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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 March 2015 (19.03.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/039025 A1

(51) International Patent Classification:
G09G 5/24 (2006.01) *G06T 11/20* (2006.01)
G09G 5/377 (2006.01)

(21) International Application Number:
PCT/US2014/055644

(22) International Filing Date:
15 September 2014 (15.09.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/960,258 13 September 2013 (13.09.2013) US
61/960,544 20 September 2013 (20.09.2013) US

(71) Applicant: **FLASHBACK SURVEY, INC.** [US/US]; 1415 Preston Spring Ln, Chapel Hill, NC 27516-8388 (US).

(72) Inventors: **MARSICO, Peter Joseph**; 1415 Preston Spring Lane, Chapel Hill, NC 27516 (US). **KUPINSKY, Stuart Howard**; 611 Hogan's Valley Way, Cary, NC 27513-5696 (US). **BURBRIDGE, Sir Robert**; 5129 Lansdowne Drive, Durham, NC 27712 (US). **ZIMMERMAN, Mark**; 313 Rose Valley Woods Drive, Cary, NC 27513 (US).

(74) Agent: **HUNT, Gregory A.**; Jenkins, Wilson, Taylor & Hunt, P.A., Suite 1200, University Tower, 3100 Tower Boulevard, Durham, NC 27707 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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).

Published:

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

(54) **Title**: METHODS AND SYSTEMS FOR USING SCANABLE CODES TO OBTAIN SCAN-TRIGGERED SERVICES

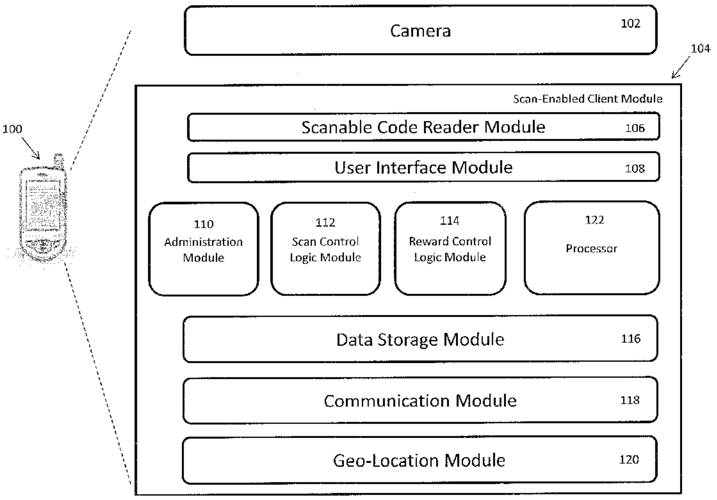


Figure 1

(57) **Abstract**: Disclosed are methods, systems and computer program products for providing scan triggered services to a user using a scanable information encoded graphic image, such as a bar code or a quick response (QR) code, near field communication (NFC) code / tag, radio frequency identification (RFID) code / tag. In one embodiment, a mobile communication device such as a smartphone, tablet computer or other mobile computer is adapted to include a scan client module for scanning and communicating scan-triggered service code information. In one embodiment, scan-triggered service code scanning is accomplished by camera module that is associated with the smartphone or other mobile computing device. The scan-enabled client module communicates the scanned service code identifying and supplementary information to an associated scan-triggered server application for collecting, processing and reporting scan data associated with the identified scan-triggered service.

WO 2015/039025 A1

TITLE

METHODS AND SYSTEMS FOR USING SCANABLE CODES TO OBTAIN SCAN-TRIGGERED SERVICES

PRIORITY CLAIM

This application claims the benefit of U.S. Provisional Patent Application Ser. No. 61/960,258, filed 9/13/2013 and U.S. Provisional Patent Application Ser. No. 61/960,544, filed 9/20/2013; the disclosures of which are incorporated herein by reference in their entireties.

TECHNICAL FIELD

The subject matter described herein relates to methods and systems for using a scanable code to initiate and facilitate a scan-triggered user service.

BACKGROUND

Applications often require users, such as the users of mobile communication devices, to manually activate and interact with software in order to utilize the associated services. For example, information collection systems that are typically deployed to gather information from a consumer of goods and services are often intrusive and time consuming from the perspective of the consumer. While such information collection systems are capable of gathering detailed information from a consumer, these systems require a relatively high level of user interaction to obtain the associated services, and furthermore do not give the user an incentive to participate nor an easy way to obtain high-utility services.

In light of these problems, what is needed is a system and method for providing high-utility scan-triggered services to a user.

SUMMARY

According to one aspect, the subject matter described herein includes systems and methods for surveying a user using a scanable information element, such as a radio frequency identification (RFID) encoded tag, a near field communication (NFC) encoded tag, or an encoded graphic image, such as a bar code or a quick response (QR) code tag. In one embodiment, a mobile communication device such as a smartphone, tablet computer, computer-integrated eyewear, wear-able computer or communication devices, or other mobile computer is adapted to include a scan-enabled client module for scanning and communicating scan-triggered service code information.

According to one aspect of the subject matter described herein, a scan-triggered service code is associated with one or more elements of personal information and a personal information requesting entity. When scanned by a user, information that can be used to identify the user along with information that can be used to identify the one or more elements of personal information is communicated to a scan-triggered service server. In response to receiving the information, the scan-triggered server is adapted to retrieve the identified personal information from a data store associated with the user's scan-triggered service account and communicate this personal information to a server or device associated with the personal information requesting entity.

According to another aspect of the subject matter described herein, a scan-triggered service code is associated with a contactable entity, such as vendor entity at a trade show or a presenter at a conference. When the service code is scanned by a user, information which can be used to identify the scanning user and the contact-able entity is communicated to a scan-triggered service server. Upon receipt of this information, the scan-triggered service server generates or updates a binding record that associates the contact-able entity identifier with the user. The contact-able entity / user binding is stored by the server. Additional information associated with the contact-able entity (e.g., PDF documents, URL links, etc.) may be provisioned and stored by the server. The user may log in to the server and access the binding information, and thereby browse a listing of all contact-able entities that have been scanned by the user. The user may also access and browse additionally provisioned materials associated with a previously scanned contact-able entity.

According to another aspect of the subject matter described herein, a scan-triggered service code is associated with a package or item that is being shipped, and where the service code is further associated with a status indicator (e.g., package is damaged, packaged arrived late, etc.). The service code may be placed in or on the associated package or item, such that it can be scanned by a user who is the recipient of the package or item. When the service code is scanned by a user, information which can be used to identify the scanning user and the associated status indicator is communicated to a scan-triggered service server. The information received at the scan-triggered server may be used to generate a customer support or "help" ticket, or may be reported to a customer support agent, and/or may be recorded and stored.

According to yet another aspect of the subject matter described herein, a scan-triggered service code is associated with a clinical drug or device trial. When the service code is scanned by a user, information which can be used to identify or contact the scanning user along with information which can be used to identify the clinical drug or device trial is communicated to a scan-triggered service server. In response to receiving the information, the scan-triggered service server may communicate one or more screening questions or screening response options to the scanning user, and collect the user's associated response information. Information collected by the scan-triggered service server may be used by a clinical trial recruitment entity (e.g., a contract research organization, etc.) to recruit and screen potential clinical trial candidates.

The subject matter described herein for facilitating scan-triggered services may be implemented in hardware, software, firmware, or any combination thereof. As such, the terms "function" or "module" as used herein refer to hardware, software, and/or firmware for implementing the feature being described. In one exemplary implementation, the subject matter described herein may be implemented using a non-transitory computer readable medium having stored thereon computer executable instructions that when executed by the processor of a computer perform steps. Exemplary computer readable media suitable for implementing the subject matter described herein include disk memory devices, programmable logic devices, application specific integrated circuits, and downloadable electrical signals. In addition, a computer readable medium that implements the subject matter described herein may be located on a single device or computing platform distributed across multiple physical devices and/or computing platforms.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the subject matter described herein will now be explained with reference to the accompanying drawings of which:

Figure 1 is a functional block diagram which illustrates a mobile communication device that includes a scanable code reader module, such as a quick response (QR) code scanner module and exemplary scan-enabled client module;

Figure 2 is a functional block diagram which illustrates an application server that includes an exemplary server application module;

Figure 3A illustrates provisioning of a scan-triggered server that is adapted to provide Trusted Square scan-triggered services;

Figures 3B and 3C illustrate a processing flow associated with a first exemplary embodiment of Trusted Square service associated with an online transaction;

Figure 3D illustrates a processing flow associated with a second exemplary embodiment of Trusted Square service associated with an online transaction;

Figure 3E illustrates a processing flow associated with a third exemplary embodiment of Trusted Square service associated with a point of sale/service transaction;

Figure 3F illustrates a processing flow associated with a fourth exemplary embodiment of Trusted Square service associated with a point of sale/service transaction;

Figures 3G and 3H illustrate a processing flow associated with a fifth exemplary embodiment of Trusted Square service associated with a point of sale/service transaction;

Figures 3I and 3J illustrate exemplary data and data structures associated with exemplary embodiments of trusted square scan-triggered service;

Figure 4A illustrates provisioning of a scan-triggered server that is adapted to provide connect square scan-triggered services;

Figure 4B illustrates a processing flow associated with an exemplary embodiment of connect square scan-triggered service;

Figure 4C illustrates exemplary data and data structures associated with exemplary embodiments of connect square scan-triggered service;

Figure 5A illustrates provisioning of a scan-triggered server that is adapted to provide RateIt square scan-triggered services;

Figure 5B illustrates a processing flow associated with an exemplary embodiment of RateIt square service;

Figures 5C and 5D illustrate exemplary data and data structures associated with exemplary embodiments of RateIt square scan-triggered service;

Figure 6A illustrates provisioning of a scan-triggered server that is adapted to provide TrackIt square scan-triggered services;

Figure 6B illustrates illustrate a processing flow associated with an exemplary embodiment of TrackIt square scan-triggered service;

Figure 6C illustrates illustrate a processing flow associated with an alternate exemplary embodiment of TrackIt square scan-triggered service;

Figure 6D illustrates exemplary data and data structures associated with exemplary embodiments of TrackIt square scan-triggered service;

Figure 7A illustrates provisioning of a scan-triggered server that is adapted to provide Clin square scan-triggered services;

Figure 7B illustrates illustrate a processing flow associated with an exemplary embodiment of Clin square scan-triggered service; and

Figures 7C and 7D illustrate exemplary data and data structures associated with exemplary embodiments of Clin square scan-triggered service.

DETAILED DESCRIPTION

Disclosed are systems and methods for using a scanable code, such as quick response (QR) code, a near field communication (NFC) code, radio frequency identification (RFID) code, or similar optical, magnetic or electrical scanable codes, to provide a service to a user who scans the code. In a one embodiment, a scan code-based services system of the subject matter described herein includes a scan-enabled client module, which may be implemented in hardware, software, firmware or a combination thereof and which resides on a mobile communication device, such as a smartphone, tablet computer, netbook computer, computer-integrated eyeglasses, computer-integrated wristwatch, wearable electronics or other mobile computing device that is capable of communicating with a network server. The scan-enabled client module may include an executable computer program (e.g., C++, Java, etc.) that is adapted to be downloaded onto the mobile communication device, installed and executed. The scan-enabled client module may also include a web browser that is adapted to access and execute web-based software (e.g., JavaScript, etc.) that provides a least a portion of the necessary scan-enabled client functionality. Figure 1 is a block diagram that illustrates an exemplary architecture of a smartphone-based scan-enabled client module. Mobile device **100**, which may be a smartphone or other mobile computing and communication device, includes a camera **102** that is adapted to capture and store an image in a digital format. Mobile device **100** also includes a scan-enabled client module **104**. Scan-enabled client module **104** is comprised of scanable code reader module **106**, a user interface module **108**, an administration module **110**, a scan control logic module**112**, a participation reward control logic module **114**, a data storage module **116**, a communication module **118**, and geo-location module **120**, and processor module **122**.

The extracted scan-triggered service information may comprise information that is representative, for example, of an alphanumeric text string, a numeric code. In one embodiment, the extracted scan-triggered service information may be used to identify and facilitate the providing of scan-triggered rewards based on the scanning of service scan codes. The decoded scan code information is provided to an associated server application module via communication module **118**. In an alternate embodiment, scanable code reader module **106** is adapted to receive digital image information from camera **102** and to communicate the digital image information (e.g., JPEG) to an associated server application module via communication module **118** where decoding processing is performed. In one embodiment, information that identifies or can be used to identify a scan-triggered service user (e.g., user name, user ID, session ID, etc.) is also provided to the server application module.

User interface module **108** is adapted to present the mobile device user with a graphical user interface for enabling the user to generally control and operate the functionality of the scan-enabled client module **104**. User interface module **108** is adapted to present a menu structure to the user and enable the user to navigate this menu structure. The menu structure provides a user with access to administrative functions, such as scan triggered service account settings (e.g., username, password, service preferences, personal information, etc.), account log-in. Such administrative functions are controlled within scan-capable or scan-enabled client module **104** via administration module **110**. The menu structure may also provide the user with the ability to control the associated smartphone camera. In some embodiments, the ability to access and operate the smartphone camera in the manner required to effectively photograph or scan a scan code icon, such as a QR code, is provided via scan control logic module **112.** In one exemplary embodiment, scan-enabled client module **104** may include a native application that is adapted to execute on mobile device **100**, and in such a case that native application may include QR scanning / decoding capability or alternatively scan-enabled client module **104** may simply invoke the services of a third-party QR scanner / decoder that is installed in the mobile device. In another exemplary embodiment, a third-party QR scanner / decoder may be invoked by the mobile device user to scan and decode a suitably provisioned QR, where decoding of the QR code causes a web browser instance to be launched and directed to a URL associated with the application server. In this case, information that identifies the relevant / necessary scan-triggered service information may be passed to the application server via the URL/URL parameters. For example, in one embodiment, information that identifies a scan-triggered service and relevant / necessary service information may be explicitly or implicitly communicated to the application server via the URL itself (e.g., the host name and/or path and/or query string components of the URL can be used by the application server to explicitly or implicitly identify the service information). In an alternate embodiment, for example, all communications between the user's mobile device and the application server may be addressed to a URL which points to a scan-based service provider (e.g., www.flashbacksurvey.com), and the information that identifies the scan-triggered service may be communicated to the scan-based service provider's application server via the path and/or query string parameter portions of the URL. In one embodiment, such a URL address associated with the scan-triggered service platform may be encoded or otherwise incorporated into a scan code associated with a scan-triggered service platform, or which requests scan-triggered application service from a scan-triggered service platform. In one embodiment, the URL which points scan-based service provider (e.g., www.flashbacksurvey.com), and the information that identifies the scan-triggered service may be encrypted, such that only a particular code scanner, native mobile code scanning application, or mobile web browser with integrated code scanning capability which has access to or is provisioned with the appropriate decryption / de-obfuscation key information can decode and process the scan-triggered service URL information and thereby facilitate the providing of the associated scan-triggered service. As such, a particular scan-triggered service code may be "locked" to all code scanners but the scanner that has access to / is provided with the appropriate decrypt / de-obfuscation key information, thereby providing users with an added measure of security with respect to accessing scan-triggered services.

The menu structure also provides the user with the ability to access and redeem participation rewards. Participation reward access and redemption functionality is provided by reward control logic module **114**. Data storage module **116** is adapted to provide both long term storage of data associated with the scan-enabled client module, as well as short term, cache-type storage of scan client related data. Exemplary uses of the data storage are discussed in more detail in the disclosure that follows.

Communications module **118** is adapted to facilitate the communication of information between scan-enabled client module **104** and an associated server application module. For example, communication module **118** may receive information from scan control logic module **112** that is to be communicated to an associated server application module. Communication module **118** may package the information according to a pre-defined message format and forward the message to a data communications interface associated with the smartphone. Exemplary data communication interfaces may include, but are not limited to, a General Packet Radio Service (GPRS) interface, an Enhanced Data Rates for GSM Evolution (EDGE), High Speed Packet Access (HSPA), WiMax, Wi-Fi, LTE, etc. For example, in one embodiment, when a user scans a service scan code associated with a scan-triggered service, communication module **118** is adapted to communicate to an associated server application module information that was encoded in the scanned service code as well as information that can be used to identify the user. Information that can be used to identify the user may include a user identifier (e.g., username, email address, mobile IP address, session ID, etc.). It will be appreciated that the communication of such user identifying information to the server module may be triggered upon scanning of the QR code or may be triggered upon startup of software associated with scan-enabled client module **104** (e.g., auto-login, manual login, etc.). As such, the communication of user identifying information and information obtained from the scanning of a scan code may be accomplished via a single message that is communicated between scan-enabled client module **104** and an associated server module, or this information may be communicated via multiple messages to the application server module. In one embodiment, when a user presents login credentials (e.g., username and password) and is successfully authenticated, a communication channel or session is established between a scan-enabled client module (e.g., a smartphone web browser or native application) and a server application module (e.g., an application residing on a network-based host computer), and all subsequent communications made via the session or channel are associated with the user's login credential / identity information. In this way, a user's identity information may be provided before, during, or even after the scanning of an associated service scanable code (e.g., QR code, NFC code, RFID code, etc.), and thereafter bound to the information derived or obtained from scanning of the code. In another embodiment, the scanning of a scan code by a user triggers the scan-enabled client module **104** to access previously stored login credential information (e.g., login credential information stored in a file or cookie that is resident on mobile communication device **100**. Scan-enabled client module **104** automatically provides the user's login credentials to the application server module, which then associates the information obtained from the scanning of the scan code with the user's account. Once the session is established, information obtained and provided to the application server module is automatically associated with the user's account. These same user identity binding techniques may be employed with any of the embodiments of the subject matter described herein.

