(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
04 October 2018 (04.10.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/178878 A1

(51) International Patent Classification:
G06Q 20/40 (2012.01) *G07F 7/10* (2006.01)
G06Q 20/20 (2012.01) *G07F 17/00* (2006.01)
G06Q 20/32 (2012.01) *G16H 20/10* (2018.01)

(21) International Application Number:
PCT/IB2018/052102

(22) International Filing Date:
27 March 2018 (27.03.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/479,959 31 March 2017 (31.03.2017) US

(71) Applicant: **BAYER HEALTHCARE LLC** [US/US]; 100 Bayer Blvd., Whippany, New Jersey 07981 (US).

(72) Inventors: **JERSTROEM, Goeran M.**; 19 Outlook Place, Glen Ridge, New Jersey 07028 (US). **DEBIASI, Michael**; 11 E. Ash St., Basking Ridge, New Jersey 07920 (US). **KAECHELE, Felix Sebastian**; 11 Muenzstrasse, 51379 Leverkusen (DE).

(74) Agent: **SPENCE, Andrew T.**; Womble Bond Dickinson (US) LLP, Attn: Patent Docketing, P.O. Box 7037, Atlanta, Georgia 30357-0037 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: BIOMETRIC AUTHENTICATION FOR, AND SECURE ELECTRONIC TRACKING OF, RESTRICTED OVER-THE-COUNTER DRUG SALES

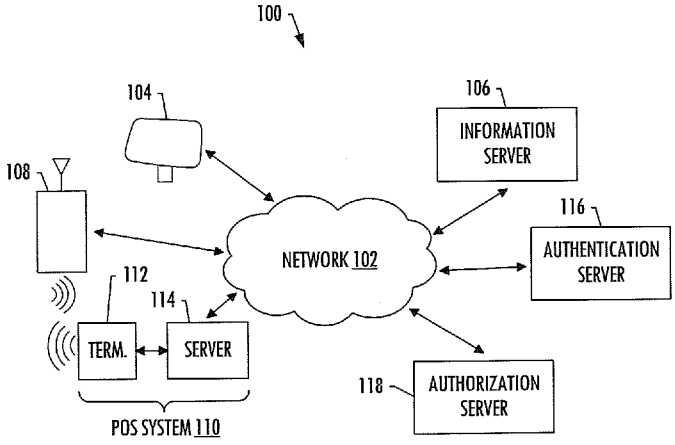

FIG. 1

(57) Abstract: A mobile device is provided that includes biometric sensor(s), and a processor that causes the biometric sensor(s) to acquire a physiological marker of a user, and identify and authenticate the user. The processor sends a message to an authentication server that indicates the user is authenticated, and receives a response from the authentication server that includes a unique authentication code. The processor receives selection of a thereby selected over-the-counter (OTC) drug, and communicates with a point-of-sale (POS) system with contactless payment capability. The processor sends a purchase message to the POS system that includes the unique authentication code, an identifier of the selected OTC drug, and payment information. And the POS system communicates with the authentication server to validate the unique authentication code, and with an authorization server to authorize payment for the selected OTC drug based on the payment information.

WO 2018/178878 A1

[Continued on next page]

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

BIOMETRIC AUTHENTICATION FOR, AND SECURE ELECTRONIC TRACKING OF, RESTRICTED OVER-THE-COUNTER DRUG SALES

TECHNOLOGICAL FIELD

The present disclosure relates generally to biometric authentication and contactless payment systems and, in particular, to biometric authentication for, and secure electronic tracking of, restricted over-the-counter drug sales.

BACKGROUND

Biometric authentication involves use of physiological markers to identify and thereby authenticate. These physiological markers include, for example, fingerprint, palm print, hand geometry, face recognition, iris recognition, retina recognition and the like. The technology is becoming more commonplace in a number of applications including contactless payment systems in which smartphones and other mobile devices use short-range communication technology to make secure payments at the point of sale. Apple Pay, Android Pay and Samsung Pay are three systems that use fingerprint authentication.

While biometric authentication and contactless payment systems have made a number of point-of-sale transactions easier and more efficient, there are a number of transactions that remain complicated. One example of a complicated point-of-sale transaction is for the sale of certain restricted over-the-counter (OTC) (i.e., non-prescription) drugs such as those drugs covered by the Combat Methamphetamine Epidemic Act of 2005 (CMEA) in the United States. The CMEA regulates products contained in certain OTC drugs including ephedrine and pseudoephedrine (PSE) because of their use in the manufacture of illegal drugs. The CMEA requires merchants to restrict public access to regulated products, verify proof of identity of all purchasers (e.g., government-issued identification), and track all purchasers and purchases.

Therefore it would be desirable to have a system and method that takes into account at least some of the issues discussed above, as well as other possible issues.

BRIEF SUMMARY

In view of the foregoing background, example implementations of the present disclosure are directed to biometric authentication and contactless payment systems and, in particular, to biometric authentication for, and secure electronic tracking of, restricted over-the-counter drug (e.g., PSE) sales.

The present disclosure thus includes, without limitation, the following example implementations.

Some example implementations provide a mobile device comprising one or more biometric sensors configured to acquire a physiological marker from which a user is identifiable and thereby authenticated; a short-range communication interface configured to implement short-range communication technology and enable contactless payment capability of the mobile device; and a processor coupled to the one or more biometric sensors and short-range communication interface, and programmed to at least: cause the one or more biometric sensors to acquire the physiological marker, and identify and authenticate the user based thereon; send a message to an authentication server that indicates the user is authenticated, and receive a

response from the authentication server that includes a unique authentication code; receive selection of a thereby selected over-the-counter (OTC) drug; and communicate with a point-of-sale (POS) system with contactless payment capability, to purchase the selected OTC drug using the short-range communication interface and the contactless payment capabilities of the mobile device and POS system, wherein the processor being programmed to communicate with the POS system includes being programmed to send a purchase message to the POS system that includes the unique authentication code, an identifier of the selected OTC drug, and payment information, the POS system being configured to communicate with the authentication server to validate the unique authentication code, and with an authorization server to authorize payment for the selected OTC drug based on the payment information.

In some example implementations of the mobile device of any preceding example implementation, or any combination of any preceding example implementations, the POS system has a known location, and the processor being programmed to authenticate the user based on the physiological marker and communicate with the POS system using the short-range communication interface locks-in the user thereby authenticated at the known location.

In some example implementations of the mobile device of any preceding example implementation, or any combination of any preceding example implementations, the authentication server is operated by a service provider, and the processor is further programmed to enable the service provider to verify an identity of the user, including the processor being programmed to at least capture data from a proof of identity of the user; and send the data to the service provider to enable the service provider to verify the identity of the user from the data, the identity of the user being verified before the authentication server is enabled to send the response that indicates the unique authentication code.

In some example implementations of the mobile device of any preceding example implementation, or any combination of any preceding example implementations, the processor is further programmed to enable the user to register an account with the service provider before the message is sent to the authentication server, and during which the processor is programmed to enable the service provider to verify the identity of the user.

Some example implementations provide apparatus configured to implement a self-service kiosk or integrated shelf dispenser, the apparatus comprising one or more biometric sensors configured to acquire a physiological marker from which a user is identifiable and thereby authenticated; and a processor coupled to the one or more biometric sensors, and programmed to at least: cause the one or more biometric sensors to acquire the physiological marker, and identify and authenticate the user based thereon; send a message to an authentication server that indicates the user is authenticated, and receive a response from the authentication server that includes a unique authentication code; receive selection of a thereby selected over-the-counter (OTC) drug; complete a purchase of the selected OTC drug, including the processor being programmed to send a purchase message to the authentication server that includes the unique authentication code, an identifier of the selected OTC drug, and payment information, the processor being programed to send the purchase message for the authentication server to validate the unique authentication code, and for the authentication server to cooperate with an authorization server to authorize payment for the selected OTC

drug based on the payment information; and receive an encrypted code to authorize release of the selected OTC drug; and a dispenser coupled to the processor and caused thereby to dispense the selected OTC drug after the purchase is completed.

In some example implementations of the apparatus of any preceding example implementation, or any combination of any preceding example implementations, the authentication server is operated by a service provider, and the processor is further programmed to enable the service provider to verify an identity of the user, including the processor being programmed to at least capture data from a proof of identity of the user; and send the data to the service provider to enable the service provider to verify the identity of the user from the data, the identity of the user being verified before the authentication server is enabled to send the response that indicates the unique authentication code.

In some example implementations of the apparatus of any preceding example implementation, or any combination of any preceding example implementations, the processor is further programmed to enable the user to register an account with the service provider before the message is sent to the authentication server, and during which the processor is programmed to enable the service provider to verify the identity of the user.

