable instructions that are executable by the one or more processors to cause the computing system to perform a transaction for a customer using the mobile wallet which is owned by another entity than the customer, comprising the following:

the computing system receiving communication from an agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that a customer desires to perform a transaction comprising a mobile wallet transaction using a third party mobile wallet, the mobile wallet transaction comprising at least one of a mobile wallet transfer in which funds are transferred from the mobile wallet of the customer to a third party mobile wallet, a mobile wallet withdrawal in which funds are withdrawn from the third party mobile wallet and provided to the customer, or a mobile wallet deposit in which funds are deposited into the third party mobile wallet;

the computing system sending the agent communication to the third party mobile wallet platform;

the computing system determining whether the mobile wallet transaction comprises the mobile wallet withdrawal and when the mobile wallet transaction is determined to comprise the mobile wallet withdrawal, generating and providing a perishable withdrawal code to the consumer, which is presented to the agent terminal to facilitate processing of the mobile wallet withdrawal;

the computing system receiving communication from the third party mobile wallet platform confirming processing of the transaction, the transaction comprising at least one of the mobile wallet transfer, the mobile wallet withdrawal or the mobile wallet deposit; and

the computing system sending communication to the agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the communication indicating confirmation of the processing of the transaction.

2. The computing system of claim 1, wherein a new transaction is performed by the computing system for a second, different customer using a second, different third party mobile wallet.

3. The computing system of claim 1, wherein the transaction further comprises the customer of confirmation of the processing of the transaction using the third party mobile wallet over at least one of the plurality of communication channels connected to the cloud-based transaction platform.

4. The computing system of claim 1, wherein the third party mobile wallet is provided by a third party mobile wallet provider.

5. The computing system of claim 4, wherein each third party mobile wallet provider has their own point of sale (POS) processing system.

6. The computing system of claim 5, wherein the third party mobile wallet providers' POS processing systems communicate with each other using the cloud-based transaction platform to process the transaction.

7. computing system of claim 1, wherein the transaction comprises the mobile wallet deposit for depositing funds into the third party mobile wallet which is owned by the entity different than the customer, including:

receiving communication from the agent terminal over one of the plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that the customer desires to deposit a specified amount of funds into the third party mobile wallet; and

crediting the third party mobile wallet with the specified amount of funds.

8. The computing system of claim 1, wherein the transaction comprises the mobile wallet withdrawal for withdrawing funds from the third party mobile wallet owned which is owned by the entity different than the customer, including:

receiving communication from the customer over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet;

providing the perishable withdrawal code to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform;

receiving communication from the agent terminal over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the perishable withdrawal code has been presented to an agent; and

debiting the third party mobile wallet by the specified amount of funds.

9. The computing system of claim **1**, wherein the transaction comprises the mobile wallet transfer for transferring money from a mobile wallet account of the customer provided by a first mobile wallet provider to a third party mobile wallet of a recipient provided by a second mobile wallet provider, the method comprising:

receiving customer communication over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to transfer a specified amount of funds to the recipient using a specified payment method from the mobile wallet account of the customer;

debiting the mobile wallet account by the specified amount of funds; and

transferring the specified amount of funds from the cloud-based transaction platform to the second third party mobile wallet platform for delivery to the specified recipient, the specified amount of funds being transferred over at least one of the plurality of channels connected to the third party mobile wallet platform.

10. The computing system of claim **1**, wherein the claimed method also includes performing a new transaction comprising a mobile wallet purchase at an agent terminal using a third party mobile wallet managed by a third party mobile wallet platform, including:

receiving communication from the customer over one of the plurality of channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from a third party mobile wallet;

returning a secure, perishable purchase code to the customer over at least one of the plurality of channels connected to the cloud-based transaction platform;

receiving communication from the agent terminal over at least one of the plurality of channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the purchase code has been presented to an agent;

debiting the third party mobile wallet by the specified amount of funds; and

crediting an agent account by the specified amount of funds.

11. At a computer system including at least one processor and a memory, a computer-implemented a method for performing a transaction for a customer using a third party mobile wallet owned by another entity than the customer, the method comprising the following:

the computing system receiving communication from an agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that a customer desires to perform a transaction comprising a mobile wallet transaction using a third party mobile wallet, the mobile wallet transaction comprising at least one of a mobile wallet transfer in which funds are transferred from the mobile wallet of the customer to a third party mobile wallet, a mobile wallet withdrawal in which funds are withdrawn from the third party mobile wallet and provided to the customer, or a mobile wallet deposit in which funds are deposited into the third party mobile wallet;

the computing system sending the agent communication to the third party mobile wallet platform;

the computing system receiving communication from the third party mobile wallet platform confirming processing of the transaction, the transaction comprising at least one of the mobile wallet transfer, the mobile wallet withdrawal or the mobile wallet deposit;

the computing system determining whether the mobile wallet transaction comprises the mobile wallet withdrawal and when the mobile wallet transaction is determined to comprise the mobile wallet withdrawal, generating and providing a perishable withdrawal code to the consumer, which is presented to the agent terminal to facilitate processing of the mobile wallet withdrawal; and

the computing system sending communication to the agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the communication indicating confirmation of the processing of the transaction, wherein the computing system includes:

one or more processors;

system memory;

an integration tier configured to manage mobile wallet sessions with a mobile device on which a mobile wallet application is installed and including web services communication mechanisms for interfacing with the mobile wallet application which is installed on a hardware SIM card as well as with a plurality of different device types over a plurality of different communication channels, the integration tier being configured to receive binary and text messages from the mobile device;

a notification services engine configured to interface with the integration tier and to send Short Message Peer-to-Peer (SSMP) messages, Short Messaging Service (SMS) messages and Simple Mail Transfer Protocol (SMTP) messages over the different communication channels to different devices, including the mobile device, to interface with the mobile wallet application installed on the hardware SIM card;

service connectors that are each configured to connect the computing system to a different third party system, each of the service connectors being configured as a separate module for integrating a corresponding external service to the computing system;

a payment handler that exposes a common API for interacting with different payment processors;

a security services engine that performs subscriber authentication utilizing a database-based Access Control List (ACL); and

a rules engine configured to enforce constraints on financial transactions performed with the mobile wallet application.

12. The computer-implemented method of claim 11, wherein a new transaction is performed by the computing system for a second, different customer using a second, different third party mobile wallet.

13. The computer-implemented method of claim 11, wherein the third party mobile wallet platform comprises a third party processor.

14. The computer-implemented method of claim 11, further comprising notifying the customer of confirmation of the processing of the transaction using the third party mobile wallet over at least one of the plurality of communication channels connected to the cloud-based transaction platform.

15. The computer-implemented method of claim 11, wherein the third party mobile wallet is provided by a third party mobile wallet provider.

16. The computer-implemented method of claim 15, wherein each third party mobile wallet provider has their own point of sale (POS) processing system.

17. The computer-implemented method of claim 16, wherein the third party mobile wallet providers' POS processing systems communicate with each other using the cloud-based transaction platform to process the transaction.

18. The computer-implemented method of claim 11, wherein the transaction comprises the mobile wallet deposit for depositing funds into the third party mobile wallet which is owned by the entity different than the customer, including:

receiving communication from the agent terminal over one of the plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that the customer desires to deposit a specified amount of funds into the third party mobile wallet; and

crediting the third party mobile wallet with the specified amount of funds.

19. The computer-implemented method of claim 11, wherein the transaction comprises the mobile wallet withdrawal for withdrawing funds from the third party mobile wallet owned which is owned by the entity different than the customer, including:

receiving communication from the customer over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet;

returning providing the perishable withdrawal code to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform;

receiving communication from the agent terminal over at least one of the plurality of communication channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the perishable withdrawal code has been presented to an agent;

debiting the third party mobile wallet by the specified amount of funds; and

crediting the agents account by the specified amount of funds.

20. The computer-implemented method of claim 11, wherein the transaction comprises the mobile wallet transfer for transferring money from a mobile wallet account of the customer provided by a first mobile wallet provider to a third party mobile wallet of a recipient provided by a second mobile wallet provider, the method comprising:

receiving customer communication over one of the plurality of communication channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to transfer a specified amount of funds to the recipient using a specified payment method from the mobile wallet account of the customer;

debiting the mobile wallet account by the specified amount of funds; and

transferring the specified amount of funds from the cloud-based transaction platform to the second third party mobile wallet platform for delivery to the specified recipient, the specified amount of funds being transferred over at least one of the plurality of channels connected to the third party mobile wallet platform.

21. The computer-implemented method of claim 11, wherein the claimed method also includes performing a new transaction comprising a mobile wallet purchase at an agent terminal using a third party mobile wallet managed by a third party mobile wallet platform, including:

receiving communication from the customer over one of the plurality of channels connected to the cloud-based transaction platform, the customer communication indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from a third party mobile wallet;

returning a secure, perishable purchase code to the customer over at least one of the plurality of channels connected to the cloud-based transaction platform;

receiving communication from the agent terminal over at least one of the plurality of channels connected to the cloud-based transaction platform, the agent terminal communication indicating that the purchase code has been presented to an agent;

debiting the third party mobile wallet by the specified amount of funds; and

crediting an agent account by the specified amount of funds.

22. One or more computer-readable hardware storage devices having stored thereon computer-executable instructions that are executable by the one or more processors of a computing system to cause the computing system to perform a transaction for a customer using a third party mobile wallet owned by another entity than the customer, comprising the following:

the computing system receiving communication from an agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that a customer desires to perform a transaction comprising a mobile wallet transaction using a third party mobile wallet, the mobile wallet transaction comprising at least one of a mobile wallet transfer in which funds are transferred from the mobile wallet of the customer to a third party mobile wallet, a mobile wallet withdrawal in which funds are withdrawn from the third party mobile wallet and provided to the customer, or a mobile wallet deposit in which funds are deposited into the third party mobile wallet;

the computing system sending the agent communication to the third party mobile wallet platform;

the computing system receiving communication from the third party mobile wallet platform confirming processing of the transaction, the transaction comprising at least one of the mobile wallet transfer, the mobile wallet withdrawal or the mobile wallet deposit;

the computing system determining whether the mobile wallet transaction comprises the mobile wallet withdrawal and when the mobile wallet transaction is determined to comprise the mobile wallet withdrawal, gen-

erating and providing a perishable withdrawal code to the consumer, which is presented to the agent terminal to facilitate processing of the mobile wallet withdrawal; and

the computing system sending communication to the agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the communication indicating confirmation of the processing of the transaction, wherein the computing system includes:

one or more processors;

system memory;

an integration tier configured to manage mobile wallet sessions with a mobile device on which a mobile wallet application is installed and including web services communication mechanisms for interfacing with the mobile wallet application which is installed on a hardware SIM card as well as with a plurality of different device types over a plurality of different communication channels, the integration tier being configured to receive binary and text messages from the mobile device;

a notification services engine configured to interface with the integration tier and to send Short Message Peer-to-Peer (SSMP) messages, Short Messaging Service (SMS) messages and Simple Mail Transfer Protocol (SMTP) messages over the different communication channels to different devices, including the mobile device, to interface with the mobile wallet application installed on the hardware SIM card;

service connectors that are each configured to connect the computing system to a different third party system, each of the service connectors being configured as a separate module for integrating a corresponding external service to the computing system;

a payment handler that exposes a common API for interacting with different payment processors;

a security services engine that performs subscriber authentication utilizing a database-based Access Control List (ACL); and

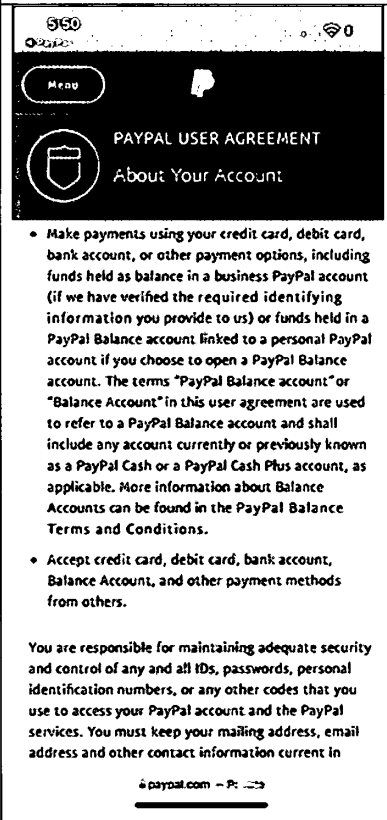
a rules engine configured to enforce constraints on financial transactions performed with the mobile wallet application.

* * * * *

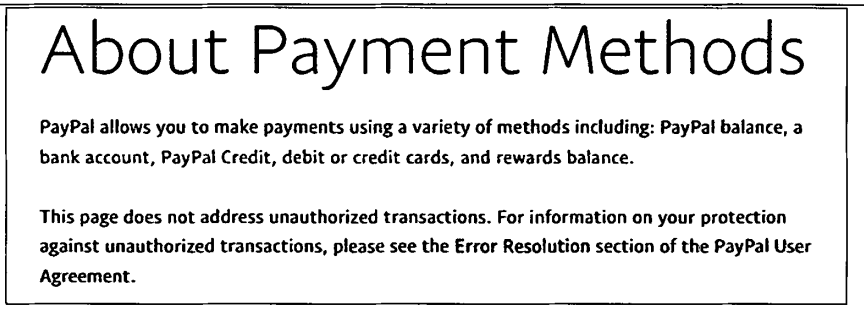
Exhibit H
PayPal Infringement Chart for U.S. Patent No. 9,208,488

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
1. A computing system for facilitating management of a mobile wallet, including:	Upon information and belief, the PayPal System facilitates the management of the PayPal Mobile Wallet. SEND AND REQUEST MONEY FOR FREE • When funded by a bank account or with your PayPal balance, it's free and secure to send money or ask for it back from friends and family in the US. • Just type a name, email or phone number and PayPal will find the right person for you if they have an account. • Request money quickly and securely from friends or family and personalize your payments with animations, stickers, emojis and more. See https://apps.apple.com/app/id283646709?mt=8 (last accessed on February 25, 2022).

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 See PayPal User Agreement on PayPal Mobile App.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 See https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022)
1[a] and 1[b] one or more processors; system memory;	On information and belief the PayPal system includes numerous servers and processors as well as system memory. See Preamble.
1[c] an integration tier configured to manage mobile wallet sessions with a mobile device and including web services communication mechanisms for interfacing with a mobile wallet application installed on a hardware SIM card as well as with a plurality of different device types over a plurality of different	Upon information and belief, the PayPal System includes an integration tier. The integration tier is configured to manage mobile wallet sessions and includes web services communication mechanisms for interfacing with a mobile wallet application on a mobile device over a plurality of different device types and a plurality of different communication channels. The integration tier, for example, handles communications to/from different mobile phones (e.g. Apple and/or Android). The PayPal system can receive data and/or plain text through binary and text messages from the mobile device. To the extent that the limitation is not found because the integration tier is not capable of interfacing with a mobile wallet application installed on a hardware SIM, the limitation is met under the doctrine of equivalents, since the location of the mobile wallet application (whether

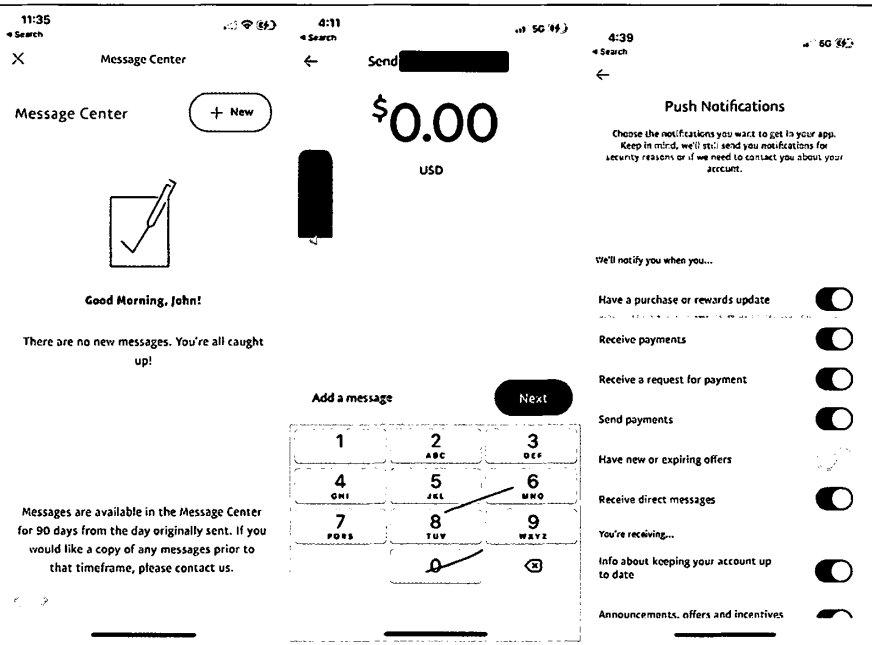
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 317 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
communication channels, the integration tier being configured to receive binary and text messages from the mobile device;	stored on a SIM card or at another location) would perform the same function, in the same way, and achieve the same result.  We have versions of our app for iOS, Android, and Windows. In a few moments you can log on to PayPal, check your balance, pay bills, and more. It is easy, fast, and secure. With PayPal there are no borders. Download Now: iPhone | Android https://www.paypal.com/bs/webapps/mpp/shop/apps (last accessed on February 25, 2022).

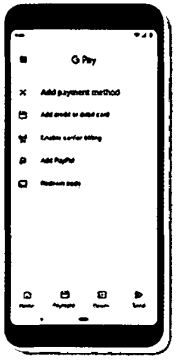
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 318 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* Screenshots of PayPal Mobile app (above) showing ability to receive messages.
1[d] a notification services engine configured to interface with the integration tier and to send Short Message Peer-to-Peer (SSMP)	*See* limitation1[c] regarding the hardware SIM card and message limitations. Upon information and belief, the PayPal System includes notification service engine. The notification services engine is configured to interface with the integration tier and to send digital messages over the various communication channels to different devices, including the mobile device and to interface with the mobile wallet application installed on the hardware SIM card.

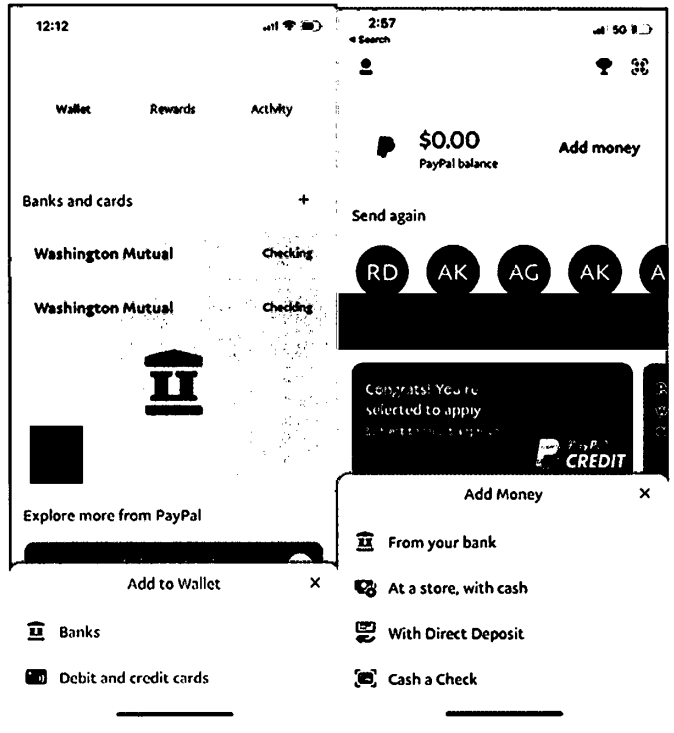
U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
messages, Short Messaging Service (SMS) messages and Simple Mail Transfer Protocol (SMTP) messages over the different communication channels to different devices, including the mobile device, to interface with the mobile wallet application installed on the hardware SIM card;	
1[e] service connectors that are each configured to connect the computing system to a different third party system, each of the service connectors being configured as a separate module for integrating a corresponding external service to the computing system;	On information and belief, the PayPal System includes service connectors that are configured to connect the PayPal system to a different third-party system.  https://www.paypal.com/bs/webapps/mpp/shop/apps (last accessed on February 25, 2022). On information and belief, the PayPal system is also connected to third-party mobile wallet payment applictions. These systems integrate the additional mobile wallet services and features to the PayPal System.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	How can I add PayPal to Samsung Pay? **You can add PayPal to Samsung Pay through the Samsung Pay app. Simply, tap the PayPal (Add PayPal) icon, then Add your PayPal, then log in to your PayPal account. You will be able to select a top up amount and a backup funding instrument for the top up. At this time Samsung Pay is only available to US customers.** *See* https://www.paypal.com/us/webapps/mpp/samsung-pay (last accessed on February 25, 2022). How to add PayPal to Google Pay. 1 When you're ready to checkout in Google products click "add payment method" 2 Enter your PayPal information & accept the terms 3 You're all set! Use PayPal to checkout on Google Play, YouTube, & the Google Store  Add PayPal as a payment method in Google Pay https://www.paypal.com/us/webapps/mpp/google-pay-paypal (last accessed on February 25, 2022).

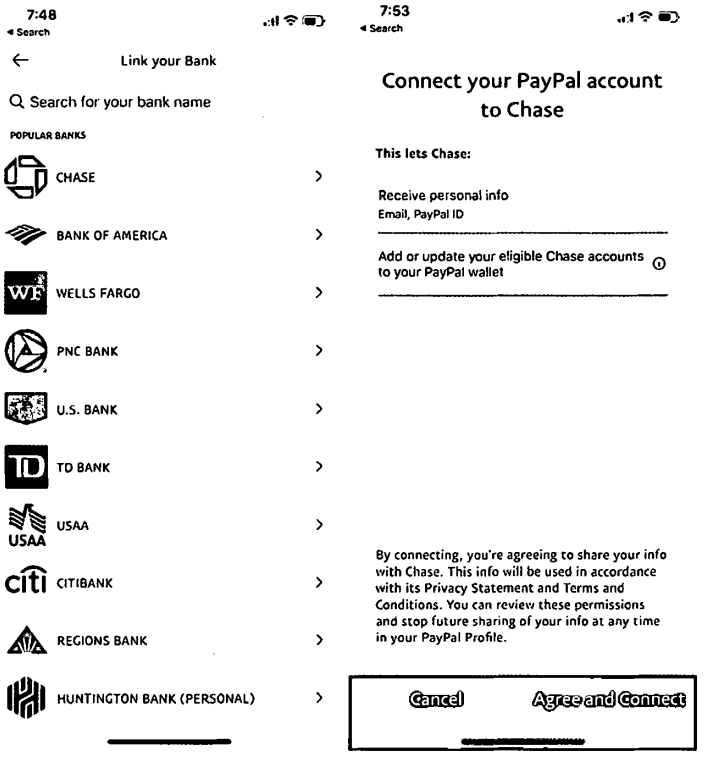
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 321 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
1[f] a payment handler that exposes a common API for interacting with different payment processors;	Upon information and belief, the PayPal System, includes a payment handler which exposes a common APIs for interacting with different payment processors. 

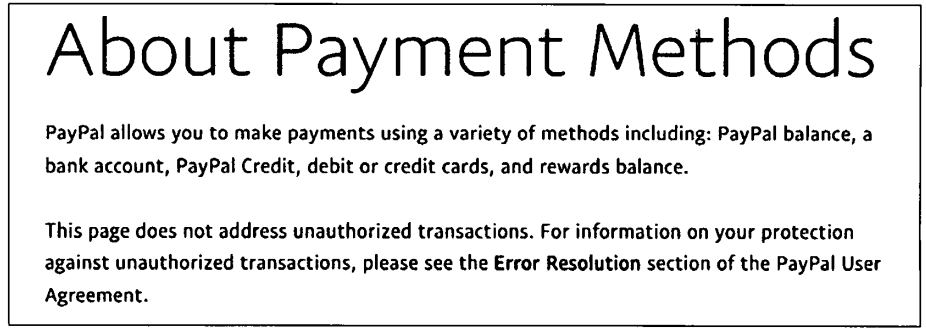
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 322 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* Screenshot of PayPal Mobile Application (above) allowing users to link credit card, bank accounts and other payment processors. *See* Screenshot of PayPal Mobile Application identifying bank account with option to add credit and debit cards.