Geo-location module **120** is adapted to determine geo-location information indicative of the geographic position of mobile communication device **100**. Geo-location information determined by module **120** may include Global Positioning System (GPS) coordinate information (e.g., latitude, longitude, elevation). Module **120** may determine this geo-location information and generally facilitate the communication of this information to an associated server application module in conjunction with the communication of scanned graphic icon (e.g., QR code) information, thereby enabling the server application module to identify and store the location at which a QR code was scanned. Alternatively, geo-location or position information may be encoded in the QR code that was scanned, and once scanned the location information may be decoded by geo-location module **120** and passed along to a server application module associated with the scan code-based service system. It is understood that with the addition of scan-enabled client module **104**, mobile device **100** becomes a special purpose computing platform that improves the functionality of mobile device **100** by providing direct access to a server application in response to receiving a scanned code from camera **102**. Mobile device **100** with scan-enable client module **104** also improves the technological field of network access to services because such services can be accessed automatically and quickly with a reduced likelihood of data entry errors. Processor **122** is adapted to facilitate the execution of software and firmware associated with the operation of modules **106**, **108**, **110**, **112**, **114**, **116**, **118** and **120**, which is used to provide the overall scan-enabled client module functionality described herein. Exemplary implementations of processor **122** include, but are not limited to, one or more single-core microprocessors, one or more multi-core microprocessors, and one or more programmable logic devices (e.g., complex programmable logic devices, field-programmable gate arrays, etc.).

Figure 2 is a block diagram that illustrates an exemplary architecture of a server application module **202**, which resides and executes on a network or cloud-hosted application server **200**. In the embodiment presented in Figure 2, the server application module is comprised of a provisioning, administration and billing module **204**, a reporting module **206**, a trusted square control logic module **208**, a reward control logic module **210**, a data storage module **212**, a communication module **214**, a RateIt square control logic module **216**, a TrackIt square control logic module **220**, a Clin square control logic module **222**, a connect square control logic module **224**, and processor **226**. The purpose and function of each of these modules and of the processor is described below. Server application module **202** executing on application server **200** makes application server **200** a special purpose computing platform that improves the functionality of application server **200** by configuring application server **200** to process received scanned codes and providing the indicated service in response to receiving the scanned codes. As such, server application module **202** improves the technological fields of network access to services by providing such services automatically in response to receiving the scanned codes and with a reduced likelihood of data entry error.

Provisioning, administration and billing module **204** is adapted to provide access for a provisioning entity or user, such as a medical office administrator, merchant entity, a delivery service vendor entity, an event venue entity, mobile user entity or a system administrator, to provision registration information, subscription configurations / preference information, service configuration information, and participation reward content information. In the context of this disclosure, a user is considered to be the operator or user of a mobile communication device (e.g., computer integrated eyewear, wearable computer, smartphone, tablet computer, etc.) that includes a scan-enabled client module, and is therefore capable of scanning a QR code (or other encoded, scanable code) and provide, trigger, initiate or facilitate the providing of a service to the user. For example, a user may be a consumer of goods and services provided by a merchant, an attendee of an event, a medical patient, a shopper, or an employee of a corporation.

In all of the embodiments disclosed herein, a scanning user may be granted or credited with a digital reward or coupon in response to the scanning of an associated scan-triggered service code. Exemplary digital rewards may include, but are not limited to, a digital or electronic coupon associated with a good or a service, a credit for an online gaming service, a credit for an online video, an audio or video download. In one embodiment, the value of a granted digital reward may be determined, based at least in part, on the type / brand / manufacturer of the mobile phone that was used to scan the associated scan-triggered service scan code. In one embodiment, such rewards may be credited or placed in a digital reward wallet associated with the user, whereby the user can access and redeem a granted reward. In one embodiment, a reward granted to a user may be granted at a first value (e.g., $1 off next purchase) and subsequently modified to a second value (e.g., $2 off next purchase) at a later by Reward Control Module **210**.

Module **210** may facilitate the sharing of a scan-triggered service platform-granted reward from one user to another user, where sharing may include the gifting, transferring, or cloning of a granted reward. In this case, a first user who is the current owner of a reward selects the reward and identifies a second user to whom the reward is to be transferred. The first user then communicates information that identifies both the reward and the "transferred to" user to module **210**. The information that identifies the "transferred to" or recipient user may be a username or user ID provided by the recipient user at the time of registration by the recipient user. Module **210** receives, processes and logs the transfer request and updates the appropriate reward data so as to execute the transfer. In one embodiment, reporting module **206** enables an administrative entity or user to view, track and analyze such reward transfers. In various embodiments of the subject matter described herein, restrictions / limitations / qualifications may be imposed on rewards that are to be transferred or gifted from one user to another. For instance, module **210** may include reward transfer or gifting rules that specify those conditions under which a reward may be transferred and/or those conditions under which a reward may not be transferred. These rules may be stored in a database, table, or data structure that is contained within or accessible by module **210**. An exemplary rule may state that a reward may only be transferred or gifted to a new user (e.g., a user that has registered for service within the past 30 days, etc.). In order to enforce this rule module **210** may access user registration data that is maintained in data storage module **212**. Another exemplary rule may state that a reward may only be transferred or gifted to a user who has not previously patronized the scan-triggered service client entity with which the reward is associated. In order to enforce this rule module **210** may access user transaction data that is maintained in data storage module **212**.

In one embodiment, reward sharing functionality includes functionality where an existing user may clone/copy, transfer or gift a reward to an individual who has not yet become a registered scan-triggered service user. To facilitate such a special transfer, the existing user communicates information that identifies both the reward and the "transferred to" or recipient user to module **210**. In this case, since the recipient user is not yet a registered user of the system / service, the existing user must specify a public contact address for the intended recipient. Exemplary public contact addresses may include, but are not limited to, an email address, a mobile telephone number, a mobile subscriber ISDN (MSISDN), a Twitter address, an instant message address. Module **210** receives processes and logs the transfer request. In one embodiment, module **210** is adapted to generate a message that is addressed to the specified public contact address (e.g., email address). In one embodiment, the message may include the transferred reward or information specifying how the transferred reward may be obtained and redeemed. In another embodiment, the message may include information that describes the pending reward transfer and also provides a hyperlink / URL associated with a web page where the intended recipient may register and thereby receive and redeem the transferred reward. The existing user that transferred or gifted the reward (thereby resulting in the recruitment / registration of a new subscriber) may be issued a new reward as a result of the transfer. The new reward may be the same as the transferred reward or different. The new reward may be issued by reward control logic module **210**.

Processor **226** is adapted to facilitate the execution of software and firmware associated with the operation of modules **204**, **206**, **208**, **210**, **212**, **214**, **216**, **218**, **220**, **222** and **224**, which is used to provide the overall server application module functionality described herein. Exemplary implementations of processor **226** include, but are not limited to, one or more single-core microprocessors, one or more multi-core microprocessors, and one or more programmable logic devices (e.g., complex programmable logic devices, field-programmable gate arrays, etc.).

Trusted Square

Figure 3A is diagram that generally illustrates the provisioning of information associated with a service of a scan code-based service system according to an embodiment of the subject matter described herein. This service is referred to herein as Trusted Square service, which is a service that facilitates the delivery by proxy of a user's personal information to a 3rd party, referred to herein as a Requesting Entity, during the course of a computer-based transaction, such as a world wide web-based online transaction. As described herein, a user's personal information may include, but is not limited to, first name, last name, middle name, street or postal address, zip code, email address, billing address, shipping address, telephone number, credit card / debit card information, merchant loyalty account number / identifier information, medical history information, medical condition information, healthcare-related information, insurance information (e.g., medical), academic credential information, and employment history information.

As indicated in Figure 3A a user of the trusted square service logs into application server **200** and provisions their personal information (steps 1 and 2), which is stored in data storage module **212**. This personal information is associated with user's account via an identifier, such as a User ID **300**. Illustrated in Tables 1 – 3 is exemplary personal information associated with a user, which includes User Name **302**, street address **306**, billing address **308**, phone number(s) **310**, and credit/debit card information **312 – 316**. In one embodiment, the user account identifier may be a username or identifier (e.g., email address, etc.) associated with a scan-triggered service account. By doing such, the user is considered to be a registered Trusted Square service user. An new, unregistered user who attempts to use the Trusted Square service by scanning a Trusted Square code will be prompted to register (i.e., provide the user account and personal information mentioned above) before such service is provided. Although not shown in Figure 3A, it will be appreciated that a requesting entity that uses the trusted square service would also log in to the system and provide basic registration information, which would result in the provisioning or assignment of a unique trusted square account identifier to the Requesting Entity (e.g., RequestingEntityID). This RequestingEntityID **318** may be used in subsequent trusted square operations and processes associated with use of the trusted square service to identify the Requesting Entity **320** (e.g., an on-line merchant, healthcare provider, etc.). In one embodiment, a RequestingEntityID may be associated with a network address (e.g., server identifier, host URL **324**, IP Address/Port **322**, etc.) which is in turn associated with a network connected computer or terminal used by the Requesting Entity (e.g., merchant, healthcare provider, etc.). Such association is generally illustrated in the exemplary data shown in Table 4 illustrated in Figure 3I. Security credentials **326** required to establish or maintain a secure connection to the requesting entity's computer/terminal/server may also be stored / obtained and used by scan-triggered server to establish a secure connection to the requesting entity's computer.

The embodiments described below relate to web-based interactions or transactions between a user and the host of an on-line service, such as an online merchant. However, it will be appreciated that embodiments of the subject matter described herein could be used to facilitate the communication of a user's personal information between a centralized Trusted Square user personal information storage system and any

Requesting Entity that is adapted to communicate with the storage system (e.g., via public or private network connection). Exemplary Requesting Entities may include, but are not limited to, merchants, web-based businesses, on-line service providers, government agencies, healthcare providers, point of sale device entities, commercial entities, etc. As used with respect to the description herein of trusted square services, the term TransactionID is intended to represent any identifier or collection of identifiers that can be used by a Requesting Entity to identify a transaction, session, or other interaction with a user that requires the collection of the user's personal information.

Figures 3B and 3C are process flow diagrams which generally illustrate use and operation of one exemplary embodiment of trusted square scan-triggered service. In this example, beginning with step 1, a user who is accessing the web site of an on-line merchant to purchase a good or service selects a desired good or service, places it in the user's cart, and proceeds to the checkout screen or otherwise reaches a point where the user's personal information is needed by the hosting / visited web site. In step 2, the Requesting Entity / merchant's web site **202** communicates a trusted square scan code request to server **200**, which may include an identifier associated with the user's session or transaction, and may also include information that specifies the particular personal information that is being requested. In one embodiment, a pre-defined personal information profile identifier may be included in the request, which conveys to server **200** information that can be used to determine or assist in the determination of the type / amount of personal information that is being requested. It will be appreciated that in other embodiments, the type / amount of personal information being requested may be agreed upon in advance by servers **200** and **202**, and as such this information may be considered to be implicit with respect to receipt of the request message.

In step 3, server **200** processes the request and generates a TrustedSquareID identifier value **328**, which is associated with the request / request information. In one embodiment, server **200** creates and stores a binding record that is adapted to associate the user session / transaction identifying information **338** with the TrustedSquareID identifier value **328**. Exemplary binding record data is shown in Tables 5 and 6. Also associated with the TrustedSquareID identifier **328** is information which can be used to identify the Requesting Entity, such as RequestingEntityID **330**. In one embodiment, a confirmation PIN or password **332** may be generated and associated with the TrustedSquareID value. This PIN may be provided to the scanning user, who can then manually enter the PIN following the scanning of the associated Trusted Square scan code. Once entered by the user, the PIN information is communicated to server **200** where it is checked against the stored PIN value **332** to provide confirmation / guard against malicious, fraudulent or computer / botnet attacks. In one embodiment, an external medium security / confirmation key **334** may be generated and associated with the TrustedSquareID value. This external medium security / confirmation key **334** may, for example, be included in an email, text message, or Tweet that is communicated to the scanning user as a click-able confirmation hyperlink. When the externally communicated confirmation email/text message is received by the scanning user and the confirmation hyperlink is clicked, a confirmation message is communicated to server **200** and is interpreted as a confirmation that the scanning user intended to cause the user's personal information to be communicated to the requesting entity. In one embodiment, information **338** that can be used to identify a user session or user transaction associated with requesting server **202** (or an associated point of sale terminal) is including in the binding. In one embodiment, TrustedSquareID **328** is associated with user personal profile identifier information **340**.

In step 4, the TrustedSquareID identifier value or a scan code (e.g., QR code) containing the TrustedSquareID identifier value is communicated to requesting server **202**. In other embodiments, the TrustedSquareID identifier value or a scan code (e.g., QR code) containing the TrustedSquareID identifier value is communicated directly to computer terminal / device **600**, where the associated QR code image is displayed to the user, for example on a web page. In step 5 of the embodiment shown in Figure 3B, server **202** communicates the trusted square scan code information to computer terminal / device **600** where it is displayed (e.g., as a trusted square QR code) to the user of mobile device **100**. Once again, encoded within the Trusted Square scan code is a unique TrustedSquareID identifier value **328** or a group of identifiers that can be used collectively to form / serve the purpose of a TrustedSquareID value. In one embodiment, a TrustedSquareID value contains, implicitly or explicitly, information that is sufficient for scan-triggered server **200** to determine the Requesting Entity and/or the identity / address of the requesting computer, terminal, server, web server / web session. For a given Requesting Entity (e.g., merchant, etc.), each TrustedSquareID value may be unique to a user transaction or user information request. For example, if a user's healthcare provider needs to collect the user's personal information (e.g., name, address, medical history, etc.), the Trusted Square scan code that is generated for this personal information exchange request / transaction will include a TrustedSquareID value that is unique to request and, as such, to the user. The TrustedSquareID may also contain information which is sufficient for server **200** to determine that the associated personal information exchange request is associated with the user's healthcare provider (e.g., RequestingEntityID or a computer/terminal/server address associated with the healthcare provider's computer system, etc.). In one embodiment, the Trusted Square QR code also includes information that identifies or can be used to identify a Trusted Square scan-triggered application service server **200**.

In an alternate embodiment (not shown), the Trusted Square QR code is generated by a client software module or application residing, for example, on a user's desktop computer. For instance a Java module may be adapted to generate a trusted square scan code similar to that described in the previous embodiment. In this case, the client software module on the desktop computer is adapted to communicate with scan-triggered server **200** so as to create and store the necessary trusted square binding record, and to generate and display the associated Trusted Square scan code that can be scanned by a user. In one embodiment, the Trusted Square QR code also includes information that identifies or can be used to identify a Trusted Square scan-triggered application service server **200**.

Returning to Figure 3B, when the trusted square QR code displayed on the screen is scanned by the user's QR code scanner in mobile device **100** (steps 6 and 7), the encoded information is extracted by the QR code scanner and the information that identifies or can be used to identify a trusted square application server is used to facilitate communication of the extracted information element(s) (i.e., TrustedSquareID, personal information profile identifier **340**, etc.) to the identified Trusted Square application server **200**. Exemplary personal information profile data elements **352**, which are associated with a PersonalInformationProfileID identifier **350** are shown in Table 8A illustrated in Figure 3J. Exemplary personal information profile date and may include, but is not limited to, name, address information, credit/debit card information, medical or healthcare information, surgical history, medical record information, academic history information, job history information, dependent (e.g., children) identifying information and associated personal information, etc. It will be appreciated that in various embodiments of the subject matter described herein, the TrustedSquareID information and user session / transaction identifying information may be encrypted or obfuscated during communication from the user's mobile communication device to the Trusted Square application server **200**. In other embodiments, the information that identifies or can be used to identify a Trusted Square application server may itself be encrypted or obfuscated when read by the QR code scanner, and may be subsequently decrypted / de-obfuscated by scan control logic module **112** so as to obtain the information necessary to identify the Trusted Square application server to be contacted. Also communicated to the Trusted Square application server **200** is information that identifies or can be used to identify the user (e.g., the person that scans the Trusted Square QR code). This user identifying information may be provided to the Trusted

Square application server **200** before, after, or at the same time that the previously discussed tuple of scanned information is provided. For example, in one embodiment, the user may log in (i.e., provide login credentials that are sufficient to identify and authenticate the user) prior to scanning the Trusted Square QR code, and application server **200** is adapted to associate the subsequently received information with the user. Alternatively, the user's login credentials may be provided at the time of / as a result of the Trusted Square QR code scan, along with the TrustedSquareID information. This is the particular example illustrated in step 7 of Figure 3B. Once the user and scanned TrustedSquareID information is received (and decrypted / de-obfuscated, if necessary), the information is stored in data storage module **212**. In embodiments where additional confirmation information is collected from the scanning user prior to communication of the user's personal information to the requesting entity (e.g., confirmation PIN, external medium confirmation, etc.), such user-provided confirmation information is collected and stored, as illustrated in exemplary data Table 7A. Exemplary confirmation information may include, but is not limited to, TrustedSquareID information **328**, user identifying information **340**, scan or confirmation timestamp information **342**, user-provided confirmation code information **344**, external confirmation code information **346** (e.g., such a confirmation code that is obtained from user activation of a confirmation hyperlink sent in an external email to the user, etc.), and granted reward identifier information **348**. Exemplary reward information is presented in Table 9A, and includes reward identifier information **354**, reward description / value information **356**, associated reward entity identifying information **357**, and reward expiration information **358**.

As indicated in step 8 of Figure 3C, application server **200** authenticates the user via the received user identifying information / login credentials (as well as any user-provided confirmation information), and examines the received scanned TrustedSquareID information. Authentication and validation processing is performed by Trusted Square Control Logic Module **208** on the scanned TrustedSquareID information to guard against fraudulent or malicious use of the Trusted Square system. For example, the received TrustedSquareID information may be compared against a list of recent Trusted Square transactions to determine the frequency of requests involving the Requesting Entity. Such service access attempt frequency analysis may also be performed with respect to the user ID information associated with received requests to identify suspicious or fraudulent use patterns. Alternatively, or in addition to such security processing, received scanned TrustedSquareID and user identifying information that fails security screening may be added to a suspicious access attempt list. Information contained in this list may be used to determine whether to allow or deny subsequent service access attempts by a user or Requesting Entity.