Some example implementations provide an apparatus configured to implement an authentication server, the apparatus comprising a processor and a memory storing executable instructions that in response to execution by the processor cause the apparatus to at least: receive a message related to a purchase of an over-the-counter (OTC) drug by a user, the message indicating the user is authenticated, the message being received from a mobile device, self-service kiosk or integrated shelf dispenser; send a response to the mobile device, self-service kiosk or integrated shelf dispenser, the response including a unique authentication code; receive a purchase message that includes the unique authentication code, an identifier of a selected OTC drug, and payment information, the purchase message being received from a point-of-sale (POS) system, or the self-service kiosk or integrated shelf dispenser; validate the unique authentication code; cooperate with an authorization server to authorize payment for the selected OTC drug based on the payment information; and return an encrypted code to the POS system, self-service kiosk or integrated shelf dispenser to authorize release of the selected OTC drug.

In some example implementations of the apparatus of any preceding example implementation, or any combination of any preceding example implementations, the memory stores executable instructions that in response to execution by the processor cause the apparatus to further at least electronically record a purchase transaction including the user, the selected OTC drug and a date or time of purchase of the selected OTC drug.

In some example implementations of the apparatus of any preceding example implementation, or any combination of any preceding example implementations, the purchase transaction identifies the user by the unique authentication code or a physiological marker of the user.

In some example implementations of the apparatus of any preceding example implementation, or any combination of any preceding example implementations, the apparatus being caused to electronically

record the purchase transaction includes being caused to electronically record the purchase transaction on a blockchain.

In some example implementations of the apparatus of any preceding example implementation, or any combination of any preceding example implementations, the purchase transaction identifies the user by the unique authentication code or a physiological marker of the user, and identifies the selected OTC drug by an identifier of the selected OTC drug that is unique to a unit thereof, wherein the identifier of the selected OTC drug is recorded on the blockchain during manufacturing or packaging, and the apparatus is thereafter caused to electronically record the purchase transaction including the unique authentication code or physiological marker of the user, the identifier of the selected OTC drug, and the date or time of purchase.

Some example implementations provide a method comprising acquiring, via one or more biometric sensors of a mobile device, a physiological marker from which a user is identifiable and thereby authenticated; and at the mobile device; identifying and authenticating the user based on the physiological marker; sending a message to an authentication server that indicates the user is authenticated, and receiving a response from the authentication server that includes a unique authentication code; receiving selection of a thereby selected over-the-counter (OTC) drug; and communicating with a point-of-sale (POS) system with contactless payment capability, to purchase the selected OTC drug using the short-range communication interface and the contactless payment capabilities of the mobile device and POS system, wherein communicating with the POS system includes sending a purchase message to the POS system that includes the unique authentication code, an identifier of the selected OTC drug, and payment information, the POS system communicating with the authentication server to validate the unique authentication code, and with an authorization server to authorize payment for the selected OTC drug based on the payment information.

In some example implementations of the method of any preceding example implementation, or any combination of any preceding example implementations, the POS system has a known location, and authenticating the user based on the physiological marker and communicating with the POS system using the short-range communication interface locks-in the user thereby authenticated at the known location.

In some example implementations of the method of any preceding example implementation, or any combination of any preceding example implementations, the authentication server is operated by a service provider, and the method further comprises enabling the service provider to verify an identity of the user, including at least capturing data from a proof of identity of the user; and sending the data to the service provider to enable the service provider to verify the identity of the user from the data, the identity of the user being verified before the authentication server is enabled to send the response that indicates the unique authentication code.

In some example implementations of the method of any preceding example implementation, or any combination of any preceding example implementations, the method further comprises enabling the user to register an account with the service provider before the message is sent to the authentication server, and during which the service provider is enabled to verify the identity of the user.

Features, aspects, and advantages of the present disclosure will be apparent from a reading of the following detailed description together with the accompanying drawings, which are briefly described below.

The present disclosure includes any combination of two, three, four or more features or elements set forth in this disclosure, regardless of whether such features or elements are expressly combined or otherwise recited in a specific example implementation described herein. This disclosure is intended to be read holistically such that any separable features or elements of the disclosure, in any of its aspects and example implementations, should be viewed as combinable, unless the context of the disclosure clearly dictates otherwise.

BRIEF DESCRIPTION OF THE DRAWING(S)

Having thus described the disclosure in general terms, reference will now be made to the accompanying drawings, which are not necessarily drawn to scale, and wherein:

FIG. 1 illustrates a system **10** according to example implementations of the present disclosure;

FIG. 2 further illustrates a dynamic display of the system of FIG. 1, according to some example implementations;

FIGS. 3A, 3B, 3C and 3D illustrate an example interaction with the dynamic display according to some example implementations;

FIGS. 4 and 5 illustrate process flow diagrams according to example implementations;

FIGS. 6, 7, 8 and 9 illustrate also process flow diagrams according to example implementations; and

FIG. 10 illustrates an apparatus according to example implementations.

DETAILED DESCRIPTION

Some implementations of the present disclosure will now be described more fully hereinafter with reference to the accompanying drawings, in which some, but not all implementations of the disclosure are shown. Indeed, various implementations of the disclosure may be embodied in many different forms and should not be construed as limited to the implementations set forth herein; rather, these example implementations are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the disclosure to those skilled in the art. As used herein, for example, the singular forms "a," "an," "the" and the like include plural referents unless the context clearly dictates otherwise. The terms "data," "information," "content" and similar terms may be used interchangeably, according to some example implementations of the present invention, to refer to data capable of being transmitted, received, operated on, and/or stored. Also, for example, reference may be made herein to quantitative measures, values, relationships or the like. Unless otherwise stated, any one or more if not all of these may be absolute or approximate to account for acceptable variations that may occur, such as those due to engineering tolerances or the like. Like reference numerals refer to like elements throughout.

FIG. 1 illustrates a system **100** according to example implementations of the present disclosure. As shown, the system may be implemented with an Internet-based computing architecture including a computer network or a number of interconnected computer networks **102** in or over which a number of systems, computers and the like communicate or otherwise operate. As shown, these include a dynamic display **104**, an information server **106**, a mobile device **108**, a point-of-sale (POS) system **110** including a POS terminal

112 and server **114**, and authentication **116** and authorization **118** server computers. Although shown and described herein in the context of an Internet-based computing architecture, it should be understood that the system may implemented with any of a number of different network-based architectures.

The network **102** may be implemented as one or more wired networks, wireless networks or some combination of wired and wireless networks. The network may include private, public, academic, business or government networks, or any of a number of different combinations thereof, and in the context of an Internet-based computing architecture, includes the Internet. The network may support one or more of any of a number of different communications protocols, technologies or the like, such as cellular telephone, Wi-Fi, satellite, cable, digital subscriber line (DSL), fiber optics and the like.

The systems and computers connected to the network **102** may also be implemented in a number of different manners. In some examples, the dynamic display **104** is implemented as a smart interactive display device, tablet computer or the like. In some examples, the dynamic display also includes a suitable user input interface such as a touch-sensitive surface that may be separate from or integrated into a touchscreen. As shown, the dynamic display is a network-connected display device, and it may be configured to communicate with another computer such as the information server **106** over the network. In other examples, the dynamic display and information server may be co-located, in which case the dynamic display may or may not be network-connected.

The information server **106** is commonly implemented as a server computer although other implementations are contemplated (e.g., mainframe computer, personal computer). The information server may be embodied as one or more servers, a network of interworking computing devices (e.g., a distributed computer implemented by multiple computers) or the like. In implementations in which the information server is implemented as a distributed computer, its multiple computers may communicate over a network such as network **102**.

The mobile device **108** is generally a small, mobile computing device such as a smartphone. Other examples of suitable mobile devices include portable computers (e.g., laptop computers, tablet computers), cellular phones, wearable computers (e.g., smartwatches, optical head-mounted displays) and the like. According to example implementations, the mobile device includes a biometric sensor or multiple biometric sensors (i.e., one or more biometric sensors) configured to acquire physiological markers from which a user is identifiable and thereby authenticated (e.g., fingerprint, palm print, hand geometry, face recognition, iris recognition, retina recognition). The mobile device also includes built-in short-range communication technology and is contactless payment capable. One example of suitable short-range communication technology is near-field communication (NFC). Other examples include radio frequency identification (RFID), personal area network technologies such as Bluetooth, Bluetooth LE, ZigBee, infrared (e.g., Infrared Data Association (IrDA)) and the like.

The POS system **110** is generally a system used by a merchant to effect sales transactions, record sales and track inventory. The POS system includes one or more of each of a number of components including the POS terminal **112** and server **114**. The POS terminal is a special-purpose computer that interfaces with payment cards and other payment technologies to make electronic funds transfers. The POS

server is configured to transmit data from the POS terminal to a merchant service provider for authorization and transfer of funds to the merchant. Similar to the mobile device **108**, the POS terminal includes built-in short-range communication technology and is contactless payment capable.

Similar to the information server **106**, the POS server **114**, authentication server **116** and authorization server **118** are each commonly implemented as a server computer although other implementations are contemplated (e.g., mainframe computer, personal computer). Any combination or all of the POS server, authentication server and authorization server may be embodied as one or more servers, a network of interworking computing devices (e.g., a distributed computer implemented by multiple computers) or the like. In implementations in which the server is implemented as a distributed computer, its multiple computers may communicate over a network such as network **102**. And in some examples, more than one of the servers (e.g., authentication server and authorization server) are co-located.