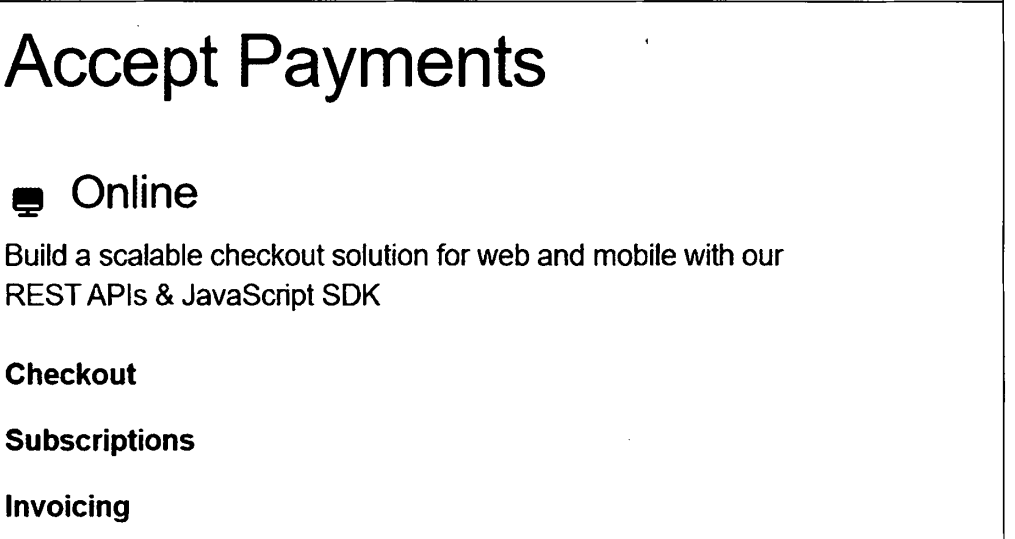
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 323 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	 *See* https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022). Upon information and belief, the PayPal System provides REST APIs for new integrations. These APIs use HTTP methods, a RESTful endpoint structure, the OAuth 2.0 protocol, and JSON-formatted payloads. The REST APIs can be used to incorporate the PayPal System's functionality into a user's web and mobile apps. Standard PayPal APIs can be accessed via the PayPal Developer Portal (*see* http://developer.paypal.com (last accessed on February 25, 2022)).

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 324 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	
1[g] a security services engine that performs subscriber authentication utilizing a database-based Access Control List (ACL);	Upon information and belief, the PayPal System also discloses a security service that authenticates a subscriber utilizing a database based Accused Control List (ACL). On information and belief, the authentication is performed based on user password authentication and/or based on authentication based on the mobile device.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	Why are limitations placed on an account? There can be several reasons for an account limitation: • *An unauthorized person may be using your account.* If PayPal believes someone is using your account without your knowledge, the account could be limited to protect you from fraudulent charges while PayPal investigates the suspicious transactions. Similar steps may be taken if your debit or credit card issuer or bank notifies PayPal that someone has used your card or bank account without permission. • *The account is out of compliance with regulatory requirements.* Limitations can also be placed on an account that has been found to be out of compliance with regulatory requirements. For example, if you receive donations, you're required to provide documents confirming you're a registered nonprofit organization. PayPal may limit your account while you gather those documents or while we're working with you to satisfy any other regulatory requirements. The same is true if you don't follow PayPal's **Acceptable Use Policy**—selling banned items, such as prescription drugs or guns, for example. • *Your account has a high number of claims and chargebacks.* When there's a high number of **buyer claims and chargebacks** to your account, we may review your account. While we're reviewing, you may experience an account limitation. • *Sudden, rapid changes in what or how much you sell.* If you start to sell an entirely new type of product, specifically higher-end items like jewelry; or there's a rapid increase in sales volume, your account may be limited while PayPal reviews it. *See* https://www.paypal.com/us/brc/article/understanding-account-limitations (last accessed on February 25, 2022). Upon information and belief, the PayPal System includes an access-control list (ACL) such as a list of permissions associated with system resources. A user can manually grant the PayPal System permissions to a third party to access specific information in the user's account at the PayPal system and perform PayPal API operations on the user's behalf. For example, if the user is integrating with a third-party shopping cart, the cart owner needs permission to the user's PayPal account to perform specific operations on behalf of the user. Upon information and belief, by way of example, the PayPal systems utilizes OAuth 2.0 protocol to provide authenticated and/or authorized access to various protected resources. In particular,

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 326 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	OAuth 2.0 scopes are used to specify or limit the type of access (i.e., ACL) that is associated with a granted access token. *See* https://oauth.net/2/scope/ (last accessed on February 25, 2022); https://developer.paypal.com/api/rest/ (last accessed on February 25, 2022).
1[h] a rules engine configured to enforce constraints on financial transactions performed with the mobile wallet application, the mobile wallet application being associated with a mobile wallet account; and	Upon information and belief, the PayPal System, includes a rule engine that track financial transactions where the mobile wallet application is associated with a mobile wallet account. **Why are limitations placed on an account?** There can be several reasons for an account limitation: • *An unauthorized person may be using your account.* If PayPal believes someone is using your account without your knowledge, the account could be limited to protect you from fraudulent charges while PayPal investigates the suspicious transactions. Similar steps may be taken if your debit or credit card issuer or bank notifies PayPal that someone has used your card or bank account without permission. • *The account is out of compliance with regulatory requirements.* Limitations can also be placed on an account that has been found to be out of compliance with regulatory requirements. For example, if you receive donations, you're required to provide documents confirming you're a registered nonprofit organization. PayPal may limit your account while you gather those documents or while we're working with you to satisfy any other regulatory requirements. The same is true if you don't follow PayPal's Acceptable Use Policy—selling banned items, such as prescription drugs or guns, for example. • *Your account has a high number of claims and chargebacks.* When there's a high number of buyer claims and chargebacks to your account, we may review your account. While we're reviewing, you may experience an account limitation. • *Sudden, rapid changes in what or how much you sell.* If you start to sell an entirely new type of product, specifically higher-end items like jewelry; or there's a rapid increase in sales volume, your account may be limited while PayPal reviews it. *See* https://www.paypal.com/us/brc/article/understanding-account-limitations (last accessed on February 25, 2022).

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 327 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
1[i] and [j] one or more computer-readable storage media having stored thereon computer-executable instructions that are executable by the one or more processors to cause the computing system to perform a transaction for a customer using the mobile wallet which is owned by another entity than the customer, comprising the following: the computing system receiving communication from an agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the agent communication indicating that a customer desires to perform a transaction comprising a mobile wallet transaction using a third party mobile wallet, the mobile wallet transaction comprising at least one of a mobile wallet transfer in which funds are transferred from the mobile wallet of the customer to a third party mobile wallet, a mobile wallet withdrawal in which funds are withdrawn from the third party	*See* Claim 1[e]. On information and belief, the PayPal System is capable of being connected to third-party mobile wallets to add additional Payment options and features. The PayPal System can be linked to another mobile wallet (*e.g.* Samsung Pay or Android Pay). On information and belief, the PayPal System linked with other mobile wallets can be used to make and initiate payments through the third-party mobile wallets. For example, a user can make payments through Samsung Pay at a grocery store store. The PayPal System includes one or more processers that will cause the computing system to perform a transaction for the customer using the Samsung Pay connected to the PayPal system. Upon information and belief, the third-party mobile wallet is owned by another entity than the customer (*e.g.* Samsung or Google). On information and belief, as a result of a transaction made by a user using a linked mobile wallet account through a cloud based transaction platform. On information and belief the funds in the PayPal System are facilitated through the third-party mobile wallet such as Samsung or Google Pay, for example through a NFC Payment. How can I add PayPal to Samsung Pay? **You can add PayPal to Samsung Pay through the Samsung Pay app. Simply, tap the PayPal (Add PayPal) icon, then Add your PayPal, then log in to your PayPal account. You will be able to select a top up amount and a backup funding instrument for the top up. At this time Samsung Pay is only available to US customers.** *See* https://www.paypal.com/us/webapps/mpp/samsung-pay (last accessed on Febraury 25, 2022).

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 328 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
mobile wallet and provided to the customer, or a mobile wallet deposit in which funds are deposited into the third party mobile wallet;	**Add or remove a PayPal account** You can add a PayPal account to Google Pay on an Android phone. You can use it in select countries to pay for some Google products and in participating stores, apps, and websites. **Add a PayPal account** 1. On your phone, open the Google Pay app. 2. At the top, tap the card button. 3. Tap Add a payment method. You might need to swipe all the way left to find this option. 4. Tap PayPal. 5. To link your PayPal account, follow the on-screen instructions. *See* https://support.google.com/googlepay/answer/10212164?hl=en (last accessed on February 25, 2022). PayPal recently migrated the horizontally scalable applications of its payment platform to Google Cloud—a significant shift in strategy to cloud-based transactions—to help ensure easy and reliable services for its customers. https://cloud.google.com/customers/paypal (last accessed on February 25, 2022).

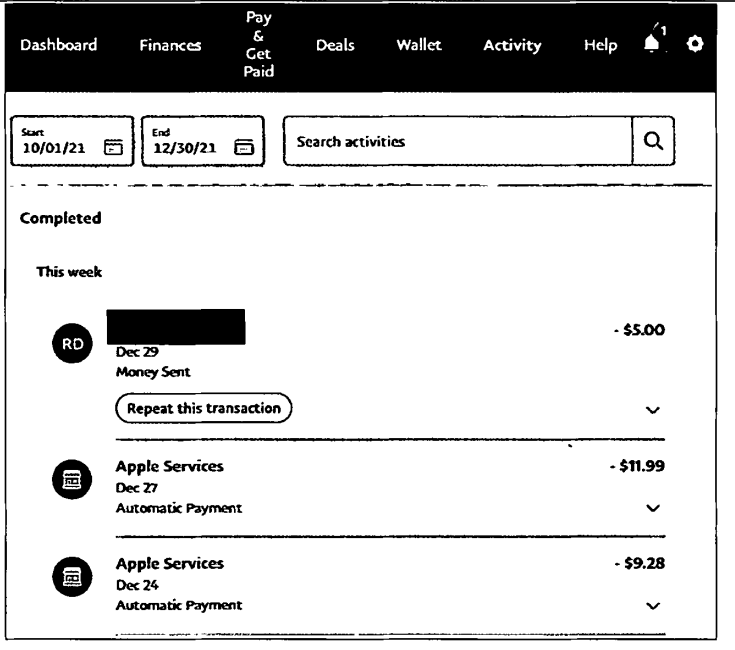
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 329 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
	6. Your Payment Obligation When you use PayPal in Google Pay for a transaction, i.e. give a payment order, you are obliged to reimburse the transaction amount to us. To this end, you authorize us to debit the respective amount from your PayPal balance. To the extent that there is no or an insufficient balance available to fund such transaction, you hereby authorize PayPal to draw the amount from your bank account via direct debit, to credit this amount in your PayPal balance and to use it immediately for the payment with PayPal in Google Pay. This means we will prioritize your PayPal balance for a payment with PayPal in Google Pay and only draw the amount from your bank account via direct debit to the extent that the balance is insufficient. https://www.paypal.com/de/webapps/mpp/ua/ppgooglepay-tnc?locale.x=en_DE#2 (last accessed on February 25, 2022).
1[k] the computing system sending the agent communication to the third party mobile wallet platform; the computing system determining whether the mobile wallet transaction comprises the mobile wallet withdrawal and when the mobile wallet transaction is determined to comprise the mobile wallet withdrawal, generating and providing a perishable withdrawal code to the consumer, which is presented to the agent terminal to	Upon information and belief, the PayPal System includes a computing system that sends agent communication to/from the third party mobile wallet platform (*e.g.* Samsung Pay and Google Pay). On information and belief when funds are withdrawn from the PayPal System a perishable withdraw code is generated and provided to the consumer. Upon information and belief, once a communication is received from the third-party mobile wallet platform confirming processing of the transaction a communication is received confirming the processing of the transaction.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 330 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 9,208,488 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal Application and Backend System ("PayPal System")**
facilitate processing of the mobile wallet withdrawal; the computing system receiving communication from the third party mobile wallet platform confirming processing of the transaction, the transaction comprising at least one of the mobile wallet transfer, the mobile wallet withdrawal or the mobile wallet deposit; and the computing system sending communication to the agent terminal over one of a plurality of communication channels connected to the cloud-based transaction platform, the communication indicating confirmation of the processing of the transaction.	 *See* Screenshot of PayPal system confirming Payment/processing of transaction. Upon information and belief, the PayPal System is able to use the mobile payment app to make touch-free purchases in stores using QR codes. When ready to pay, shoppers can open the PayPal app (or the merchant's app) on their mobile device and check in at the merchant's location such that to prompt the PayPal app (or the merchant's app) to send a unique QR code or a one-time four-digit code to authenticate the purchase. This exemplary payment method, for example, is perishable and will expire after a certain time if the transaction is not completed.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 331 of 381

Exhibit I
U.S. Patent No. 10,438,196

US010438196B2

(12) **United States Patent**
Liberty

(10) **Patent No.: US 10,438,196 B2**
(45) **Date of Patent: *Oct. 8, 2019**

(54) **USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS**

(71) Applicant: **Mozido, Inc.**, Austin, TX (US)

(72) Inventor: **Michael A. Liberty**, Orlando, FL (US)

(73) Assignee: **MOZIDO, INC.**, Austin, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 601 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/928,521**

(22) Filed: **Oct. 30, 2015**

(65) **Prior Publication Data**

US 2016/0055483 A1 Feb. 25, 2016

Related U.S. Application Data

(63) Continuation of application No. 13/680,824, filed on Nov. 19, 2012, now Pat. No. 9,208,488.
(Continued)

(51) **Int. Cl.**
G06Q 20/00 (2012.01)
G06Q 20/36 (2012.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G06Q 20/3674*** (2013.01); ***G06Q 20/065*** (2013.01); ***G06Q 20/202*** (2013.01); ***G06Q 20/36*** (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,717,374 A 2/1998 Smith
5,828,739 A 10/1998 Nakanishi
(Continued)

FOREIGN PATENT DOCUMENTS

CA 2666616 4/2008
CN 101606400 12/2009
(Continued)

OTHER PUBLICATIONS

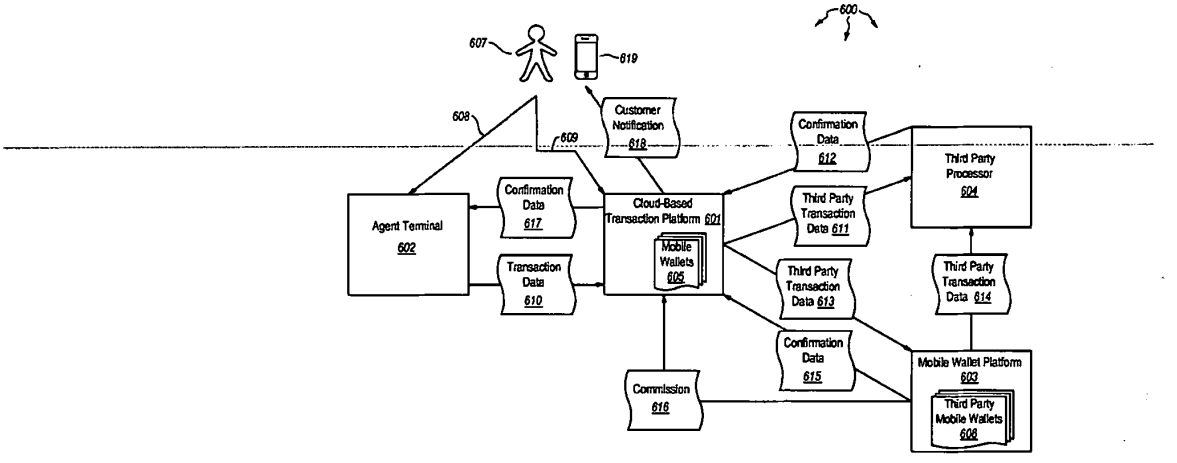
U.S. Appl. No. 14/928,105, filed Oct. 30, 2015, Liberty, Michael A.
(Continued)

Primary Examiner — Paul Danneman
(74) *Attorney, Agent, or Firm* — Workman Nydegger

(57) **ABSTRACT**

Embodiments are directed to performing a transaction using a third party mobile wallet, performing a transaction using a third party point of sale (POS) system and to making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. In one scenario, a cloud-based transaction platform is provided, which receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that a customer desires to perform a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the agent communication to a third party mobile wallet platform, receives communication from the third party mobile wallet platform confirming processing of the transaction, and sends communication to the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

22 Claims, 9 Drawing Sheets



Related U.S. Application Data

(60) Provisional application No. 61/562,301, filed on Nov. 21, 2011.

(51) **Int. Cl.**
G06Q 20/06 (2012.01)
G06Q 20/20 (2012.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,991,749 A 11/1999 Morrill
6,021,397 A 2/2000 Jones et al.
6,175,823 B1 1/2001 Van Dusen
6,185,545 B1 2/2001 Resnick
6,250,557 B1 6/2001 Forslund
6,415,156 B1 7/2002 Stadelmann
6,622,015 B1 9/2003 Himmel
6,697,839 B2 2/2004 Sini
6,714,797 B1 3/2004 Rautila
6,736,322 B2 5/2004 Gobburu
6,819,219 B1 11/2004 Bolle
6,840,448 B2 1/2005 Fukushima
6,862,575 B1 3/2005 Anttila et al.
6,873,974 B1 3/2005 Schutzer
6,957,342 B2 10/2005 Vatanen
7,016,532 B2 3/2006 Boncyk
7,024,174 B2 4/2006 Nagy
7,054,430 B2 5/2006 Lynam
7,069,001 B2 6/2006 Rupp
7,089,208 B1 8/2006 Levchin
7,099,850 B1 8/2006 Mann
7,100,821 B2 9/2006 Rasti
7,107,247 B2 9/2006 Kinoshita
7,110,972 B1 9/2006 Handa
7,221,939 B2 5/2007 Ylitalo
7,240,836 B2 7/2007 Vrotsos
7,248,855 B2 7/2007 Joyce
7,255,264 B2 8/2007 De Leon
7,275,685 B2 10/2007 Gray
7,322,043 B2 1/2008 Letsinger
7,325,132 B2 1/2008 Takayama
7,334,720 B2 2/2008 Hulst et al.
7,347,361 B2 3/2008 Lovett
7,349,871 B2 3/2008 Labrou
7,353,382 B2 4/2008 Labrou
7,363,261 B2 4/2008 Whitehead
7,370,017 B1 5/2008 Lindeman
7,403,652 B2 7/2008 Boncyk
7,421,410 B1 9/2008 Schechtman et al.
7,461,010 B2 12/2008 Kwan
7,461,028 B2 12/2008 Wronski
7,477,780 B2 1/2009 Boncyk
7,494,055 B2 2/2009 Fernandes
7,512,098 B2 3/2009 Jiang
7,527,194 B2 5/2009 Truitt
7,548,915 B2 6/2009 Ramer
7,562,818 B1 7/2009 Bierbaum
7,564,469 B2 7/2009 Boncyk
7,565,008 B2 7/2009 Boncyk
7,606,560 B2 10/2009 Labrou
7,657,489 B2 2/2010 Stambaugh
7,677,973 B2 3/2010 Van Luchene
7,680,324 B2 3/2010 Boncyk
7,689,506 B2 3/2010 Fei et al.
7,694,876 B2 4/2010 Barnes et al.
7,699,218 B2 4/2010 Garcia
7,708,194 B2 5/2010 Vawter
7,729,963 B1 6/2010 Lego
7,729,987 B1 6/2010 Wakim
7,748,618 B2 7/2010 Vawter
7,774,076 B2 8/2010 Skowronek
7,774,231 B2 8/2010 Pond
7,775,437 B2 8/2010 Boncyk
7,784,684 B2 8/2010 Labrou
7,801,826 B2 9/2010 Labrou
7,819,307 B2 10/2010 Lyons
7,822,688 B2 10/2010 Labrou
7,823,772 B2 11/2010 Vawter
7,848,500 B2 12/2010 Lynam
7,848,504 B2 12/2010 Lynam
7,865,414 B2 1/2011 Fung
7,865,431 B2 1/2011 Takayama
7,877,605 B2 1/2011 Labrou
7,881,529 B2 2/2011 Boncyk
7,886,962 B2 2/2011 Vawter
7,890,424 B1 2/2011 Wakim
7,899,243 B2 3/2011 Boncyk
7,899,252 B2 3/2011 Boncyk
7,937,302 B1 5/2011 Lego
7,937,305 B1 5/2011 Lego
7,942,317 B2 5/2011 Racz et al.
7,958,052 B2 6/2011 Powell
7,967,196 B1 6/2011 Bierbaum
7,979,026 B2 7/2011 Hulvey
7,988,060 B2 8/2011 Killian
8,016,185 B2 9/2011 Modi
8,019,365 B2 9/2011 Fisher
8,033,458 B2 10/2011 Hulst et al.
8,041,338 B2 10/2011 Chen
8,052,042 B2 11/2011 Kolinski-Schultz
8,060,012 B2 11/2011 Sklovsky
8,061,598 B2 11/2011 Racz et al.
8,073,783 B2 12/2011 Felsted
8,077,042 B2 12/2011 Peeters
8,090,945 B2 1/2012 Singhal
8,095,113 B2 1/2012 Kean
8,116,734 B2 2/2012 Vawter
8,116,773 B2 2/2012 Chitrapu
8,118,221 B2 2/2012 Racz et al.
8,121,945 B2 2/2012 Rackley
8,130,242 B2 3/2012 Boncyk
8,145,568 B2 3/2012 Rackley
8,160,959 B2 4/2012 Rackley
8,170,485 B2 5/2012 Hulvey
8,190,087 B2 5/2012 Fisher et al.
8,195,576 B1 6/2012 Grigg et al.
8,196,131 B1 6/2012 von Behren
8,213,470 B2 7/2012 Gu
8,218,873 B2 7/2012 Boncyk
8,229,354 B2 7/2012 Sklovsky
8,239,325 B2 8/2012 Schwarz
8,275,312 B2 9/2012 Fisher
8,290,433 B2 10/2012 Fisher
8,332,272 B2 12/2012 Fisher
8,333,319 B2 12/2012 Roth
8,336,772 B2 12/2012 Racz et al.
8,352,323 B2 1/2013 Fisher
8,355,670 B2 1/2013 White
8,359,265 B2 1/2013 Van Rensburg
8,360,329 B2 1/2013 Grigg
8,374,916 B2 2/2013 White
8,380,177 B2 2/2013 Laracey
8,396,793 B2 3/2013 Hill
8,487,771 B2 7/2013 Hsieh et al.
8,538,845 B2 9/2013 Liberty
8,577,803 B2 11/2013 Chatterjee et al.
8,612,325 B2 11/2013 Laracey
8,632,000 B2 1/2014 Laracey
9,208,488 B2 * 12/2015 Liberty G06Q 20/202
2001/0011248 A1 8/2001 Himmel
2001/0037264 A1 11/2001 Husemann
2001/0042785 A1 11/2001 Walker et al.
2002/0042776 A1 4/2002 Woo
2002/0052754 A1 5/2002 Joyce
2002/0060246 A1 5/2002 Gobburu
2002/0065774 A1 5/2002 Young
2002/0069123 A1 6/2002 Soderlind
2002/0131404 A1 9/2002 Mehta
2002/0141586 A1 10/2002 Margalit
2002/0152177 A1 10/2002 Wolf
2002/0161708 A1 10/2002 Offer
2003/0001010 A1 1/2003 Schmidt
2003/0026404 A1 2/2003 Joyce
2003/0055735 A1 3/2003 Cameron