Assuming authentication and security processing is concluded successfully, Trusted Square Control Logic Module **208** is adapted to access the user's stored personal information using the received user identifying information or using information associated with the received user identification information. Application server **200** is adapted to communicate the user's personal information to a computer / server associated with the Requesting Entity and/or the received TrustedSquareID information (step 9). In one embodiment, application server **200** may access pre-provisioned communication parameters for the associated Requesting EntityID, such as is generally illustrated in Table 4. For example, application server **200** may establish a secure connection to a server associated with the Requesting EntityID using pre-provisioned destination Internet protocol (IP) address and port information. In an alternate embodiment, application server **200** may establish a secure connection to a server associated with the Requesting EntityID using a pre-provisioned uniform resource locator (URL) address. Alternatively, a permanent or quasi-permanent connection may be established and maintained between application server **200** and a Requesting Entity's server, such as merchant web server **202** shown in Figure 3C.

Regardless of how the connection is established, once the connection between application server **200** and the Requesting Entity server **202** is established, the user's personal information is communicated from application server **200** to the Requesting Entity server **202**, as indicated in step 9. This information may be encrypted by application server **200** for the purposes of security during transmission, and subsequently decrypted by Requesting Entity server **202**. Any number of well-known encryption and/or obfuscation techniques may be employed and, as such, will not be described in detail here.

Once received by Requesting Entity server **202**, the user's personal information may be used to complete the on-line transaction or other personal information-requiring transaction, as indicated in step 10. It will be appreciated that in one embodiment, the Requesting Entity server **202** may display on-screen (or cause to be displayed) some or all of the user's personal information so that it can be viewed by the user who scanned the Trusted Square QR code which triggered the personal information transfer to the merchant. From a security standpoint, it may be advantageous to prevent the user from editing or changing the shipping address that is communicated from application server **200** to Requesting Entity server **202**.

Shown in Figure 3D is an alternate embodiment of the trusted square service. As indicated in step 1 of Figure 3D, in this embodiment, a user engaged in an on-line transaction places a good or service in the user's cart and proceeds to the checkout page or otherwise reaches a point where personal information needs to be provided to the Requesting Entity's web site. In step 2, the Requesting Entity server **202** is adapted to generate a TrustedSquareID value and to create and store a binding record which associates the TrustedSquareID value and the user session / transaction. In one embodiment, the TrustedSquareID value generated by Requesting Entity server **202** is adapted to include or incorporate information that can be used by scan-triggered server **200** to identify the Requesting Entity, Requesting Entity server **202** or another computer / server associated with the Requesting Entity. In one embodiment, the associated trusted square scan code (e.g., QR code) that includes the TrustedSquareID value also includes encoded information that can be used to identify a trusted square scan-triggered server **200**. In step 3 the trusted square QR code image that is then displayed to the user via computer screen **600**. When the trusted square QR code displayed on the screen is scanned by the user's QR code scanner (step 4), the encoded TrustedSquareID and trusted square server identifier or address information is extracted by the QR code scanner and the information that identifies or can be used to identify a trusted square application server is used to facilitate communication of the extracted TrustedSquareID information to the identified trusted square application server (step 5). It will be appreciated that in various embodiments of the subject matter described herein, the TrustedSquareID information may be encrypted or obfuscated during communication from the user's mobile communication device to the trusted square application server. In other embodiments, the information that identifies or can be used to identify a trusted square application server may itself be encrypted or obfuscated when read by the QR code scanner, and may be subsequently decrypted / de-obfuscated by scan control logic module **112** so as to obtain the information necessary to identify the trusted square application server to be contacted. Also communicated to the trusted square application server is information that identifies or can be used to identify the user (e.g., the person that scans the trusted square QR code). This user identifying information may be provided to the trusted square application server **200** before, after, or at the same time that the previously discussed scanned information is provided. For example, in one embodiment, the user may log in (i.e., provide login credentials that are sufficient to identify and authenticate the user) prior to scanning the trusted square QR code, and application server **200** is adapted to associate the subsequently received TrustedSquareID information with the user. Alternatively, the user's login credentials may be provided at the time of / as a result of the trusted square QR code scan, along with the TrustedSquareID information. This is the particular example illustrated in step 5 of Figure 3D. Once the user and scanned

TrustedSquareID information is received (and decrypted / de-obfuscated, if necessary), the information is stored in data storage module **212**. Exemplary scan transaction stored data is shown in Table 7A and includes received TrustedSquareID **328**, userID information **340**, scan timestamp information **342**, received confirmation PIN information **344**, received external confirmation key information **346**, and granted Reward identifier information **348**.

Application server **200** authenticates the user via the received user identifying information / login credentials, and examines the received scanned TrustedSquareID information (step 6). Authentication and validation processing is performed by trusted square control logic module **208** on the scanned TrustedSquareID information to guard against fraudulent or malicious use of the trusted square system. For example, the received TrustedSquareID information may be compared against a list of recent trusted square transactions to determine the frequency of requests involving the TrustedSquareID. Such access attempt frequency analysis may also be performed with respect to the user ID information associated with received requests to identify suspicious or fraudulent use patterns. Alternatively, or in addition to such security processing, received scanned TrustedSquareID and user identifying information that fails security screening may be added to a suspicious access attempt list. Information contained in this list may be used to determine whether to allow or deny subsequent service access attempts by a user or merchant.

Assuming authentication and security processing is concluded successfully, trusted square control logic module **208** is adapted to access the user's stored personal information using the received user identifying information or using information associated with the received user identification information. Application server **200** is adapted to communicate the user's personal information to a computer associated with the received TrustedSquareID information (step 7). In one embodiment, application server **200** may access pre-provisioned communication parameters for the associated Requesting EntityID, such as is generally illustrated in Table 4.

For example, application server **200** may establish a secure connection to a server associated with the Requesting EntityID using pre-provisioned destination Internet protocol (IP) address and port information. In an alternate embodiment, application server **200** may establish a secure connection to a server associated with the Requesting EntityID using a pre-provisioned uniform resource locator (URL) address. Alternatively, a permanent or semi-permanent connection may be established and maintained between application server **200** and a Requesting Entity's server.

Regardless of how the connection is established, once the connection between application server **200** and the Requesting Entity server **202** is established, the user's personal information is communicated from application server **200** to the Requesting Entity server **202**, as indicated in step 8. This information may be encrypted by application server **200** for the purposes of security during transmission, and subsequently decrypted by Requesting Entity server **202**. Any number of well-known encryption and/or obfuscation techniques may be employed and, as such, will not be described in detail here.

Once received by server **202**, the user's personal information may be used to complete the on-line transaction, as indicated in step 9. It will be appreciated that in one embodiment, server **202** may display on-screen (or cause to be displayed) some or all of the user's personal information so that it can be viewed by the user who scanned the trusted square QR code which triggered the personal information transfer to the merchant. From a security standpoint, it may be advantageous to prevent the user from editing or changing the shipping address that is communicated from application server **200** to Requesting Entity server **202**.

It will be appreciated with regard to the trusted square service embodiments described above that such services may also be provided via a native trusted square application that is installed on the user's smartphone. In such cases, information that identifies or can be used to identify the address of a trusted square server to which the TransactionID information should be communicated need not be encoded within the trusted square QR code that is displayed to and scanned by a user. In such native application deployments, the information that identifies or can be used to identify the address of a trusted square server may be pre-configured and stored in the smartphone's memory, such as in data storage module **116**. Alternatively, the native application may dynamically determine the address of the appropriate trusted square server at the time of the trusted square QR code scan by a user. In such scenarios, trusted square processing is very similar to that described above, except that the address of the trusted square server is not obtained by a user scan of a trusted square QR code.

The embodiments described below relate to in-store interactions or transactions between a user and a place of business, such as a restaurant. However, it will be appreciated that embodiments of the subject matter described herein could be used to facilitate the communication of a user's personal information between a centralized trusted square user personal information storage system and Requesting Entity associated with any type of commercial or non-commercial organization. Exemplary Requesting Entities may include, but are not limited to, merchants, brick-and-mortar businesses, healthcare providers, insurance providers, government agencies, commercial entities, etc. As used with respect to the description herein of trusted square services, the term TrustedSquareID is intended to represent any identifier or collection of identifiers that can be used to identify a transaction, session, or other interaction with a user that requires the collection of the user's personal information.

Figure 3E illustrates an exemplary process flow diagram which generally illustrates use and operation of one embodiment of the trusted square service that involves a point of sale / service (PoS) terminal. Beginning with step 1, a PoS terminal **602** (e.g., a cash register, restaurant order management system, etc.) associated with a merchant (e.g., a restaurant) generates a customer transaction and an associated customer bill, for example, a transaction and bill associated with a meal in the merchant's restaurant. In one embodiment, the trusted square QR code is generated by the merchant's PoS system **602**, for example, using a trusted square software module that has been incorporated into or is accessible to the merchant's PoS system. In this case, the trusted square software module is adapted to generate a scan code identifier, such as a TrustedSquareID value, which is associated with the user's checkout / personal information request or transaction and which can, in some embodiments, be used by the trusted square server **200** to identify the requesting entity (e.g., merchant, healthcare provider, etc.). The trusted square software module then generates and display a trusted square QR code that encodes / includes the TrustedSquareID value and, in one embodiment, information that identifies or can be used to identify trusted square application server **200**.

In step 2, the trusted square QR code is printed and displayed on the customer's bill. When the trusted square QR code displayed on the bill is scanned by the user's QR code scanner (step 3), the encoded information is extracted by the QR code scanner and the information that identifies or can be used to identify a trusted square application server is used to facilitate communication of the extracted information element (i.e., TrustedSquareID) to the identified trusted square application server, as indicated in step 4. In other embodiments, scan-enabled client module **104** may be programmed with or may determine the address of the trusted square server to which the scan information is to be sent for processing. Exemplary information that identifies or can be used to identify a trusted square scan-triggered application service server includes, but is not limited to, a uniform resource locator URL), Internet protocol address and port, etc. This same server identification approach may be applied to any and all of the other embodiments of scan-based services described herein. It will be appreciated that in various embodiments of the subject matter described herein, the merchant identifying information and user transaction identifying information (i.e., TrustedSquareID) may be encrypted or obfuscated during communication from the user's mobile communication device to the trusted square application server. In other embodiments, the information that identifies or can be used to identify a trusted square application server may itself be encrypted or obfuscated when read by the QR code scanner, and may be subsequently decrypted / de-obfuscated by scan control logic module **112** so as to obtain the information necessary to identify the trusted square application server to be contacted. Also communicated to the trusted square application server is information that identifies or can be used to identify the user (e.g., the person that scans the trusted square QR code). This user identifying information may be provided to the trusted square application server **200** before, after, or at the same time that the previously discussed tuple of scanned information is provided. For example, in one embodiment, the user may log in (i.e., provide login credentials that are sufficient to identify and authenticate the user) prior to scanning the trusted square QR code, and application server **200** is adapted to associate the subsequently received information with the user. Alternatively, the user's login credentials may be provided at the time of / as a result of the trusted square QR code scan, along with the TrustedSquareID information. This is the particular example illustrated in step 5 of Figure 3E. Once the user and scanned TrustedSquareID information is received (and decrypted / de-obfuscated, if necessary), the information is stored in data storage module **212**. Exemplary stored data is shown in Table 7A.

As indicated in step 5, application server **200** authenticates the user via the received user identifying information / login credentials, and examines the received scanned TrustedSquareID information. Authentication and validation processing is performed by trusted square control logic module **208** on the scanned TrustedSquareID information to guard against fraudulent or malicious use of the trusted square system. For example, the received TrustedSquareID information may be compared against a list of recent trusted square transactions to determine the frequency of requests involving the Requesting Entity / POS device. Such service access attempt frequency analysis may also be performed with respect to the user ID information associated with received requests to identify suspicious or fraudulent use patterns. Alternatively, or in addition to such security processing, received scanned TrustedSquareID and user identifying information that fails security screening may be added to a suspicious access attempt list. Information contained in this list may be used to determine whether to allow or deny subsequent service access attempts by a user or Requesting Entity.

Assuming authentication and security processing is concluded successfully, trusted square control logic module **208** is adapted to access the user's stored personal information using the received user identifying information or using information associated with the received user identification information. Application server **200** is adapted to communicate the user's personal information to a computer associated with the Requesting Entity and/or received TransactionID information. In one embodiment, application server **200** may access pre-provisioned communication parameters for the associated Requesting EntityID, such as is generally illustrated in Table 4. For example, application server **200** may establish a secure connection to a server associated with the Requesting EntityID using pre-provisioned destination Internet protocol (IP) address and port information. In an alternate embodiment, application server **200** may establish a secure connection to a server associated with the Requesting EntityID using a pre-provisioned uniform resource locator (URL) address. Alternatively, a permanent or semi-permanent connection may be established and maintained between application server **200** and a merchant's server, such as merchant POS system **602**.

Regardless of how the connection is established, once the connection between application server **200** and the merchant POS system **602** is established, the user's personal information is communicated from application server **200** to the merchant POS system **602**, as indicated in step 6. This information may be encrypted by application server **200** for the purposes of security during transmission, and subsequently decrypted by merchant POS system **602**. Any number of well-known encryption and/or obfuscation techniques may be employed and, as such, will not be described in detail here.

Once received by merchant POS system **602**, the user's personal information may be used to complete the in-store transaction, as indicated in step 7. It will be appreciated that in one embodiment, the merchant POS system **602** may display on-screen (or cause to be displayed) some or all of the user's personal information so that it can be viewed by the user who scanned the trusted square QR code which triggered the personal information transfer to the merchant.

Shown in Figure 3F is yet another embodiment of the trusted square service. In this embodiment, a user engaged in an in-store transaction, such as the restaurant transaction previously described in a manner similar to that described in the previous embodiment that was shown in Figure 3E. In this previous embodiment, the merchant's / requesting entity's POS terminal generated a TrustedSquareID and associated trusted square scan code, which was presented to the user for scanning. In the present embodiment, the requesting entity's / merchant's POS system **602** is adapted to first communicate a trusted square binding request message to trusted square application server **200** (step 1). The binding request includes information which identifies or can be used to identify the user's bill, order, transaction, or other session that requires or is associated with the collection of personal information from the user. In one embodiment, information which can be used to identify the Requesting Entity / POS terminal may also be included in the request message. In this example, trusted square scan-triggered server **200** receives the request and generates a TrustedSquareID and associates this identifier with the provided user session / transaction information. This association information is stored by server **200** in a binding record. The TrustedSquareID information is communicated to the requesting POS **602** in step 2. From this point forward, steps 3 through 8 proceed in a manner that is similar to the analogous steps previously described in the embodiment shown in Figure 3E, and as such a detailed discussion of these steps is not repeated here.

Shown in Figures 3G and 3H is yet another embodiment of the trusted square service. In this exemplary embodiment, operation and processing initially proceeds in a manner somewhat similar to that shown in Figure 3F. The one key difference is related to the communication and subsequent use of order / transaction / invoice / session detail information (e.g., 1 drink @ $1, 2 fries @ $2, etc.), which is communicated from requesting POS **602** to scan-triggered trusted square server **200**, as indicated in step 1 of Figure 3G. Server **200** receives and processes this order detail information, along with user session / transaction identifier information, which includes generating a TrustedSquareID value, binding the TrustedSquareID value to the user session / transaction identifier and order detail information, and storing this associated information in a binding record. In step 2, the TrustedSquareID value and/or the associated trusted square scan code (e.g., QR code) is communicated to requesting POS **602**. As discussed in previous embodiments and examples, in some embodiments, information which can be used to identify scan-triggered trusted square server **200** may be included / encoded in the associated trusted square scan code (e.g., QR code) that is presented for scanning to the user. In other embodiments, scan-enabled client module **104** may be programmed with or may determine the address of the trusted square server to which the scan information is to be sent for processing. Exemplary information that identifies or can be used to identify a trusted square scan-triggered application service server includes, but is not limited to, a uniform resource locator URL), Internet protocol address and port, etc. Steps 3 – 6 proceed in a manner similar to that previously described in other embodiments in this disclosure and hence a detailed description of these steps is not repeated here.

In step 5, user **100** scans the trusted square scan code provided by requesting POS **602** and in response, as shown in Figure 3H, scan-triggered server **200** accesses the previously stored binding record associated with the scanned/provided TrustedSquareID value. Server **200** extracts order / bill / invoice detail information from the binding record and communicates this information to user **100** in step 7. In one embodiment, server **200** also communicates / displays to user **100** a confirmation option, such as a tap-able confirmation button that is displayed on the screen of the user's mobile device (along with the order detail information). In such an embodiment, server **200** is adapted to wait to receive positive confirmation / authorization from the user (e.g., the user taps the on-screen confirmation button or clicks a confirmation / authorization hyperlink in an external email / text message that is sent to the user, etc.) prior to completing / fulfilling the personal information transfer request made by requesting POS **602**. In step 8, the user **100** submits confirmation / authorization instruction information to server **200**. In steps 9 and 10, server **200** communicates the requested personal information associated with the user to requesting POS **602** where it is used to complete the transaction / personal information request session.

It will be appreciated that a merchant may provision participation rewards which may be distributed via any number of distribution algorithms in response to the use of trusted square service by a user. In one embodiment, reward Control Logic Module **210** may distribute a participation reward to a user in response to the scanning of a trusted square QR code by the user. Exemplary participation reward data provisioned by a merchant is shown in Table 9B, and includes RewardID information **354**, reward description information **356**, reward entity / issuer information **357**, and reward expiration date information **358**. Such digital rewards may be credited to a digital reward wallet associated with the user's scan-triggered trusted square service account.