Reference is now made to FIG. 2 which further illustrates the dynamic display **104** according to some example implementations. As explained above, merchants of certain OTC drugs such as those regulated by the CMEA restrict public access to those products. A number of merchants advertise these products with other products in a retail shelf environment but with cards that are redeemed for the product at the time of purchase. These product cards are often inconveniently placed and occupy valuable space on shelves. The dynamic display of example implementations offers the same information as product cards and may be free-standing or shelf mounted, and may free the shelf space otherwise occupied by product cards for more physical products and packages.

FIGS. 3A, 3B, 3C and 3D illustrate an example interaction with the dynamic display **104** according to some examples in which the dynamic display includes a touchscreen. In the illustrated example, the dynamic display communicates with the information server **106** (co-located or across network **102**) to deliver information regarding allergy and cold medicines. In some examples, a user may be led to allergy and cold medicines by first selecting a condition from a plurality of conditions. The dynamic display may then identify a number of brands of allergy and cold medicines. As shown in FIG. 3A, the dynamic display identifies brands of medicines by images of their packaging, but other manners of identifying brands are contemplated.

From the display in FIG. 3A, the user selects a brand of medicine which in turn causes the dynamic display **104** to present information regarding the selected brand. In instances in which the brand has a number of varieties, the dynamic display may first identify those varieties for selection. This is shown in FIG. 3B in which the varieties are identified by images of their packaging, although again, other manners of identifying the varieties of a selected brand of medicine are also contemplated.

FIG. 3C illustrates the dynamic display **104** presenting information regarding a selected band of medicine, or a selected variety of the selected brand. As shown, this drug-specific information includes the same or similar information to the drug label on the packaging of the selected medicine, although other information may be presented in addition to or in lieu of the drug label. This information serves to inform and educate the user regarding the selected product. The dynamic display also provides purchase instructions, which in some but not all examples includes directing the user as to how to ask the merchant

(pharmacist) for the selected medicine. In some examples, the manufacturer of the selected medicine may offer a mobile app that the user can install on their mobile device **108** to expedite purchase of the medicine. In these examples, the dynamic display may present instructions to the user to download the app, as shown in FIG. 3D.

As also explained above, not only does the CMEA requires merchants to restrict public access to regulated products (e.g., PSE), but the CMEA also requires merchants to verify proof of identity of all purchasers, and track all purchasers and purchases. This is time consuming and inconvenient. Some example implementations of the present disclosure include a mobile app for a mobile device **108** that enables biometric authentication for restricted over-the-counter (OTC) drug sales, as well as the secure electronic tracking of those sales. In some examples, the mobile app is provided by a service provider with which a user of the mobile app registers an account, and during this registration, the service provider verifies the user's identity by a valid proof of identity such as a government-issued identification card, driver's license or the like.

FIG. 4 illustrates a process flow diagram **400** with various operations performed to carry out a restricted OTC drug sale according to some example implementations of the present disclosure. As shown, the service provider operates the authentication server **116** that implements a mobile app server or other appropriate middleware component for providing back-end functionality to the mobile app installed on a mobile device **108**.

As also shown, the mobile app causes one or more biometric sensors on the mobile device **108** to acquire a physiological marker from which a user may be identified and thereby authenticated. This physiological marker may be considered a biometric identifier (ID). The mobile app may identify and thereby authenticate the user based on this biometric ID and data locally on the mobile device, or communicate the biometric ID to the authentication server **116** to perform the identification/authentication. In instances in which the mobile app performs the identification/authentication, the mobile app may instead send a message to the authentication server that indicates the user has been authenticated. In either instance, the authentication server is responsive to an authenticated user with a unique authentication code transmitted back to the mobile app.

The mobile app on the mobile device **108** allows the user to select a desired OTC drug. The mobile device interacts with the POS terminal **112** of the POS system **110** to purchase the selected OTC drug using respective short-range communication and contactless payment capabilities of the devices. This short-range communication between the mobile device and POS terminal may lock-in the biometric ID and the location of the mobile device (the POS terminal's location being known). The mobile app sends a purchase message including the unique authentication code, an identifier of the desired OTC drug, and appropriate payment information. This payment information may include payment (credit, debit) card information, or other appropriate information such as a payment token as may be used in systems such as Apple Pay, Android Pay or Samsung Pay.

In some examples, the purchase message is sent to the authentication server **116** or authorization server **118** which cooperate with one another to enable the authentication server to validate the

authentication code, and enable the authorization server to authorize the payment based on the payment information. The authentication server may also at this time electronically record the purchase transaction including the purchaser, OTC drug and date/time of the purchase. The purchaser may be identified by the authentication code or a unique identifier of the user (e.g., biometric ID). The OTC drug may be identified by its identifier, which may be unique to the product or unit of the product such as in the case of a unique serial number.

After the authentication code is validated and the payment authorized, and the purchase transaction recorded, the authentication server **116** or authorization server **118** returns an encrypted code back to the POS system **110** to authorize the merchant to release the OTC drug to the user/purchaser. In some examples, the encrypted code may also be added to packaging of the OTC drug. This may be accomplished in a number of different manners such as by printing on the packaging, printing on another substrate affixed to the packaging, electronically reading to electronic media (e.g., RFID) on the packaging, or the like.

As described above, one or more of the servers **106**, **114**, **116**, **118** of the system **100** may be embodied as a network of interworking computing devices. In some examples, the servers may be embodied as or otherwise form part of network of interworking computing devices, such as in a peer-to-peer computing architecture. This may enable a number of configurations of the system or in which the system participates. One example of a suitable configuration is a distributed database that maintains the record of purchase transactions. And one example of a suitable distributed database is a blockchain, which is a shared, immutable ledger for recording the history of transactions. FIG. 5 is a process flow diagram **500** for a restricted OTC drug sale that expands on the diagram **400** in FIG. 4, and includes a blockchain to record purchase transactions.

As shown in FIG. 5, each OTC drug may be associated with a unique identifier for the unit of product (e.g., serial number), which may be recorded on the blockchain during manufacturing / packaging. The product may be purchased according to the process described above with reference to FIG. 4. During this process, the product blockchain may be used as its identifier. The product blockchain may be merged with the authentication code or user identifier (e.g., biometric ID) and recorded on the blockchain with the date/time of the purchase. In some examples, the data may be encrypted and serve as the aforementioned encrypted code, which may also be added to packaging of the OTC drug. The blockchain may then be used as a secure electronic record of the purchase.

To further illustrate example implementations of the present disclosure, FIG. 6 is a process flow diagram **600** of a typical sale of an allergy medicine that may be streamlined according to example implementations. FIG. 7 illustrates a process flow diagram **700** similar to be streamlined relative to the diagram **600** in FIG. 6 according to some examples. As shown in FIG. 7, after the user (consumer) understands their allergies and treatment needs and options, the user visits the pharmacy where a dynamic display **104** on an aisle with other medicines amplifies information and helps the user find their product and answer questions. In some examples, the dynamic display or a mobile app on the user's mobile device **108** allows the user to choose a medicine and order ahead to the pharmacy for a quicker pickup. In the case of

the mobile app, the order may be placed without the user first visiting the pharmacy and interacting with the dynamic display.

FIG. 8 illustrates another process flow diagram **800** similar to be streamlined relative to the diagram **600** in FIG. 6 according to some examples. As shown in FIG. 8, the dynamic display is implemented by a self-service kiosk or integrated shelf dispenser that combines functionality of the dynamic display **104** and mobile device **108**. In some examples, the kiosk / shelf dispenser allows the user to find a product and answer questions, and includes biometric sensors for biometric authentication, and perhaps also a scanner to scan a valid proof of identity. The kiosk / shelf dispenser may then complete the purchase (implementing aspects of the POS system **110**) and dispense the medicine. In some examples, the user's mobile device includes a mobile app to enable the user to place an order dispensed by the kiosk / shelf dispenser.

FIG. 9 illustrates yet another process flow diagram **900** similar to be streamlined relative to the diagram **600** in FIG. 6 according to some examples. As shown in FIG. 9, the user goes through an initial onboarding process with the pharmacist or other service provider, similar to described above for registering an account with the service provider providing the mobile app. The user can then use their mobile app to request medicines for pickup at the pharmacist. In some examples, the mobile device **108** performs biometric authentication, as described above. Additionally or alternatively, in some examples, a separate device at the pharmacy includes biometric sensors for biometric authentication, and perhaps also a scanner to scan a valid proof of identity.

According to example implementations of the present disclosure, the system **100** and its subsystems including the dynamic display **104**, information server **106**, mobile device **108**, POS terminal **112**, POS server **114**, authentication server **116** and authorization server **118** may be implemented by various means. Means for implementing the system and its subsystems may include hardware, alone or under direction of one or more computer programs from a computer-readable storage medium. In some examples, one or more apparatuses may be configured to function as or otherwise implement the system and its subsystems shown and described herein. In examples involving more than one apparatus, the respective apparatuses may be connected to or otherwise in communication with one another in a number of different manners, such as directly or indirectly via a wired or wireless network or the like.