(56) **References Cited**

U.S. PATENT DOCUMENTS

2003/0071115 A1 4/2003 Horn
2003/0154165 A1 8/2003 Horn
2003/0195842 A1 10/2003 Reece
2004/0117302 A1 6/2004 Weichert et al.
2004/0181531 A1 9/2004 Becker
2004/0205618 A1 10/2004 Sini
2004/0235450 A1 11/2004 Rosenberg
2004/0248554 A1 12/2004 Khan
2005/0070265 A1 3/2005 Korpinen
2005/0071512 A1 3/2005 Kim et al.
2005/0080697 A1 4/2005 Foss
2005/0199709 A1 9/2005 Linlor
2005/0222961 A1 10/2005 Staib
2005/0283434 A1 12/2005 Hahn-Carlson
2006/0116892 A1 6/2006 Grimes
2006/0136901 A1 6/2006 Nichols
2006/0165060 A1 7/2006 Dua
2006/0179452 A1 8/2006 Amodeo
2006/0200427 A1 9/2006 Morrison
2006/0253335 A1 11/2006 Keena et al.
2006/0287004 A1 12/2006 Fuqua
2007/0006327 A1 1/2007 Lal et al.
2007/0033285 A1 2/2007 Shiigi
2007/0106564 A1 5/2007 Matotek
2007/0123305 A1 5/2007 Chen
2007/0125838 A1 6/2007 Law
2007/0125840 A1 6/2007 Law
2007/0162471 A1 7/2007 Samuelsson
2007/0179885 A1 8/2007 Bird
2007/0198432 A1 8/2007 Pitroda
2007/0203850 A1 8/2007 Singh
2007/0241189 A1 10/2007 Slavin
2007/0244811 A1 10/2007 Tumminaro
2007/0255620 A1 11/2007 Tumminaro et al.
2007/0255652 A1 11/2007 Tumminaro et al.
2007/0255653 A1 11/2007 Tumminaro
2007/0265984 A1 11/2007 Santhana
2008/0006685 A1 1/2008 Rackley
2008/0010191 A1 1/2008 Rackley
2008/0010196 A1 1/2008 Rackley
2008/0010204 A1 1/2008 Rackley
2008/0010215 A1 1/2008 Rackley
2008/0011825 A1 1/2008 Giordano
2008/0017704 A1 1/2008 VanDeburg
2008/0040265 A1 2/2008 Rackley
2008/0040285 A1 2/2008 Wankmueller
2008/0052192 A1 2/2008 Fisher
2008/0065490 A1 3/2008 Novick et al.
2008/0097851 A1 4/2008 Bemmel
2008/0126145 A1 5/2008 Rackley
2008/0126929 A1 5/2008 Bykov
2008/0143487 A1 6/2008 Hulvey
2008/0197190 A1 8/2008 Fujita
2008/0204358 A1 8/2008 Sato
2008/0208743 A1 8/2008 Arthur
2008/0208744 A1 8/2008 Arthur
2008/0208762 A1 8/2008 Arthur
2008/0210751 A1 9/2008 Kim
2008/0249927 A1 10/2008 Rethorn
2008/0249928 A1 10/2008 Hill
2008/0249930 A1 10/2008 Hill
2008/0249933 A1 10/2008 Rethorn
2008/0255947 A1 10/2008 Friedman
2008/0275779 A1 11/2008 Lakshminarayanan
2008/0281737 A1 11/2008 Fajardo
2009/0024526 A1 1/2009 Erickson
2009/0037326 A1 2/2009 Chitti
2009/0055322 A1 2/2009 Bykov
2009/0063312 A1 3/2009 Hurst
2009/0081989 A1 3/2009 Wuhrer
2009/0098854 A1 4/2009 Park
2009/0104888 A1 4/2009 Cox
2009/0106148 A1 4/2009 Prada
2009/0108015 A1 4/2009 Kreamer
2009/0119190 A1 5/2009 Realini
2009/0132362 A1 5/2009 Fisher
2009/0132392 A1 5/2009 Davis
2009/0138366 A1 5/2009 Bemmel
2009/0144161 A1 6/2009 Fisher
2009/0156190 A1 6/2009 Fisher
2009/0157546 A1 6/2009 Garcia
2009/0177578 A1 7/2009 Garcia
2009/0177581 A1 7/2009 Garcia
2009/0210308 A1 8/2009 Toomer
2009/0222353 A1 9/2009 Guest
2009/0222358 A1 9/2009 Bednarek
2009/0234751 A1 9/2009 Chan et al.
2009/0248537 A1 10/2009 Sarkeshik
2009/0254440 A1 10/2009 Pharris
2009/0254479 A1 10/2009 Pharris
2009/0265272 A1 10/2009 Dill et al.
2009/0281904 A1 11/2009 Pharris
2009/0288012 A1 11/2009 Hertel
2009/0299844 A1 12/2009 Reilly
2009/0307132 A1 12/2009 Phillips
2010/0010964 A1 1/2010 Skowronek
2010/0023449 A1 1/2010 Skowronek
2010/0030651 A1 2/2010 Matotek et al.
2010/0044430 A1 2/2010 Song
2010/0048226 A1 2/2010 Owen
2010/0049599 A1 2/2010 Owen
2010/0051685 A1 3/2010 Royyuru
2010/0057614 A1 3/2010 Rainey
2010/0057619 A1 3/2010 Weller
2010/0057624 A1 3/2010 Hurt
2010/0063895 A1 3/2010 Dominguez
2010/0088188 A1 4/2010 Kumar
2010/0114739 A1 5/2010 Johnston
2010/0125495 A1 5/2010 Smith
2010/0125510 A1 5/2010 Smith
2010/0146607 A1 6/2010 Piepenbrink et al.
2010/0151790 A1 6/2010 Hoeksel et al.
2010/0197326 A1 8/2010 Ngo
2010/0223110 A1 9/2010 Slavin
2010/0235283 A1 9/2010 Gerson
2010/0248710 A1 9/2010 Sklovsky
2010/0250356 A1 9/2010 Gillenson
2010/0250436 A1 9/2010 Loevenguth
2010/0260388 A1 10/2010 Garrett
2010/0333129 A1 12/2010 Alhadeff et al.
2011/0047016 A1 2/2011 Cook
2011/0057025 A1 3/2011 Denzer
2011/0087529 A1 4/2011 Angell
2011/0087610 A1 4/2011 Batada
2011/0105022 A1 5/2011 Vawter
2011/0113473 A1 5/2011 Corda
2011/0131421 A1 6/2011 Jogand-Coulomb et al.
2011/0145049 A1 6/2011 Hertel
2011/0145149 A1 6/2011 Valdes
2011/0179113 A1 7/2011 Thomas
2011/0196788 A1 8/2011 Lu et al.
2011/0218911 A1 9/2011 Spodak
2011/0246284 A1 10/2011 Chaikin
2011/0250866 A1 10/2011 Fisher
2011/0251941 A1 10/2011 Dunwoody
2011/0258024 A1 10/2011 Prince
2011/0258115 A1 10/2011 Mulhim
2011/0276417 A1 11/2011 Campbell
2011/0295750 A1 12/2011 Rammal
2011/0302016 A1 12/2011 Haddad
2011/0302406 A1 12/2011 Machani
2011/0313924 A1 12/2011 Carell
2011/0320243 A1 12/2011 Khan
2011/0320293 A1 12/2011 Khan
2011/0320294 A1 12/2011 Votaw
2011/0320345 A1 12/2011 Taveau
2012/0005076 A1 1/2012 Dessert
2012/0011058 A1 1/2012 Pitroda et al.
2012/0011063 A1 1/2012 Killian
2012/0028612 A1 2/2012 Hurst
2012/0029990 A1 2/2012 Fisher
2012/0047070 A1 2/2012 Pharris
2012/0074232 A1 3/2012 Spodak
2012/0078735 A1 3/2012 Bauer

(56) **References Cited**

U.S. PATENT DOCUMENTS

2012/0079521 A1 3/2012 Garg et al.
2012/0084203 A1 4/2012 Mehew
2012/0095855 A1 4/2012 Sterling
2012/0095856 A1 4/2012 Sanjeev
2012/0122447 A1 5/2012 Craft
2012/0123841 A1 5/2012 Taveau
2012/0123868 A1 5/2012 Brudnicki
2012/0123880 A1 5/2012 Craft
2012/0123935 A1 5/2012 Brudnicki
2012/0123937 A1 5/2012 Spodak
2012/0131653 A1 5/2012 Pasquero
2012/0143752 A1 6/2012 Wong
2012/0150669 A1 6/2012 Langley
2012/0158589 A1 6/2012 Katzin
2012/0166311 A1 6/2012 Dwight
2012/0171992 A1 7/2012 Cheong
2012/0172026 A1 7/2012 Kwon
2012/0172089 A1 7/2012 Bae
2012/0174189 A1 7/2012 Lim
2012/0191557 A1 7/2012 Fisher
2012/0191612 A1 7/2012 Spodak
2012/0196586 A1 8/2012 Grigg
2012/0197691 A1 8/2012 Grigg
2012/0197740 A1 8/2012 Grigg
2012/0197743 A1 8/2012 Grigg
2012/0197745 A1 8/2012 Fisher
2012/0197787 A1 8/2012 Grigg
2012/0203610 A1 8/2012 Grigg et al.
2012/0203632 A1 8/2012 Blum
2012/0209688 A1 8/2012 Lamothe
2012/0209749 A1 8/2012 Hammad
2012/0215701 A1 8/2012 Mehta
2012/0221421 A1 8/2012 Hammad
2012/0221475 A1 8/2012 Grigg
2012/0226610 A1 9/2012 Gill
2012/0229647 A1 9/2012 Calman
2012/0229657 A1 9/2012 Calman
2012/0231424 A1 9/2012 Calman
2012/0231425 A1 9/2012 Calman
2012/0232937 A1 9/2012 Calman
2012/0232977 A1 9/2012 Calman
2012/0232983 A1 9/2012 Bertha
2012/0245986 A1 9/2012 Regan
2012/0253852 A1 10/2012 Pourfallah
2012/0259598 A1 10/2012 Yurrow
2012/0259686 A1 10/2012 Yurow
2012/0259732 A1 10/2012 Sasankan
2012/0265677 A1 10/2012 Rackley
2012/0265685 A1 10/2012 Brudnicki
2012/0271712 A1 10/2012 Katzin
2012/0284131 A1 11/2012 Soffer
2012/0286928 A1 11/2012 Mullen
2012/0290376 A1 11/2012 Dryer
2012/0290449 A1 11/2012 Mullen
2012/0290478 A1 11/2012 Crofts et al.
2012/0293303 A1 11/2012 Khan
2012/0296708 A1 11/2012 Bachmann
2012/0296720 A1 11/2012 Pirillo
2012/0296722 A1 11/2012 Gosavi
2012/0296741 A1 11/2012 Dykes
2012/0297204 A1 11/2012 Buer
2012/0302204 A1 11/2012 Gupta
2012/0303425 A1 11/2012 Katzin
2012/0310720 A1 12/2012 Balsan
2012/0310760 A1 12/2012 Phillips
2012/0310824 A1 12/2012 Liberty
2012/0310826 A1 12/2012 Chatterjee
2012/0316950 A1 12/2012 LaPorte
2012/0316951 A1 12/2012 Fisher
2012/0316992 A1 12/2012 Oborne
2012/0317019 A1 12/2012 Carnes
2012/0323653 A1 12/2012 Fisher
2012/0323664 A1 12/2012 Klems
2012/0323670 A1 12/2012 Fisher
2012/0323777 A1 12/2012 Liberty
2012/0329394 A1 12/2012 Fisher
2012/0330737 A1 12/2012 Liberty
2012/0330792 A1 12/2012 Kashanian
2013/0012125 A1 1/2013 Fisher
2013/0012126 A1 1/2013 Fisher
2013/0012131 A1 1/2013 Fisher
2013/0013352 A1 1/2013 Fisher
2013/0013353 A1 1/2013 Fisher
2013/0013355 A1 1/2013 Fisher
2013/0013432 A1 1/2013 Fisher
2013/0013434 A1 1/2013 Fisher
2013/0013490 A1 1/2013 Keller
2013/0013498 A1 1/2013 Fisher
2013/0013501 A1 1/2013 Rackley
2013/0017784 A1 1/2013 Fisher
2013/0018738 A1 1/2013 Faires
2013/0018740 A1 1/2013 Fisher
2013/0018742 A1 1/2013 Fisher
2013/0018793 A1 1/2013 Wong
2013/0023209 A1 1/2013 Fisher
2013/0023294 A1 1/2013 Singh
2013/0024220 A1 1/2013 Fisher
2013/0024221 A1 1/2013 Fisher
2013/0024223 A1 1/2013 Thomas
2013/0024280 A1 1/2013 Fisher
2013/0024364 A1 1/2013 Fisher
2013/0024371 A1 1/2013 Hariramani
2013/0024372 A1 1/2013 Spodak
2013/0024377 A1 1/2013 Stong
2013/0029646 A1 1/2013 Chowdhury
2013/0030828 A1 1/2013 Pourfallah
2013/0030960 A1 1/2013 Kashanian
2013/0030997 A1 1/2013 Spodak
2013/0035035 A1 2/2013 Fisher
2013/0035036 A1 2/2013 Fisher
2013/0035037 A1 2/2013 Fisher
2013/0035068 A1 2/2013 Fisher
2013/0035069 A1 2/2013 Fisher
2013/0035070 A1 2/2013 Fisher
2013/0035071 A1 2/2013 Fisher
2013/0035072 A1 2/2013 Fisher
2013/0035087 A1 2/2013 Fisher
2013/0035967 A1 2/2013 Fisher
2013/0035968 A1 2/2013 Fisher
2013/0035969 A1 2/2013 Fisher
2013/0035970 A1 2/2013 Fisher
2013/0040568 A1 2/2013 Fisher
2013/0040569 A1 2/2013 Fisher
2013/0041699 A1 2/2013 Fisher
2013/0041700 A1 2/2013 Fisher
2013/0041701 A1 2/2013 Roth
2013/0041736 A1 2/2013 Coppinger
2013/0041743 A1 2/2013 Coppinger
2013/0041744 A1 2/2013 Coppinger
2013/0041745 A1 2/2013 Coppinger
2013/0041769 A1 2/2013 Fisher
2013/0046608 A1 2/2013 Coppinger
2013/0046634 A1 2/2013 Grigg
2013/0046645 A1 2/2013 Grigg
2013/0048723 A1 2/2013 King
2013/0052952 A1 2/2013 Fisher
2013/0054336 A1 2/2013 Graylin
2013/0054337 A1 2/2013 Brendell
2013/0054412 A1 2/2013 Brendell
2013/0054441 A1 2/2013 Kamdar
2013/0057392 A1 3/2013 Bullock
2013/0060618 A1 3/2013 Barton
2013/0073373 A1 3/2013 Fisher
2013/0073377 A1 3/2013 Heath
2013/0073458 A1 3/2013 Sherwin
2013/0080228 A1 3/2013 Fisher
2013/0080229 A1 3/2013 Fisher
2013/0080230 A1 3/2013 Fisher
2013/0080231 A1 3/2013 Fisher
2013/0080232 A1 3/2013 Fisher
2013/0080233 A1 3/2013 Fisher
2013/0080240 A1 3/2013 Fisher
2013/0080241 A1 3/2013 Fisher
2013/0080329 A1 3/2013 Royyuru

(56) **References Cited**

U.S. PATENT DOCUMENTS

2013/0091012	A1	4/2013	Liberty
2013/0246141	A1	4/2013	Liberty
2013/0132219	A1	5/2013	Liberty
2013/0238455	A1	9/2013	Laracey
2013/0246203	A1	9/2013	Laracey
2013/0013499	A1	10/2013	Kalgi
2013/0317928	A1	11/2013	Laracey
2013/0332347	A1	12/2013	Liberty
2013/0346309	A1	12/2013	Giori
2014/0006048	A1	1/2014	Liberty
2014/0014721	A1	1/2014	Lindeman
2014/0201070	A1	7/2014	Liberty
2015/0039517	A1	2/2015	Liberty
2016/0055483	A1	2/2016	Liberty
2016/0314443	A1	10/2016	Liberty

FOREIGN PATENT DOCUMENTS

CN	102073958	5/2011
DE	10119808	9/2002
EP	1280115	1/2003
EP	2284783	2/2011
JP	2001-297198	10/2001
JP	2001357164	12/2001
JP	2002-99716	4/2002
KR	10-2002-0065989	8/2002
KR	10-2003-0068603	8/2003
KR	10-2007-0092400	9/2007
WO	199834203	8/1998
WO	9913636	3/1999
WO	0171627	9/2001
WO	2001097118	12/2001
WO	2002071354	9/2002
WO	2003012717	2/2003
WO	2004010393	1/2004
WO	2004023353	3/2004
WO	2004053640	6/2004
WO	2004088641	10/2004
WO	2005079254	9/2005
WO	2005086593	9/2005
WO	2007145500	12/2007
WO	2008008735	1/2008
WO	2012025824	3/2012
WO	2013009444	1/2013
WO	2013009446	1/2013
WO	2013025273	2/2013
WO	2013078176	5/2013
WO	2013166174	11/2013

OTHER PUBLICATIONS

Chen, Jiajun Jim et al, Short-Range Wireless Technologies with Mobile Payments Systems. Proceedings of the 6th International Conference on Electronic Commerce [Online] 2004, pp. 649-656.

Clarke, Irvine III, "Emerging Value Propositions for M-commerce," *Journal of Business Strategies*, vol. 25, Issue 2, Fall 2008, p. 41-57, ISSN: 0887-2058.

Edwin, et al., "Technobiography," Oct. 2004, 29 pages.

European Search Report for EP12824344 dated Sep. 29, 2014.

Gao, Jerry, et al., "P2P-Paid: A Peer-to-Peer Wireless Payment System," Proceedings of the 2005 Second IEEE International Workshop on Mobile Commerce and Services (WMCS'05) Jul. 2005, 10 pages.

International Search Report and Written Opinion for PCT/US2012/066013 dated Jan. 29, 2013.

International Search Report and Written Opinion for PCT/US2012/040131 dated Jan. 29, 2013.

International Search Report and Written Opinion for PCT/US2012/043321 dated Sep. 6, 2012.

International Search Report and Written Opinion for PCT/US2012/058849 dated Jan. 4, 2013.

International Search Report and Written Opinion for PCT/US2012/43458 dated Aug. 17, 2012.

International Search Report and Written Opinion for PCT/US2013/039100 dated Aug. 23, 2013.

Labrou, Yannis et al, Wireless Wallet. Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services [Online] 2004, pp. 1-10.

Motorola, Motorola M-Wallet Solution. [Online] 2006 http://www.motorola.com/networkoperators/pdfs/M-Wallet-Brochure.pdf (Accessed Oct. 4, 2012).

Sykes, et al. "Securing Mobile Banking," Credit Union Management, Nov. 2010, vol. 33 No. 11; ISSN 0273-9267.

Valcourt, E. et al., "Investigating Mobile Payment," Wireless and Mobile Computing, Networking and Communications, 2005. (WiMob'2005), IEEE International Conference on Aug. 22-24, 2005, Aug. 2005, vol. 4, pp. 29-36.

Wei, et al., "Development of a Web-Based Mobile Airline Ticketing Model with Usability Features," 2005, Industrial Management + Data Systems; vol. 105 No. 9, ISSN: 0263-5577.

U.S. Appl. No. 13/484,199, Dec. 26, 2012, Office Action.

U.S. Appl. No. 13/484,199, Jun. 7, 2013, Notice of Allowance.

U.S. Appl. No. 13/527,466, Apr. 15, 2013, Office Action.

U.S. Appl. No. 13/527,466, Dec. 4, 2013, Final Office Action.

U.S. Appl. No. 13/964,707, Feb. 24, 2014, Office Action.

U.S. Appl. No. 14/213,543, May 6, 2014, Office Action.

U.S. Appl. No. 13/680,824, Jun. 16, 2014, Office Action.

U.S. Appl. No. 13/528,720, Jun. 25, 2014, Office Action.

U.S. Appl. No. 13/964,707, Jul. 10, 2014, Office Action.

U.S. Appl. No. 13/527,466, Aug. 1, 2014, Office Action.

U.S. Appl. No. 14/012,822, Aug. 7, 2014, Office Action.

U.S. Appl. No. 13/528,720, Dec. 10, 2014, Final Office Action.

U.S. Appl. No. 14/012,822, Jan. 7, 2015, Final Office Action.

U.S. Appl. No. 13/680,824, Feb. 6, 2015, Final Office Action.

U.S. Appl. No. 13/964,707, Mar. 16, 2015, Final Office Action.

U.S. Appl. No. 14/213,543, Apr. 8, 2015, Office Action.

U.S. Appl. No. 13/874,192, Jul. 14, 2015, Office Action.

U.S. Appl. No. 13/527,466, Jul. 16, 2015, Office Action.

U.S. Appl. No. 13/528,720, Jul. 22, 2015, Office Action.

U.S. Appl. No. 14/012,822, Sep. 11, 2015, Office Action.

U.S. Appl. No. 13/680,824, Sep. 18, 2015, Notice of Allowance.

U.S. Appl. No. 14/213,543, Jan. 6, 2016, Final Office Action.

U.S. Appl. No. 15/201,152, Aug. 8, 2017, Notice of Allowance.

U.S. Appl. No. 13/527,466, Aug. 9, 2017, Office Action.

U.S. Appl. No. 13/874,192, Apr. 18, 2016, Final Office Action.

International Search Report and Written Opinion for PCT/US2015/58886 dated Feb. 4, 2016.

European Search Report for EP12851211 dated Feb. 18, 2016.

U.S. Appl. No. 13/528,720, Mar. 2, 2016, Final Office Action.

U.S. Appl. No. 14/012,822, May 6, 2016, Final Office Action.

U.S. Appl. No. 15/201,152, Oct. 25, 2016, Office Action.

U.S. Appl. No. 15/201,152, Jun. 15, 2017, Final Office Action.

U.S. Appl. No. 13/527,466, Dec. 14, 2016, Office Action.

Ron White, How Computers Work, Oct. 15, 2003, Paul Boger, Illustrated by Timothy Edward Dwons, 7th Edition (Year: 2003).

U.S. Appl. No. 14/341,605, Nov. 27, 2017, Office Action.

U.S. Appl. No. 13/527,466, Apr. 1, 2016, Office Action.

U.S. Appl. No. 15/809,872, filed Nov. 10, 2017, Liberty, Michael A.

U.S. Appl. No. 61/493,064, filed Jun. 3, 2011, Liberty, Michael A.

U.S. Appl. No. 61/522,099, filed Aug. 10, 2011, Liberty, Michael A.

U.S. Appl. No. 62/075,657, filed Nov. 5, 2014, Liberty, Michael A.

U.S. Appl. No. 61/498,957, filed Jun. 20, 2011, Liberty, Michael A.

U.S. Appl. No. 61/499,927, filed Jun. 22, 2011, Liberty, Michael A.

U.S. Appl. No. 61/562,301, filed Nov. 21, 2011, Liberty, Michael A.

U.S. Appl. No. 61/694,118, filed Aug. 28, 2012, Liberty, Michael A.

U.S. Appl. No. 61/641,677, filed May 2, 2012, Liberty, Michael A.

U.S. Appl. No. 61/862,437, filed Aug. 5, 2012, Liberty, Michael A.

U.S. Appl. No. 14/928,105, Aug. 27, 2018, Office Action.

Medhi et al., "Mobile-banking adoption and usage by low-literate, low-income users in the developing world", 2009, N. Aykin (Ed.): Internationalization, Design, LNCS 5623, pp. 485-486.

Mbogo, "The impact of mobile payments on the success and growth of micro-business: the case of M-Pesa in Kenya", The Journal of

(56) **References Cited**

OTHER PUBLICATIONS

Language, Technology & Entrepreneurship in Africa, vol. 2, No. 1, 2010, ISSN 1998-1279, pp. 182-203.

Jack et al., "Monetary Theory and electronic money: reflections on the Kenyan experience", economic quarterly, vol. 96, No. 1, first quarter 2010, pp. 83-122.

Comninos et al., "M-banking the unbanked", towards evidence-based ICT policy and regulation, vol. 1, 2008, policy paper 4, pp. 1-15.

Lonie, "M-PESA: finding new ways to serve the unbanked in Kenya", innovations in rural and agricultural finance, Jul. 2010, focus 18, brief 8, pp. 1-3.

Plyler et al., "Community level economic effects of M-PESA in Kenya: initial findings (executive summary)", financial services assessment, IRIS center, university of maryland college park, Mar. 30, 2010, pp. 1-4, accessible at <http://www.fsassessment.umd.edu/>.

Hughes et al., "M-PESA: mobile money for the 'unbanked' turning cellphones into 24-hour tellers in Kenya", winter & spring 2007, innovations, pp. 63-81.

Omwansa, "M-PESA: Progress and prospects", innovations case discussion: M-PESA, 2009, innovations, mobile world congress, pp. 107-123.

Mas et al., "Designing mobile money services—lessons from M-PESA", innovations, spring 2009, pp. 77-91.

Porteous, "Just how transformational is m-banking?", commissioned by FinMark Trust, bankable frontier associates LLC, Feb. 2007, pp. 1-32.

Morawczynski et al., "Poor people using mobile financial services: observations on customer usage impact from M-PESA", CGAP, Aug. 2009, pp. 1-4.

Jack et al., "The economics of M-PESA", Aug. 2010, commissioned by the Centre Bank of Kenya, managed by Financial Sector Deepening, administered by the Steadman Group, pp. 1-20.

"RadioShack and Trumpet Mobile launch prepaid mobile phone service nationwide with unique mobile money transfer capabilities", Apr. 1, 2008, Source: Trumpet Mobile, pp. 1-3.

Sultana, "Mobile banking: overview of regulatory framework in emerging markets", Grameenphone Ltd, Celebration Point, Bangladesh, electronic copy available at <http://ssrn.com/abstract=1554160>, pp. 1-17.

Ivatury et al., "The early experience with branchless banking", CGAP, No. 46, Apr. 2008, electronic copy available at <http://ssrn.com/abstract=1655257> pp. 1-16.

Porteous, "The enabling environment for mobile banking in Africa", version 3.1, report commissioned by Department for International Development (DFID), Bankable Frontier Associates, May 2006, pp. 1-57.

Jack et al., "Mobile money: the economics of M-PESA", working paper 16721, National Bureau of Economic Research (NBER) working paper series, Jan. 2011, accessible at <http://www.nber.org/papers/w16721>, pp. 1-30.

Rice, "Kenya sets world first with money transfers by mobile", The Guardian, Mar. 20, 2007, pp. 1-3, accessed via <https://www.theguardian.com/money/2007/mar/20/kenya.mobilephones> on Mar. 25, 2019.