It will be appreciated with regard to the trusted square service embodiments described above that such services may also be provided via a native trusted square application that is installed on the user's smartphone. In such cases, information that identifies or can be used to identify the address of a trusted square server to which the TrustedSquareID information should be communicated need not be encoded within the trusted square QR code that is displayed to and scanned by a user. In such native application deployments, the information that identifies or can be used to identify the address of a trusted square server may be pre-configured and stored in the smartphone's memory, such as in data storage module **116**. Alternatively, the native application may dynamically determine the address of the appropriate trusted square server at the time of the trusted square QR code scan by a user or may have address information associated with a trusted square service providing server statically provisioned in the native app residing on the mobile communication device. In such scenarios, trusted square processing is very similar to that described above, except that the address of the trusted square server is not obtained by a user scan of a trusted square QR code.

It will be appreciated that embodiments of the present trusted square system are particularly useful in minimizing the risks associated with credit card / personal identity theft, as the user's credit card need never leave the user's possession during the course of the entire transaction. Additionally, embodiments of the present trusted square system are useful in minimizing the risks associated with malicious keystroke logging viruses and worms that commonly infect the computers of on-line users / shoppers, as no personal information need be typed by the user in order to complete an on-line transaction.

According to one aspect of the subject matter described herein, a system for facilitating the communication of personal information using information obtained from the scanning of a scanable code by the user of a scan-enabled client module is provided. The system includes a computing platform having at least one processor. The system further includes a server application module executable by or embedded within the at least one processor and configured to store personal information associated with a user. The server application module is further configured to receive from a communication terminal associated with the requesting entity, a request that includes information that can be used to identify a personal information request transaction between a requesting entity and the user. The server application module is further configured to, in response to receiving the request, create and store a scan code identifier that is bound to the personal information transaction request. The server application module is further configured to communicate the scan code identifier to computer associated with the requesting entity for inclusion in a user scanable service request code that is displayed to the user. The server application module is further configured to receive, in response to the scanning of the user scanable service code by the user, the scan code identifier and information that can be used to identify the user. The server application module is further configured to, in response to receiving the scan code identifier and information that can be used to identify the user, accessing the user's stored personal information. The server application module is further configured to communicate the user's personal information to a communication terminal associated with the requesting entity.

Connect Square

Shown in Figure 4A is diagram that generally illustrates the provisioning of information associated with one embodiment of a scan-triggered service provided by a scan-triggered application server. This scan-triggered service is referred to herein as Connect Square service, which is a service that facilitates the addition of an item to a list for the user that is triggered via the scanning of a Connect Square service scan code by the user. One exemplary use of Connect Square service might involve a vendor who is displaying goods or services at a trade show. A user who would like to remember a particular vendor or later access information /materials associated with the vendor scans a Connect Square QR code associated with the particular vendor using the QR code scanner on the user's mobile phone. Scanning of the Connect Square causes descriptive information (e.g., name, address, phone number, email address, web site URL, product description information) about that particular vendor to be saved in the user's Connect Square data vault. The user can then log into the user's Connect Square vault at any time and browse information about that vendor. According to one aspect of the disclosed subject matter presented herein, module **224** enables an information sharing entity (e.g., a merchant, corporate personnel, healthcare staff, etc.) to provision data / information that is to be shared with one or more users. An exemplary information

Share may be a link/URL that points to a Google Drive Shared document / file. If the information sharing entity wishes to distribute or make this information Share link available to a select set of individuals (e.g., only users of the connect square scan triggered service system), then simply encoding a generic QR scan code with the web address / URL of the information Share link would not provide the information sharing entity with sufficient access controls, since anyone could scan the associated generic QR code and access the Shared information. The scan-triggered system disclosed herein provides a unique way for users to authenticated / authorized with respect to the information Share, where the authentication / authorization is performed by the scan-triggered service provider. Once a scanning user has been authenticated (e.g., by the presenting of valid scan-triggered service log-in credentials, etc.) by sever **200** at the time of the scan, the user is granted access to the associated information Share. In one embodiment, the information Share content may be hosted / stored on a server(s) / network storage (e.g., Google servers, Amazon web Service servers, Dropbox servers, etc.) that is not part of the scan-triggered service platform / server **200**, and server **200** simply stores or maintains binding information that associates a ConnectSquareID with an information Share, and binding information that associates selected information Shares with a user's scan-triggered service account. In one case, user access to remotely hosted / stored information Share data is proxied by scan-triggered application server **200** on behalf of the scanning user. In other embodiments, some of the information Share or materials may be stored and served up by server **200** or cloud-storage resources controlled by / accessible to server **200**. In one embodiment, if a scanning user is not a registered user (i.e., does not have a scan-triggered service account associated with the provider of connect square scan-triggered service), then the scanning user is not granted access to the associated information Share, or may be only allowed limited access (e.g., only access to information stored by / at server **200**, and no access to remote information Shares (e.g., Dropbox share, etc.)). In one embodiment, server **200** may selectively grant (and proxy if necessary) access to an information Share based on one or more user actions. Exemplary user actions may include, but are not limited to, scanning of a predetermined number of scan codes associated with the scan-triggered service system, scanning of a predetermined sequence of scan codes associated with the scan-triggered service system, providing of feedback information (e.g., "I had a bad experience", a response option identifier that may be used by server **200** to identify an element of feedback response, etc.) to server 200, and providing rating score information (e.g., "service was 10 on a scale of 1 to 10", a rating score value or identifier that may be used by server **200** to identify a rating score based on a rating scale provided by server **200**, etc.) to server **200**. The connect square service may also provide the user with an electronic coupon or Reward for scanning the connect square associated with a particular vendor, or for scanning a certain number of Connect Square scan codes associated with the vendor. The connect square service may facilitate and track redemption of the reward by the user.

In this example, to provision a connect square code, a vendor uses computer terminal **600** to log into a provisioning interface associated with scan-triggered application server **200** that is hosting the connect square application, as indicated in step 1. In step 2, ConnectSquareID identifier information **406**, resource or information sharing entity information such as, vendor name **408**, vendor email address **412**, vendor phone number **414**, vendor street address, product stock keeping unit (SKU) information, universal product code (UPC) information, product description text, uniform resource identifier or locator information **410** associated with the vendor's website or product, related product identifiers / descriptions, product price information, sale date information, in-stock quantity information, and associated participation reward (e.g., a reward that is granted in response to scanning the connect square code) information is provisioned, as illustrated in Table 8B illustrated in Figure 4C. A user may provide user account information, which is stored by server **200**. Exemplary user scan-triggered service account information is shown in Table 7B and includes user identifier information **400**, username information **402** (e.g., email address, screen name, etc.), and address / zip code information **404**. Participation reward information may be provisioned and stored by server **200**. Exemplary reward information is shown in Table 9B and includes an associated ConnectSquareID value **406**, a reward identifier **416**, a reward description / value **418**, a reward entity **419** (e.g., issuing entity / merchant), and reward expiration information **420**. Shown in Table 11 is additional exemplary data / information that is associated with a ConnectSquareID and which may be made available to a user who scans the associated connect square service scan code, including cloud-hosted share service provider (e.g., Dropbox, Google Drive, etc.) identifier information **430**, Shared resource identifier (such as a URL link to the shared resource) **432**, shared access security key / credential information **434**, and share duration identifier information **436**. Digital reward information may include, but is not limited to, a RewardID **416**, a reward description **418**, and a reward expiration date **420**. Exemplary data tables and data structures associated with various embodiments of connect square service are presented in Figure 4C. In step 3, a ConnectSquareID value is created and bound to the provisioned information / information Share data, and stored by server **200**. In step 4, a connect square scan code information is communicated to provisioning entity **600**. In step 5, one or more copies of the associated Connect Square scan code are produced and displayed to users. For example, once provisioning is completed for the product, a connect square QR code **704** is generated, where the connect square QR code includes ConnectSquareID identifier information that is bound to / associated with the information owner / sharer, and can consequently be used by server **200** to identify a vendor / entity wishing to provide access to a resource (e.g., a document, web page, contact information, a cloud-hosted information/data Share, etc.). In this example, a ConnectSquareID value **406** is generated by Connect Control Logic Module **224** and incorporated into connect square QR code **704**.

In one embodiment, information that identifies or can be used to identify application server **200** is also encoded in the connect square QR code. The exemplary connect square QR code also includes information that identifies or can be used to identify and establish communications with a network server or host computer that provides scan-triggered connect square service. Exemplary information that identifies or can be used to identify a network server or host computer for providing connect square service may include, but is not limited to, a uniform resource locator (URL) and URL parameters, an Internet protocol (IP) address and port identifier. Alternatively, the native application may dynamically determine the address of the appropriate connect square server at the time of the connect square QR code scan by a user or may have address information associated with a connect square service providing server statically provisioned in the native app residing on the mobile communication device. In such scenarios, connect square processing is very similar to that described above, except that the address of the connect square server is not obtained by a user scan of a connect square QR code.

Copies of the connect square QR code **704** may be deployed in any number of ways and formats including, but not limited to, in a trade show booth, printed tags that are placed on the shelf that holds/displays the associated product, direct mailing collateral, in-store displays, computer monitor display, magazine advertisements, purchase receipts, etc.

In Figure 4B, step 1, a user scans connect square code **704**. Scanning of the connect square code causes the scan-enabled client module **104** to communicate user identifying / user login credentials (e.g., scan-triggered service login credentials, etc.) and extracted ConnectSquareID information to connect square scan-triggered service application server **200**. When the connect square QR code is scanned by the user's QR code scanner, the encoded ConnectSquareID information and, in one embodiment, a connect square scan-triggered service server identifier or address information is extracted by the QR code scanner and the information that identifies or can be used to identify a connect square application server is used to facilitate communication of the extracted ConnectSquareID information to the identified Connect Square application server (step 2). Alternatively, the native application may dynamically determine the address of the appropriate trusted square server at the time of the connect square QR code scan by a user. It will be appreciated that in various embodiments of the subject matter described herein, the ConnectSquareID information may be encrypted or obfuscated during communication from the user's mobile communication device to the connect square application server. In other embodiments, the information that identifies or can be used to identify a connect square application server may itself be encrypted or obfuscated when read by the QR code scanner, and may be subsequently decrypted / de-obfuscated by scan control logic module **112** so as to obtain the information necessary to identify the connect square application server to be contacted. Also communicated to the connect square application server is information that identifies or can be used to identify the user (e.g., the person that scans the connect square QR code). This user identifying information may be provided to the connect square application server **200** before, after, or at the same time that the previously discussed scanned information is provided. For example, in one embodiment, the user may log in (i.e., provide login credentials that are sufficient to identify and authenticate the user) prior to scanning the connect square QR code, and application server **200** is adapted to associate the subsequently received ConnectSquareID information with the user. Alternatively, the user's login credentials may be provided at the time of / as a result of the connect square QR code scan, along with the ConnectSquareID information.

Connect square scan-triggered application server **200** receives the scan code information, which includes user identifying / user login credentials and information share / information sharing entity identifying information (e.g., ConnectSquareID), and may respond with an acknowledgement message. Server **200** creates and stores a scan transaction record which binds or associates the user identifying information and the ConnectSquareID identifier, as indicated in step 3. Exemplary scan transaction record information is presented in Table10 and includes scanning user identifying information **422**, scanned ConnectSquareID information **424**, scan timestamp information **426**, granted reward identifier information **428**, and user survey feedback / response information or rating score information. In one embodiment, creation of this binding or transaction record associates the information / information share with the user and effectively places the information / information share in a digital library / vault / information repository that is associated with the user's scan-triggered service account. The user can log in to the user's connect square scan triggered service account and browse / view / download any of the information that the user has placed in the user's digital repository via the prior scanning of connect square service scan codes. In one embodiment, the scanning user may be prompted to confirm that the user would like the associated information / information share placed in the user's vault or digital information repository. In step 4, server **200** is adapted to provide access to any information or information shares that are local to or directly controlled by scan-triggered service server **200**. As such, the scanning user **100** may immediately browse / view / download such locally hosted information. Step 6 illustrates a situation where an information Share is associated with the scanned Connect Square scan code, and where the information Share is associated with a 3rd party or remote information repository (e.g., Dropbox, Google Drive, etc.). In this situation, server **200** is adapted to proxy access to the information Share on behalf of scanning user **100**. For example, scan-triggered server **200** may contact 3rd party / remote information repository server **604** and provide access credentials (e.g., security key, password, access code, etc.) necessary to access the associated information Share on behalf of user **100**. In step 7, remote information share host **604** grants access to and provides the associated information share content to server **200**, where it is relayed to user **100**, step 8. In alternate embodiments, server **604** may establish / negotiate a direct connection to user **100** (with or without the assistance of server **200**), such that the remote information Share is made accessible to user **100** directly by server **604**. In any event, user **100** is provided access, following a scan of the associated connect square scan code, to the remote information Share data.

If connect square control logic module **224** determines that the user has not already scanned this connect square code, then the associated information / information share is bound to the user's Connect data log or vault using the received vendor identifying information (step 3). Via a mobile user browsing interface or a desktop user interface, the user may log into the Connect square application server **200** and browse the contents of the user's Connect data / vault at a later time. In this example, the user can log in through a desktop / laptop or tablet computer and browse the information that the user agreed to accept or have placed in the information repository vault associated with the user's scan-triggered service account. In one embodiment, the scanning user of mobile device **100** may be granted permission / access to an online shared folder (e.g., Google Drive folder, Dropbox folder, etc.) in response to scanning of connect square scan code **704**. In this case, scan-triggered server **200** may proxy the granting of access permission to the shared resource. For example, server **200** may receive ConnectSquareID and user identifying information as a result of the scan of connect square code **704** by user **100**, and server **200** may communicate with a network-based share provider (e.g., Google Drive, Dropbox, etc.) in order to obtain access permission for a shared resource on behalf of the scanning user **100**. As such, user **100** may subsequently access the shared resource using access credentials obtained by or provided by scan-triggered connect square server **200**. Exemplary network-based resource share information and connect square scan code binding information is presented in Table 11, and includes a ConnectSquareID **406**, an information / information share provider ID **430**, a share resource address / identifier (e.g., URL + parameters) **432**, share access / security credentials **434**, share duration information **436**.

In one embodiment, connect square control logic module **224** may determine (based on prior provisioned rules) whether the user should be granted a reward in exchange for scanning the Connect Square code. If a reward is to be granted, reward control logic module **210** may facilitate the crediting of the granted reward to the user's account. In one embodiment, a digital reward may be credited to a reward wallet associated with the user's scan-triggered service account.

It will be appreciated with regard to the connect square service embodiments described above that such services may also be provided via a native connect square application that is installed on the user's smartphone. In such cases, information that identifies or can be used to identify the address of a connect square server to which the appointment information should be communicated need not be encoded within the connect square QR code that is displayed to and scanned by a user. In such native application deployments, the information that identifies or can be used to identify the address of a connect square server may be pre-configured and stored in the smartphone's memory, such as in data storage module **116**. Alternatively, the native application may dynamically determine the address of the appropriate Connect Square server at the time of the connect square QR code scan by a user. In such scenarios, connect square processing is very similar to that described above, except that the address of the connect square server is not obtained by a user scan of a connect square QR code.

It will be appreciated that embodiments of the connect square service enable a user to collect and maintain vendor contact information (and associated goods/services information) in a manner that keeps the user's identity and interest hidden from the vendor who generates and displays the connect square scan code. Users may, at their discretion, choose to allow a vendor associated with a connect square code that the users have scanned to obtain access to information that identifies the users.

According to another aspect, the subject matter described herein includes a system for facilitating access to stored information via the scanning of a scanable code by a scan-enabled client module. The system includes a computing platform having at least one processor. The system further includes a server application module executable by or embedded within the at least one processor. The server application module is configured to create and store a scan code identifier that is bound to an element of sharable information. The server application is configured to receive from a scan-enabled client module, the scan code identifier that is obtained from the scanning of an associated scanable service code by a user. The server application module is further configured to create and store an association between the received scan code identifier and the user. The server application module is further configured to, in response to receiving a request to access the element of sharable information, provide access to the element of sharable information.

RateIt Square

Shown in Figure 5A is diagram that generally illustrates the provisioning of information associated with one embodiment of a service of a scan code-based, scan-triggered service system. This service is referred to herein as RateIt square service, which is a service that enables a user to quickly and easily express feedback through the use of a tap-able or touch-controlled rating scale interface (e.g., sliding-scale interface, etc.), where presentation of the rating-scale interface and collection of the user-specified rating value is facilitated via the scanning of a RateIt square service scan code by the user, where the RateIt square is associated with a ratable entity or item. One exemplary use of RateIt square service might involve a wine merchant that is hosting a wine tasting event for users, which has 3 different bottles of wine for tasting. The wine merchant logs into the merchant's RateIt square account and provisions 3 RateIt square scan codes (e.g., QR codes), a unique RateIt square QR code is provisioned and generated for each of the 3 bottles of wine (i.e., each bottle of wine is a ratable entity). Each RateIt Square QR code is placed near or on the associated bottle of wine. As a user tastes a bottle of wine, the user scans the RateIt square QR code associated with that bottle. RateIt square identifier information encoded in the scanned RateIt square scan code is decoded and used to access a RateIt square server. The RateIt square server communicates information back to the scanning user's smartphone which causes a touchoperable variable rating scale to be displayed on the user's smartphone. In one embodiment, the user uses his or her finger to operate the variable rating scale, such as a linear or rotary sliding scale interface, and specify a particular rating score or value. The rating scale may be continuous (i.e., analog) or may be incremented / decremented in discrete amounts. Once a rating value is selected the user taps a button which causes the specified rating value information to be communicated to a RateIt square scan-triggered application server, where it is stored. Once stored the rating information may be visible to the user, the wine merchant, or both. For example, in one embodiment, a statistic or metric associated with aggregate rating score values collected from many users may be displayed to the scanning user following the Rating Square scan code.

It will be appreciated that user information, such as user account information associated with scan-triggered service server **200** may be provisioned by a user or other provisioning entity. Exemplary user account information is shown in Table 12 illustrated in Figure 5C and includes user identifying information **400**, username information **402**, and user address / zip code information **404**.