FIG. 10 illustrates an apparatus **1000** according to some example implementations of the present disclosure. Generally, an apparatus of exemplary implementations of the present disclosure may comprise, include or be embodied in one or more fixed or portable electronic devices. The apparatus may include one or more of each of a number of components such as, for example, a processor **1002** connected to a memory **1004** (e.g., storage device).

The processor **1002** may be composed of one or more processors alone or in combination with one or more memories. The processor is generally any piece of computer hardware that is capable of processing information such as, for example, data, computer programs and/or other suitable electronic information. The processor is composed of a collection of electronic circuits some of which may be packaged as an integrated circuit or multiple interconnected integrated circuits (an integrated circuit at times more commonly referred

to as a "chip"). The processor may be configured to execute computer programs, which may be stored onboard the processor or otherwise stored in the memory **1004** (of the same or another apparatus).

The processor **1002** may be a number of processors, a multi-core processor or some other type of processor, depending on the particular implementation. Further, the processor may be implemented using a number of heterogeneous processor systems in which a main processor is present with one or more secondary processors on a single chip. As another illustrative example, the processor may be a symmetric multi-processor system containing multiple processors of the same type. In yet another example, the processor may be embodied as or otherwise include one or more ASICs, FPGAs or the like. Thus, although the processor may be capable of executing a computer program to perform one or more functions, the processor of various examples may be capable of performing one or more functions without the aid of a computer program. In either instance, the processor may be appropriately programmed to perform functions or operations according to example implementations of the present disclosure.

The memory **1004** is generally any piece of computer hardware that is capable of storing information such as, for example, data, computer programs (e.g., computer-readable program code **1006**) and/or other suitable information either on a temporary basis and/or a permanent basis. The memory may include volatile and/or non-volatile memory, and may be fixed or removable. Examples of suitable memory include random access memory (RAM), read-only memory (ROM), a hard drive, a flash memory, a thumb drive, a removable computer diskette, an optical disk, a magnetic tape or some combination of the above. Optical disks may include compact disk – read only memory (CD-ROM), compact disk – read/write (CD-R/W), DVD or the like. In various instances, the memory may be referred to as a computer-readable storage medium. The computer-readable storage medium is a non-transitory device capable of storing information, and is distinguishable from computer-readable transmission media such as electronic transitory signals capable of carrying information from one location to another. Computer-readable medium as described herein may generally refer to a computer-readable storage medium or computer-readable transmission medium.

In addition to the memory **1004**, the processor **1002** may also be connected to one or more interfaces for displaying, transmitting and/or receiving information. The interfaces may include one or more communications interfaces and/or one or more user interfaces. The communications interface(s) may be configured to transmit and/or receive information, such as to and/or from other apparatus(es), network(s) or the like. The communications interface may be configured to transmit and/or receive information by physical (wired) and/or wireless communications links. The communications interface(s) may include interface(s) **1008** to connect to a network (e.g., network **102**), such as using technologies such as cellular telephone, Wi-Fi, satellite, cable, digital subscriber line (DSL), fiber optics and the like. And at least in instances in which the apparatus **1000** is configured to implement the mobile device **108** or POS terminal **112**, the communications interface(s) may include one or more short-range communications interfaces **1010** configured to connect devices using short-range communications technologies such as NFC, RFID, Bluetooth, Bluetooth LE, ZigBee, infrared (e.g., IrDA) or the like.

The user interfaces may include a display **1012** and/or one or more user input interfaces **1014**. The display may be configured to present or otherwise display information to a user, suitable examples of which include a liquid crystal display (LCD), light-emitting diode display (LED), plasma display panel (PDP) or the like. The user input interfaces may be wired or wireless, and may be configured to receive information from a user into the apparatus, such as for processing, storage and/or display. Suitable examples of user input interfaces include a microphone, image or video capture device, keyboard or keypad, joystick, touch-sensitive surface (separate from or integrated into a touchscreen) or the like. In instances in which the apparatus **1000** is configured to implement the mobile device **108**, the user interfaces may include one or more biometric sensors **1016** such as cameras or scanners capable of acquiring markers for or enabling technology such as fingerprint, palm print, hand geometry, face recognition, iris recognition, retina recognition. The user interfaces may further include one or more interfaces for communicating with peripherals such as printers, scanners or the like.

As indicated above, program code instructions may be stored in memory, and executed by processor that is thereby programmed, to implement functions of the systems, subsystems, tools and their respective elements described herein. As will be appreciated, any suitable program code instructions may be loaded onto a computer or other programmable apparatus from a computer-readable storage medium to produce a particular machine, such that the particular machine becomes a means for implementing the functions specified herein. These program code instructions may also be stored in a computer-readable storage medium that can direct a computer, processor or other programmable apparatus to function in a particular manner to thereby generate a particular machine or particular article of manufacture. The instructions stored in the computer-readable storage medium may produce an article of manufacture, where the article of manufacture becomes a means for implementing functions described herein. The program code instructions may be retrieved from a computer-readable storage medium and loaded into a computer, processor or other programmable apparatus to configure the computer, processor or other programmable apparatus to execute operations to be performed on or by the computer, processor or other programmable apparatus.

Retrieval, loading and execution of the program code instructions may be performed sequentially such that one instruction is retrieved, loaded and executed at a time. In some example implementations, retrieval, loading and/or execution may be performed in parallel such that multiple instructions are retrieved, loaded, and/or executed together. Execution of the program code instructions may produce a computer-implemented process such that the instructions executed by the computer, processor or other programmable apparatus provide operations for implementing functions described herein.

Execution of instructions by processor, or storage of instructions in a computer-readable storage medium, supports combinations of operations for performing the specified functions. In this manner, an apparatus **1000** may include processor **1002** and a computer-readable storage medium or memory **1004** coupled to the processor, where the processor is configured to execute computer-readable program code **1006** stored in the memory. It will also be understood that one or more functions, and combinations of functions, may be implemented by special purpose hardware-based computer systems and/or processor

which perform the specified functions, or combinations of special purpose hardware and program code instructions.

As explained above, the present disclosure includes any combination of two, three, four or more features or elements set forth in this disclosure, regardless of whether such features or elements are expressly combined or otherwise recited in a specific example implementation described herein. This disclosure is intended to be read holistically such that any separable features or elements of the disclosure, in any of its aspects and example implementations, should be viewed as combinable, unless the context of the disclosure clearly dictates otherwise.

Many modifications and other implementations of the disclosure set forth herein will come to mind to one skilled in the art to which the disclosure pertains having the benefit of the teachings presented in the foregoing description and the associated drawings. Therefore, it is to be understood that the disclosure is not to be limited to the specific implementations disclosed and that modifications and other implementations are intended to be included within the scope of the appended claims. Moreover, although the foregoing description and the associated drawings describe example implementations in the context of certain example combinations of elements and/or functions, it should be appreciated that different combinations of elements and/or functions may be provided by alternative implementations without departing from the scope of the appended claims. In this regard, for example, different combinations of elements and/or functions than those explicitly described above are also contemplated as may be set forth in some of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

WHAT IS CLAIMED IS:

1. A mobile device comprising:

one or more biometric sensors configured to acquire a physiological marker from which a user is identifiable and thereby authenticated;

a short-range communication interface configured to implement short-range communication technology and enable contactless payment capability of the mobile device; and

a processor coupled to the one or more biometric sensors and short-range communication interface, and programmed to at least:

cause the one or more biometric sensors to acquire the physiological marker, and identify and authenticate the user based thereon;

send a message to an authentication server that indicates the user is authenticated, and receive a response from the authentication server that includes a unique authentication code;

receive selection of a thereby selected over-the-counter (OTC) drug; and

communicate with a point-of-sale (POS) system with contactless payment capability, to purchase the selected OTC drug using the short-range communication interface and the contactless payment capabilities of the mobile device and POS system,

wherein the processor being programmed to communicate with the POS system includes being programmed to send a purchase message to the POS system that includes the unique authentication code, an identifier of the selected OTC drug, and payment information, the POS system being configured to communicate with the authentication server to validate the unique authentication code, and with an authorization server to authorize payment for the selected OTC drug based on the payment information.

2. The mobile device of claim 1, wherein the POS system has a known location, and the processor being programmed to authenticate the user based on the physiological marker and communicate with the POS system using the short-range communication interface locks-in the user thereby authenticated at the known location.

3. The mobile device of claim 1, wherein the authentication server is operated by a service provider, and the processor is further programmed to enable the service provider to verify an identity of the user, including the processor being programmed to at least:

capture data from a proof of identity of the user; and

send the data to the service provider to enable the service provider to verify the identity of the user from the data, the identity of the user being verified before the authentication server is enabled to send the response that indicates the unique authentication code.

4. The mobile device of claim 3, wherein the processor is further programmed to enable the user to register an account with the service provider before the message is sent to the authentication server,

and during which the processor is programmed to enable the service provider to verify the identity of the user.