PYMNTS, "Mobile payments go viral: M-PESA in Kenya", Aug. 4, 2010, Business Wire, from 'Yes Africa can: success stories from a dynamic continent, world bank'—May 2010, pp. 1-30, accessed via <https://www.pymnts.com/business-wire/2010/mobile-payments-go-viral-m-pesa-in-kenya/> on Mar. 25, 2019.

Youtube video, "M-PESA: send money home tv commercial", accessed via <https://www.youtube.com/watch?v=nEZ30K5dBWU> on Mar. 25, 2019.

Graham, "M-PESA: Kenya's mobile wallet revolution", technology of business reporter, BBC news, Nov. 22, 2010, pp. 1-18, accessed via <https://www.bbc.com/news/business-11793290> on Mar. 25, 2019.

Starita, "Mobile cash transfers pose threat to banks", Feb. 26, 2009, News & Commentary, Philanthropy Action, pp. 1-4, accessed via <philanthropyaction.com/nc/mobile_cash_transfers_pose_threat_to_banks/> on Mar. 25, 2019.

Anonymous Staff Writer, "Portuguese firm flourishing in Mozambique", Africa Business Insight, How We Made It in Africa, pp. 1-2, accessed via <https://howwemadeitinafrica.com/portuguese-firm-flourishing-in-mozambique/3599/> on Mar. 25, 2019.

Njihia, "What you dont now about Mpesa . . . ", The Mind of Mbugua Njihia, Jul. 15, 2009, adapted from an article by Olga Morawczynski from CGAP dated Jul. 14, 2009, pp. 1-3, accessed via <www.mbuguanjihia.com/business/what-you-dont-now-about-mpesa.html> on Mar. 25, 2019.

McKinley, "Trumpet Mobile Wallet Takes-Off", May 6, 2008, CardFlash, pp. 1-5, accessed via <https://cardweb.com/news/2008/05/trumpet-mobile-wallet-takes-off> on Mar. 25, 2019.

Anonymous, "Radioshack, Trumpet launch prepaid mobile money", Apr. 1, 2008, FierceWireless, pp. 1-3, accessed via <https://www.fiercewireless.com/wirelessiradioshack-trumpet-launch-prepaid-mobile-money> on Mar. 25, 2019.

Anonymous, "RadioShack to offer Trumpet Mobile service—plan includes mobile money transfer capabilities", Apr. 1, 2008, The Prepaid Press—Where Prepaid Converges, pp. 1-2, accessed via <www.prepaidpress.com/features/radioshack-to-offer-trumpet-moblie-service.html> on Mar. 25, 2019.

Lugmayr, "RadioShack and Trumpet Mobile launch prepaid mobile phone service", posted Apr. 1, 2008, updated Aug. 11, 2010, I4U News, pp. 1-5, accessed via <https://www.i4u.com/19814/radioshack-and-trumpet-mobile-launch-prepaid-mobile-phone-service> on Mar. 25, 2019.

U.S. Appl. No. 14/928,105, Mar. 7, 2019, Final Office Action.

* cited by examiner

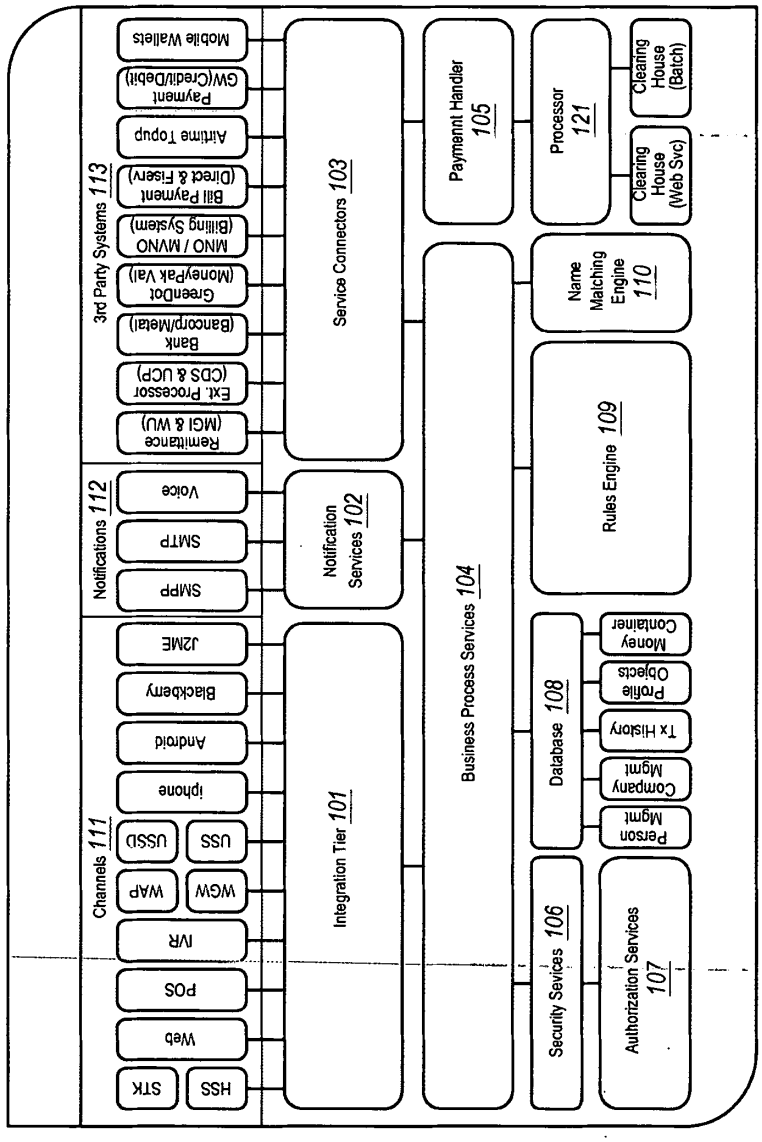


FIG. 1

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 339 of 381

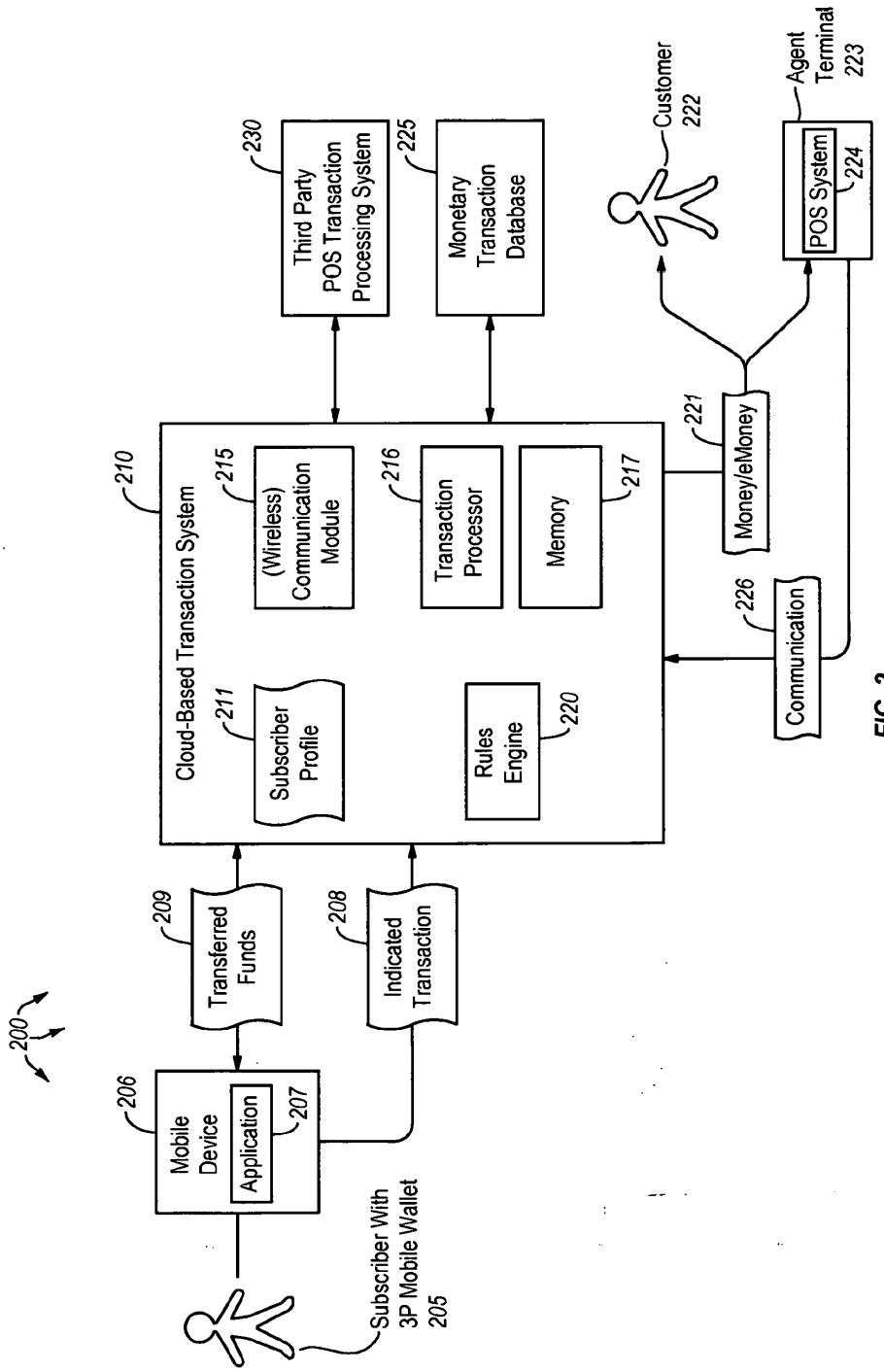


FIG. 2

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 340 of 381

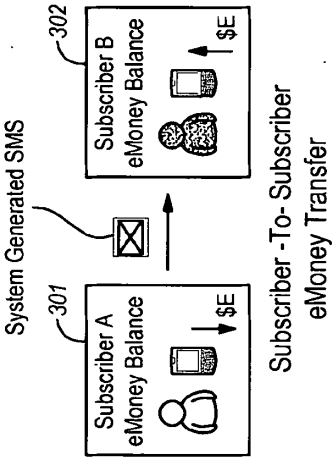


FIG. 3A

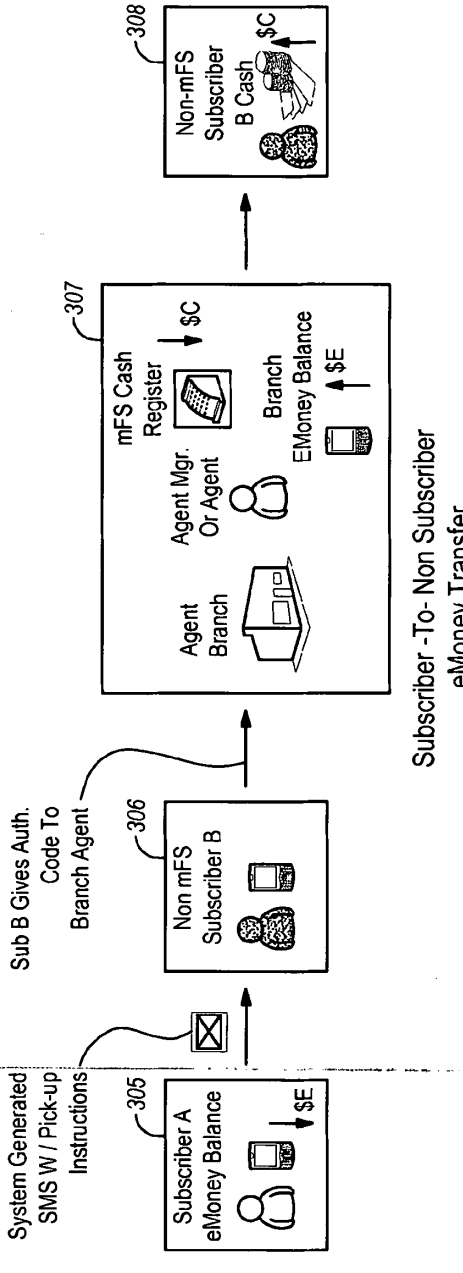
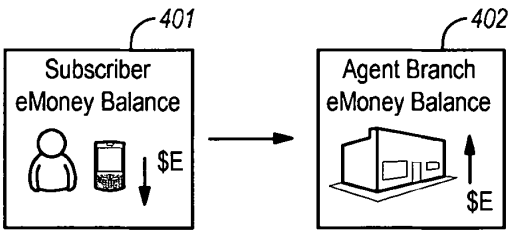


FIG. 3B

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 341 of 381



Subscriber Makes Retail Purchase

FIG. 4

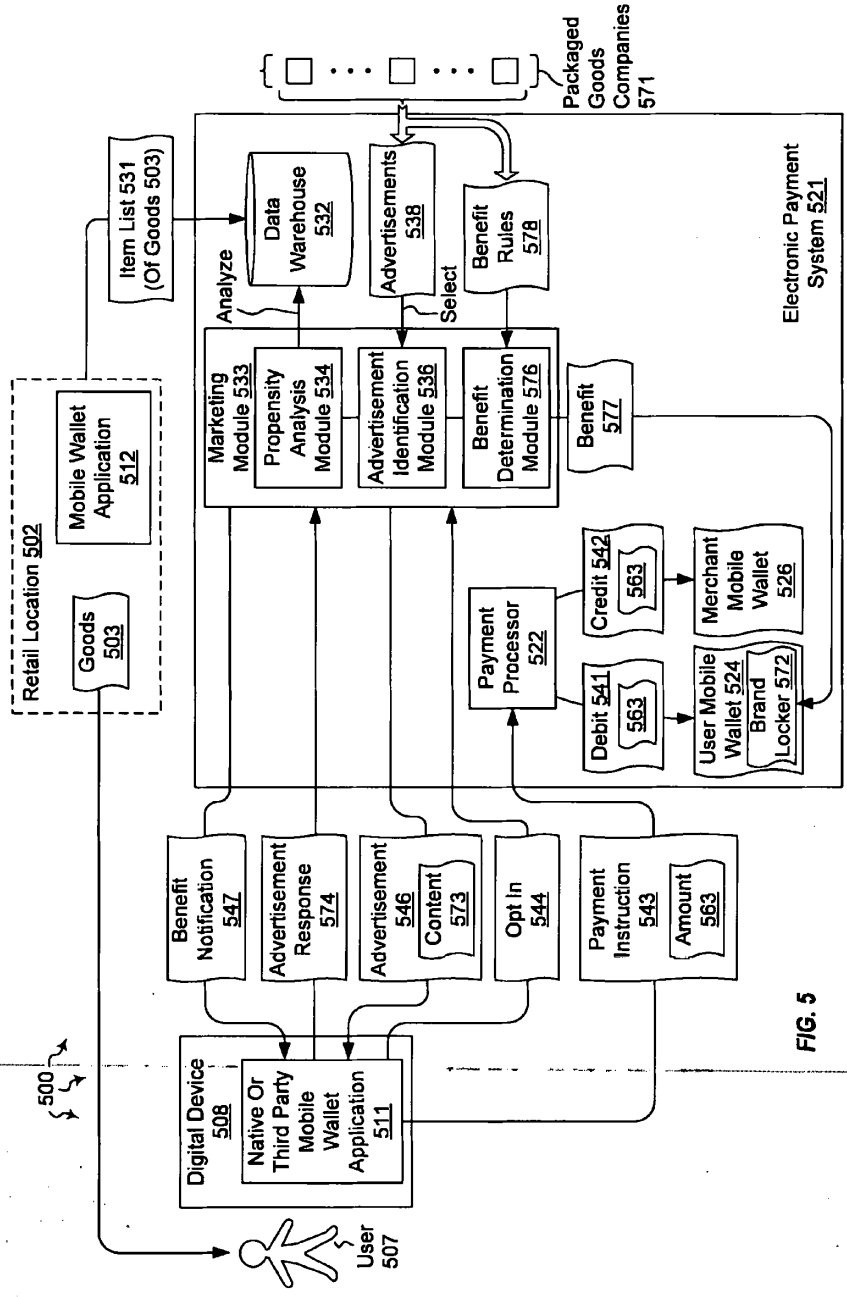


FIG. 5

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 343 of 381

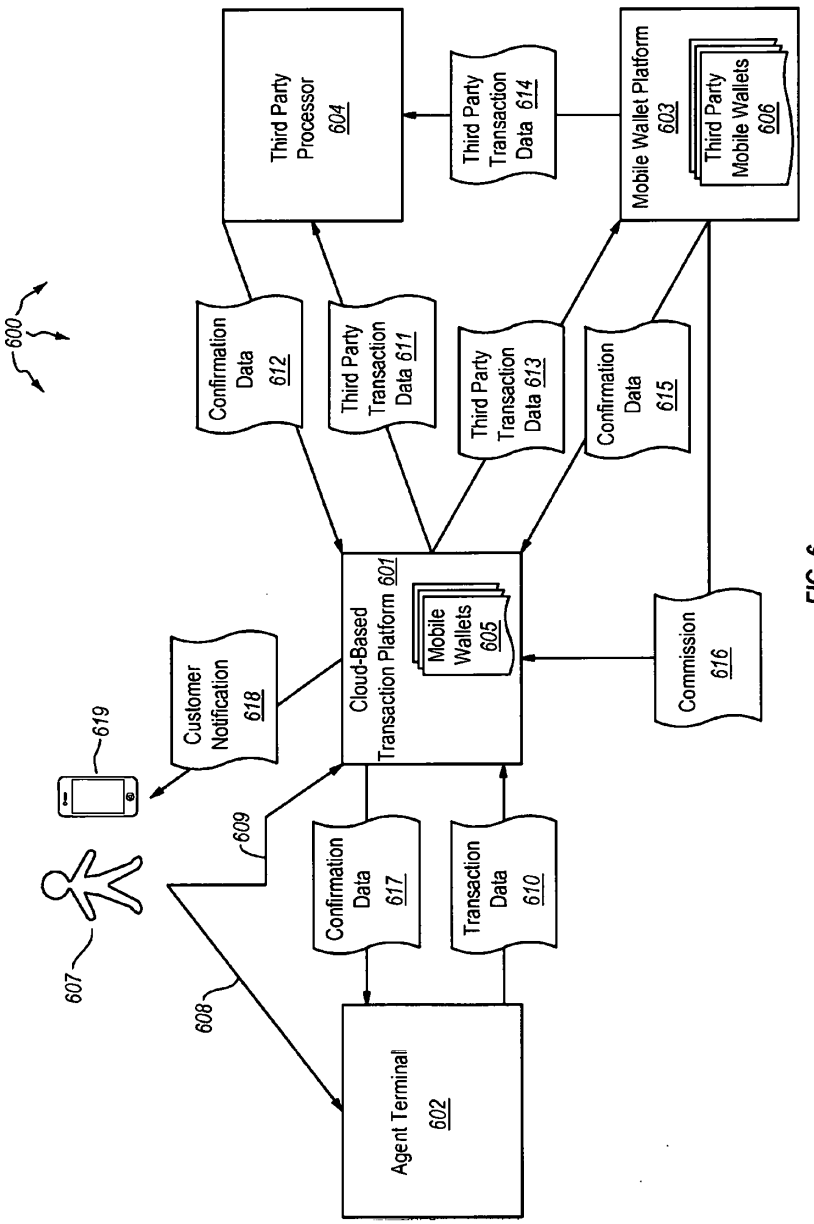


FIG. 6

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 344 of 381

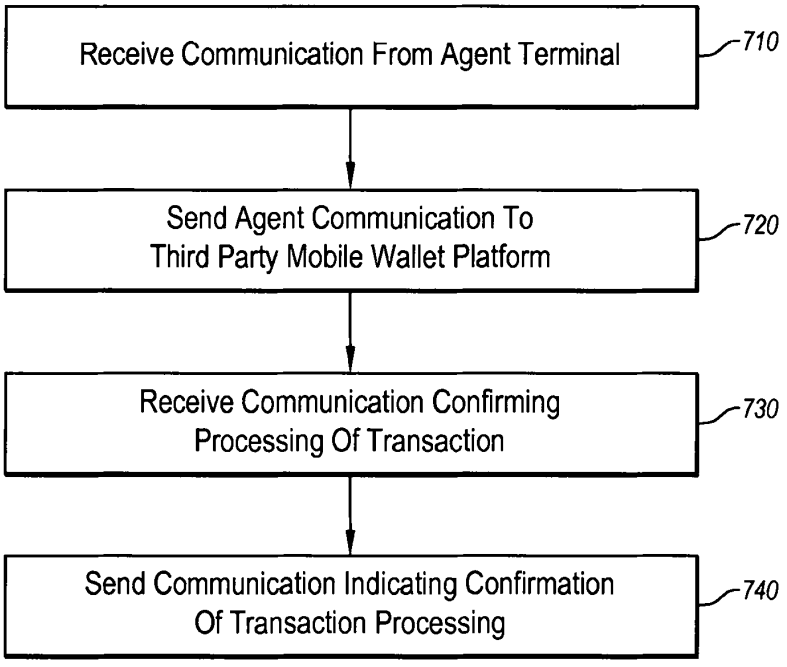

Receive Communication From Agent Terminal
710
Send Agent Communication To Third Party Mobile Wallet Platform
720
Receive Communication Confirming Processing Of Transaction
730
Send Communication Indicating Confirmation Of Transaction Processing
740

FIG. 7

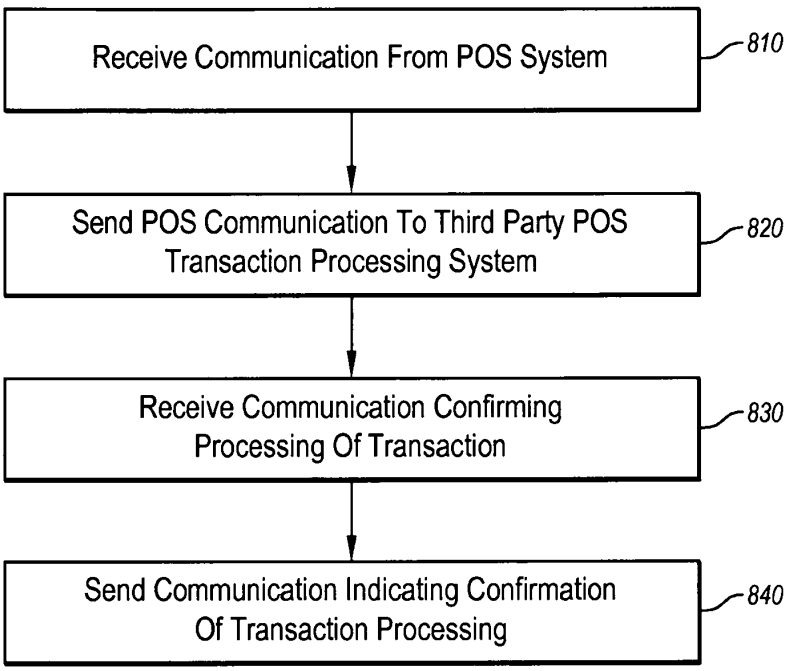

Receive Communication From POS System
810
Send POS Communication To Third Party POS Transaction Processing System
820
Receive Communication Confirming Processing Of Transaction
830
Send Communication Indicating Confirmation Of Transaction Processing
840

FIG. 8

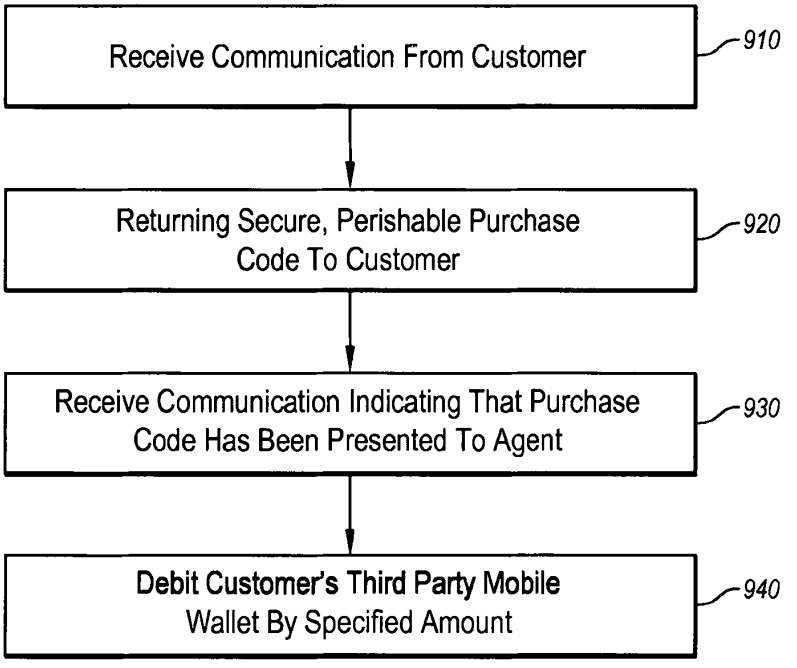

Receive Communication From Customer
910
Returning Secure, Perishable Purchase Code To Customer
920
Receive Communication Indicating That Purchase Code Has Been Presented To Agent
930
Debit Customer's Third Party Mobile Wallet By Specified Amount
940

FIG. 9

USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT MULTIPLE MOBILE WALLET PROVIDERS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of, and claims priority to, U.S. patent application Ser. No. 13/680,824, entitled "Using A Mobile Wallet Infrastructure To Support Multiple Mobile Wallet Providers", filed Nov. 19, 2012, which claims the benefit of U.S. Provisional Application Ser. No. 61/562,301, entitled "Using A Mobile Wallet Infrastructure To Support Multiple Mobile Wallet Providers", filed Nov. 21, 2011, which is herein incorporated by reference in its entirety.