Continuing with Figure 5A, a merchant **458** or other provisioning entity logs into RateIt square server **200** and provides the information necessary to provision a RateIt square, as indicated in steps 1 and 2. In this example, the provisioner provides a RateIt square entity identifier **452** which can be used by the merchant **458** to uniquely identify the RateIt square scan code that is being provisioned and the good, service, idea, or other ratable entity with which it is associated (e.g., a ratable entity may be any good or service with which a RateIt square scan code can be associated). In this example, each of the 3 different bottles of wine is a unique ratable entity that is assigned a unique RateIt square entity identifier value **452**. The RateIt square entity identifier can be a human read-able text string, such as "Bottle #1." It will be appreciated that RateIt square control logic module **216**, in this embodiment, also assigns an internal identifier that is associated with the RateIt square scan code that is being provisioned, RateItSquareID **450** shown in Table 13 of Figure 5C. A merchant identifier or other scan code owner / administering identifier **456** may be associated with RateItSquareID **450**, as well as a merchant name **458** and location information **460** (e.g., store / branch location identifier, geo-location coordinates, etc.). Also provided is information that specifies rating scale information **454**, which represents the allowed / permitted range of rating values or scale to be used in rating the associated RateIt square entity **452**. In one embodiment, rating scale information may be comprised of a highest rating score value, a lowest rating score value, and a rating score increment / resolution value. For example, rating scale information associated with a RateIt square entity may include a highest rating score value of 10, a lowest rating score value of 1, and a rating score increment / resolution value of .5 units. As such, a user who scans the RateIt square code associated with the RateIt square entity would be provided with a user interface that displays rating scale with a highest rating score of 10, a lowest rating score of 1, and a user touch-slide-able selector that moves on-screen and can be used to select a rating score in increments of .5 units. It will be appreciated, that RateIt square control logic module **216** may also assign a default rating scale range and resolution, in the event that none is specified by the provisioner at provision time. It will also be appreciated that the scale range may include a collection of non-numeric values (e.g., worst, bad, ok, good, best), in which case the resolution value may be optionally omitted.

Participation reward information may be provisioned and stored by server **200**. Exemplary reward information is shown in Table 14 and includes an associated RateItSquareID value **450**, a reward identifier **462**, a reward description / value **464**, a reward entity **465** (e.g., issuing entity / merchant), and reward expiration information **466**.

In step 3, server **200** creates and stores a binding record which associates the assigned RateItSquareID value **450** and the associated ratable / RateIt entity **452** and other provisioned information. In step 4, scan-triggered application server **200** responds either with a ready-to-deploy RateIt Square QR code scanable image (e.g., png or jpeg formatted image, etc.) or with RateIt square information that is used by a QR code image generator which is resident on the merchant's computer **600**. In either case, a RateIt square QR code is generated which includes information that can be used to identify the RateIt entity and, for example, the associated merchant. In one embodiment, information that identifies or can be used to identify application server **200** is also encoded in the RateIt square QR code. It will be appreciated that embodiments of the subject matter described herein may combine or concatenate identifiers, such that a single identifier may be used which is capable of identifying both the merchant and the RateIt square entity. In this example it is assumed that the RateIt square entity identifier includes sufficient information so as to effectively identify both the merchant and the RateIt entity. Furthermore, the RateIt square entity and merchant identifying information may be encrypted/obfuscated prior to inclusion in the RateIt square QR code. In such cases, decrypted/de-obfuscated by scan control module **112** prior to transmission to application server **200**, or by RateIt square control logic module **216** once it is received by scan-triggered service application server **200**.

The exemplary RateIt square QR code also includes information that identifies or can be used to identify and establish communications with a network server or host computer that provides RateIt square service (e.g., scan-triggered server **200**). Exemplary information that identifies or can be used to identify a network server or host computer for providing RateIt square service may include, but is not limited to, a uniform resource locator (URL) and URL parameters, an Internet protocol (IP) address and port identifier. Such scan-triggered server identifying information encoded in a RateIt square scan code may be optionally encrypted / obfuscated. It will be appreciated with regard to the RateIt square service embodiments described above that such services may also be provided via a native RateIt square application that is installed on the user's smartphone. In such cases, information that identifies or can be used to identify the address of a RateIt square server to which the appointment information should be communicated need not be encoded within the RateIt square QR code that is displayed to and scanned by a user. In such native application deployments, the information that identifies or can be used to identify the address of a RateIt square server may be pre-configured and stored in the smartphone's memory, such as in data storage module **116**. Alternatively, the native application may dynamically determine the address of the appropriate RateIt Square server at the time of the RateIt square QR code scan by a user. In such scenarios, RateIt square processing is very similar to that described above, except that the address of the RateIt Square server is not obtained by a user scan of a RateIt Square QR code.

In Figure 5B, a user scans RateIt square code **706**. Scanning of the RateIt square code causes the scan-enabled client module **104** to communicate user identifying / user login credentials and RateItSquareID information to RateIt square application server **200**, as indicated in steps 1 and 2. It will be appreciated that embodiments of the subject matter described herein may be deployed, wherein user identifying information is not collected / submitted to application server **200**. In such, "anonymous" modes of operation, rating score information solicited and collected from users via the scanning of an associated RateIt square scan code may be stored in a binding record by application server **200**, where the record does not contain user identifying information. However, for the sake of illustration, the embodiments described here assume that user identifying information is provided by / obtained from the scanning user **100**. When the RateIt square QR code is scanned by the user's QR code scanner, the encoded RateItSquareID information and RateIt square application server identifier or address information is extracted by the QR code scanner and the information that identifies or can be used to identify a RateIt square application server is used to facilitate communication of the extracted RateItSquareID information to the identified RateIt square application server. It will be appreciated that in various embodiments of the subject matter described herein, the RateItSquareID information may be encrypted or obfuscated during communication from the user's mobile communication device to the RateIt square application server. In other embodiments, the information that identifies or can be used to identify a RateIt square application server may itself be encrypted or obfuscated when read by the QR code scanner, and may be subsequently decrypted / de-obfuscated by scan control logic module **112** so as to obtain the information necessary to identify the RateIt square application server to be contacted. Also communicated to the RateIt square application server is information that identifies or can be used to identify the user (e.g., the person that scans the RateIt square QR code). This user identifying information may be provided to the RateIt square application server **200** before, after, or at the same time that the previously discussed scanned information is provided. For example, in one embodiment, the user may log in (i.e., provide login credentials that are sufficient to identify and authenticate the user) prior to scanning the RateIt square QR code, and application server **200** is adapted to associate the subsequently received RateIt square entity ID information with the user. Alternatively, the user's login credentials may be provided at the time of / as a result of the RateIt square QR code scan, along with the RateItSquareID information.

RateIt square application server **200** receives the information, which includes user identifying / user login credentials and RateItSquareID information. Module **216** uses the received RateItSquareID information to access previously provisioned RateIt square binding record information, which includes product/service identifying information and rating scale information, as discussed previously. In step 3, server **200** and responds to the scanning user with user-operable rating control elements (e.g., on-screen, touch-driven sliding scale control, rotary scale control user interface element, etc.) which display rating score / scale range information that, for example, specifies the associated good/service identifying information (i.e., a text description of what is being rated) and range of the RateIt scale and resolution (e.g., 1 – 10, resolution .5 units). Through a user interface, which may include a touch driven sliding scale or other touch driven variable selection user interface user input control construct (e.g., graphic analog sliding selector, analog dial, etc.) the user specifies a rating value within the rating range. It will be appreciated that in one embodiment, a default rating range scale and resolution (e.g., 1 – 5, .5) may be applied if no rating scale and resolution information is provided by application server **200**. User **100** taps or touches one or more rating controls that are displayed on the screen of the user's mobile device in order to select or specify a rating score value. The specified rating value information is then communicated to application server **200**, as shown in step 4.

RateIt square control logic module **216** receives and records / logs the information, as indicated in step 5. In step 5, the provided rating value may be bound to or associated with the scanning user identifying information (if provided), such as is generally illustrated in Table 15 of Figure 5C. Table 15 includes exemplary scan transaction information such as, UserID information **468**, the associated RateItSquareID value **470**, the rating score value provided by the user **472**, timestamp information associated with the scan **474**, and information that can be used to identify a reward **476** that is granted to the user (e.g., as a reward for scanning the code).

In an alternate embodiment, anonymous RateIt data may be collected in a manner similar to that described above. In such a scenario, the information communicated from the user's smartphone to the application server **200** does not include user identifying information or login credentials. Such RateIt data received by application server **200** may be stored without a user association as an anonymous user rating score input.

In step 6, rating score and/or rating score statistics associated with user scans of the RateIt square scan code **706** are reported or made available, for example, to a merchant / merchant computer **606**.

In one embodiment, RateIt square control logic module **216** may determine (based on prior provisioned rules) whether the user should be granted a reward in exchange for scanning the RateIt square code. If a reward is to be granted, Reward Control Logic Module **210** may facilitate the crediting of the granted reward to the user's account. In one embodiment, a digital reward may be credited to a reward wallet associated with the user's scan-triggered service account, step 7. Exemplary reward data is shown in

Table 14 and includes the value of the RateItSquareID **450** with which the reward is associated, a reward identifier **462**, a reward description **464**, a reward issuing entity **465**, reward expiration date information **466**. Also indicated in step 7, is a mode of operation whereby the scanning user **100** is provided with a rating score summary or statistics (which are displayed on the user's mobile device screen post-scan) associated with other users who have scanned the same or a similar RateIt square scan code.

In one exemplary embodiment, a RateItSquareID identifier value may be generated by scan-triggered application server **200** and associated a particular beverage, such as a beer. The RateItSquareID value is encoded in a scanable code, such as a QR code, which can be printed on, for example, a drink coaster or a beer glass / cup. When the code is scanned by a user, the RateItSquareID is communicated to scan-triggered server **200**, in a manner similar to that described previously. Optionally, user identifying information (e.g., a scan-triggered service account username, email address, username, IP address, mobile phone number, etc.) may also be communicated to scan-triggered server **200**. In response to receiving the RateItSquareID scan information, server **200** is adapted to communicate multiple rating categories **478** and associated rating scale / scoring scale information **480**. Exemplary rating category information that may be provisioned and stored by server **200** is shown in Table 16. For example, server **200** may communicate beer judging guidelines (e.g., Beer Judge Certification Program style guidelines, American Homebrewers Association guidelines, etc.) which include multiple rating categories, with multiple rating scales. In such embodiments, a single RateItSquareID value **450**, associated with the single RateIt entity **452**, may be associated with multiple rating categories **478** and their associated rating criteria / rating scales **480**. Exemplary multi-category rating provisioning data is illustrated in Table 16 of Figure 5D. As such, the scanning user is presented with multiple rating categories and their associated rating scales. In a manner similar to that described previously, the user may select or specify a rating score value for each rating category and the specified rating score values are communicated to and recorded / logged by server **200**. Exemplary category-based user response / scan transaction data is illustrated in Table 17 and includes UserID information **468** (if available), associated RateItSquareID information **486**, Rating Category identifying information **488**, Category-specific rating score information **490** provided by the user, and scan transaction timestamp information **492**. As such, rating category-specific rating score values for a particular type / brand / style of beer may be collected from users by scan-triggered server **200**. In an alternate embodiment, a RateItSquareID identifier value may be generated by scan-triggered application server **200** and associated a group or flight of beers. When this RateItSquare code is scanned by a user, server **200** receives the associated RateItSquareID and communicates a menu of beer selections to the user's mobile scanning device, where the menu is displayed to the user. The user may tap-to-select an onscreen button associated with a particular beer that the user is drinking. In one embodiment, a rating information may be collected from the user as described above, and subsequently communicated to server **200** where it is stored / associated with the previously selected beer. In another embodiment, when the user taps an on-screen button to specify the user's beer selection / beer that the user intends to rate, this beer selection information is communicated to server **200**, where it is used to select one or more of the rating categories that are subsequently communicated / presented to the user. It will be appreciated that similar embodiments of the subject matter described herein may be associated with types / vintages of wine and used in a similar manner to facilitate the collection of user ratings for different wines. In one embodiment, when a user scans a RateIt square associated with an item (e.g., beer, wine, etc.), the user is shown metrics / statistics / data associated with rating scores provided by other users who have also scanned the same (or related) RateIt square scan codes associated with the item. As illustrated in Table 13 of Figure 5C, location information **460** may be associated with a RateItSquareID, such that location information may be inferred from scan data that is received from users who scan the associated RateIt square scan code and subsequently provide rating score feedback information. Such location information may be stored and analyzed by server **200** to determine user preference trends based on location / geo-location. A scanning user may be credited with a digital reward in response to scanning of a RateIt square scan code and/or the providing of rating score feedback information for the associated item.

It will be appreciated with regard to the RateIt square service embodiments described above that such services may also be provided via a native RateIt square application that is installed on the user's smartphone. In such cases, information that identifies or can be used to identify the address of an RateIt square application server (e.g., scan-triggered server **200**) to which the rating score information should be communicated need not be encoded within the RateIt square QR code that is displayed to and scanned by a user. In such native application deployments, the information that identifies or can be used to identify the address of a RateIt square server may be pre-configured and stored in the smartphone's memory, such as in data storage module **116**. Alternatively, the native application may dynamically determine the address of the appropriate RateIt square application server at the time of the RateIt square QR code scan by a user. In such scenarios, RateIt square processing is very similar to that described above, except that the address of the RateIt Square server is not obtained by a user scan of a RateIt square QR code.

TrackIt Square

Shown in Figure 6A is diagram that generally illustrates exemplary information flow and processing associated with a scan code-based service system according to an embodiment of the subject matter described herein. This service is referred to herein as TrackIt square service, which is a service that facilitates the reporting of the status and/or condition of shipped packages to a status requesting entity (e.g., a merchant, the shipper of a package, etc.), where the reporting or notification is triggered via the scanning of a TrackIt square service scan code by the user. One exemplary use of TrackIt square service might involve the receipt of a package that was shipped from a merchant to a user. The merchant generates a TrackIt square QR code that is either affixed to the outside of the package or placed inside the box (e.g., printed on the shipping invoice). The TrackIt square QR code includes information that identifies or can be used to identify the shipping merchant. In one embodiment, the TrackIt square QR code may also include information that identifies or can be used to identify a status value associated with the package (e.g., arrived damaged, arrived missing an order item, etc.). In one embodiment, may also include information that identifies or can be used to identify the intended receiver of the package / shipment (e.g., customer identifier, invoice number, customer name / address info, etc.). In one embodiment, a separate / different TrackIt square scan code may be generated, where each scan code represents a different tracking status response option (e.g., status response option 1: arrived damaged, status response option 2: arrived missing an order item, etc.) and these scan codes may all be included in or on the shipped package / item. When the user scans the desired TrackIt square QR code, for example a QR code representative of response option 2 "arrived missing an item", information that identifies or can be used to identify the merchant, the associated status response option value, and the user (i.e., the scanner of the QR code) is communicated to an application server associated with the TrackIt square service. The information is logged and made available / reported to the merchant.

In an alternate embodiment, a single TrackIt square service scan code may be generated and associated with a shipped package / item, where the scan code, when scanned, is adapted to cause tracking status response option information (e.g., status response option 1: arrived damaged, status response option 2: arrived missing an order item, etc.) to be communicated to and displayed to the scanning user, who can then touch/tap or otherwise select the appropriate tracking status response option. In response, the associated status response option value, and the user (i.e., the scanner of the QR code) is communicated to an application server associated with the TrackIt square service. The information is logged and made available / reported to the merchant.

It will be appreciated that user information, such as user account information associated with scan-triggered service server **200** may be provisioned by a user or other provisioning entity. Exemplary user account information is shown in Table 18, and includes user identifying information **300**, username information **302**, and user address / zipcode information **304**.

Continuing with Figure 6A, a merchant logs into TrackIt square server **200** and provides the information necessary to provision a TrackIt square, as indicated in steps 1 and 2. Exemplary shipment / package data is shown in Table 19, and may include status requesting entity identifying information **502** (e.g., information that can be used to identify the shipper / shipping merchant, etc.), status response option identifier information **504**, status response option description information **506**, associated shipper / merchant order or invoice identifier information **508**, and shipment / package receiver identifying information **509**. In step 3, module **220** creates and assigns a TrackItSquareID value **500** to the provisioned shipment / package information, and stores the association in a binding record. This binding information may be used later by server **200** to interpret received TrackIt square scan code information generated by a user scan of the associated service scan code. In this example, the provisioner (e.g., merchant) provides or TrackIt square control logic module **220** assigns a TrackItSquareID identifier **500** which can be used by the merchant to uniquely identify the TrackIt square that is being provisioned and the associated status response option identifier **504** (e.g., "arrived damaged", "arrived missing order items").

Participation reward information may be provisioned and stored by server **200**. Exemplary reward information is shown in Table 20 and includes a reward identifier **510**, a reward description / value **512**, a reward entity **513** (e.g., issuing entity / merchant), and reward expiration information **524**.

In step 4, application server **200** responds either with a pre-generated, ready-to-deploy TrackIt square QR code scanable image (e.g., png or jpeg formatted image, etc.) or with TrackItSquareID information that is used by a QR code image generator. The TrackIt square scan code may be deployed in any number of ways including printed on a sticker / label that is affixed to the package, printed on a shipping invoice that is included in the package, etc.), as indicated in step 5. In either case, a TrackIt square QR code is generated which includes information that can be used by server **200** to identify the associated status option (e.g., "damaged", "late", "wrong item", etc.) and the associated merchant. In one embodiment, information that identifies or can be used to identify application server **200** (e.g., URL address, IP address, etc.), is also encoded in the TrackIt square QR code. It will be appreciated that embodiments of the subject matter described herein may combine or concatenate identifiers, such that a single identifier may be used which is capable of identifying both the requesting entity and the status option. In this example the TrackItSquareID identifier can be used by server **200** to identify both the requesting entity and a specified / selected status option. In other embodiments, the TrackItSquareID identifier may be encrypted/obfuscated prior to inclusion in the TrackIt square QR code. In such cases, decrypted/de-obfuscated by scan control module **112** prior to transmission to application server **200**, or by TrackIt square control logic module **220** once it is received by application server **200**.