5. An apparatus configured to implement a self-service kiosk or integrated shelf dispenser, the apparatus comprising:

one or more biometric sensors configured to acquire a physiological marker from which a user is identifiable and thereby authenticated; and

a processor coupled to the one or more biometric sensors, and programmed to at least:

cause the one or more biometric sensors to acquire the physiological marker, and identify and authenticate the user based thereon;

send a message to an authentication server that indicates the user is authenticated, and receive a response from the authentication server that includes a unique authentication code;

receive selection of a thereby selected over-the-counter (OTC) drug;

complete a purchase of the selected OTC drug, including the processor being programmed to send a purchase message to the authentication server that includes the unique authentication code, an identifier of the selected OTC drug, and payment information, the processor being programed to send the purchase message for the authentication server to validate the unique authentication code, and for the authentication server to cooperate with an authorization server to authorize payment for the selected OTC drug based on the payment information; and

receive an encrypted code to authorize release of the selected OTC drug; and

a dispenser coupled to the processor and caused thereby to dispense the selected OTC drug after the purchase is completed.

6. The apparatus of claim 5, wherein the authentication server is operated by a service provider, and the processor is further programmed to enable the service provider to verify an identity of the user, including the processor being programmed to at least:

capture data from a proof of identity of the user; and

send the data to the service provider to enable the service provider to verify the identity of the user from the data, the identity of the user being verified before the authentication server is enabled to send the response that indicates the unique authentication code.

7. The apparatus of claim 6, wherein the processor is further programmed to enable the user to register an account with the service provider before the message is sent to the authentication server, and during which the processor is programmed to enable the service provider to verify the identity of the user.

8. An apparatus configured to implement an authentication server, the apparatus comprising:

a processor and a memory storing executable instructions that in response to execution by the processor cause the apparatus to at least:

receive a message related to a purchase of an over-the-counter (OTC) drug by a user, the message indicating the user is authenticated, the message being received from a mobile device, self-service kiosk or integrated shelf dispenser;

send a response to the mobile device, self-service kiosk or integrated shelf dispenser, the response including a unique authentication code;

receive a purchase message that includes the unique authentication code, an identifier of a selected OTC drug, and payment information, the purchase message being received from a point-of-sale (POS) system, or the self-service kiosk or integrated shelf dispenser;

validate the unique authentication code;

cooperate with an authorization server to authorize payment for the selected OTC drug based on the payment information; and

return an encrypted code to the POS system, self-service kiosk or integrated shelf dispenser to authorize release of the selected OTC drug.

9. The apparatus of claim 8, wherein the memory stores executable instructions that in response to execution by the processor cause the apparatus to further at least:

electronically record a purchase transaction including the user, the selected OTC drug and a date or time of purchase of the selected OTC drug.

10. The apparatus of claim 9, wherein the purchase transaction identifies the user by the unique authentication code or a physiological marker of the user.

11. The apparatus of claim 9, wherein the apparatus being caused to electronically record the purchase transaction includes being caused to electronically record the purchase transaction on a blockchain.

12. The apparatus of claim 11, wherein the purchase transaction identifies the user by the unique authentication code or a physiological marker of the user, and identifies the selected OTC drug by an identifier of the selected OTC drug that is unique to a unit thereof, and

wherein the identifier of the selected OTC drug is recorded on the blockchain during manufacturing or packaging, and the apparatus is thereafter caused to electronically record the purchase transaction including the unique authentication code or physiological marker of the user, the identifier of the selected OTC drug, and the date or time of purchase.

13. A method comprising:

acquiring, via one or more biometric sensors of a mobile device, a physiological marker from which a user is identifiable and thereby authenticated; and at the mobile device;

identifying and authenticating the user based on the physiological marker;

sending a message to an authentication server that indicates the user is authenticated, and receiving a response from the authentication server that includes a unique authentication code;

receiving selection of a thereby selected over-the-counter (OTC) drug; and

communicating with a point-of-sale (POS) system with contactless payment capability, to purchase the selected OTC drug using the short-range communication interface and the contactless payment capabilities of the mobile device and POS system,

wherein communicating with the POS system includes sending a purchase message to the POS system that includes the unique authentication code, an identifier of the selected OTC drug, and payment information, the POS system communicating with the authentication server to validate the unique authentication code, and with an authorization server to authorize payment for the selected OTC drug based on the payment information.

14. The method of claim 13, wherein the POS system has a known location, and authenticating the user based on the physiological marker and communicating with the POS system using the short-range communication interface locks-in the user thereby authenticated at the known location.

15. The method of claim 13, wherein the authentication server is operated by a service provider, and the method further comprises enabling the service provider to verify an identity of the user, including at least:

capturing data from a proof of identity of the user; and

sending the data to the service provider to enable the service provider to verify the identity of the user from the data, the identity of the user being verified before the authentication server is enabled to send the response that indicates the unique authentication code.

16. The method of claim 15 further comprising enabling the user to register an account with the service provider before the message is sent to the authentication server, and during which the service provider is enabled to verify the identity of the user.

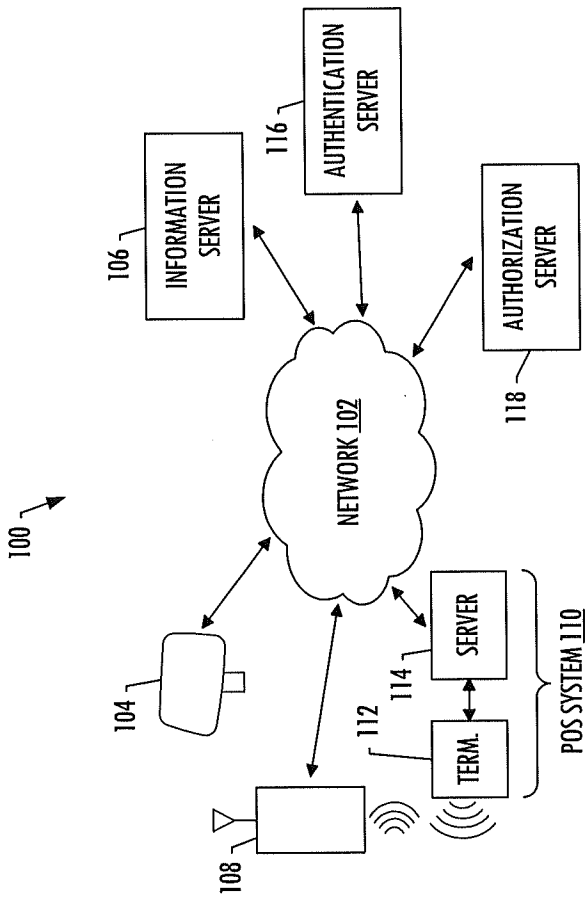
100
NETWORK 102
INFORMATION SERVER
106
AUTHENTICATION SERVER
116
AUTHORIZATION SERVER
118
104
108
112
SERVER
114
TERM.
POS SYSTEM 110

FIG. 1

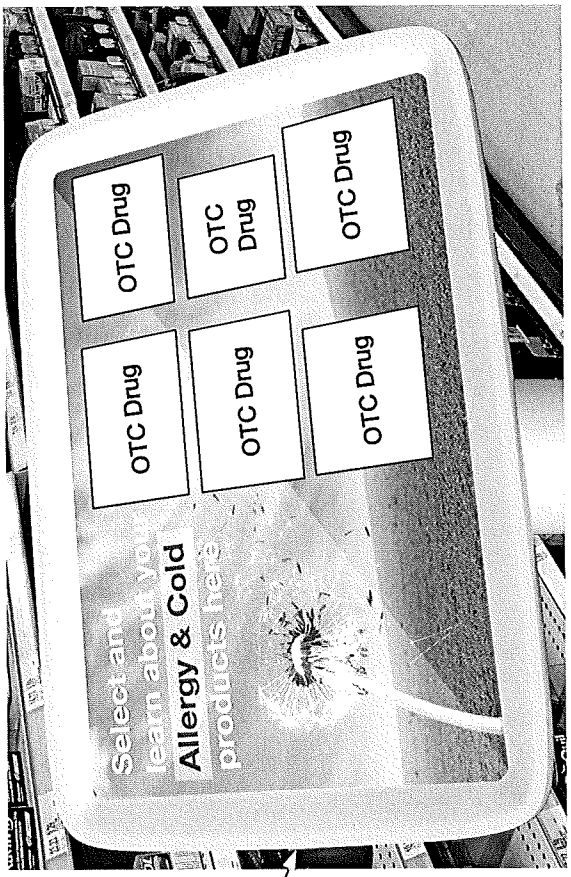
OTC Drug
OTC Drug
OTC Drug
OTC Drug
OTC Drug
OTC Drug
Allergy & Cold
104