BACKGROUND

Mobile phones and other digital devices have become increasingly popular in recent years. Many mobile device users use their devices to perform countless different daily tasks. For instance, mobile devices allow users to check email, send and receive instant messages, check calendar items, take notes, set up reminders, browse the internet, play games or perform any number of different things using specialized applications or "apps". These applications allow mobile devices to communicate with other computer systems and perform a wide variety of network-connected tasks previously not possible with a mobile device.

BRIEF SUMMARY

Embodiments described herein extend to methods, systems, and computer program products for a cloud-based transaction platform. Embodiments include an infrastructure that can be used with third party mobile wallets provided by third party mobile wallet providers. Users with native or third party mobile wallets can use the cloud-based transaction platform to enroll a customer for a third party mobile wallet, add a stored value account (either hosted by the cloud-based transaction platform or a third party), add a bank/credit union account to a third party mobile wallet, add a debit/credit card account to a third party mobile wallet, deposit funds in a third party mobile wallet, withdraw funds from a third party mobile wallet, pay bills from a third party mobile wallet, top up a prepaid mobile account through a third party mobile wallet, transfer funds through a third party mobile wallet, and make in store purchases from a third party mobile wallet.

Embodiments described herein are directed to performing a transaction using a third party mobile wallet, performing a transaction using a third party point of sale (POS) system and to making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. In one embodiment, a cloud-based transaction platform is provided, which receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that a customer desires to perform a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the agent communication to a third party mobile wallet platform, receives communication from the third party mobile wallet platform confirming processing of the transaction, and sends communication to the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

In another embodiment, a cloud-based transaction platform performs a transaction using a third party point of sale (POS) system. The cloud-based transaction platform receives communication from a specified POS system implemented at an agent terminal over a communication channel connected to the cloud-based transaction platform. The POS communication indicates that a customer has initiated a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the POS communication to a corresponding third party POS transaction processing system that has been established to process POS transactions from the specified POS system, receives communication from the third party POS transaction processing system confirming processing of the transaction, and sends communication to the specified POS system implemented at the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

In yet another embodiment, a cloud-based transaction platform is provided which allows users to make purchases from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform receives communication from a customer over a communication channel connected to the cloud-based transaction platform. The customer communication indicates that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's third party mobile wallet. The cloud-based transaction platform returns a secure, perishable purchase code to the customer over at least one the communication channels connected to the cloud-based transaction platform and receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent terminal communication indicates that the purchase code has been presented to an agent. The cloud-based transaction platform then debits the customer's third party mobile wallet by the specified amount of funds to complete the purchase.

This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

Additional features and advantages will be set forth in the description which follows, and in part will be apparent to one of ordinary skill in the art from the description, or may be learned by the practice of the teachings herein. Features and advantages of embodiments described herein may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. Features of the embodiments described herein will become more fully apparent from the following description and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

To further clarify the above and other features of the embodiments described herein, a more particular description will be rendered by reference to the appended drawings. It is appreciated that these drawings depict only examples of the embodiments described herein and are therefore not to be considered limiting of its scope. The embodiments will be

described and explained with additional specificity and detail through the use of the accompanying drawings in which:

FIG. **1** illustrates a monetary transaction system architecture in which embodiments described herein may operate.

FIG. **2** illustrates an example embodiment of a cloud-based transaction platform.

FIGS. **3**A and **3**B illustrate example data flows for performing subscriber-to-subscriber and subscriber-to-non-subscriber eMoney transfers via a mobile wallet, respectively.

FIG. **4** illustrates an example data flow for making a retail purchase using a mobile wallet.

FIG. **5** illustrates an example embodiment of a monetary transaction system architecture.

FIG. **6** illustrates an alternate example embodiment of a cloud-based transaction platform.

FIG. **7** illustrates an example embodiment data flow for performing a transaction using a third party mobile wallet.

FIG. **8** illustrates an example embodiment data flow for performing a transaction using a third party point of sale (POS) system.

FIG. **9** illustrates an example embodiment data flow for making a purchase from a third party mobile wallet provided by a third party mobile wallet provider.

DETAILED DESCRIPTION

Embodiments described herein extend to methods, systems, and computer program products for a cloud-based transaction platform. Embodiments include an infrastructure that can be used with third party mobile wallets provided by third party mobile wallet providers. Users with native or third party mobile wallets can use the cloud-based transaction platform to enroll a customer for a third party mobile wallet, add a stored value account (either hosted by the cloud-based transaction platform or a third party), add a bank/credit union account to a third party mobile wallet, add a debit/credit card account to a third party mobile wallet, deposit funds in a third party mobile wallet, withdraw funds from a third party mobile wallet, pay bills from a third party mobile wallet, top up a prepaid mobile account through a third party mobile wallet, transfer funds through a third party mobile wallet, and make in store purchases from a third party mobile wallet.

Embodiments described herein are directed to performing a transaction using a third party mobile wallet, performing a transaction using a third party point of sale (POS) system and to making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. In one embodiment, a cloud-based transaction platform is provided, which receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that a customer desires to perform a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the agent communication to a third party mobile wallet platform, receives communication from the third party mobile wallet platform confirming processing of the transaction, and sends communication to the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

In another embodiment, a cloud-based transaction platform performs a transaction using a third party point of sale (POS) system. The cloud-based transaction platform receives communication from a specified POS system implemented at an agent terminal over a communication channel connected to the cloud-based transaction platform. The POS communication indicates that a customer has initiated a mobile wallet transaction using their third party mobile wallet. The cloud-based transaction platform sends the POS communication to a corresponding third party POS transaction processing system that has been established to process POS transactions from the specified POS system, receives communication from the third party POS transaction processing system confirming processing of the transaction, and sends communication to the specified POS system implemented at the agent terminal over a communication channel connected to the cloud-based transaction platform, where the communication indicates confirmation of the processing of the transaction.

In yet another embodiment, a cloud-based transaction platform is provided which allows users to make purchases from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform receives communication from a customer over a communication channel connected to the cloud-based transaction platform. The customer communication indicates that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's third party mobile wallet. The cloud-based transaction platform returns a secure, perishable purchase code to the customer over at least one the communication channels connected to the cloud-based transaction platform and receives communication from an agent terminal over a communication channel connected to the cloud-based transaction platform. The agent terminal communication indicates that the purchase code has been presented to an agent. The cloud-based transaction platform then debits the customer's third party mobile wallet by the specified amount of funds to complete the purchase. Such purchases may be for items that are provided by the cloud-based transaction platform, either directly or via a third-party provider. These items may include music, movies, games and other downloadable content, physical items that can be shipped to the user and other items such as health care services.

Embodiments described herein may comprise or utilize a special purpose or general-purpose computer including computer hardware, such as, for example, one or more processors and system memory, as discussed in greater detail below. Embodiments described herein also include physical and other computer-readable media for carrying or storing computer-executable instructions and/or data structures. Such computer-readable media can be any available media that can be accessed by a general purpose or special purpose computer system. Computer-readable media that store computer-executable instructions in the form of data are computer storage media. Computer-readable media that carry computer-executable instructions are transmission media. Thus, by way of example, and not limitation, embodiments described herein can comprise at least two distinctly different kinds of computer-readable media: computer storage media and transmission media.

Computer storage media includes RAM, ROM, EEPROM, CD-ROM, solid state drives (SSDs) that are based on RAM, Flash memory, phase-change memory (PCM), or other types of memory, or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store desired program code means in the form of computer-executable instructions, data or data structures and which can be accessed by a general purpose or special purpose computer.

A "network" is defined as one or more data links and/or data switches that enable the transport of electronic data between computer systems and/or modules and/or other electronic devices. When information is transferred or provided over a network (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a transmission medium. Transmission media can include a network which can be used to carry data or desired program code means in the form of computer-executable instructions or in the form of data structures and which can be accessed by a general purpose or special purpose computer. Combinations of the above should also be included within the scope of computer-readable media.

Further, upon reaching various computer system components, program code means in the form of computer-executable instructions or data structures can be transferred automatically from transmission media to computer storage media (or vice versa). For example, computer-executable instructions or data structures received over a network or data link can be buffered in RAM within a network interface module (e.g., a network interface card or "NIC"), and then eventually transferred to computer system RAM and/or to less volatile computer storage media at a computer system. Thus, it should be understood that computer storage media can be included in computer system components that also (or even primarily) utilize transmission media.

Computer-executable (or computer-interpretable) instructions comprise, for example, instructions which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. The computer executable instructions may be, for example, binaries, intermediate format instructions such as assembly language, or even source code. Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the described features or acts described above. Rather, the described features and acts are disclosed as example forms of implementing the claims.

Those skilled in the art will appreciate that various embodiments may be practiced in network computing environments with many types of computer system configurations, including personal computers, desktop computers, laptop computers, message processors, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, mobile telephones, PDAs, tablets, pagers, routers, switches, and the like. Embodiments described herein may also be practiced in distributed system environments where local and remote computer systems that are linked (either by hardwired data links, wireless data links, or by a combination of hardwired and wireless data links) through a network, each perform tasks (e.g. cloud computing, cloud services and the like). In a distributed system environment, program modules may be located in both local and remote memory storage devices.

In this description and the following claims, "cloud computing" is defined as a model for enabling on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). The definition of "cloud computing" is not limited to any of the other numerous advantages that can be obtained from such a model when properly deployed.

For instance, cloud computing is currently employed in the marketplace so as to offer ubiquitous and convenient on-demand access to the shared pool of configurable computing resources. Furthermore, the shared pool of configurable computing resources can be rapidly provisioned via virtualization and released with low management effort or service provider interaction, and then scaled accordingly.

A cloud computing model can be composed of various characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service, and so forth. A cloud computing model may also come in the form of various service models such as, for example, Software as a Service ("SaaS"), Platform as a Service ("PaaS"), and Infrastructure as a Service ("IaaS"). The cloud computing model may also be deployed using different deployment models such as private cloud, community cloud, public cloud, hybrid cloud, and so forth. In this description and in the claims, a "cloud computing environment" is an environment in which cloud computing is employed.

Additionally or alternatively, the functionally described herein can be performed, at least in part, by one or more hardware logic components. For example, and without limitation, illustrative types of hardware logic components that can be used include Field-programmable Gate Arrays (FPGAs), Program-specific Integrated Circuits (ASICs), Program-specific Standard Products (ASSPs), System-on-a-chip systems (SOCs), Complex Programmable Logic Devices (CPLDs), and other types of programmable hardware.

Still further, system architectures described herein can include a plurality of independent components that each contribute to the functionality of the system as a whole. This modularity allows for increased flexibility when approaching issues of platform scalability and, to this end, provides a variety of advantages. System complexity and growth can be managed more easily through the use of smaller-scale parts with limited functional scope. Platform fault tolerance is enhanced through the use of these loosely coupled modules. Individual components can be grown incrementally as business needs dictate. Modular development also translates to decreased time to market for new functionality. New functionality can be added or subtracted without impacting the core system.

Various terminology will be used herein to describe the cloud-based transaction platform (also referred to as a "monetary transaction system", "mobile wallet platform", "mobile wallet program", "mobile wallet transaction system", "mobile financial services (mFS) platform" or "electronic payment system"). The term "agent" is used to refer to an individual with mFS transaction system tools and training to support specific mFS functions. These mFS functions include subscriber registration and activation, and the deposit and withdrawal of funds from the mFS transaction system. Agents are representatives of the mFS transaction system or "program". Agents can be employees or contractors of the program provider, or other companies and organizations that partner with the program provider to provide these services themselves. Agents may be found in every facet of a typical economy, and may include large retailers, mobile network operators (MNO) airtime sales agents, gas stations, kiosks, or other places of business.

The cloud-based transaction platform includes an infrastructure that allows native mobile wallet application and third party mobile wallet applications to interact both with the transaction system and with each other. This allows the user of a native or a third party mobile wallet to make purchases, transfer money or perform any of the other transactions described herein. The cloud-based transaction

platform may include a mobile wallet application and a web interface or some other type of functionality that allows the user to interact with the cloud-based transaction platform using their mobile device. The native and third party mobile wallet applications may include a subscriber identity module (SIM) application, an Unstructured Supplementary Service Data (USSD) application, a smartphone application, a web application, a mobile web application, a Wireless Application Protocol (WAP) application, a Java 2 Platform, Micro Edition (J2ME) application, a tablet application or any other type of application or interface that provides tools for the agent to register, activate, and offer other services to the mFS subscriber.

As used herein, a mobile wallet application is a mobile wallet application installed on a SIM card or elsewhere on a mobile device. The mobile wallet application may either be native (i.e. provided by the provider of the cloud-based transaction platform) or third party (i.e. provided by a provider other than the provider of the cloud-based transaction platform).

A USSD application is an application that implements USSD for various functionality including prepaid callback service, location-based content services, menu-based information services and other mobile wallet platform services. A web application is one that implements or uses the internet to provide mobile wallet platform functionality. A mobile web application is similar to a web application, but is tailored for mobile devices. A WAP application is one that uses the wireless application protocol to communicate with the mobile wallet platform to provide the platform's functionality. A J2ME application is an application developed in Java and is designed to provide mobile wallet functionality on a variety of different hardware. A tablet application is an application specifically designed for a touchscreen-based tablet that provides mobile wallet platform functionality for tablet devices. Any of these applications (or any combination thereof) may be provided on the user's mobile device. This functionality can also be made available on a retail point of sale (POS) system or web site. Indeed, the cloud-based transaction platform allows different POS systems to interact with each other and conduct transactions between themselves.

The term "agent administrator" refers to an individual with mFS program tools and training to administrate the allocation of funds to agent branches (e.g. retail locations). As agents perform mFS transactions with subscribers, such as depositing and withdrawing money, the agents are adding and removing money from their own accounts. Any of the applications referred to above may be configured to provide tools used by the agent administrator to view the agent company balance, view the agent branch balances, and transfer funds into and out of agent branch mobile wallets. This functionality can also be made available on a website for easier access.

In some embodiments, the mFS platform application may utilize triple data encryption standard (3DES) encryption (or some other type of encryption), encrypted message signing, and password security on some or all of its communications with the mFS transaction system in order to ensure that the transactions are properly secured and authenticated.

The term "agent branch" refers to any location where an agent provides support for subscriber services of the mFS platform. Funds are allocated by the agent administrator from the agent company's main account to each agent branch to fund the subscriber mFS functions such as depositing or withdrawing cash, in-store purchases, bill payments, prepaid airtime top-ups and money transfers. In some cases, multiple agents may work in a single branch. However, at least in some cases, monetary funds are allocated to from the agent company's main account on a per branch basis.

The term "agent branch account balance" refers to the amount of money residing in a particular agent branch account at a given time. Funds can be deposited into the branch account by the agent administrator, or the funds can come from participating in subscriber mFS transactions such as depositing or withdrawing cash from the subscriber's mobile wallet accounts, or making retail purchases with the mobile wallet.

In some embodiments, in countries with more developed economies, it may be beneficial to use program-issued pre-paid debit cards, pre-paid access accounts, stored value accounts or gift cards to conduct business along with the added convenience of card processing networks such as Cirrus, STAR, or Visa for POS and automated teller machine (ATM) functionality. Agents, particularly those in retail outlets and kiosks, can still support subscribers with deposits, withdrawals, and other transfers, but in this case bank external card processors manage the mobile wallet and branch account balances and provide the real-time transfer of funds.

The term "agent branch ledger" refers to a written (or electronic) ledger maintained by the mFS platform. Agent branch transactions are performed on the agent's and subscriber's mobile phones where an electronic record of the transaction is generated and stored on the mFS platform. These electronic transactions are then reconciled with agent branch ledgers to ensure the security and integrity of the transaction. Agent branch ledgers are printed or electronic transaction logs that are distributed to the agent branch locations in hard copy form to serve as a backup record to the electronic transactions.

The term "agent company" refers to a business that registers to participate in the mFS program as a partner of the mFS program provider or owner. The agent company has one or more agent branches which conduct mFS business with mFS program subscribers. In some cases, the agent company may be referred to as a distributor or retailer.

The term "agent company account balance" refers to the sum of the funds deposited at a "partner bank" (defined below) by the agent company to fund the agent company's daily transactions. The funds in the agent company account are then distributed to agent branches by the agent company's agent administrator to conduct everyday business such as accepting cash deposits and cash withdrawals from mFS subscribers. This balance is sometimes referred to as the "agent company float".

An "agent manager" is a supervisor of company agents for a given company. The agent manager has the training and tools to create, delete or modify agent accounts for a company, as well as monitor the transactions performed by agents. The agent manager may have a special application or an increased level of rights to access applications features not available to other users. The special application is a program installed on the agent manager's terminal. This application provides the agent manager the ability to securely perform agent manager functions such as registering and activating new agent accounts. The mFS agent manager application may be installed on any terminal or device. It communicates with the mFS platform using binary and/or text SMS messages. A wireless service provider or MNO provides the GSM SMS network infrastructure on which the mFS platform operates.

As subscribers, agents, and other mFS program participants conduct business in the mFS program, value is trans-

ferred from one account to the next as payment for services rendered or goods purchased. This value can be in the form of real currency or the electronic representation referred to herein as eMoney. Among other situations, eMoney is used in mFS implementations where the real-time processing of financial transactions including card processing is not practical. The mFS platform utilizes an internal transaction processor for managing the real-time balance of mobile wallet and agent accounts as value (eMoney) is transferred from one mobile wallet to another in payment for services.

The term "mFS program master account" refers to a bank account maintained by the mFS program partner bank to provide funds and float for the operation of the mFS platform. Depending on the type of mFS implementation, the master account can include sub-accounts for each of the agent branches and subscriber mobile wallets, giving the bank visibility into all transactions on a per-user basis. The mFS platform can also manage the balance of sub-accounts and interact with the bank's master account when funds need to be deposited or withdrawn from the account.

The term mobile network operator (MNO) refers to a provider of mobile phone service including basic voice, SMS, unstructured supplementary service data (USSD) and data service, and may also be referred to as a "wireless service provider".

The term "mobile wallet" or "mobile wallet account" refers to a stored value account or prepaid access account (PPA) that allows the owner (or "subscriber") to pay for goods and services on the mFS platform from his or her mobile wallet account. When the mFS eMoney transaction processor is used, the mobile wallet balance is maintained by the mFS platform and value is exchanged within the mFS program as eMoney. When the mFS platform is integrated to an external card processor, the mobile wallet utilizes funds from the subscriber's prepaid debit card and bank account to exchange value on the mFS platform.

The term "partner bank" refers to the primary bank participating in the mFS program. The partner bank is responsible for holding the mFS program master accounts that hold the funds for all mFS services and transactions. A "PIN" refers to a numeric password that may be required to perform a transaction via the mobile wallet application.

The term "subscriber" refers to a participant of the mFS mobile wallet platform. The subscriber maintains a mobile wallet balance and performs transactions using the mFS application. An "unbanked subscriber" is a subscriber that does not have (or does not have access to) a bank account or credit union account. The application or "mobile wallet application" provides mobile wallet functionality to the (unbanked) subscriber. The mobile wallet application is installed on a mobile device in the device's memory, on a SIM card (such as a GSM SIM card) or is otherwise accessible to the mobile device. The mobile wallet application provides the subscriber the ability to securely perform subscriber functions such as making retail purchases, paying bills, or transferring money to other mFS subscribers and non-subscribers. The mobile wallet application communicates with the mFS platform using binary and text SMS messages, among other forms of wireless communication. A wireless service provider or MNO provides the GSM network infrastructure on which the mFS platform operates.

FIG. **1** illustrates an example system architecture for a cloud-based transaction platform. Integration tier **101** is configured to manage mobile wallet sessions and maintain integrity of financial transactions. Integration tier **101** can also include a communication (e.g., Web services) API and/or other communication mechanisms to accept messages from channels **111**. Other mechanisms include, but are not limited to: International Standards Organization ("ISO") **8583** for Point of Sale ("POS") and Automated Teller Machines ("ATM") devices and Advanced Message Queuing Protocol ("AMQP") for queue based interfaces. Each of channels **111** can be integrated to one or more mechanisms for sending messages to integration tier **101**. Notification services **102** is configured to send various notifications through different notification channels **112**, such as, for example, Short Message Peer-to-Peer ("SSMP") for Short Messaging Service ("SMS") and Simple Mail Transfer Protocol ("SMTP") for emails. Notification services **102** can be configured through a web services API.

Service connectors **103** are a set of connectors configure to connect to 3rd party systems **113**. Each connector can be a separate module intended to integrate an external service to the system architecture. Business process services **104** are configured to implement business workflows, including executing financial transactions, auditing financial transactions, invoking third-party services, handling errors, and logging platform objects. Payment handler **105** is configured to wrap APIs of different payment processors, such as, for example, banking accounts, credit/debit cards or processor **121**. Payment handler **105** exposes a common API to facilitate interactions with many different kinds of payment processors.

Security services **106** are configured to perform subscriber authentication. Authorization services **107** are configured to perform client authorization, such as, for example, using a database-based Access Control List ("ACL") table.

Database **108** is configured to manage customer accounts (e.g., storing customer accounts and properties), manage company accounts (e.g., storing company accounts and properties), manage transaction histories (e.g., storing financial transaction details), store customer profiles, storing dictionaries used by the mobile wallet platform, such as, for example, countries, currencies, etc., and managing money containers. Rules engine **109** is configured to gather financial transaction statistics and uses the statistics to provide transaction properties, such as, for example, fees and bonuses. Rules engine **109** is also configured to enforce business constraints, such as, for example, transactions and platform license constraints.

Name matching engine **110** is configured to match different objects according to specified configuration rules. Matching engine **110** can be used to find similarities between names, addresses, etc. Transaction processor **121** is configured to manage financial accounts and transactions. The transaction processor **121** can be used to hold, load, withdraw and deposit funds to mobile wallet accounts. Transaction processor **121** can also be used as a common interface to a third party processor system. When used as a common interface, financial operations may be delegated to the external processor. A Clearing House subsystem of transaction processor **121** can be used to exchange the financial information with a bank.

Components of a mobile wallet platform can be connected to one another over (or be part of) a system bus and/or a network. Networks can include a Local Area Network ("LAN"), a Wide Area Network ("WAN"), and even the Internet. Accordingly, components of the mobile wallet platform can be "in the cloud". As such, mobile wallet platform components as well as any other connected computer systems and their components, can create message related data and exchange message related data (e.g., Internet Protocol ("IP") datagrams and other higher layer protocols that utilize IP datagrams, such as, Transmission Control

Protocol ("TCP"), Hypertext Transfer Protocol ("HTTP"), Simple Mail Transfer Protocol ("SMTP"), etc.) over the system bus and/or network.

The components depicted in FIG. **1** can interoperate to provide a number of financial and other services including but not limited to enrolling a customer for a mobile wallet, adding a stored value account (either hosted by a mobile wallet platform or a third party), adding a bank or credit union account to a third party mobile wallet, adding a debit or credit card account to a third party mobile wallet, depositing funds in a third party mobile wallet, withdrawing funds from a third party mobile wallet, paying bills from a third party mobile wallet, topping up a prepaid mobile account through a third party mobile wallet, transferring funds through a third party mobile wallet (nationally or internationally), making in-store purchases using a third party mobile wallet, selecting health care providers and paying for health care services, paying for music, games, movies or other downloadable provided by a third party provider and made available over the cloud-based transaction system, and various other tasks as described herein below.

FIG. **2** depicts a monetary transaction architecture **200** similar to that described in FIG. **1**. The monetary transaction architecture **200** may provide a more simplified system structure in which each of the above services may be provided. The system includes a subscriber **205**. The subscriber may have access to a bank account, or may be an unbanked subscriber. The subscriber has a profile **211** with the cloud-based transaction system **210**. The profile includes the subscriber's know your customer (KYC) information, as well as any associated bank accounts, credit union accounts, bill pay accounts or other accounts. The subscriber has (or has access to) a mobile device **206** such as a phone or tablet. The mobile device runs the native or third party mobile wallet application **207**.