The exemplary TrackIt square QR code also includes information that identifies or can be used to identify and establish communications with a network server or host computer that provides TrackIt square service. Exemplary information that identifies or can be used to identify a network server or host computer for providing TrackIt square service may include, but is not limited to, a uniform resource locator (URL) and URL parameters, an Internet protocol (IP) address and port identifier. It will be appreciated with regard to the TrackIt square service embodiments described above that such services may also be provided via a native TrackIt square application that is installed on the user's smartphone. In such cases, information that identifies or can be used to identify the address of a TrackIt square server to which the rating score information should be communicated need not be encoded within the TrackIt square QR code that is displayed to and scanned by a user. In such native application deployments, the information that identifies or can be used to identify the address of a TrackIt square server may be pre-configured and stored in the smartphone's memory, such as in data storage module **116**. Alternatively, the native application may dynamically determine the address of the appropriate TrackIt square server at the time of the TrackIt square QR code scan by a user. In such scenarios, TrackIt square processing is very similar to that described above, except that the address of the TrackIt square server is not obtained by a user scan of a TrackIt square QR code.

Shown in Figure 6B, a user scans TrackIt square code **708**. Scanning of the TrackIt square code causes the scan-enabled client module **104** to communicate user identifying / user login credentials and TrackItSquareID information to TrackIt square application server **200**, as indicated in step 1. When the TrackIt square QR code is scanned by the user's QR code scanner, the encoded TrackItSquareID information and TrackIt square server identifier or address information is extracted by the QR code scanner and the information that identifies or can be used to identify a TrackIt square application server is used to facilitate communication of the extracted TrackItSquareID information to the identified TrackIt square application server. It will be appreciated that in various embodiments of the subject matter described herein, the TrackItSquareID information may be encrypted or obfuscated during communication from the user's mobile communication device to the TrackIt square application server. In other embodiments, the information that identifies or can be used to identify a TrackIt square application server may itself be encrypted or obfuscated when read by the QR code scanner, and may be subsequently decrypted / de-obfuscated by scan control logic module **112** so as to obtain the information necessary to identify the TrackIt square application server to be contacted. Also communicated to the TrackIt square application server is information that identifies or can be used to identify the user (e.g., the person that scans the TrackIt square QR code). This user identifying information may be provided to the TrackIt square application server **200** before, after, or at the same time that the previously discussed scanned information is provided. For example, in one embodiment, the user may log in (i.e., provide login credentials that are sufficient to identify and authenticate the user) prior to scanning the TrackIt square QR code, and application server **200** is adapted to associate the subsequently received TrackItSquareID information with the user. Alternatively, the user's login credentials may be provided at the time of / as a result of the TrackIt square QR code scan, along with the TrackItSquareID information.

TrackIt square application server **200** receives the information, which includes user identifying / user login credentials and TrackItSquareIDTrackItSquareID information (step 2). TrackIt square application server **200** binds the received TrackItSquareID information to the UserID of the scanning user, and stores the information in a scan transaction record that is placed in data storage module **212** (step 3). Exemplary scan transaction record information is shown in Tables 21 and 22, and includes user identifying information **516**, TrackItSquareID value information **518**, scan timestamp information **520**, return authorization information **522**, granted reward identifying information **524**, and StatusResponseOptionID information **526**. In other embodiments, UserID information may not be communicated to server **200**, and in such cases the TrackItSquareIDTrackItSquareID information may be used to determine or locate associated order / invoice information previously stored in the provisioning binding record, which serves to identify the user. The status option information associated with the TrackItSquareID is made available to the shipper / merchant. In one exemplary embodiment, the shipper may log in to application server **200** and view the received status option information (step 4). Application server **200** may be adapted to actively notify the shipper / merchant of the received status option information from the user. In such cases, application server **200** may notify the merchant via email, text message service, instant message service, a social media messaging service, or other electronic communications service.

In this example, the merchant / shipper responds by indicating to application server **200** that the merchant / shipper would like a communication sent to the user that includes information, such as return authorization information **522**, contact telephone number information, contact email address information, return shipping address information, return shipping instructions, etc. Some or all of this information may be provided by the merchant in step 5, or some or all of this information may be provisioned ahead of time by the merchant. In the later case, the communication associated with step 5 serves to trigger application server **200** to include the specified information in a communication to the user. As such, TrackIt square application server **200** may, in one embodiment, act as a communication proxy on behalf of the merchant. TrackIt square application server **200** may generate an email, text message, instant message, voice mail message, or other message that includes the merchant-specified information and transmit the message to the user, as generally indicated in step 6. In one embodiment, the scanning user **100** may be granted / issued a digital reward for scanning the TrackItSquare and providing package / shipment status (step 7). In one embodiment, such a digital reward may be credited to the user's scan-triggered service account and stored in an associated digital reward wallet.

Shown in Figure 6C is an alternate embodiment, wherein the TrackItSquareID value **518** obtained from user **100**'s scan of TrackIt square scan code **708** in step 1 is provided to TrackIt square server **200** in step 2, in a manner similar to that described with respect to the previous embodiment. In step 3, server **200** logs the received scan data and creates a scan transaction record that associates the received TrackItSquareID value with the user. In step 4, server **200** uses the received TrackItSquareID value information to access the provisioned binding record that includes the associated status response option information **504**. In this case, multiple possible status response options would be associated with the

TrackItSquareID code value. The located status response option information (e.g., status response option 1: arrived damaged, status response option 2: arrived missing an order item, etc.) is communicated to mobile device / user **100**, where it is displayed to the user, as indicated in step 5. In one embodiment, each status response option is associated with a touch-selectable / tap-able button that is displayed on the touch-screen of the user's mobile device **100**. In step 6, the user's status response option selection information (e.g., StatusResponseOptionID **526**) is communicated to server **200**, where it is associated with the user's scan transaction record and stored. It will be appreciated that steps similar to steps 4 – 7 of the embodiment shown in Figure 6B may be subsequently performed in a similar manner with respect to this embodiment.

It will be appreciated that in an alternate embodiment, a merchant may provision order identification information, which may be associated with the TrackItSquareID of a unique TrackIt square QR code, as indicated in Table 19 of Figure 6D. When this TrackIt square QR code is scanned by a user, the associated TrackItSquareID provided to application server **200** as a result of the scan can be used to identify the merchant order identification information. This information can then be provided to or made available to the merchant upon receipt of the scan.

It will be appreciated with regard to the TrackIt square service embodiments described above that such services may also be provided via a native TrackIt square application that is installed on the user's smartphone. In such cases, information that identifies or can be used to identify the address of a TrackIt square server to which the appointment information should be communicated need not be encoded within the TrackIt square QR code that is displayed to and scanned by a user. In such native application deployments, the information that identifies or can be used to identify the address of a TrackIt square server may be pre-configured and stored in the smartphone's memory, such as in data storage module **116**. Alternatively, the native application may dynamically determine the address of the appropriate TrackIt square server at the time of the TrackIt square QR code scan by a user. In such scenarios, TrackIt square processing is very similar to that described above, except that the address of the TrackIt square server is not obtained by a user scan of a TrackIt square QR code.

According to one aspect of the subject matter describer herein, a system for facilitating the communication of status information associated with a delivery item via the scanning of a scanable code by a scan-enabled client module is provided. The system includes a computing platform having at least one processor. The system further includes a server application module executable by or embedded within the at least one processor and configured to create and store a scan code identifier that is bound to a delivery item, receive from a scan-enabled client module, the scan code identifier that is obtained from the scanning of an associated scanable service code by a user, store the received scan code identifier; and grant a reward to the user.

ClinSquare

Shown in Figure 7A is diagram that generally illustrates exemplary information flow and processing associated with a scan code-based service system according to an embodiment of the subject matter described herein. This service is referred to herein as ClinSquare service, which is a service that facilitates the recruitment of patients and/or volunteers for a clinical drug or medical device trial that is triggered via the scanning of a ClinSquare service scan code by the user. One exemplary use of ClinSquare service involves a contract research organization (CRO) that needs to recruit volunteers for a pharmaceutical drug trial study. In steps 1 and 2, the CRO study coordinator entity **606** logs into an application server **200**, which is hosting ClinSquare application software. The study coordinator entity provisions the ClinSquare application with clinical trial study recruitment information. Exemplary clinical trial study recruitment information is shown in Tables 23 – 25 illustrated in Figure 7C and may include, but is not limited to, a study identifier **532**, a study administrator or coordinator **534**, a study description or name **536**, study coordinator contact information **538**, study or deployment location information 540, participant screening question identification information **544**, screening question text (or URL link where text can be found, etc.) **546**, screening question response option information 547, and pass criteria information **548**, and is shown in Tables 22 – 25. It will be appreciated that the clinical trial study, screening question information, associated contact information, and participation reward information presented in Tables 22 – 29 illustrated in Figures 7C and 7D is merely illustrative, and that a CRO / study coordinator entity may provision and store in application server **200** other data associated with the recruitment of volunteers / patients for a particular clinical trial study. If screening questions are provisioned, associated screening rule information may also be provisioned. Screening rules may be stored and implemented in any number of ways by ClinSquare Control Logic Module **222**. In general, such screening rules, however they are specified and implemented, are adapted to determine whether a responding user (i.e., a potential study recruit) provides screening question answers which are sufficient to warrant further contact / communication with the user. For instance, a particular screening question asks the user for the user's gender, and the user responds with an indication that the user is "male." If the associated clinical trial study is only interested in female patients / volunteers, then the user would not "pass" the screening and would not warrant further consideration, further processing, or a follow-up communication, etc.

Information which identifies or can be used to identify deployment entities **550 – 552** and/or associated deployment locations **554 – 556** for ClinSquare QR codes associated with the clinical trial study patient recruitment campaign may also be provided at provisioning time by the study coordinator entity. Again, exemplary deployment entity and deployment location information is shown in Table 26, and may include pharmacies, retail store locations, physician's offices, hospitals, etc. As such, a study coordinator can use the ClinSquare platform to implement and enforce service agreements with 3rd parties (e.g., a major pharmacy chain, a physician's office, a dental practice, a hospital, etc.) which provide compensation to the 3rd party for each ClinSquare QR code scan or for each ClinSquare QR code scan that leads to an enrolled patient / study volunteer.

In step 3, ClinSquare control logic module **222** of application server **200** is adapted to generate a ClinSquareID identifier, which is associated with or bound to the provisioned study information. Exemplary study recruitment bind recording data is shown in Table 23 (and relationally associated Tables 24 – 26), where ClinSquareID value **530** is associated with the provisioned clinical study / trial information elements discussed above. ClinSquare scan code information is communicated to the provisioning entity **606** in step 4, and for example, the study coordinator generates a ClinSquare QR code that is printed on recruitment collateral materials (e.g., flyers, brochures, table tents, handbills, direct mailing pieces, etc.) and generally made available to members of the "recruit-able" public, as indicated in step 5. In this example, the ClinSquare QR code includes a ClinSquareID identifier that is associated with the provision study information, as generally illustrated in Figures 7C – 7D. For example, a ClinSquareID can be used by server **200** to identify the study coordinator and associated clinical trial study for which volunteers are being recruited (along with many other provisioned study attributes, such as the deployment location of the scan code, whether a reward should be granted, what type of reward should be granted, etc.). It will be appreciated that the information sufficient to identify the study coordinator and associated clinical trial study may be incorporated into or encoded in the ClinSquare QR code in the form of a single ClinSquareID identifier or alternatively via multiple identifiers. In this example, a single ClinSquareID is used which can be used to identify both the study coordinator and the associated clinical trial study. The exemplary ClinSquare QR code also includes information that identifies or can be used to identify the deployment entity and deployment location. It will be appreciated that inclusion of the information that identifies or can be used to identify a deployment entity and deployment location is not required. The exemplary ClinSquare QR code also includes information that identifies or can be used to identify and establish communications with a network server or host computer that provides ClinSquare service. Exemplary information that identifies or can be used to identify a network server or host computer for providing ClinSquare service may include, but is not limited to, a uniform resource locator (URL) and URL parameters, an Internet protocol (IP) address and port identifier. It will be appreciated with regard to the ClinSquare service embodiments described above that such services may also be provided via a native ClinSquare application that is installed on the user's smartphone. In such cases, information that identifies or can be used to identify the address of a ClinSquare server to which the appointment information should be communicated need not be encoded within the ClinSquare QR code that is displayed to and scanned by a user. In such native application deployments, the information that identifies or can be used to identify the address of a ClinSquare server may be pre-configured and stored in the smartphone's memory, such as in data storage module **116**. Alternatively, the native application may dynamically determine the address of the appropriate ClinSquare server at the time of the ClinSquare QR code scan by a user. In such scenarios, ClinSquare processing is very similar to that described above, except that the address of the ClinSquare server is not obtained by a user scan of a ClinSquare QR code.

Participation reward information may be provisioned and stored by server **200**. Exemplary reward information is shown in Table 27 and includes a reward identifier **558**, a reward description / value **560**, a reward entity **561** (e.g., issuing entity / merchant), and reward expiration information **562**.

It will be appreciated that user information, such as user account information associated with scan-triggered service server **200** may be provisioned by a user or other provisioning entity. Exemplary user account information is shown in Table 22, and includes user identifying information **300**, username information **302**, and user address / zipcode information **304**.

Shown in Figure 7B, a user scans ClinSquare code **710**. Scanning of the ClinSquare code causes the scan-enabled client module **104** to communicate user identifying / user login credentials, ClinSquareID information, Deployment EntityID information, and Deployment LocationID information to ClinSquare scan-triggered application server **200**, as indicated in step 1. When the ClinSquare QR code is scanned by the user's QR code scanner, the encoded ClinSquareID information and ClinSquare/scan-triggered server identifier or address information is extracted by the QR code scanner and the information that identifies or can be used to identify a ClinSquare application server is used to facilitate communication of the extracted ClinSquareID information to the identified ClinSquare application server, step 2. It will be appreciated that in various embodiments of the subject matter described herein, the ClinSquareID information may be encrypted or obfuscated during communication from the user's mobile communication device to the ClinSquare application server. In other embodiments, the information that identifies or can be used to identify a ClinSquare application server may itself be encrypted or obfuscated when read by the QR code scanner, and may be subsequently decrypted / de-obfuscated by scan control logic module **112** so as to obtain the information necessary to identify the ClinSquare application server to be contacted. Also communicated to the ClinSquare application server is information that identifies or can be used to identify the user (e.g., the person that scans the ClinSquare QR code). This user identifying information may be provided to the ClinSquare application server **200** before, after, or at the same time that the previously discussed scanned information is provided. For example, in one embodiment, the user may log in (i.e., provide login credentials that are sufficient to identify and authenticate the user) prior to scanning the ClinSquare QR code, and application server **200** is adapted to associate the subsequently received ClinSquareID information with the user. Alternatively, the user's login credentials may be provided at the time of / as a result of the ClinSquare QR code scan, along with information that can be used by server **200** to identify the Study, Deployment Entity, and Deployment Location, and other pre-provisioned information associated with the study.

ClinSquare application server **200** receives the information, which includes user identifying / user login credentials and ClinSquareID information. ClinSquare application server **200** binds the received ClinSquareID information to the UserID of the scanning user, and stores the information in a scan transaction record that is placed in data storage module **212**. ClinSquare Control Logic Module **222** uses the provided ClinSquareID information to access one or more screening questions **546** (via ScreeningQuestionID **544**) associated with the study. Module **222** responds to the scanning user with one or more screening questions, as indicated in step 3. It will be appreciated that server **200** may communicate an entire structured "tree" of questions, which includes an initial question and one or more levels of follow-up questions that may be dependent on the answers given / response options selected by the user. Such a question tree / follow-up question information may be communicated in one message (such as is shown in step 3) or serially in multiple messages. In one embodiment, user **100** may enter a free text response(s) to the study question(s), which are communicated to server **200** where the user is logged / bound to the associated user identifying information. In one embodiment, module **222** provides user **100** with one or more possible response options **547** associated with a screening question, and these response options are displayed on the screen of the user's mobile device. For example, with regard to the question "What is your gender?" module **222** may communicate the question text to user **100** along with two response options, "Male", "Female". These two response options may be displayed to the user in the form of touch-selectable or tap-able buttons that are displayed on the screen of mobile device **100**. Using user interface module **108**, the user provides answers to the screening questions and the answers are communicated to application server **200**, where the user is logged and bound to the associated user identifying information, as indicated in step 4. Exemplary scan transaction record / log information is shown in Tables 28 and 29, which include UserID information **564**, scanned ClinSquareID information **566**, scan timestamp information **568**, granted RewardID information **570**, presented or asked screening question identifier information **568**, associated screening question response / answer identifying information **572**, and screening results / status indicator information **574**. ClinSquare Control Logic Module **222** evaluates the respondent's answers using previously provisioned screening rules / pass criteria **548**. In one embodiment, if the user does not pass the screening / vetting process, application server **200** communicates a message to the user indicating that the user does not qualify for the study (not shown in Figure 7B), or for example, no further screening questions or follow-up questions are presented to the user. In one embodiment, if the user does pass the screening process, application server **200** is adapted to perform a study recruitment action. Exemplary study recruitment actions may include, but are not limited to, communicating study coordinator contact or advanced screening coordinator contact information to the user, such as providing the user with a telephone number (and/or other contact information) associated with, for example, a study coordinator, study screening center, or study physician, as indicated in step 5. Application server **200** may also collect and store personal information associated with the user, such as name, address, zip code, telephone number and email address information. Another study recruitment action includes for example, a situation where application server **200** may generate and communicate information to the study coordinator that can be used to facilitate further contact / communications with the user (e.g., a telephone number, an email address, etc.), as indicated in step 6. Yet another study recruitment action includes for example, a situation where application server **200** may generate and communicate an externally communicated message (e.g., email or text) addressed to the user, where the message includes information associated with the clinical trial study, contact information associated with the study (e.g., contact information associated with a study coordinator, study screening center, or study physician, etc.), and scheduling information associated with an appointment to meet with a study coordinator, study screening center, or study physician, as indicated in step 7.