FIG. 2

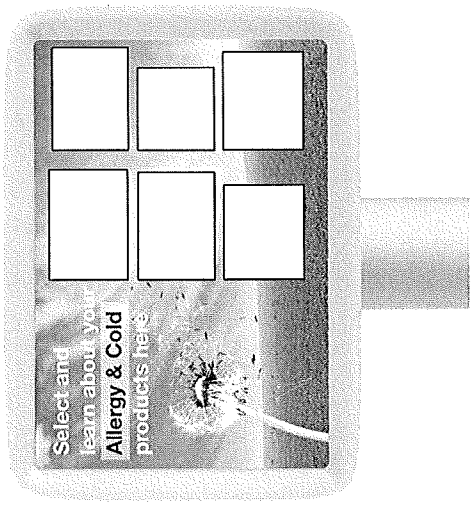

FIG. 3A

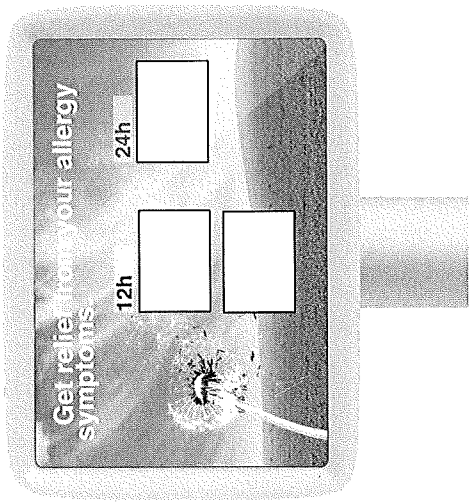

FIG. 3B

FIG. 3C

FIG. 3D

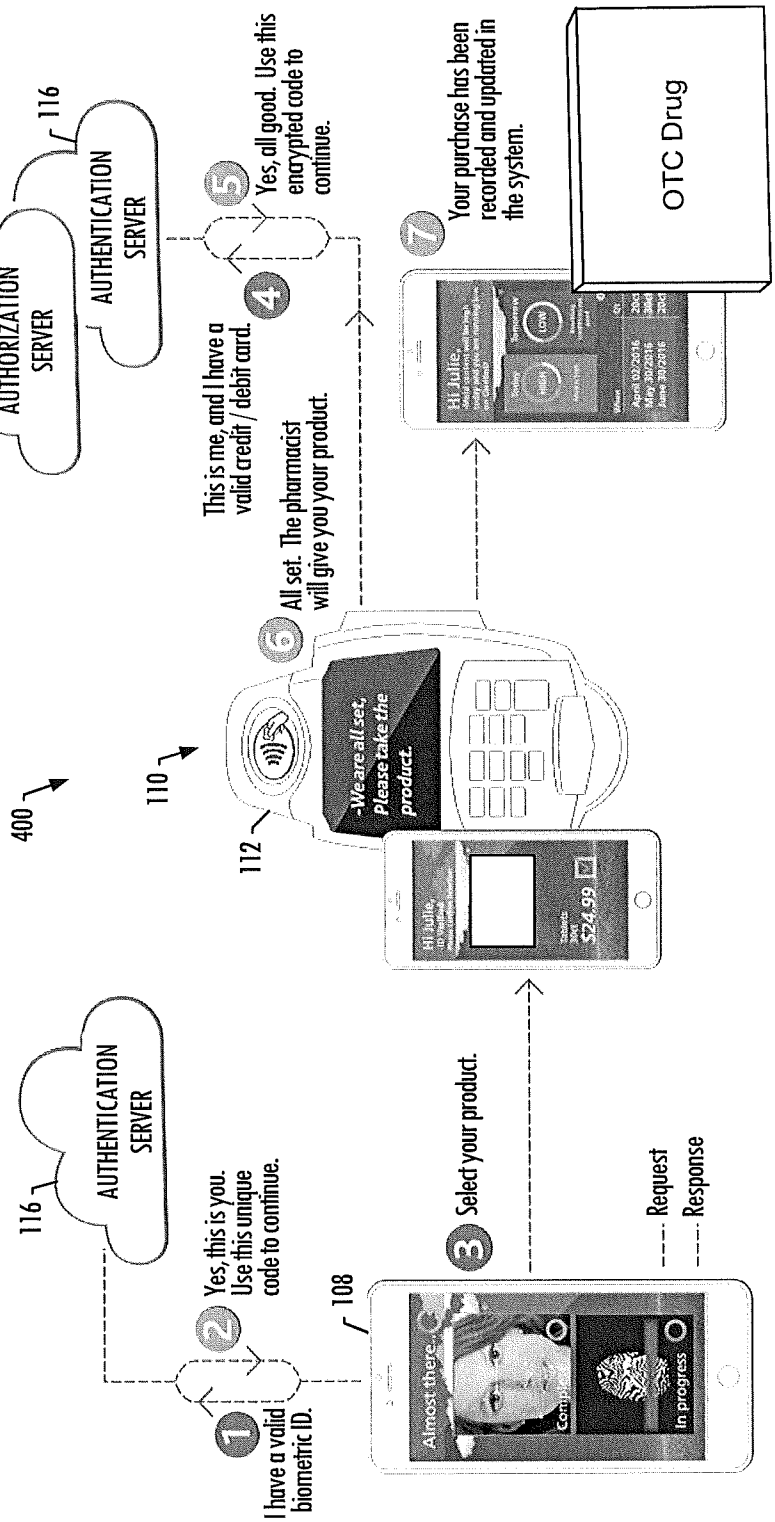
400
110
112
108
116
AUTHENTICATION SERVER
116
AUTHENTICATION SERVER
118
AUTHORIZATION SERVER
1 I have a valid biometric ID.
2 Yes, this is you. Use this unique code to continue.
3 Select your product.
4 This is me, and I have a valid credit / debit card.
5 Yes, all good. Use this encrypted code to continue.
6 All set. The pharmacist will give you your product.
7 Your purchase has been recorded and updated in the system.
-We are all set. Please take the product.
OTC Drug
Request
Response

FIG. 4

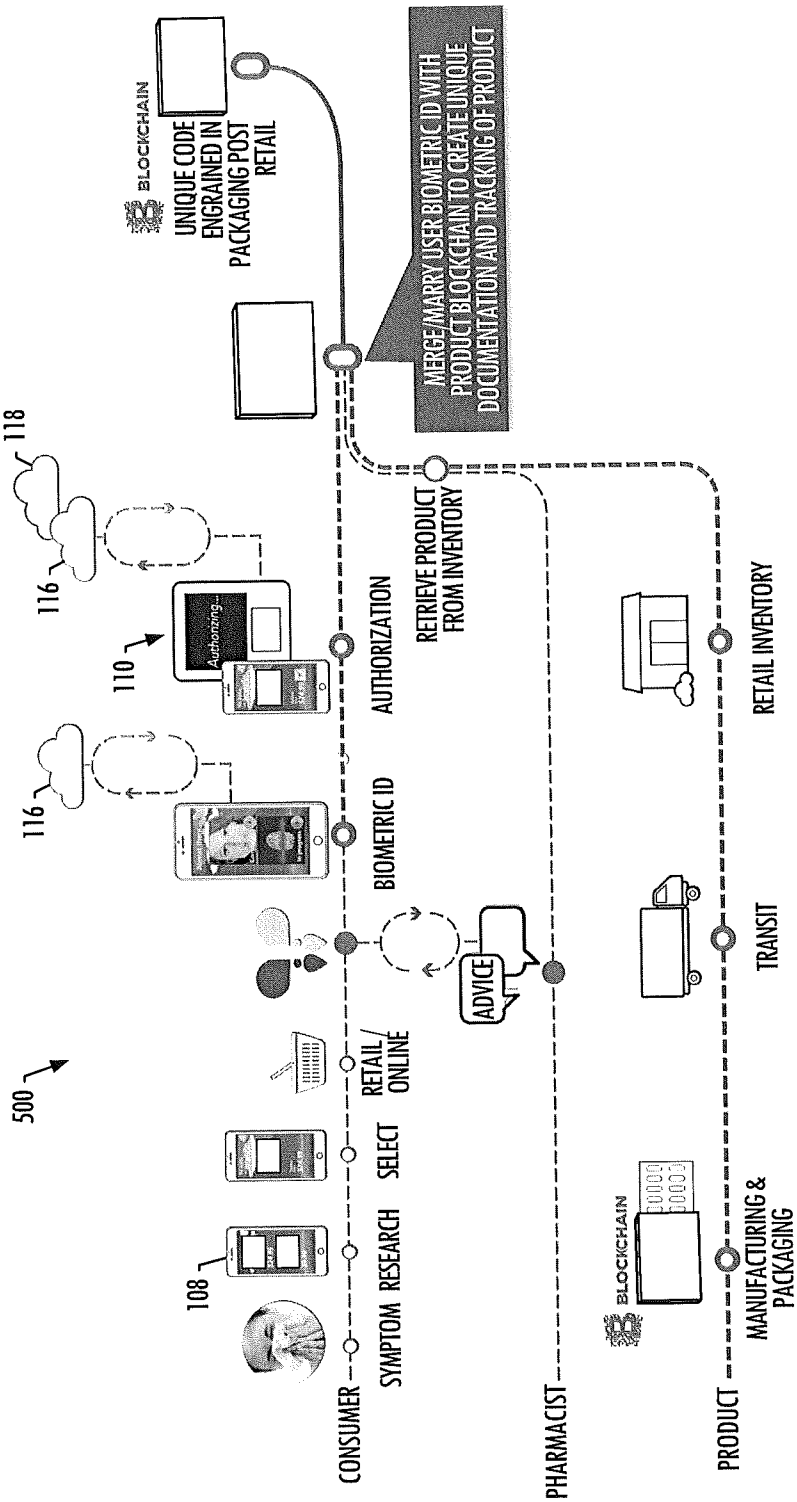
500
108
110
116
116
118
CONSUMER
SYMPTOM RESEARCH
SELECT
RETAIL / ONLINE
BIOMETRIC ID
AUTHORIZATION
ADVICE
PHARMACIST
RETRIEVE PRODUCT FROM INVENTORY
MERGE/MARRY USER BIOMETRIC ID WITH PRODUCT BLOCKCHAIN TO CREATE UNIQUE DOCUMENTATION AND TRACKING OF PRODUCT
UNIQUE CODE ENGRAINED IN PACKAGING POST RETAIL
BLOCKCHAIN
BLOCKCHAIN
RETAIL INVENTORY
TRANSIT
MANUFACTURING & PACKAGING
PRODUCT