The subscriber can indicate, using the mobile wallet application **207**, which transaction or other action he or she would like to perform. The indicated transaction **208** is sent to the mobile wallet platform **210** to be carried out by the platform. The transaction processor **216** (which may be similar to or the same as transaction processor **121** of FIG. **1**) performs the transaction(s) specified by the (unbanked) subscriber **205**. The transaction processor may implement various other components to perform the transaction including memory **217**, (wireless) communication module **215**, rules engine **220** and/or a transaction database **225**.

Performing the specified transactions may include communicating with the monetary transaction database **225** to determine whether the transaction is permissible based on data indicated in the unbanked subscriber's profile (for instance, whether the subscriber has enough eMoney **221** in his or her stored value account, or has enough money in his or her bank account). Rules engine **220** may also be consulted to determine whether the subscriber has exceeded a specified number of allowed transactions. Then, if funds are available, and the transaction is otherwise permissible, the monetary transaction system can transfer money or eMoney **221** to or from an entity such as a user or agent (e.g. customer **222**) to or from an establishment such as an agent terminal (i.e. a retail store or agent company) **223**.

In some cases, the cloud-based transaction system **210** provides a web interface that allows subscribers of third party mobile wallet applications to perform the same functions provided for native subscribers. For instance, mobile wallet application **207** may provide a web interface that allows a user to enroll for a native or third party mobile wallet. The web interface (or the mobile wallet application itself) receives a subscriber-initiated transaction over one of a plurality of communication channels (**111** from FIG. **1**) connected to the cloud-based transaction system **210**. The web interface or mobile wallet application may prompt for and receive enrollment information (e.g. KYC information) for the (unbanked) subscriber **205** over at least one of the plurality of communication channels (e.g. web, point-of-sale (POS), interactive voice response (IVR, etc.). The web interface or mobile wallet application may then send activation instructions over the same or a different channel to activate the (unbanked) subscriber **205** and create a subscriber account for the (unbanked) subscriber.

Once the subscriber has an account, the cloud-based transaction system generates (or allows the third party provider to generate) a corresponding mobile wallet for the unbanked subscriber (available via the web interface and/or the mobile wallet application). The system then presents the (unbanked) subscriber's account data associated with the mobile wallet and/or a notification indicating that enrollment was successful to the subscriber. Accordingly, the mobile wallet application or the web interface may be used to provide user enrollment functionality. It should also be understood that either the mobile wallet application or the web interface may be used to provide substantially all of the third party or native mobile wallet functionality described herein.

It should also be noted that the mobile device **206** may be any type of plan-based phone or tablet, or prepaid phone or tablet. Many subscribers, such as unbanked subscribers, may primarily use prepaid phones. The mobile wallet application **207** may be installed on both plan-based phones and prepaid phones. The mobile wallet application may be installed on the device's SIM card, or on the device's main memory. Accordingly, the monetary transaction system **200** may be accessed and used via substantially any type of plan-based or prepaid mobile device.

The components depicted in FIG. **1** can interoperate to provide a number of financial and other services including but not limited to enrolling a customer for a third party mobile wallet, adding a stored value account (either hosted by an electronic payment system or a third party), adding a bank/credit union account to a third party mobile wallet, adding a debit/credit card account to a third party mobile wallet, depositing funds in a third party mobile wallet, withdrawing funds from a third party mobile wallet, paying bills from a third party mobile wallet, topping up a prepaid mobile account through a third party mobile wallet, transferring funds through a third party mobile wallet, making in store purchases from a third party mobile wallet, or transferring money or eMoney from one business account to another business account (i.e. from one business's mobile vault to another business's mobile vault, as will be shown in FIG. **4**).

FIG. **3**A depicts a subscriber-to-subscriber eMoney transfer. In a merchant and distributor scenario, either or both of the merchant and the distributor (including any delivery personnel) may be subscribers. To perform such a transfer, subscriber A (**301**) enters some type of identification information identifying subscriber B (e.g. subscriber B's phone number) and an amount of money he or she wishes to transfer. The transaction processor **216** of the monetary transaction system **210** determines if there are sufficient funds to complete the transfer. If sufficient funds are available, the monetary transaction system **210** decrements subscriber A's account and credits subscriber B's account (**302**). The system then sends some kind of notification (e.g. SMS) to subscriber B indicating that a certain amount of money

was transferred to their account. Subscriber A may also receive a notification that the transfer was successful. Accordingly, eMoney may be transferred between two cloud-based platform subscribers, one or both of which may be unbanked. The cloud-based transaction system **210** processes the subscribers' requests, updates the subscribers' eMoney balances, logs the transactions, and sends transaction information to a specified bank when needed.

FIG. **3**B illustrates a subscriber-to-non-subscriber eMoney transfer. Accordingly, as mentioned above, either or both of the merchant and the distributor may be non-subscribers. In graphic **305**, subscriber A wishes to send eMoney to another individual that is not a subscriber to the cloud-based transaction platform. The transaction is initiated in the same fashion as the subscriber-to-subscriber transfer scenario. However, since non-subscriber B does not have a mobile wallet account, the cloud-based transaction system **210** cannot credit them with eMoney. Instead, the cloud-based transaction system **210** sends a notification (e.g. via SMS) to non-subscriber B with instructions for how to pick-up the transferred money, along with an authorization code (**306**). The cloud-based transaction system **210** puts a hold on subscriber A's account for the amount transferred. Subscriber B then has a specified number of days to pick up the cash before the hold expires and the amount is credited back to subscriber A's eMoney account by the monetary transaction system **210**.

When non-subscriber B goes to pick up the money at an agent branch, the agent branch's manager or agent verifies the authorization code via an agent manager or agent mobile wallet application (that, in turn, accesses the cloud-based transaction platform). Once the transfer has been validated, the agent gives the cash to non-subscriber B. The agent branch's mFS account is credited with the transfer amount (**307**) and the user leaves with the cash in hand (**308**). The cloud-based transaction platform processes the transfer request, updates subscriber A's eMoney balance, logs the transaction, and sends transaction details to a platform-specified bank.

FIG. **4** illustrates a mobile wallet subscriber making a retail purchase. Mobile wallet subscribers can make retail purchases at agent branches directly from their mobile device. Agent branches, as explained above, are retail stores or other entities that have registered with the cloud-based transaction platform and are able to accept native and third party mobile wallet payments. Accordingly, a subscriber can select the items they wish to purchase, and indicate (via the mobile wallet application) to the agent branch that they wish to pay for the items. The mobile wallet application then communicates with the agent branch and the monetary transaction system to indicate the price of the transaction. The monetary transaction system **210** then debits the subscriber's eMoney account (**401**) and credits the agent branch's eMoney account (**402**). The agent branch (and/or the agent manager or agent) receives confirmation that subscriber paid for the purchase. The subscriber may also receive a summary of the retail purchase and may be asked to confirm the purchase by entering a PIN. The monetary transaction system processes the purchase request, updates the agent branch and subscriber's eMoney balances, logs the transaction, and sends transaction details to a cloud-based transaction platform-specified bank.

In one embodiment, the cloud-based transaction system **210** is implemented to make a purchase from a mobile wallet. The communications module **215** of the monetary transaction system **210** receives a communication from a subscriber over a communication channel **111**. The subscriber communication indicates that an unbanked subscriber **205** desires to purchase an item for a specified amount of funds using a specified payment method from the unbanked subscriber's native or third party mobile wallet.

The monetary transaction system **210** then returns a secure, perishable purchase code to the unbanked subscriber over at least one of the channels connected to the monetary transaction system and receives a subsequent agent branch communication over a channel indicating that the purchase code has been presented to an agent (branch). The monetary transaction system **210** validates the status of the specified payment method, determines if the specified payment method can accommodate a purchase for the specified amount, performs a limit check and/or a velocity check on the selected payment method, debits the specified payment method by the specified amount of funds, returns a notification to the agent branch authorizing the purchase and sends a receipt to the unbanked subscriber over a communication channel. The cloud-based transaction system **210** may thus be used in this manner to make a retail purchase using a native or third party mobile wallet.

FIG. **5** depicts a physical environment and corresponding computer system architecture **500** for allowing a user to participate in various services using a native or third party mobile wallet (e.g. **511**). Some of these services include allowing the user **507** to access disruptively priced or free financial services or items in exchange for participation in opt-in advertising. The environment **500**, like the scenarios described in FIGS. **3**A, **3**B and **4**, involves the use of a native or third party mobile wallet application **511**. The mobile wallet application **511** can be used to provide disruptively priced or free financial services or items in exchange for participation in opt-in advertising. The mobile wallet application may be run on any type of digital device including a mobile phone, tablet, laptop or other digital device. Embodiments include providing digital data (e.g., coupons or vouchers) for obtaining disruptively priced or free items (e.g., consumer goods or groceries) to such digital devices.

In some embodiments, a user has an account with a mobile payment system. The cloud-based transaction system (e.g. **210** of FIG. **2** or electronic payment system **521** of FIG. **5**) can provide the user **507** with a variety of functionality including purchasing items (see FIG. **4**), depositing funds, withdrawing funds, transferring funds (see FIGS. **3**A and **3**B), and others all from a third party wallet. Accordingly, the user can use a digital device to interact with the electronic payment system **521** to pay for goods and/or services.

In exchange for some type of financial benefit, the user opts in to receive advertisements. The financial benefits may include coupons, vouchers, promotions, Buy One Get One ("BOGO") offers or any other type of benefit (such as a reduced cost or free financial service or good) from the electronic payment system. The benefit may be targeted to the user based on the user's age, location or other demographic information, or based on the user's past purchases. At least in some embodiments, when the user agrees to participate in opt-in advertising, the electronic payment system **521** is permitted to store (e.g., by capturing purchase orders), track, and analyze items that the user purchases through their account with the electronic payment system. The electronic payment system stores and maintains lists of the users' purchased items in a data warehouse. The electronic payment system may also store information about the user (anonymous or otherwise) including age, income level, an indication of whether kids are in the family, or other information that may be useful in targeting ads or benefits to the user.

The electronic payment system analyzes **534** the users purchasing habits to identify advertisements and/or promotions that may be of interest to the user. The advertisements and/or promotions can be for items the user has purchased **503**. The advertisements and/or promotions can also be for items related to items the user has purchase. For example, if user has purchased a particular brand of razor, advertisements for the brand's shaving cream can be identified. Advertisements for related items can also be used for cross-promotion.

From time to time, at specified intervals, or based on location (e.g., having a coupon for a merchant this is with a specified proximity) the electronic payment system sends identified advertisements and/or promotions to the user's digital device. When specified advertising thresholds are satisfied (e.g., a specified number and/or type of advertisements and/or promotions are presented), the electronic payment system confers a financial benefit on the user's account. For example, the electronic payment system can provide the user's account with a low cost (e.g., reduced fee) or free financial service, such as, for example, one reduced cost bill pay or one free bill pay. Alternately, the electronic payment system can provide the user's account with a coupon or voucher for an item (e.g., an item a user has pre-selected or an item the user has purchased in the past).

In some embodiments, a client application for the electronic payment system runs on the user's digital device (e.g. mobile wallet application **511**). The user interacts with the electronic payment system through the client application. From a screen of the client application, the user can agree to accept opt in advertising. Accordingly, embodiments of the invention essentially permit a user to self-monetize themselves through their digital device.

As further depicted in FIG. **5**, computer architecture **500** includes digital device **508**, retail location **502**, and electronic payment system **521**. Digital device **508** further includes mobile wallet application **511**. Retail location **502** further includes its own mobile wallet application **512**. Electronic payment system **521** includes marketing module **533**, data warehouse **532**, advertisements **538**, payment processor **522**, user mobile wallet **524** (user **507**'s mobile wallet), and merchant mobile wallet **526** (retail location **502**'s mobile wallet).

Generally, each company in packaged goods companies **571** (or retailers that sell the packaged goods or other goods or services) can send advertisement data to electronic payment system **521**. Advertisements **538** represent the collection of advertisement data sent from packaged goods companies **571**. Each company in packaged goods companies **571** can also submit benefit rules to electronic payment system **521**. Benefit rules **578** represent the collection of benefit rules sent from packaged goods companies **571**. Benefit rules **578** define when a benefit, such as, for example, a free financial service, a coupon, a promotion, etc, is to be granted to a user of electronic payment system **521**. For example, in response to completing a questionnaire linked to a product advertisement, a user can be given a coupon for the product or for a related product.

In general, user **507** can use native or third party mobile wallet application **511** to pay for goods purchased at retail location **502** (as shown in FIG. **4**). For example, user **507** can use mobile wallet application **511** to purchase goods **503**. To pay for goods **503**, mobile wallet application **511** can send payment instruction **543** in amount **563** to electronic payment system **521**. Payment processor **522** can receive payment instruction **543**. In response, payment processor **522** can debit **541** user mobile wallet **524** by amount **563**. Payment processor **522** can also credit **542** merchant mobile wallet **526** by amount **563**.

User **507** can use mobile wallet application **511** to participate in opt-in advertising. For example, user **507** can use mobile wallet application **511** to send opt-in **544** to electronic payment system **521**. Advertising module **533** can receive opt-in **544** and record that mobile wallet application **511** has opted in for advertising. As such, when user **507** makes a purchase using mobile wallet application **511**, a list of purchased items is sent to electronic payment system **521**. For example, upon purchasing goods **503**, item list **531** is sent to electronic payment system **521** and stored in data warehouse **532**.

Propensity analysis module **534** can analyze user **507**'s purchases, including item list **531**. From the analysis, propensity analysis module **534** can identify items or categories of items user **507** may be interested in. The items can be items user **507** has purchased in the past (e.g., an item in goods **503**) or items related to items user **507** has purchases in the past. Propensity analysis module **534** can indicate identified items or categories of items to advertisement identification module **536**. These identified items or categories are items that the user is likely interested in and, as such, may have a propensity toward buying these items. The propensity analysis module may use past purchases, personal preferences, lifestyle or demographic information or other data in the propensity analysis.

Advertisement identification module **536** can then select advertisements from advertisements **538** that correspond to the identified items or categories of items. For example, advertisement identification module **536** can select advertisement **546** for presentation at mobile wallet application **511**. Advertisement **546** can be an advertisement for a product made by a company in packaged goods companies **571**. Additionally or alternatively, the advertisement **546** may be created by the merchant and may advertise products or services sold by that merchant.

Advertising module **533** can send selected advertisements to mobile wallet application **511**. For example, advertising module **533** can send advertisement **546** (e.g., related to an item in goods **503**) to mobile wallet application **511**. In general, advertisements can include interactive content. For example, advertisement **546** includes content **573**. Content **573** can be a video, a link to a company website (e.g., for a company in packaged goods companies **571**), a call to action (such as a questionnaire), or some other content user **507** can interact with through digital device **508**. User **507** can interact with content **573**, for example, responding to questions in content **573**. Advertisement response **574** can indicate how user **507** has interacted with content **573**. In one embodiment, a call to action may be to post an update on Facebook® or some other website such as a retail establishment ranking website. If the user makes such a post or performs some other call to action, the user may be rewarded with a benefit. That benefit may be related to the product about which the user posted on the various websites.

Based on advertisement response **574**, benefit determination module **576** can determine if a benefit is to be conferred upon user **507**. Benefit determination module **576** can refer to benefit rules **578** when making a determination whether or not to confer a benefit. Thus, when user **507** interacts with advertisement **546** in a specified way (e.g., completes a survey, watches a video, etc.), benefit rules **578** can indicate that a company benefit (e.g., benefit **577**) is to be conferred upon user **507**. For example, benefit determination module **576** can confer benefit **577** on user **507**. When user **507**

receives an advertisement for a razor, for instance, and answers a questionnaire on how often they shave, a razor manufacture can give user **507** a coupon for reduced cost or free razor blades.

When a benefit is to be conferred on a user, the benefit can be stored in the user's brand locker. For example, benefit determination module **576** can store benefit **577** in brand locker **572** (part of user mobile wallet **524**). Benefit **577** can be a coupon, a reduced cost or free financial service, a voucher, a promotion, a free bill pay, etc.

Benefit determination module **576** can also track aggregate statistics, such as, for example, specified number and/or type of advertisements received, for advertisements presented at native or third party mobile wallet application **511**. Benefits can also be conferred upon users based on the aggregate statistics. For example, benefit determination module **576** can confer a benefit upon user **507** in response to twenty advertisements being presented at mobile wallet application **511**. Thus, conferred benefits can be company-specified benefits or can be electronic payment system-specified benefits. Electronic payment system **521** can notify a user when a benefit is conferred. For example, electronic payment system **521** can send benefit notification **547** to mobile wallet application **511** to indicate benefit **577** being stored in brand locker **572**.

When user **507** makes subsequent purchases through user mobile wallet **524**, electronic payment system **521** can automatically check brand locker **572** for benefits related to any purchases items. If benefits for an item are identified, user **507** can be notified through mobile wallet application **511**. In some cases, if benefits are identified, those benefits can be applied automatically when the user purchases that item or service. Thus, if the benefit is a coupon or a buy one get one free offer, that benefit may be applied automatically when the user uses his or her mobile wallet application **511** to purchase that item. Accordingly, embodiments of the invention permit user **507** to self monetize digital device **508** through agreeing to participate in opt-in advertising.

Although not depicted, various other modules from the architecture of FIG. **1** or **2** can also be included electronic payment system **521**. The modules expressly depicted in FIG. **5** can interoperate with these other modules as appropriate to facilitate desired functionality.

FIGS. **7-9** will now be described in conjunction with the computer architecture **600** illustrated in FIG. **6**. FIG. **6** depicts a mobile wallet platform **601** that may have an architecture as shown in FIG. **1**. As further depicted in FIG. **6**, mobile wallet platform **601** communicates with an agent terminal **602** or a customer **607** to process transactions using a native or third party mobile wallet **605**. Mobile wallet platform **601** may also communicate with a third party processor **604** to process transactions using a mobile wallet or third party mobile wallet. Mobile wallet platform **601** may also communicate with a third party mobile wallet platform **603** to process transactions using a mobile wallet owned or managed by a third party mobile wallet provider.

Mobile wallet platform **601** may also process the mobile wallet transaction or third party mobile wallet transaction internally, without the use of third party processors or third party mobile wallet platforms. In particular, mobile wallet platform **601** may process transactions using third party mobile wallets in the same or similar manner that transactions are processed as shown in FIGS. **2-5**. Accordingly, the physical environment and corresponding computer system architecture **600** shown in FIG. **6** allows a cloud-based transaction platform **601** to support multiple third party mobile wallet providers.

Mobile wallet platform **601** communicates with agent terminal **602**, third party mobile wallet platform **603**, third party processor **604**, and customer's mobile phone **619** through a variety of communication channels. For example, the communication between mobile wallet platform **601** and any one of these entities may be through communication channels **111**, notification channels **112**, or third party systems **113**, as shown in FIG. **1**. Communication between mobile wallet platform **601** and any one of these entities may also be through processor **121** shown in FIG. **1**.

With respect to the entire description of FIG. **6**, and as explained above, the term "mobile wallet" encompasses not only mobile wallets owned or managed by the mobile wallet platform, but also third party mobile wallets owned by third party mobile wallet providers or managed by third party mobile wallet platforms. In contrast, the term "third party mobile wallet" refers only to third party mobile wallets owned by third party mobile wallet providers or managed by third party mobile wallet platforms. Accordingly, cloud-based transaction platform **601** may manage and process transactions using mobile wallets **605**, which may be mobile wallets owned by cloud-based transaction platform **601** or mobile wallets owned by a third party mobile wallet provider.

As shown in FIG. **6**, customer **607** initiates a mobile wallet transaction **608** at agent terminal **602**. Agent terminal **602** may be part of an agent network consisting of one or more agent terminals that communicate with cloud-based transaction platform **601**. Examples of agent terminals are stores and other commercial establishments. Alternatively, customer **607** may initiate a mobile wallet transaction **609** by communicating with cloud-based transaction platform **601** through a channel selected by the customer.

Mobile wallet transactions **608** and **609** may be one or more of any type of transaction that can be performed using a mobile wallet, including but not limited to, a deposit, withdrawal, transfer, purchase, bill payment, topping up of a prepaid mobile account, or any other transaction described herein. Customer **607** may initiate transactions **608** and **609** in a variety of ways. For example, customer **607** can initiate a deposit into a mobile wallet, a withdrawal from a mobile wallet, a bill payment from a mobile wallet, topping up of a prepaid mobile account using a mobile wallet, a transfer from a mobile wallet, a remittance transaction, a selection of health care provider or payment of health services, a purchase of music, movies, games or other downloadable content, or other purchases using a mobile wallet.

After customer **607** initiates transaction **609** through agent terminal **602**, agent terminal **602** then communicates with cloud-based transaction platform **601** by sending transaction data **610** to cloud-based transaction platform **601**. Once cloud-based transaction platform **601** has received the transaction either through transaction data **610** from agent terminal **602** or from transaction **609** initiated by customer **607**, cloud-based transaction platform **601** may then process the transaction in a variety of ways.

For example, cloud-based transaction platform **601** may process the transaction by communicating with third party processor **604** by sending third party transaction data **611**, which may include some or all of the information in transaction data **610**. Third party processor can then perform the requested transactional processing and respond by sending confirmation data **612** to cloud-based transaction platform **601**. Confirmation data **612** can indicate whether the requested mobile wallet transaction was processed successfully or unsuccessfully.

In another example, cloud-based transaction platform **601** may process the transaction by communicating with third party mobile wallet platform **603** by sending third party transaction data **613**, which may include some or all of the information in transaction data **610**. Third party mobile wallet platform **603** may have any architecture which is suitable for processing mobile wallet transactions. Third party mobile wallet platform **603** may have an architecture that is the same or similar to the architecture shown in FIG. **1**.

Alternatively, third party mobile wallet platform **603** may have a different architecture. In addition, any aspects of cloud-based transaction platform **601** or functionality provided by that platform may also be present in third party mobile wallet platform **603**. After receiving third party transaction data **613**, third party mobile wallet platform **603** may process the transaction itself or forward the transaction to third party processor **604** by sending third party transaction data **614**.

Once processing of the transaction is complete, third party mobile wallet platform **603** may respond to cloud-based transaction platform **601** by sending confirmation data **615**. Confirmation data **615** can indicate whether the requested mobile wallet transaction was processed successfully or unsuccessfully. In addition, following the processing performed by third party mobile wallet platform **603** after receiving third party transaction data **613**, the third party mobile wallet platform **603** may provide a commission or transaction fee **616** to cloud-based transaction platform **601**.

In a further example, mobile wallet platform **601** may process the transaction internally within cloud-based transaction platform **601**. Specifically, cloud-based transaction platform **601** may process a transaction using a third party mobile wallet entirely within cloud-based transaction platform **601**.

Once processing of the transaction is complete, cloud-based transaction platform **601** may communicate with agent terminal **602** by sending confirmation data **617** indicating information such as whether the transaction was successful or not. Also following processing of the transaction, mobile wallet platform may send customer notification **618** through an appropriate channel such as to the customer's mobile phone **619**. For example, customer notification **618** may be sent using the notification services **102** and notification channels **112** (e.g. SMPP, SMTP, voice) of FIG. **1**.

With reference now to FIGS. **2**, **6** and **7**, the cloud-based transaction system **210** receives communication **226** from an agent terminal **223** over a communication channel connected to the cloud-based transaction platform **210/601** (act **710**). The agent communication indicates that a customer **222/205** desires to perform a mobile wallet transaction using their third party mobile wallet **207**. The cloud-based transaction system **210** sends the agent communication to a third party mobile wallet platform **603** (act **720**). The cloud-based transaction system **210** then receives communication **611** from the third party mobile wallet platform confirming processing of the transaction **612** (act **730**) and sends communication **617** to the agent terminal **602** over communication channels **111** connected to the cloud-based transaction platform indicating confirmation of the processing of the transaction (act **740**).

As mentioned above, multiple different types of transactions may be performed using the infrastructure provided by the cloud-based transaction system. The transactions may be a performed not only by a first customer that uses a first mobile wallet provider, but also by a second, different customer using a second, different third party mobile wallet provider. The third party mobile wallet platform may use a third party processor to perform (at least parts of) the transaction. The customer may be notified of confirmation of the processing of the transaction using the third party mobile wallet over various communication channels connected to the cloud-based transaction platform. In some cases, each third party mobile wallet provider has their own point of sale (POS) processing system **230**. The third party mobile wallet providers' POS processing systems may communicate with each other using the cloud-based transaction platform to process the transaction.

One of the transactions made possible by the cloud-based transaction platform **601** is depositing funds into a third party mobile wallet owned by an entity different than the customer. The cloud-based transaction system may receive a communication **226** from the agent terminal **223** over a communication channel connected to the cloud-based transaction platform. The agent communication indicates that the customer desires to deposit a specified amount of funds into their third party mobile wallet **605**. The cloud-based transaction system may then credit the third party mobile wallet with the specified amount of funds.