In one embodiment, Reward Control Logic Module **210** is adapted to communicate to the user or credit to the user's ClinSquare account a participation reward associated with the scanning of the ClinSquare QR code by the user. In one embodiment, Reward Control Logic Module **210** is adapted to communicate to the user or credit to the user's ClinSquare or other scan-triggered service account a participation reward once the user has answered some or all of the screening questions, step 8. It will be appreciated that the participation reward granted to a user may be dependent on the deployment entity or deployment location associated with the scanned ClinSquare QR code. For example, if a user scans a ClinSquare scan code that is associated with and deployed at a Walgreen's Pharmacy (e.g., the deployment entity ID **550** associated with the encoded ClinSquareID refers to Walgreen's Pharmacy, then the user may be granted a reward for a discount on goods or services provided by Walgreen's Pharmacy, etc.).

It will be appreciated with regard to the ClinSquare service embodiments described above that such services may also be provided via a native ClinSquare application that is installed on the user's smartphone or mobile computing device (e.g., iPad, Kindle, etc.). In such cases, information that identifies or can be used to identify the address of a ClinSquare server to which the appointment information should be communicated need not be encoded within the ClinSquare QR code that is displayed to and scanned by a user. In such native application deployments, the information that identifies or can be used to identify the address of a ClinSquare server may be pre-configured and stored in the smartphone's memory, such as in data storage module **116**. Alternatively, the native application may dynamically determine the address of the appropriate ClinSquare server at the time of the ClinSquare QR code scan by a user. In such scenarios, ClinSquare processing is very similar to that described above, except that the address of the ClinSquare server is not obtained by a user scan of a ClinSquare QR code.

According to one aspect of the subject matter described herein, a system for facilitating the recruitment of study participants for a clinical trial study via the scanning of a scanable code by a scan-enabled client module is provided. The system includes a computing platform having at least one processor. The system further includes a server application module executable by the at least one processor. The server application module is configured to create and store a scan code identifier that is bound to a clinical trial study, receive from a scan-enabled client module, the scan code identifier that is obtained from the scanning of an associated scanable service code by a user, communicate screening question information to the user, receive associated response information from the user; and, in response to determining that the user passes a screening criteria, perform a study recruitment action.

It will be appreciated that in all of the above described embodiments, in cases where a scanning user is not registered with the scan-based service system at the time of the service code scan, the user may be prompted to register first, before proceeding further. In some cases, where appropriate, service may be made available to un-registered users. For example, RateIt square service may be made available using the present scan-based service system to unregistered users. Any user information that is needed to provide the requested scan-code triggered service which is not available to the service at the time of the user scan may be collected by the service following the scan. Such user information may be stored in the scan code-based system for future use in providing requested services to the user.

It will be understood that various details of the subject matter described herein may be changed without departing from the scope of the subject matter described herein. Furthermore, the foregoing description is for the purpose of illustration only, and not for the purpose of limitation, as the subject matter described herein is defined by the claims as set forth hereinafter.

CLAIMS

What is claimed is:

1. A system for facilitating the collection of rating score information via the scanning of a scanable code by a scan-enabled client module, the system comprising:

    a computing platform including at least one processor:

    a server application module executable by or embedded within the at least one processor and configured to:

        receive from the scan-enabled client module a request that includes information which can be used to identify a ratable entity that is to be rated;

        in response, provide to the scan-enabled client module rating scale information associated with the ratable entity;

        receive from the scan-enabled client module a user-specified rating value; and

        store the user-specified rating value in a manner that associates it with the ratable entity.

2. The system of claim 1 wherein the server application module is configured to receive from the scan-enabled client module information that can be used to identify the user.

3. The system of claim 2 wherein the information that can be used to identify the user includes a user identifier associated with a scan-triggered service account.

4. The system of claim 2 wherein storing the user-specified rating value in a manner that associates it with the ratable entity includes binding the associated user identifier or user identity information derived from it with the user-specified rating value.

5. The system of claim 1 wherein the server application module is configured to grant the user a reward in response to receiving from the scan-enabled client module a user-specified rating value.

6. The system of claim 1 wherein the rating scale information includes category-based rating scale information.

7. A method for facilitating the collection of rating score information via the scanning of a scanable code by a scan-enabled client module, the method comprising:

8. The method of claim 7 including receiving from the scan-enabled client module information that can be used to identify the user.

9. The method of claim 8 wherein the information that can be used to identify the user includes a user identifier associated with a scan-triggered service account.

10. The method of claim 8 wherein storing the user-specified rating value in a manner that associates it with the ratable entity includes binding the associated user identifier or user identity information derived from it with the user-specified rating value.

11. The method of claim 7 including granting the user a reward in response to receiving from the scan-enabled client module a user-specified rating value.

12. The method of claim 7 wherein the rating scale information includes category-based rating scale information.

13. A system for facilitating the collection of rating score information via the scanning of a scanable code by a scan-enabled client module, the system comprising:

a computing platform including at least one processor:

a server application module executable by or embedded within the at least one processor and configured to:

create and store a scan code identifier that is bound to a ratable entity;

receive from a scan-enabled client module, the scan code identifier which is obtained in response to the scanning of an associated scanable service code by a user;

in response to receiving the scan code identifier, provide to the scan-enabled client module rating scale information associated with the ratable entity;

receive from the scan-enabled client module a user-specified rating value; and

store the user-specified rating value.

14. The system of claim 13 wherein the server application module is configured to receive from the scan-enabled client module information that can be used to identify the user.

15. The system of claim 14 wherein the information that can be used to identify the user includes a user identifier associated with a scan-triggered service account.

16. The system of claim 14 wherein storing the user-specified rating value includes binding user identifier or user identity information derived from it with the user-specified rating value.

17. The system of claim 13 wherein the server application module is configured to grant the user a reward in response to receiving from the scan-enabled client module a user-specified rating value.

18. The system of claim 13 wherein the rating scale information includes category-based rating scale information.

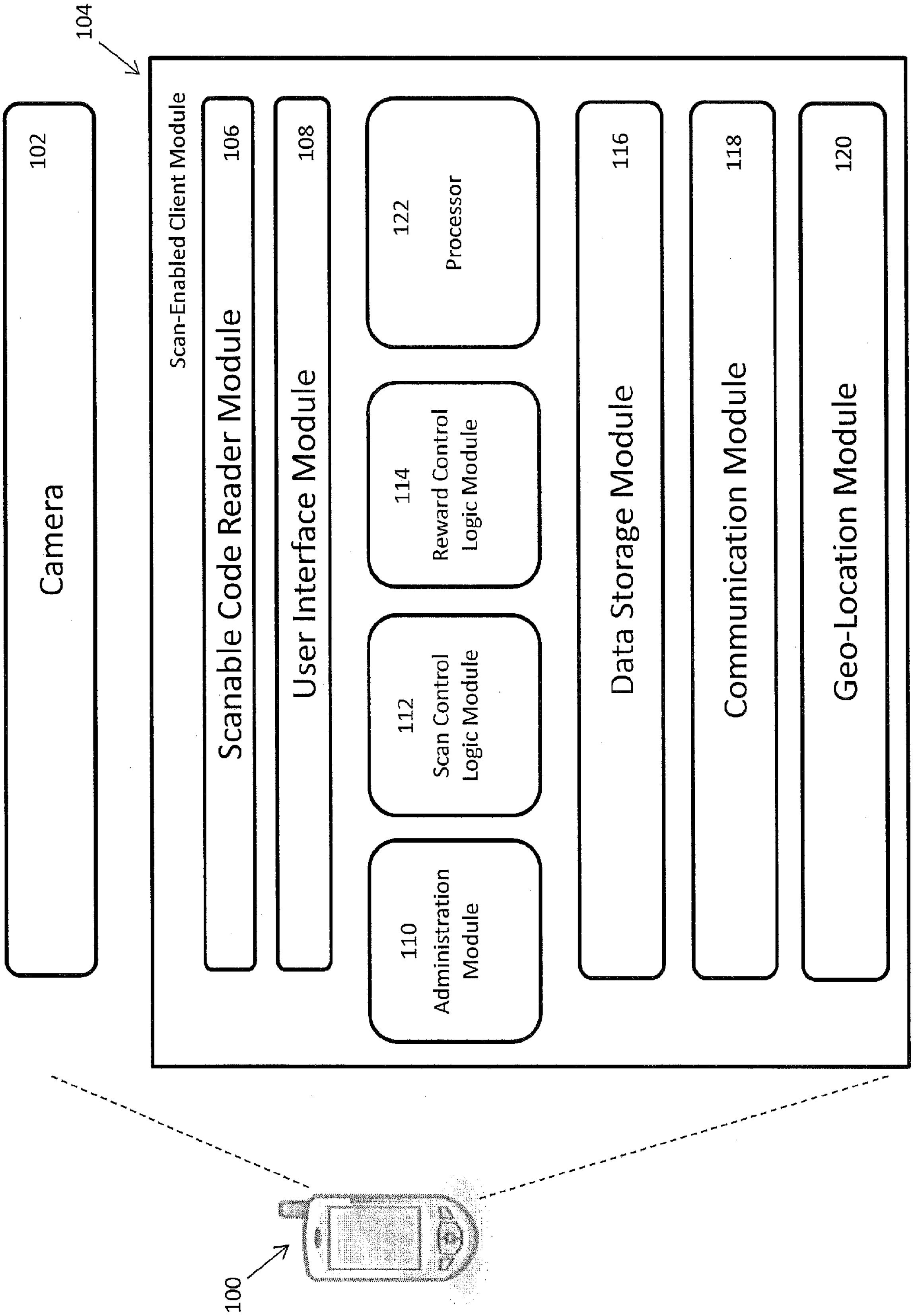

104
Camera
102
Scan-Enabled Client Module
Scanable Code Reader Module
106
User Interface Module
108
122
Processor
114
Reward Control Logic Module
112
Scan Control Logic Module
110
Administration Module
Data Storage Module
116
Communication Module
118
Geo-Location Module
120
100

Figure 1

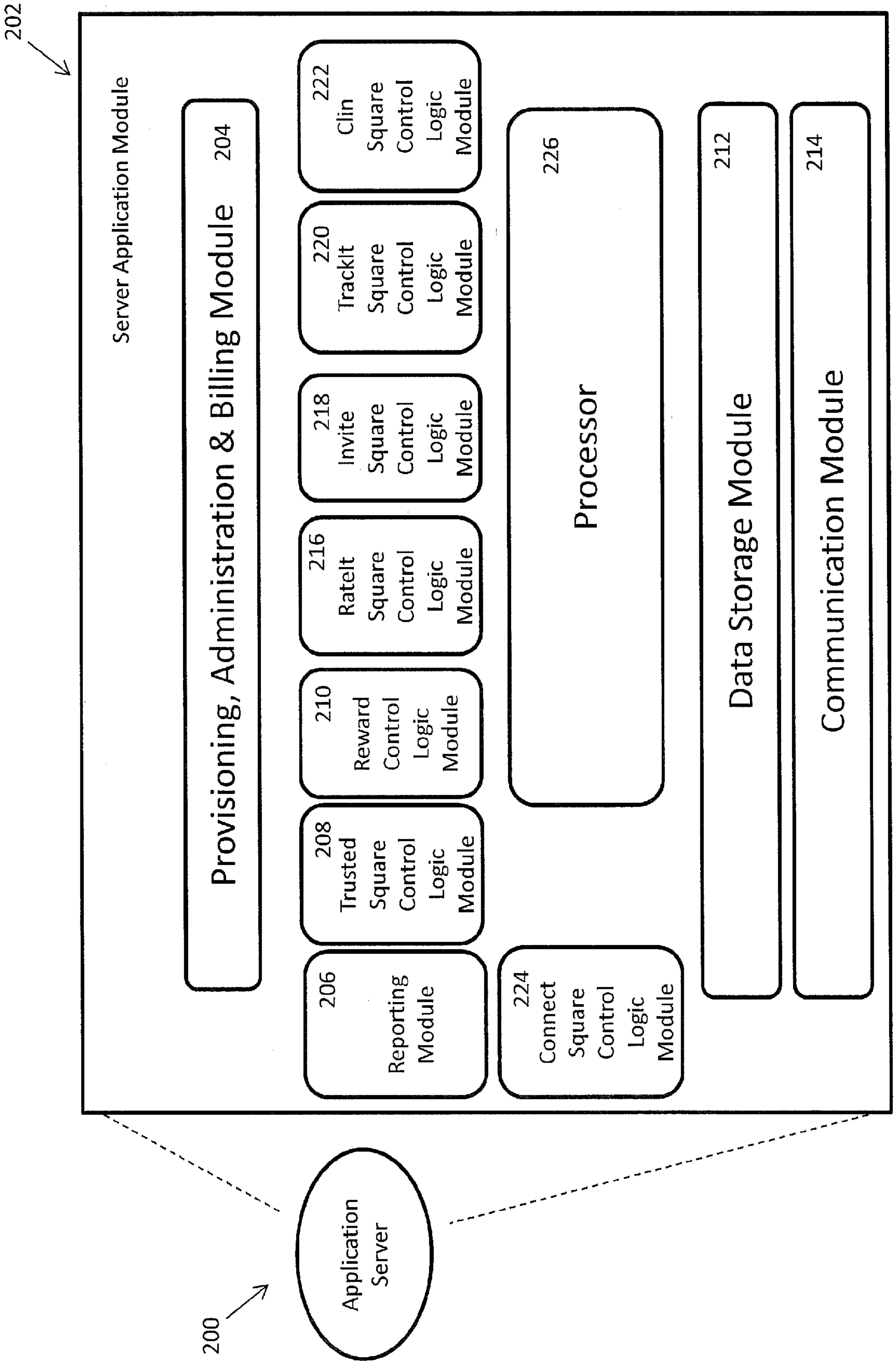

202
Server Application Module
Provisioning, Administration & Billing Module
204
206
Reporting Module
208
Trusted Square Control Logic Module
210
Reward Control Logic Module
216
RateIt Square Control Logic Module
218
Invite Square Control Logic Module
220
TrackIt Square Control Logic Module
222
Clin Square Control Logic Module
224
Connect Square Control Logic Module
Processor
226
Data Storage Module
212
Communication Module
214
200
Application Server

Figure 2

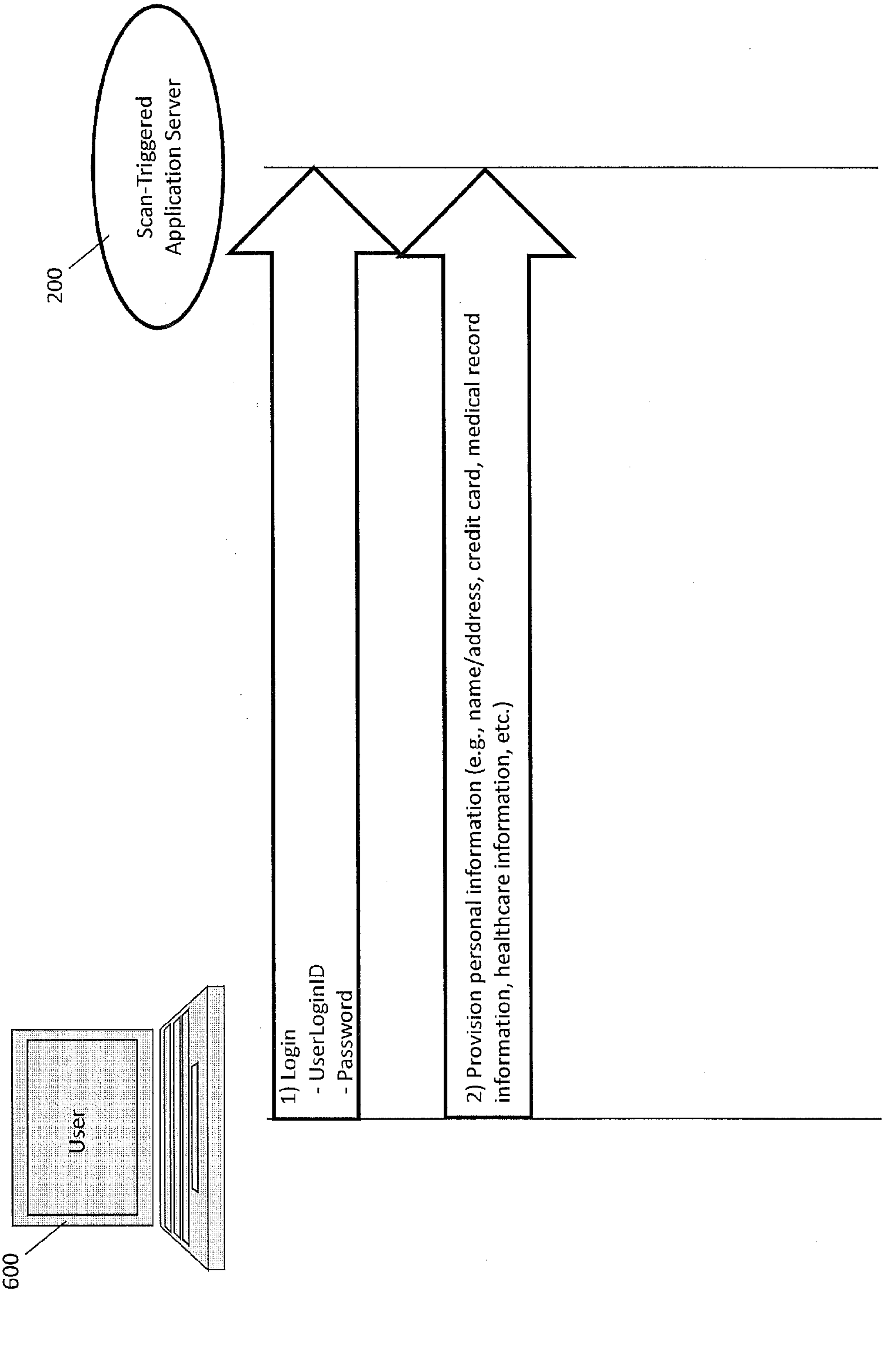

200
Scan-Triggered Application Server
600
User
1) Login
- UserLoginID
- Password
2) Provision personal information (e.g., name/address, credit card, medical record information, healthcare information, etc.)