FIG. 5

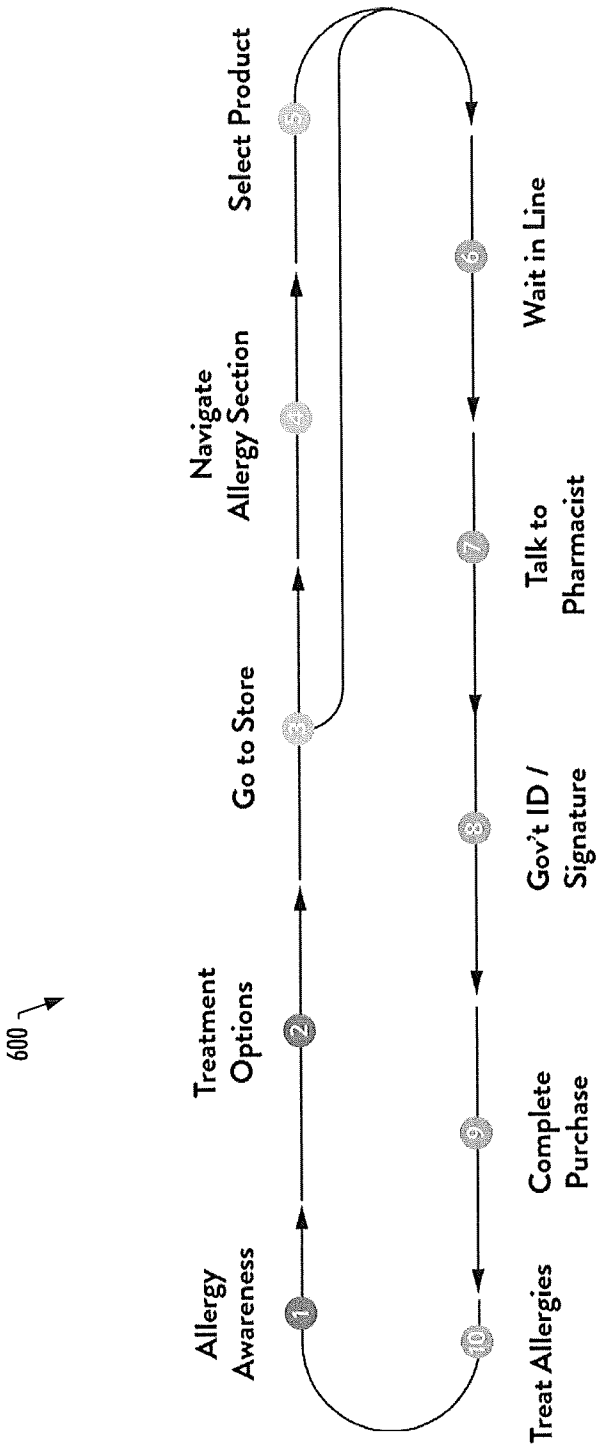
600
Allergy Awareness
Treatment Options
Go to Store
Navigate Allergy Section
Select Product
Wait in Line
Talk to Pharmacist
Gov't ID / Signature
Complete Purchase
Treat Allergies
1
2
3
4
5
6
7
8
9
10

FIG. 6

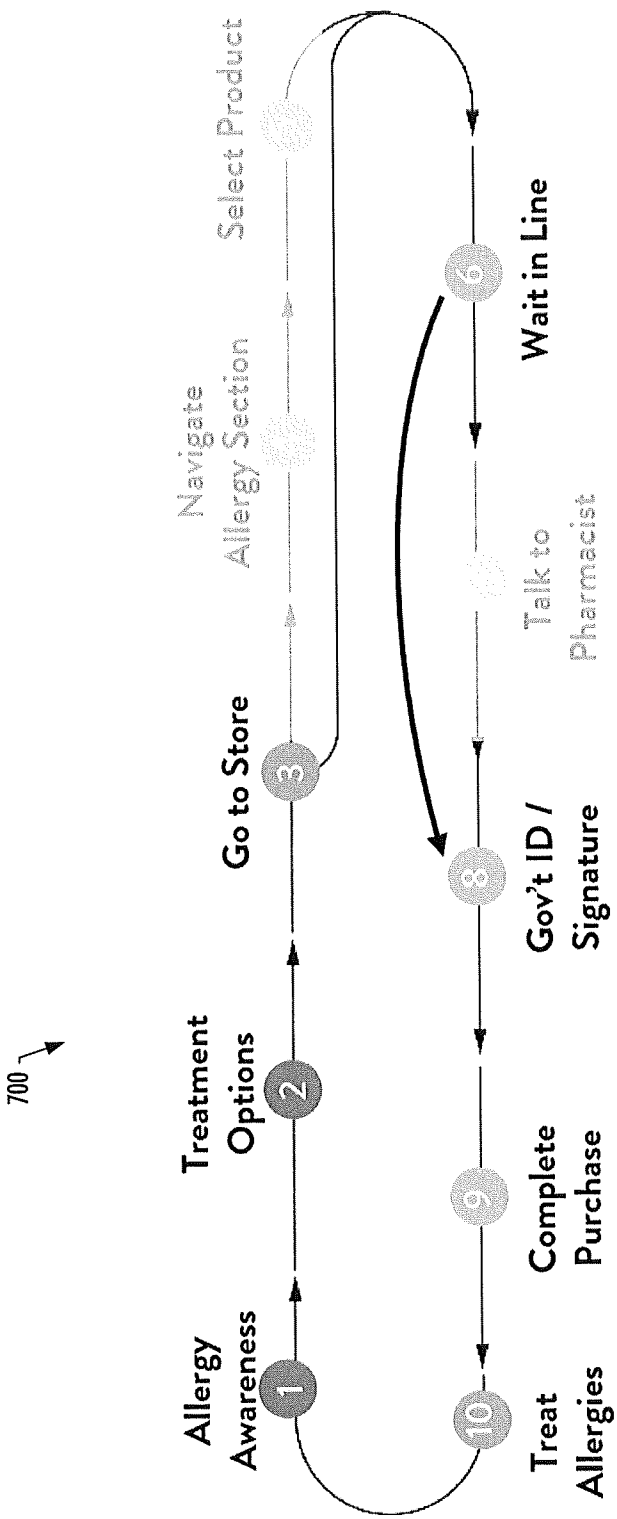
700
Allergy Awareness
1
Treatment Options
2
Navigate
Allergy Section
Select Product
Go to Store
3
Wait in Line
4
Talk to
Pharmacist
Gov't ID /
Signature
8
Complete
Purchase
9
Treat
Allergies
10