Another transaction provided by the cloud-based transaction platform **601** is withdrawing funds from a third party mobile wallet owned by an entity different than the customer. The cloud-based transaction platform receives communication **208** from the customer **205** indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet. The cloud-based transaction platform **601** returns a secure, perishable withdrawal code to the customer over at least one of the communication channels connected to the cloud-based transaction platform. It also receives communication from the agent terminal **223** indicating that the withdrawal code has been presented to an agent and debits the third party mobile wallet by the specified amount of funds.

Another transaction provided by the cloud-based transaction platform **601** is transferring money from a third party mobile wallet within the cloud-based transaction platform to a recipient at a second third party mobile wallet provided by a second mobile wallet provider. In this transaction, the platform **601** receives a customer communication **208** indicating that a customer **205** desires to transfer a specified amount of funds to a specified recipient using a specified payment method from the third party mobile wallet **606**. The cloud-based transaction platform debits the third party mobile wallet by the specified amount of funds and transfers the specified amount of funds from the cloud-based transaction platform to the second different third party mobile wallet platform for delivery to the specified recipient. The specified amount of funds is then transferred to the second third party mobile wallet platform.

Yet another transaction provided by the cloud-based transaction platform **601** is making a purchase from a third party mobile wallet managed by a third party mobile wallet platform. In this transaction, the cloud-based transaction platform receives communication **208** from the customer **205** indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from the customer's third party mobile wallet **606**. The cloud-based transaction platform returns a secure, perishable purchase code to the customer, receives communication **226** from the agent terminal **223** indicating that the purchase code has been presented to an agent, and debits the customer's third party mobile wallet by the specified amount of funds.

In another embodiment, as shown in FIG. **8**, a cloud-based transaction system performs or facilitates a transaction using a third party point of sale (POS) system. The cloud-based transaction system receives communication **226** from a specified POS system **224** implemented at an agent terminal **223** over a communication channels **111** connected to the cloud-based transaction platform **210** (act **810**). The POS communication indicates that a customer **205** has initiated a mobile wallet transaction using their third party mobile wallet **207**. The cloud-based transaction system sends the POS communication to a corresponding third party POS transaction processing system **230** that has been established to process POS transactions from the specified POS system (act **820**). The cloud-based transaction system then receives communication from the third party POS transaction processing system **230** confirming processing of the transaction (act **830**) and sends communication to the specified POS system **224** implemented at the agent terminal **223** indicating confirmation of the processing of the transaction (act **840**).

In some cases, transaction fees or commissions **616** may be paid by the third party mobile wallet platform to the cloud-based transaction platform for facilitating the transaction. One of the transactions allowed by the cloud-based transaction system is depositing funds into a third party mobile wallet provided by a third party mobile wallet provider. In this transaction, the cloud-based transaction platform **210** receives communication **226** from a specified POS system **224** implemented at the agent terminal **223** over a communication channels **111** connected to the cloud-based transaction platform. The POS communication indicates that the customer **205/222** desires to deposit a specified amount of funds into the third party mobile wallet **606** provided by the third party mobile wallet provider. The cloud-based transaction system validates the status of the third party mobile wallet provided by the third party mobile wallet provider, determines if the specified POS system implemented at the agent terminal is authorized to deposit money, performs a limit check or a velocity check on the third party mobile wallet provided by the third party mobile wallet provider, credits the third party mobile wallet provided by the third party mobile wallet provider with the specified amount of funds, returns a notification to the specified POS system implemented at the agent terminal confirming the deposit and notifies the customer that the specified amount of funds were deposited in the third party mobile wallet provided by the third party mobile wallet provider over a communication channel connected to the cloud-based transaction platform **210**.

Another transaction provided by the cloud-based transaction platform **210** is withdrawing funds from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform **210** receives communication **208** from a customer **205** indicating that the customer desires to withdraw a specified amount of funds from the third party mobile wallet **606** provided by the third party mobile wallet provider. The cloud-based transaction platform **210** validates the status of the third party mobile wallet provided by the third party mobile wallet provider, determines if the balance of the third party mobile wallet provided by the third party mobile wallet provider is sufficient to accommodate the requested withdrawal for the specified amount of funds, performs a limit check and/or a velocity check on the third party mobile wallet, returns a secure, perishable withdrawal code to the customer over a communication channel **111** connected to the cloud-based transaction platform, receives subsequent POS communication **226** indicating that the withdrawal code has been presented to an agent (e.g. at agent terminal **223**), debits the third party mobile wallet provided by the third party mobile wallet provider by the specified amount of funds, returns a notification to the POS system at the agent terminal confirming the withdrawal and notifies the customer **205** (e.g. in confirmation **617**) that the specified amount of funds were withdrawn from the third party mobile wallet.

In yet another transaction provided by the cloud-based transaction platform, money is transferred using a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction platform **210** receives customer communication **208** indicating that the customer **205** desires to transfer a specified amount of funds to a specified recipient having a third party mobile wallet **606**, where the transfer uses a specified payment method from the customer's third party mobile wallet at the cloud-based transaction platform **210**. The cloud-based transaction platform validates the status of the specified payment method, performs a limit check and/or a velocity check on the specified payment method, performs a check on the specified recipient having a third party mobile wallet to comply with the office of foreign assets control, debits the customer's mobile wallet at the cloud-based transaction platform by the specified amount of funds, transfers the specified amount of funds to third party mobile wallet provider for delivery to the third party mobile wallet of the specified recipient over a communication channel connected between the cloud-based transaction platform and the third party mobile wallet provider, and notifies the customer that the specified amount of funds was transferred to the specified recipient.

In another transaction provided by the cloud-based transaction platform **210**, a purchase is made from a third party mobile wallet provided by a third party mobile wallet provider. In this transaction, the cloud-based transaction system receives communication **208** from the customer **205** indicating that the customer desires to purchase an item for a specified amount of funds using a specified payment method from the customer's third party mobile wallet **606**. The cloud-based transaction system returns a secure, perishable purchase code to the customer, receives subsequent agent terminal communication indicating that the purchase code has been presented to an agent, validates the status of the specified payment method, determines if the specified payment method can accommodate a purchase for the specified amount, performs a limit check and/or a velocity check on the specified payment method, debits the customer's third party mobile wallet by the specified amount of funds by sending communication to the third party mobile wallet provider, returns a notification to the POS system at the agent terminal authorizing the purchase and sends a receipt to the customer over at least one of the plurality of communication channels connected to the cloud-based transaction platform.

FIG. **9** describes a further embodiment in which a cloud-based transaction platform facilitates making a purchase from a third party mobile wallet provided by a third party mobile wallet provider. The cloud-based transaction system **210** receives communication **208** from a customer **205** over a communication channel connected to the cloud-based transaction platform (act **910**). The customer communication indicating that a customer desires to purchase an item for a specified amount of funds using a specified payment method indicated by the customer's third party mobile wallet **606**. The cloud-based transaction system returns a secure, perishable purchase code to the customer (act **920**) and receives communication from an agent terminal **223**

over at least one of the communication channels connected to the cloud-based transaction platform indicating that the purchase code has been presented to an agent (act **930**). The cloud-based transaction system **210** then debits the customer's third party mobile wallet **606** by the specified amount of funds (act **940**).

Substantially any item may be purchased using this transaction technique including items provided directly by the cloud-based transaction system, or items provided by third party retailers through the cloud-based transaction system. These items may include health care services, physical, shippable items, music, games, movies or any other digital or downloadable content.

Embodiments of the invention can adhere to Know Your Customer (KYC) rules in the United States by performing Customer Identification Program (CIP) checks as required by the Bank Secrecy Act and U.S. PATRIOT Act. A minimum amount of information can be gathered about a customer, such as, for example, First Name, Last Name, Date of Birth, Government ID Type, Government ID Number, Address. The CIP processes are designed to validate customer identity against government blacklists and assist in the prevention of money laundering and terrorist financing. A combination of non-documentary and documentary verification can be used to ensure beyond a reasonable doubt the identity of the customer.

Non-Documentary Verification can occur through the presentment of the information that was collected from the user to an external third party, such as, for example, Lexis Nexis. Documentary Verification can occur if non-documentary verification fails, then the user is asked to present an unexpired government ID. Various differ forms of identification including Driver's license, Passport, Alien identification (e.g., green card or work visa), and Mexican Consular identification card, can be accepted.

Embodiments of the invention can perform Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) checks. AML and CFT checks can be performed using transaction monitoring methods to flag names and suspicious transactions for further investigation. The mobile wallet platform can perform AML and CFT checks on all electronic financial transactions to ensure that electronic funds are not being used for money laundering or terrorism. Transaction limits can be placed on user accounts. The transaction limits are fully configurable for each particular use case, channel and payment method that allows maximum flexibility to restrict higher risk use cases. Velocity checks can also be performed. Velocity Checks ensure that subscribers are not abusing the mobile wallet platform within the allowable limits.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed:

1. A computing system for facilitating management of a mobile wallet, comprising:

one or more processors;

system memory;

an integration tier configured to manage mobile wallet sessions with a mobile device and including web services communication mechanisms for interfacing with a mobile wallet application and a plurality of different device types over a plurality of different communication channels, the integration tier being configured to receive binary and text messages from a mobile device;

a notification services engine configured to interface with the integration tier and to send a plurality of corresponding different types of messages over the different communication channels to different devices, including a customer's mobile device, to interface with a mobile wallet application installed on the customer's mobile device;

service connectors that are each configured to connect the computing system to a different third party system;

a payment handler that exposes a common API for interacting with different payment processors;

a security services engine that performs subscriber authentication utilizing a database-based Access Control List (ACL);

a rules engine configured to enforce constraints on financial transactions performed with the mobile wallet application, the mobile wallet application being associated with a mobile wallet account; and

one or more computer-readable storage media having stored thereon computer-executable instructions which are executable by the one or more processors, to facilitate a transaction for a customer using the mobile wallet by causing the computing system to perform at least the following:

receive communication from the customer over one of the plurality of channels connected to the computing system, the customer communication indicating that the customer desires to purchase an item at an agent terminal for a specified amount of funds using a specified payment method from a mobile wallet;

return a secure, perishable purchase code to the customer over at least one of the plurality of channels connected to the computing system;

receive communication from the agent terminal over at least one of the plurality of channels connected to the computing system, the agent terminal communication indicating that the purchase code has been presented to an agent;

debit the mobile wallet by the specified amount of funds;

credit an agent account by the specified amount of funds; and

after selecting a particular channel included in the plurality of channels, send a notification communication from the computing system to the agent terminal using the particular channel, which is connected to the computing system, the notification communication providing a notification indicating confirmation of the processing of the transaction.

2. The computing system of claim **1**, wherein the computing system notifies the customer of confirmation of the processing of the transaction using the mobile wallet over at least one of the plurality of communication channels connected to the computing system.

3. The computing system of claim **1**, wherein the mobile wallet is a native mobile wallet.

4. The computing system of claim **1**, wherein the mobile wallet is a third party mobile wallet.

5. The computing system of claim **4**, wherein the third party mobile wallet is provided by a third party mobile wallet provider.

6. The computing system of claim **5**, wherein each third party mobile wallet provider has their own point of sale (POS) processing system.

7. The computing system of claim 1, wherein the customer communication is initiated by the customer through the mobile wallet application installed on a device of the customer.

8. A computer-implemented method of facilitating management of a mobile wallet, the computer-implemented method being performed by one or more hardware processors executing computer executable instructions for the computer-implemented method, and the computer-implemented method comprising:

a computer system receiving communication from a customer over one of a plurality of channels connected to the computer system, the customer communication indicating that the customer desires to purchase an item at an agent terminal for a specified amount of funds using a specified payment method from a mobile wallet;

returning a secure, perishable purchase code to the customer over at least one of the plurality of channels connected to the computer system;

receiving communication from the agent terminal over at least one of the plurality of channels connected to the computer system, the agent terminal communication indicating that the purchase code has been presented to an agent;

debiting the mobile wallet by the specified amount of funds;

crediting an agent account by the specified amount of funds; and

after selecting a particular channel included in the plurality of channels, sending a notification communication from the computer system to the agent terminal using the particular channel, which is connected to the computer system, the notification communication providing a notification indicating confirmation of the processing of the transaction, wherein the computer system includes at least the following:

one or more processors;

system memory;

an integration tier configured to manage mobile wallet sessions with a mobile device on which a mobile wallet application is installed and including web services communication mechanisms for interfacing with the mobile wallet application and a plurality of different device types over the plurality of different communication channels, the integration tier being configured to receive binary and text messages from the mobile device;

a notification services engine configured to interface with the integration tier and to send a plurality of corresponding different types of messages over the different communication channels to different devices, including the mobile device, to interface with the mobile wallet application installed on the mobile device;

service connectors that are each configured to connect the computer system to a different third party system, each of the service connectors being configured as a separate module for integrating a corresponding external service to the computer system;

a payment handler that exposes a common API for interacting with different payment processors;

a security services engine that performs subscriber authentication utilizing a database-based Access Control List (ACL); and

a rules engine configured to enforce constraints on financial transactions performed with the mobile wallet application.

9. The method of claim 8, further comprising notifying the customer of confirmation of the processing of the transaction using the mobile wallet over at least one of the plurality of communication channels connected to the computer system.

10. The method of claim 8, wherein the mobile wallet is a native mobile wallet.

11. The method of claim 8, wherein the mobile wallet is a third party mobile wallet.

12. The method of claim 11, wherein the third party mobile wallet is provided by a third party mobile wallet provider.

13. The method of claim 12, wherein each third party mobile wallet provider has their own point of sale (POS) processing system.

14. The method of claim 13, wherein the third party mobile wallet providers' POS processing systems communicate with each other using the computer system to process the transaction.

15. The method of claim 8, wherein the customer communication is initiated by the customer through the mobile wallet application installed on a device of the customer.

16. A computer program product comprising one or more hardware storage devices having stored thereon computer-executable instructions that are executable by one or more processors of a computer system and that configure the computer system to facilitate management of a mobile wallet, including computer-executable instructions that configure the computer system to perform at least the following:

receive communication from a customer over one of a plurality of communication channels connected to the computing system, the customer communication indicating that the customer desires to purchase an item at an agent terminal for a specified amount of funds using a specified payment method from a mobile wallet;

return a secure, perishable purchase code to the customer over at least one of the plurality of channels connected to the computing system;

receive communication from the agent terminal over at least one of the plurality of channels connected to the computing system, the agent terminal communication indicating that the purchase code has been presented to an agent;

debit the mobile wallet by the specified amount of funds;

credit an agent account by the specified amount of funds; and

after selecting a particular channel included in the plurality of channels, send a notification communication from the computer system to the agent terminal using the particular channel, which is connected to the computer system, the notification communication providing a notification indicating confirmation of the processing of the transaction, wherein the computer system includes at least the following:

one or more processors;

system memory;

an integration tier configured to manage mobile wallet sessions with a mobile device on which a mobile wallet application is installed and including web services communication mechanisms for interfacing with the mobile wallet application and a plurality of different device types over the plurality of different communication channels, the integration tier being configured to receive binary and text messages from the mobile device;

a notification services engine configured to interface with the integration tier and to send a plurality of corresponding different types of messages over the different

communication channels to different devices, including the mobile device, to interface with the mobile wallet application;

service connectors that are each configured to connect the computer system to a different third party system, each of the service connectors being configured as a separate module for integrating a corresponding external service to the computer system;

a payment handler that exposes a common API for interacting with different payment processors;

a security services engine that performs subscriber authentication utilizing a database-based Access Control List (ACL); and

a rules engine configured to enforce constraints on financial transactions performed with the mobile wallet application.

17. The computer program product of claim **16**, wherein the computer system notifies the customer of confirmation of the processing of the transaction using the mobile wallet over at least one of the plurality of communication channels connected to the computing system.

18. The computer program product of claim **16**, wherein the mobile wallet is a native mobile wallet.

19. The computer program product of claim **16**, wherein the mobile wallet is a third party mobile wallet.

20. The computer program product of claim **16**, wherein the customer communication is initiated by the customer through the mobile wallet application installed on a device of the customer.

21. A computing system for facilitating management of a mobile wallet, including:

one or more processors;

system memory;

an integration tier configured to manage mobile wallet sessions with a mobile device and including web services communication mechanisms for interfacing with a mobile wallet application installed on computer readable media executable by the mobile device as well as with a plurality of different device types over a plurality of different communication channels, the integration tier being configured to receive digital communications from the mobile device;

a notification services engine configured to interface with the integration tier and to send digital messages over the different communication channels to different devices, including the mobile device, to interface with the mobile wallet application installed on the computer readable media executable by the mobile device;

service connectors that are each configured to connect the computing system to a different third party system, each of the service connectors being configured as a separate module for integrating a corresponding external service to the computing system;

a payment handler that exposes a common API for interacting with different payment processors;

a security services engine that performs subscriber authentication utilizing a database-based Access Control List (ACL);

a rules engine configured to enforce constraints on financial transactions performed with the mobile wallet application, the mobile wallet application being associated with a mobile wallet account; and

one or more computer-readable storage media having stored thereon computer-executable instructions that are executable by the one or more processors to cause the computing system to perform a transaction for a customer using the mobile wallet which is owned by another entity than the customer, comprising the following:

the computing system receiving communication from an agent terminal over one of a plurality of communication channels connected to a cloud-based transaction platform, the communication from the agent terminal indicating that a customer desires to perform a transaction comprising a mobile wallet transaction using a third party mobile wallet, wherein the mobile wallet transaction comprises at least one of a mobile wallet transfer in which funds are transferred from the mobile wallet of the customer to a third party mobile wallet, a mobile wallet withdrawal in which funds are withdrawn from the third party mobile wallet and provided to the customer, or a mobile wallet deposit in which funds are deposited into the third party mobile wallet;

the computing system sending the communication from the agent terminal to the third party mobile wallet platform;

the computing system determining whether the mobile wallet transaction comprises the mobile wallet withdrawal and when the mobile wallet transaction is determined to comprise the mobile wallet withdrawal, generating and providing a perishable withdrawal code to the customer, which is presented to the agent terminal to facilitate processing of the mobile wallet withdrawal;

the computing system receiving communication from the third party mobile wallet platform confirming processing of the transaction, the transaction comprising at least one of the mobile wallet transfer, the mobile wallet withdrawal or the mobile wallet deposit; and

after selecting a particular communication channel included in the plurality of communication channels, the computing system sending a notification communication to the agent terminal using the particular communication channel, which is connected to the cloud-based transaction platform, the notification communication to the agent terminal providing a notification indicating confirmation of the processing of the transaction.

22. A computing system for facilitating management of a mobile wallet, including:

one or more processors;

system memory;

an integration tier configured to manage mobile wallet sessions with a mobile device and including web services communication mechanisms for interfacing with a mobile wallet application installed on computer readable media executable by the mobile device as well as with a plurality of different device types over a plurality of different communication channels, the integration tier being configured to receive digital communications from the mobile device;

a notification services engine configured to interface with the integration tier and to send digital messages over the different communication channels to different devices, including the mobile device, to interface with the mobile wallet application installed on the computer readable media executable by the mobile device;

service connectors that are each configured to connect the computing system to a different third party system, each of the service connectors being configured as a separate module for integrating a corresponding external service to the computing system;

a payment handler that exposes a common API for interacting with different payment processors;

a security services engine that performs subscriber authentication utilizing a database-based Access Control List (ACL);

a rules engine configured to enforce constraints on financial transactions performed with the mobile wallet application, the mobile wallet application being associated with a mobile wallet account; and

one or more computer-readable storage media having stored thereon computer-executable instructions that are executable by the one or more processors to cause the computing system to perform a transaction for a customer using the mobile wallet which is owned by another entity than the customer, comprising the following:

the computing system receiving communication from an agent terminal over one of a plurality of communication channels connected to a cloud-based transaction platform, the communication from the agent terminal indicating that a customer desires to perform a transaction comprising a mobile wallet transaction using a third party mobile wallet, wherein the mobile wallet transaction comprises digitally transferring of funds for a purchase;

the computing system sending the communication from the agent terminal to the third party mobile wallet platform;

the computing system, upon determining that the mobile wallet transaction comprises the the digital transfer of funds, generating and providing a perishable withdrawal code to the customer, which is presented to the agent terminal to facilitate processing of the mobile wallet withdrawal;

the computing system receiving communication from the third party mobile wallet platform confirming processing of the transaction, the transaction comprising at least one of the mobile wallet transfer, the mobile wallet withdrawal or the mobile wallet deposit; and

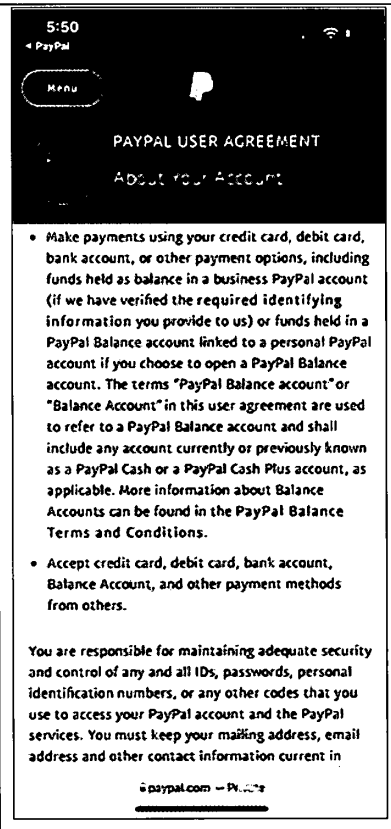
after selecting a particular communication channel included in the plurality of communication channels, the computing system sending a notification communication to the agent terminal using the particular communication channel, which is connected to the cloud-based transaction platform, the notification communication to the agent terminal providing a notification indicating confirmation of the processing of the transaction.

* * * * *

Exhibit J
PayPal Infringement Chart for
U.S. Patent No. 10,438,196

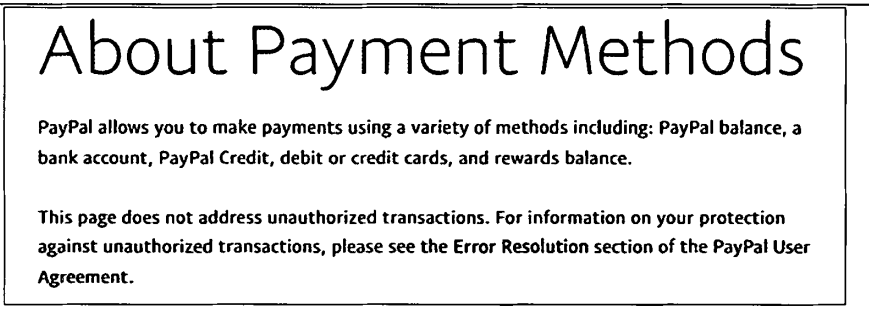
U.S. Patent No. 10,438,196 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal System ("PayPal System")**
1. A computing system for facilitating management of a mobile wallet, comprising:	Upon information and belief, the PayPal System facilitates the management of the PayPal Mobile Wallet. SEND AND REQUEST MONEY FOR FREE • When funded by a bank account or with your PayPal balance, it's free and secure to send money or ask for it back from friends and family in the US. • Just type a name, email or phone number and PayPal will find the right person for you if they have an account. • Request money quickly and securely from friends or family and personalize your payments with animations, stickers, emojis and more. See https://apps.apple.com/app/id283646709?mt=8 (last accessed on February 25, 2022).

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 10,438,196 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal System ("PayPal System")**
	 See PayPal User Agreement on PayPal Mobile App (above).

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 365 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 10,438,196 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal System ("PayPal System")**
	 See https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022).
1[a] and 1[b] one or more processors; system memory;	On information and belief the PayPal System includes numerous servers and processors as well as system memory. See Preamble.
1[c] an integration tier configured to manage mobile wallet sessions with a mobile device and including web services communication mechanisms for interfacing with a mobile wallet application and a plurality of different device types over a plurality of different communication channels, the	Upon information and belief, the PayPal System includes an integration tier. The integration tier is configured to manage mobile wallet sessions and includes web services communication mechanisms for interfacing with a mobile wallet application on a mobile device over a plurality of different device types and a plurality of different communication channels. The integration tier, for example, handles communications to/from mobile wallets on different mobile phones (e.g. Apple, Google, and/or Android) that use the PayPal System. On information and belief, the PayPal System is capable of receiving binary and text messages from a mobile device through the receipt of data and text from a mobile device.