FIG. 7

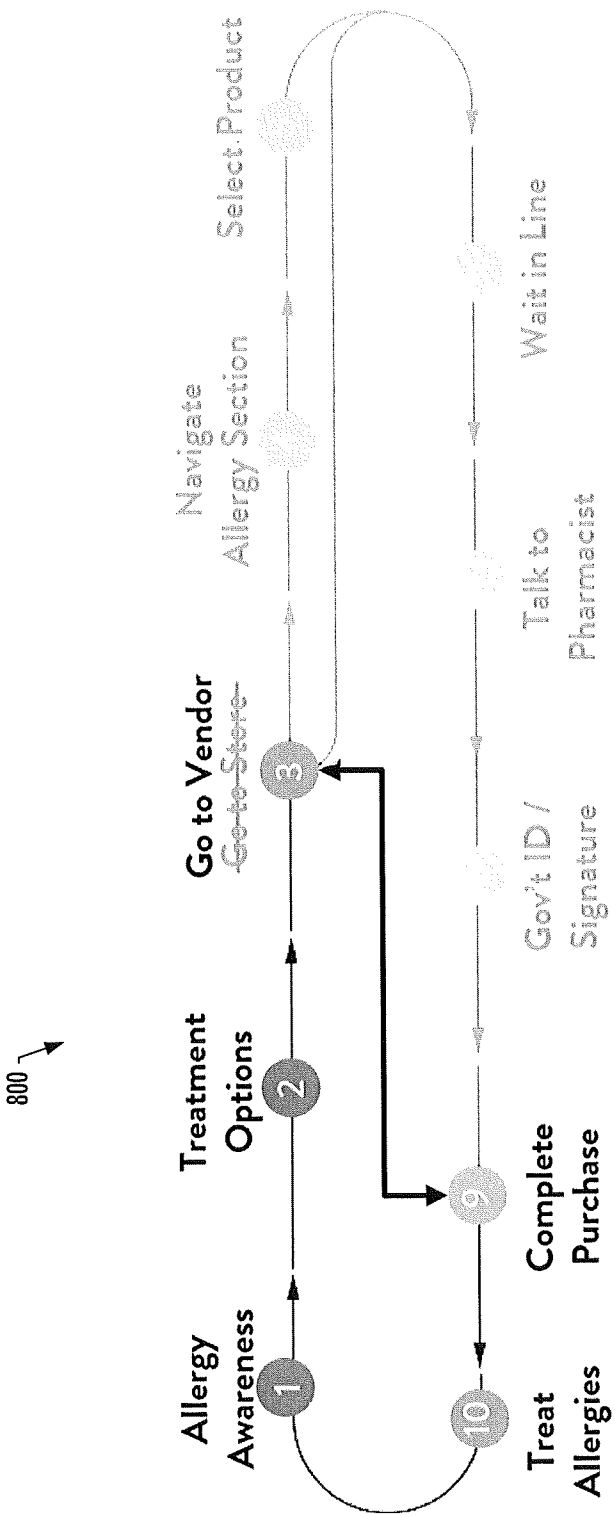
800
Allergy Awareness
1
Treatment Options
2
Go to Vendor
Go-to-Store
3
Navigate
Allergy Section
Select Product
Wait in Line
Talk to
Pharmacist
Gov't ID /
Signature
Complete
Purchase
9
10
Treat
Allergies

FIG. 8

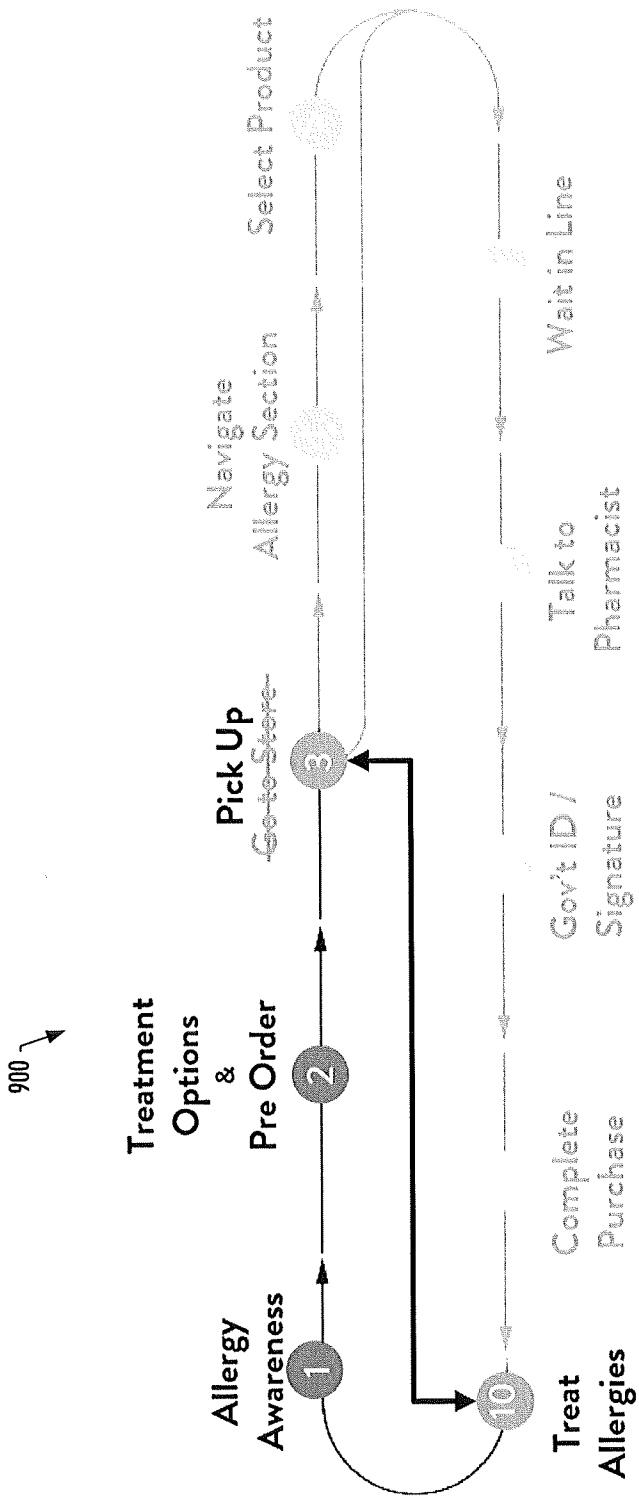
900
Allergy Awareness
1
Treatment Options & Pre Order
2
Pick Up
Go to Store
3
Navigate Allergy Section
Select Product
Wait in Line
Talk to Pharmacist
Gov't ID / Signature
Complete Purchase
10
Treat Allergies

FIG. 9

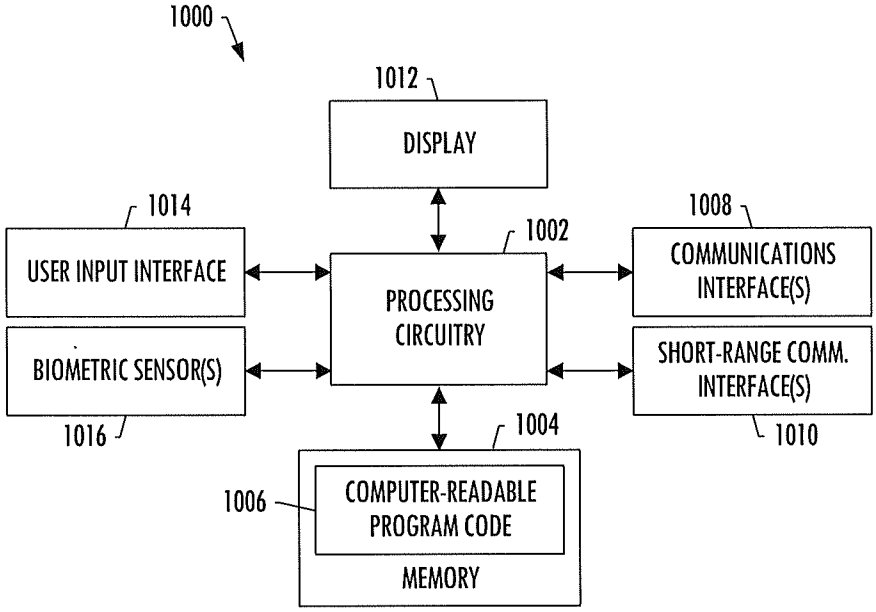
1000
1012
DISPLAY
1014
USER INPUT INTERFACE
1002
PROCESSING CIRCUITRY
1008
COMMUNICATIONS INTERFACE(S)
BIOMETRIC SENSOR(S)
1016
SHORT-RANGE COMM. INTERFACE(S)
1010
1004
1006
COMPUTER-READABLE PROGRAM CODE
MEMORY

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2018/052102

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/40 G06Q20/20 G06Q20/32 G07F7/10 G07F17/00
G16H20/10
ADD.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q G07F G16H

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/269947 A1 (BEANE JOHN A [US] ET AL) 30 October 2008 (2008-10-30) abstract; figures paragraphs [0041] - [0051], [0058] - [0061], [0071], [0084] - [0086], [0100], [0109] - [0110], [0116], [0125]	1-16
X	US 2008/086326 A1 (MOURA FERNANDO [US] ET AL) 10 April 2008 (2008-04-10) abstract; figures paragraphs [0011], [0013], [0019] - [0026]	1-16
X	US 2009/138366 A1 (BEMMEL VINCENT [US] ET AL) 28 May 2009 (2009-05-28) abstract; figures paragraphs [0045] - [0068], [0087] - [0089]	1-16

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 June 2018	28/06/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Schöndienst, Thilo

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2018/052102

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016/292668 A9 (PAYPAL INC [US]) 6 October 2016 (2016-10-06) abstract; figures paragraphs [0090] - [0096], [0106] - [0122] -----	1-16
A	US 2016/117471 A1 (BELT JAN [US] ET AL) 28 April 2016 (2016-04-28) abstract; figures paragraphs [0087] - [0091] -----	9-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2018/052102

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008269947 A1	30-10-2008	US 2008269947 A1	30-10-2008
		US 2011047043 A1	24-02-2011
US 2008086326 A1	10-04-2008	CA 2665497 A1	17-04-2008
		US 2008086326 A1	10-04-2008
		WO 2008045746 A2	17-04-2008
US 2009138366 A1	28-05-2009	EP 2044721 A2	08-04-2009
		US 2008046366 A1	21-02-2008
		US 2009138366 A1	28-05-2009
		WO 2008002979 A2	03-01-2008
US 2016292668 A9	06-10-2016	NONE	
US 2016117471 A1	28-04-2016	NONE	