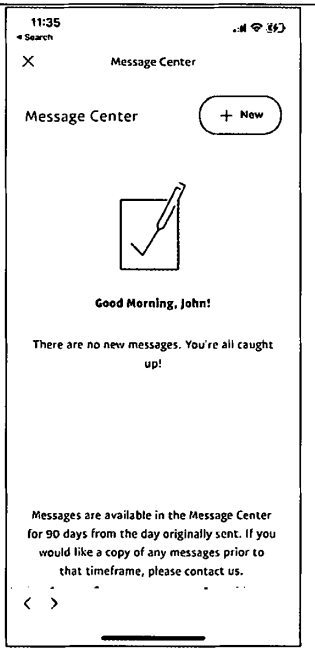
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 366 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 10,438,196 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal System ("PayPal System")**
integration tier being configured to receive binary and text messages from a mobile device;	 We have versions of our app for iOS, Android, and Windows. In a few moments you can log on to PayPal, check your balance, pay bills, and more. It is easy, fast, and secure. With PayPal there are no borders. Download Now: iPhone | Android https://www.paypal.com/bs/webapps/mpp/shop/apps

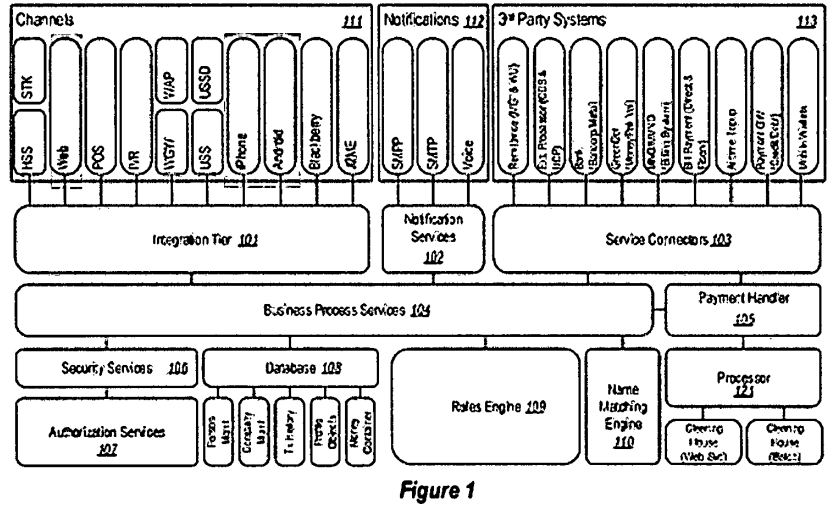
PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 367 of 381

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 10,438,196 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal System ("PayPal System")**
	 *See* Screenshots of PayPal Mobile apps (above) showing ability to send/receive messages.

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 368 of 381

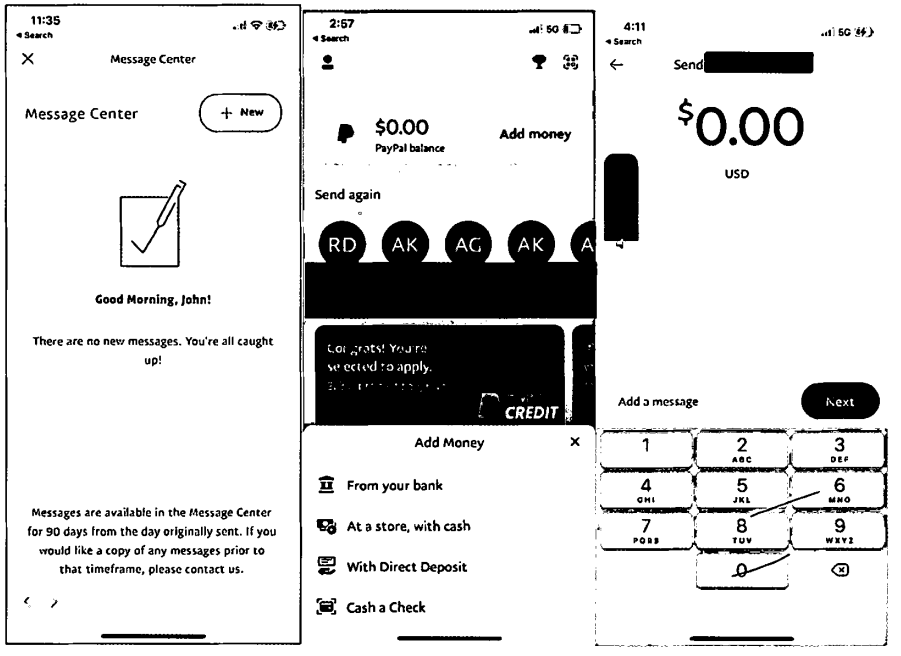
PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

U.S. Patent No. 10,438,196 (Claim 1)	
Claims	**Accused Instrumentalities –PayPal System ("PayPal System")**
	 **Figure 1** *See e.g.* '386 Patent Figure 1.

U.S. Patent Feb. 13, 2018 Sheet 1 of 46 US 9,892,386 B2

PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 369 of 381

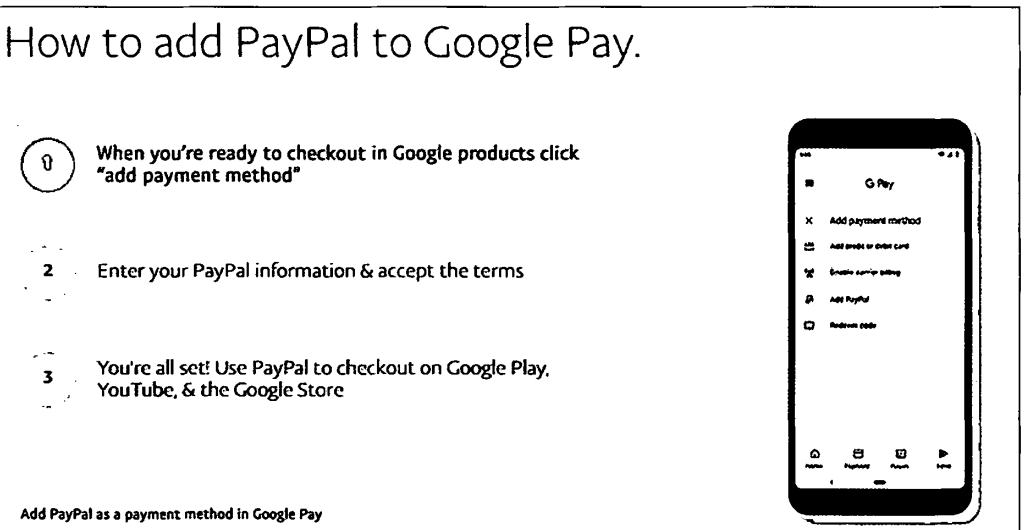
PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

1[d] a notification services engine configured to interface with the integration tier and to send a plurality of corresponding different types of messages over the different communication channels to different devices, including a customer's mobile device, to interface with a mobile wallet application installed on the customer's mobile device;	Upon information and belief, the PayPal System includes notification service engine that is configured to interface with the integration tier and to send digital messages over the various communication channels to different devices, including the mobile device. The notification services engine is configured to interface with the integration tier and to send different types of messages over the various communication channels to different devices, including the mobile device and to interface with the mobile wallet application installed on the hardware SIM card.  *See* Screenshots of PayPal and Venmo mobile app (above) showing ability to send/receive messages.

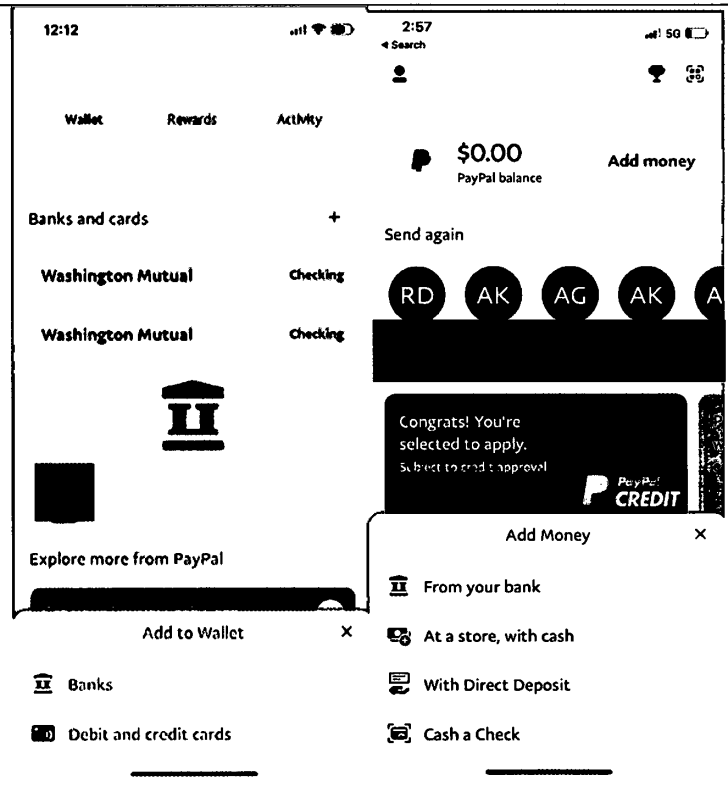
PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

1[e] service connectors that are each configured to connect the computing system to a different third party system,	On information and belief, the PayPal System includes service connectors that are configured to connect the PayPal system to a different third-party system. The service connectors are configured to connect the computing system to a different third-party system, including for example mobile wallets (*e.g.* Samsung Pay and Android Pay) that provide additional mobile wallet capabilities.  https://www.paypal.com/bs/webapps/mpp/shop/apps (last accessed on February 25, 2022). How can I add PayPal to Samsung Pay? **You can add PayPal to Samsung Pay through the Samsung Pay app. Simply, tap the PayPal (Add PayPal) icon, then Add your PayPal, then log in to your PayPal account. You will be able to select a top up amount and a backup funding instrument for the top up. At this time Samsung Pay is only available to US customers.** *See* https://www.paypal.com/us/webapps/mpp/samsung-pay (last accessed on February 25, 2022).

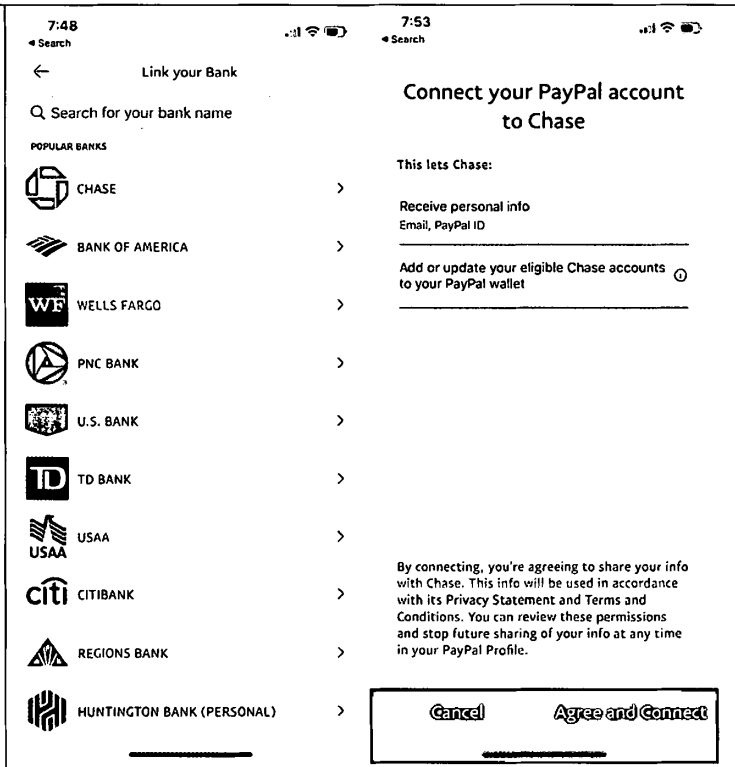
PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

	 https://www.paypal.com/us/webapps/mpp/google-pay-paypal (last accessed on February 25, 2022).
1[f] a payment handler that exposes a common API for interacting with different payment processors;	Upon information and belief, the PayPal System, includes a payment handler which exposes a common APIs for interacting with different payment processors. Upon information and belief, the common API is used to interface with different payment processors.

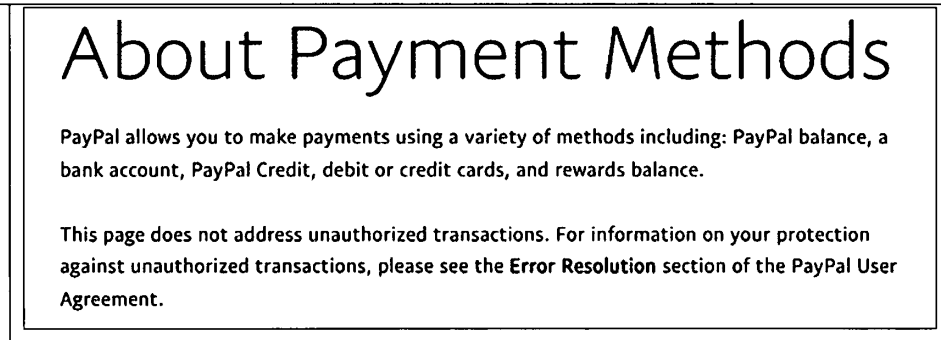
PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

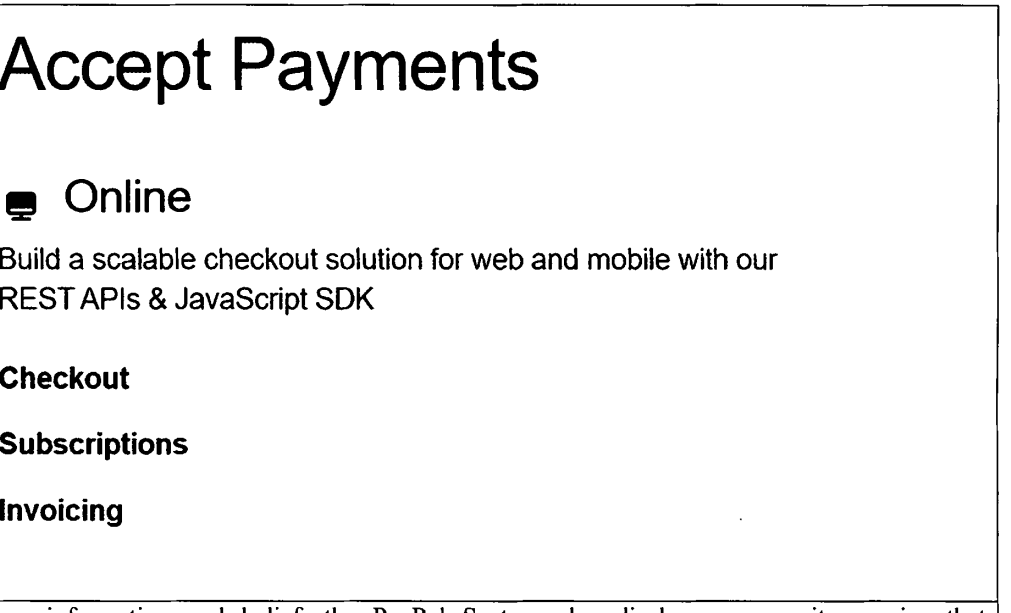


PayPal - Exhibit 1010
PayPal v. Fintiv - IPR2023-00744
Page 373 of 381



See Screenshot of PayPal Mobile Application allowing users to link credit card and/or bank accounts.

	 *See* https://www.paypal.com/us/webapps/mpp/popup/about-payment-methods (last accessed on February 25, 2022). Upon information and belief, the PayPal System provides REST APIs for new integrations. These APIs use HTTP methods, a RESTful endpoint structure, the OAuth 2.0 protocol, and JSON-formatted payloads. The REST APIs can be used to incorporate the PayPal System's functionality into a user's web and mobile apps. Standard PayPal APIs can be accessed via the PayPal Developer Portal (*see* http://developer.paypal.com (last accessed on February 25, 2022)).

	
1[g] a security services engine that performs subscriber authentication utilizing a database-based Access Control List (ACL);	Upon information and belief, the PayPal System also discloses a security service that authenticates a subscriber utilizing a database based Accused Control List (ACL). On information and belief the authentication is performed based on user password authentication and or based on device. Upon information and belief, the PayPal System includes an access-control list (ACL) such as a list of permissions associated with system resources. A user can manually grant the PayPal System permissions to a third party to access specific information in the user's account at the PayPal system and perform PayPal API operations on the user's behalf. For example, if the user is integrating with a third-party shopping cart, the cart owner needs permission to the user's PayPal account to perform specific operations on behalf of the user. Upon information and belief, by way of example, the PayPal systems utilizes OAuth 2.0 protocol to provide authenticated and/or authorized access to various protected resources. In particular,

	OAuth 2.0 scopes are used to specify or limit the type of access (i.e., ACL) that is associated with a granted access token. *See* https://oauth.net/2/scope/ (last accessed on February 25, 2022); https://developer.paypal.com/api/rest/ (last accessed on February 25, 2022). **Why are limitations placed on an account?** There can be several reasons for an account limitation: • *An unauthorized person may be using your account.* If PayPal believes someone is using your account without your knowledge, the account could be limited to protect you from fraudulent charges while PayPal investigates the suspicious transactions. Similar steps may be taken if your debit or credit card issuer or bank notifies PayPal that someone has used your card or bank account without permission. • *The account is out of compliance with regulatory requirements.* Limitations can also be placed on an account that has been found to be out of compliance with regulatory requirements. For example, if you receive donations, you're required to provide documents confirming you're a registered nonprofit organization. PayPal may limit your account while you gather those documents or while we're working with you to satisfy any other regulatory requirements. The same is true if you don't follow PayPal's **Acceptable Use Policy**—selling banned items, such as prescription drugs or guns, for example. • *Your account has a high number of claims and chargebacks.* When there's a high number of **buyer claims and chargebacks** to your account, we may review your account. While we're reviewing, you may experience an account limitation. • *Sudden, rapid changes in what or how much you sell.* If you start to sell an entirely new type of product, specifically higher-end items like jewelry; or there's a rapid increase in sales volume, your account may be limited while PayPal reviews it. *See* https://www.paypal.com/us/brc/article/understanding-account-limitations (last accessed on February 25, 2022).
1[h] a rules engine configured to enforce constraints on financial transactions performed with the mobile wallet application, the mobile wallet	Upon information and belief, the PayPal System, includes a rule engine that track financial transactions where the mobile wallet application is associated with a mobile wallet account.

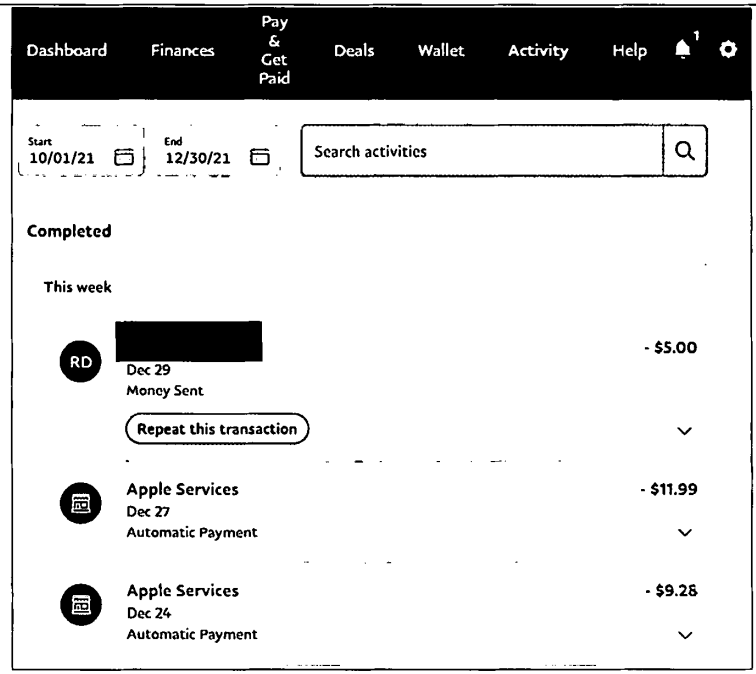
application being associated with a mobile wallet account; and	**Why are limitations placed on an account?** **There can be several reasons for an account limitation:** • ***An unauthorized person may be using your account.*** **If PayPal believes someone is using your account without your knowledge, the account could be limited to protect you from fraudulent charges while PayPal investigates the suspicious transactions. Similar steps may be taken if your debit or credit card issuer or bank notifies PayPal that someone has used your card or bank account without permission.** • ***The account is out of compliance with regulatory requirements.*** **Limitations can also be placed on an account that has been found to be out of compliance with regulatory requirements. For example, if you receive donations, you're required to provide documents confirming you're a registered nonprofit organization. PayPal may limit your account while you gather those documents or while we're working with you to satisfy any other regulatory requirements. The same is true if you don't follow PayPal's Acceptable Use Policy—selling banned items, such as prescription drugs or guns, for example.** • ***Your account has a high number of claims and chargebacks.*** **When there's a high number of buyer claims and chargebacks to your account, we may review your account. While we're reviewing, you may experience an account limitation.** • ***Sudden, rapid changes in what or how much you sell.*** **If you start to sell an entirely new type of product, specifically higher-end items like jewelry; or there's a rapid increase in sales volume, your account may be limited while PayPal reviews it.** *See* https://www.paypal.com/us/brc/article/understanding-account-limitations (last accessed on February 25, 2022).
1[i] and [j] one or more computer-readable storage media having stored thereon computer-executable instructions which are executable by the one or more processors, to facilitate a transaction for a customer using the mobile wallet by causing the computing system to perform at least the following:	On information and belief, the PayPal system is capable of facilitating a transaction through the PayPal System by causing receiving a communication from the customer indicating the customer desires topurchase an item at a terminal for a specified amount of funds using a Payment method froma mobile wallet. On information and belief, the PayPal system linked with other mobile wallets can initiate payment as a result of a transaction made by a user using a linked mobile wallet account. On information and belief, the funds in the PayPal System and through the third-party mobile wallet are used to perform a transaction. Upon information and belief, the transaction is reflected at both the PayPal System and the third-party mobile application.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

1[k] receive communication from the customer over one of the plurality of channels connected to the computing system, the customer communication indicating that the customer desires to purchase an item at an agent terminal for a specified amount of funds using a specified payment method from a mobile wallet;	How can I add PayPal to Samsung Pay? **You can add PayPal to Samsung Pay through the Samsung Pay app. Simply, tap the PayPal (Add PayPal) icon, then Add your PayPal, then log in to your PayPal account. You will be able to select a top up amount and a backup funding instrument for the top up. At this time Samsung Pay is only available to US customers.** *See* https://www.paypal.com/us/webapps/mpp/samsung-pay (last accessed on February 25, 2022). Add or remove a PayPal account You can add a PayPal account to Google Pay on an Android phone. You can use it in select countries to pay for some Google products and in participating stores, apps, and websites. Add a PayPal account 1. On your phone, open the Google Pay app. 2. At the top, tap the card button. 3. Tap Add a payment method. You might need to swipe all the way left to find this option. 4. Tap PayPal. 5. To link your PayPal account, follow the on-screen instructions. *See* https://support.google.com/googlepay/answer/10212164?hl=en (last accessed on February 25, 2022).

	PayPal recently migrated the horizontally scalable applications of its payment platform to Google Cloud—a significant shift in strategy to cloud-based transactions—to help ensure easy and reliable services for its customers. https://cloud.google.com/customers/paypal (last accessed on February 25, 2022). 6. Your Payment Obligation When you use PayPal in Google Pay for a transaction, i.e. give a payment order, you are obliged to reimburse the transaction amount to us. To this end, you authorize us to debit the respective amount from your PayPal balance. To the extent that there is no or an insufficient balance available to fund such transaction, you hereby authorize PayPal to draw the amount from your bank account via direct debit, to credit this amount in your PayPal balance and to use it immediately for the payment with PayPal in Google Pay. This means we will prioritize your PayPal balance for a payment with PayPal in Google Pay and only draw the amount from your bank account via direct debit to the extent that the balance is insufficient. https://www.paypal.com/de/webapps/mpp/ua/ppgooglepay-tnc?locale.x=en_DE#2 (last accessed on February 25, 2022).
1 [l], [m], [n], [o] return a secure, perishable purchase code to the customer over at least one of the plurality of channels connected to the computing system;	Upon information and belief, the PayPal System returns a secure, perishable purchase code to the customer over one of the channels. On information and belief, the mobile wallet is debited and the agent account is credited by the specified transaction amount. On information and belief, a notification confirming the transaction is received.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY'S WORK PRODUCT

receive communication from the agent terminal over at least one of the plurality of channels connected to the computing system, the agent terminal communication indicating that the purchase code has been presented to an agent; debit the mobile wallet by the specified amount of funds; credit an agent account by the specified amount of funds; and after selecting a particular channel included in the plurality of channels, send a notification communication from the computing system to the agent terminal using the particular channel, which is connected to the computing system, the notification communication providing a notification indicating confirmation of the processing of the transaction.	 Upon information and belief, the PayPal System utilizes perishable purchase codes such as transaction codes that expire. In particular, when a user makes a payment to a merchant with a PayPal account, the user can follow the processing of the payment through the "Status" column the account overview. First, the PayPal System places a temporary hold on the purchase amount in user's account, making it unavailable to the user. The PayPal System then allows the merchant three days to capture the payment. If the merchant doesn't collect the funds within three days, the PayPal System marks the transaction "expired" and returns the funds to the user's available balance.