Figure 3A

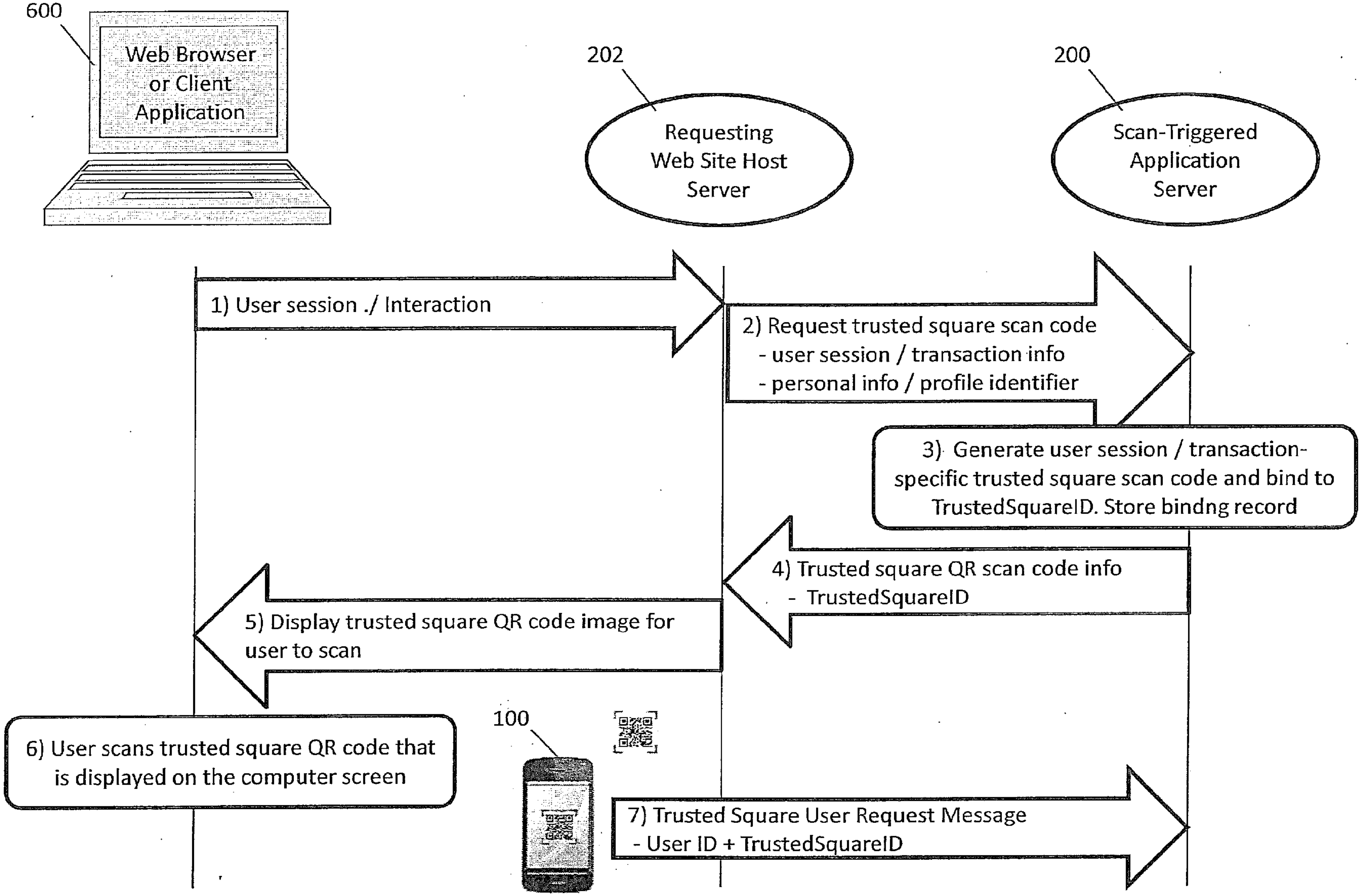

600
Web Browser or Client Application
202
Requesting Web Site Host Server
200
Scan-Triggered Application Server
1) User session ./ Interaction
2) Request trusted square scan code
- user session / transaction info
- personal info / profile identifier
3) Generate user session / transaction-specific trusted square scan code and bind to TrustedSquareID. Store bindng record
4) Trusted square QR scan code info
- TrustedSquareID
5) Display trusted square QR code image for user to scan
6) User scans trusted square QR code that is displayed on the computer screen
100
7) Trusted Square User Request Message
- User ID + TrustedSquareID

Figure 3B

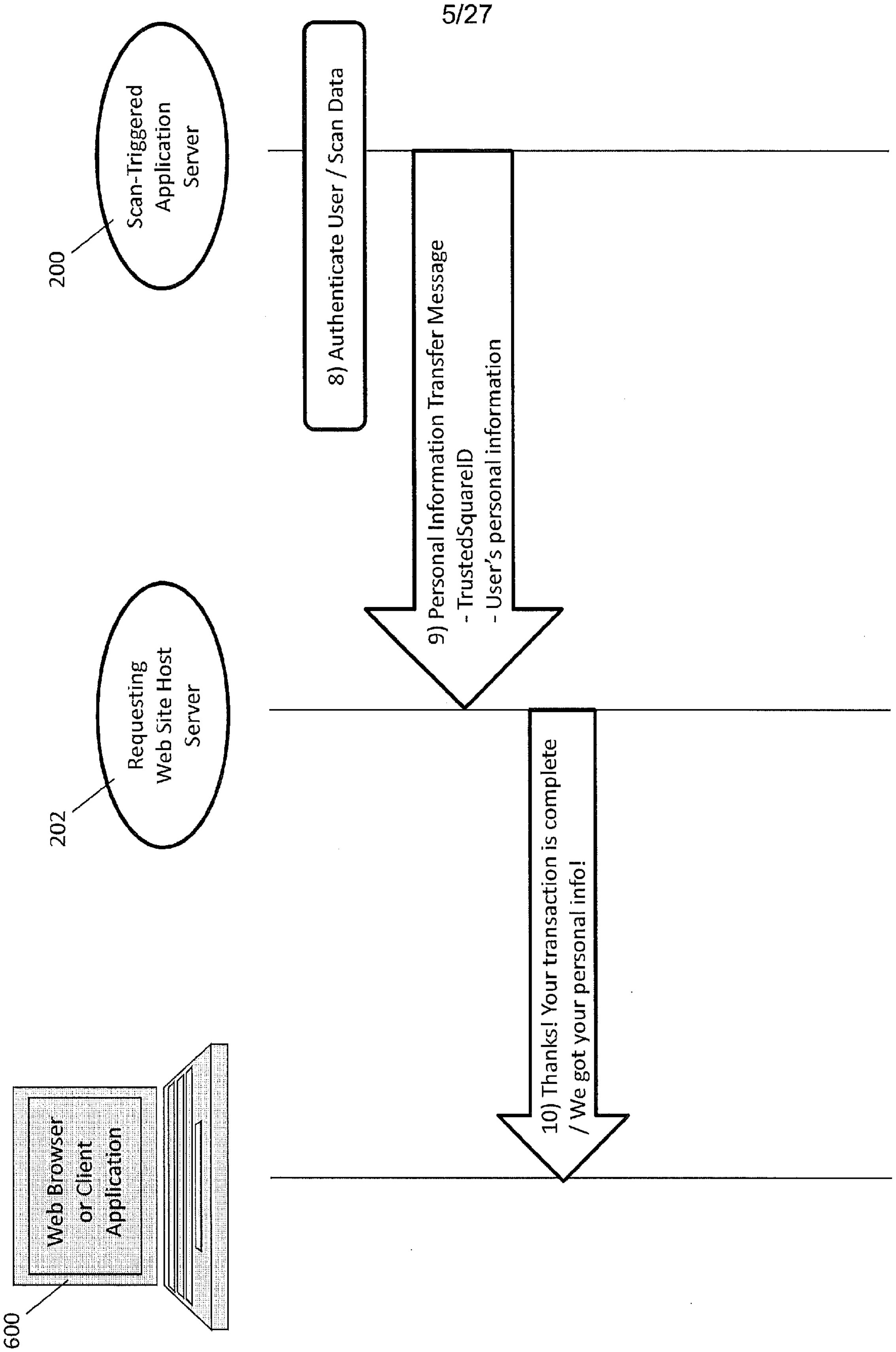

200
Scan-Triggered Application Server
8) Authenticate User / Scan Data
9) Personal Information Transfer Message
- TrustedSquareID
- User's personal information
202
Requesting Web Site Host Server
10) Thanks! Your transaction is complete / We got your personal info!
600
Web Browser or Client Application

Figure 3C

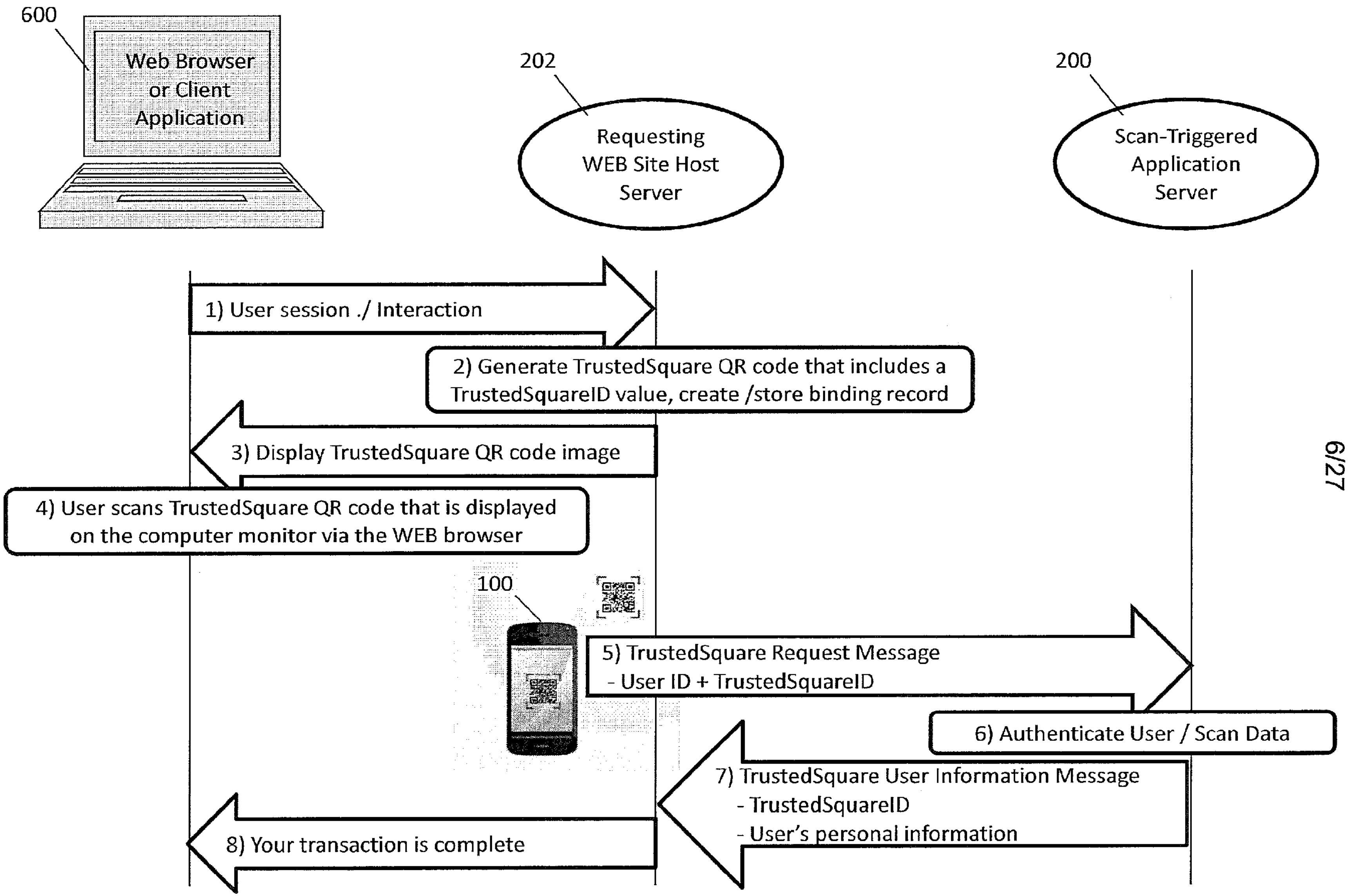
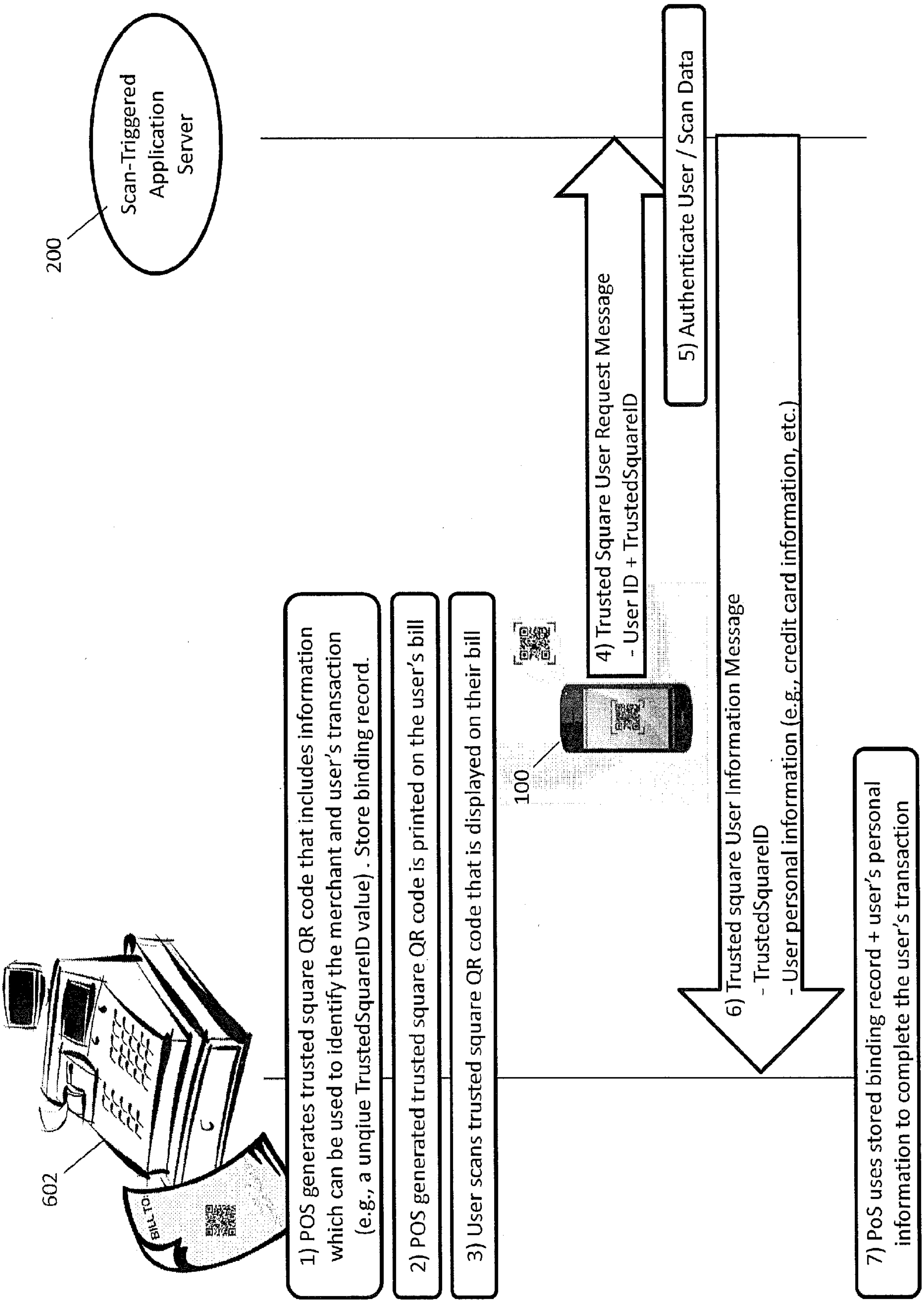

600
Web Browser or Client Application
202
Requesting WEB Site Host Server
200
Scan-Triggered Application Server
1) User session ./ Interaction
2) Generate TrustedSquare QR code that includes a TrustedSquareID value, create /store binding record
3) Display TrustedSquare QR code image
4) User scans TrustedSquare QR code that is displayed on the computer monitor via the WEB browser
100
5) TrustedSquare Request Message
- User ID + TrustedSquareID
6) Authenticate User / Scan Data
7) TrustedSquare User Information Message
- TrustedSquareID
- User's personal information
8) Your transaction is complete

Figure 3D



1) POS generates trusted square QR code that includes information which can be used to identify the merchant and user's transaction (e.g., a unqiue TrustedSquareID value) . Store binding record.

2) POS generated trusted square QR code is printed on the user's bill

3) User scans trusted square QR code that is displayed on their bill

4) Trusted Square User Request Message
- User ID + TrustedSquareID

5) Authenticate User / Scan Data

6) Trusted square User Information Message
- TrustedSquareID
- User personal information (e.g., credit card information, etc.)

7) PoS uses stored binding record + user's personal information to complete the user's transaction

Figure 3E

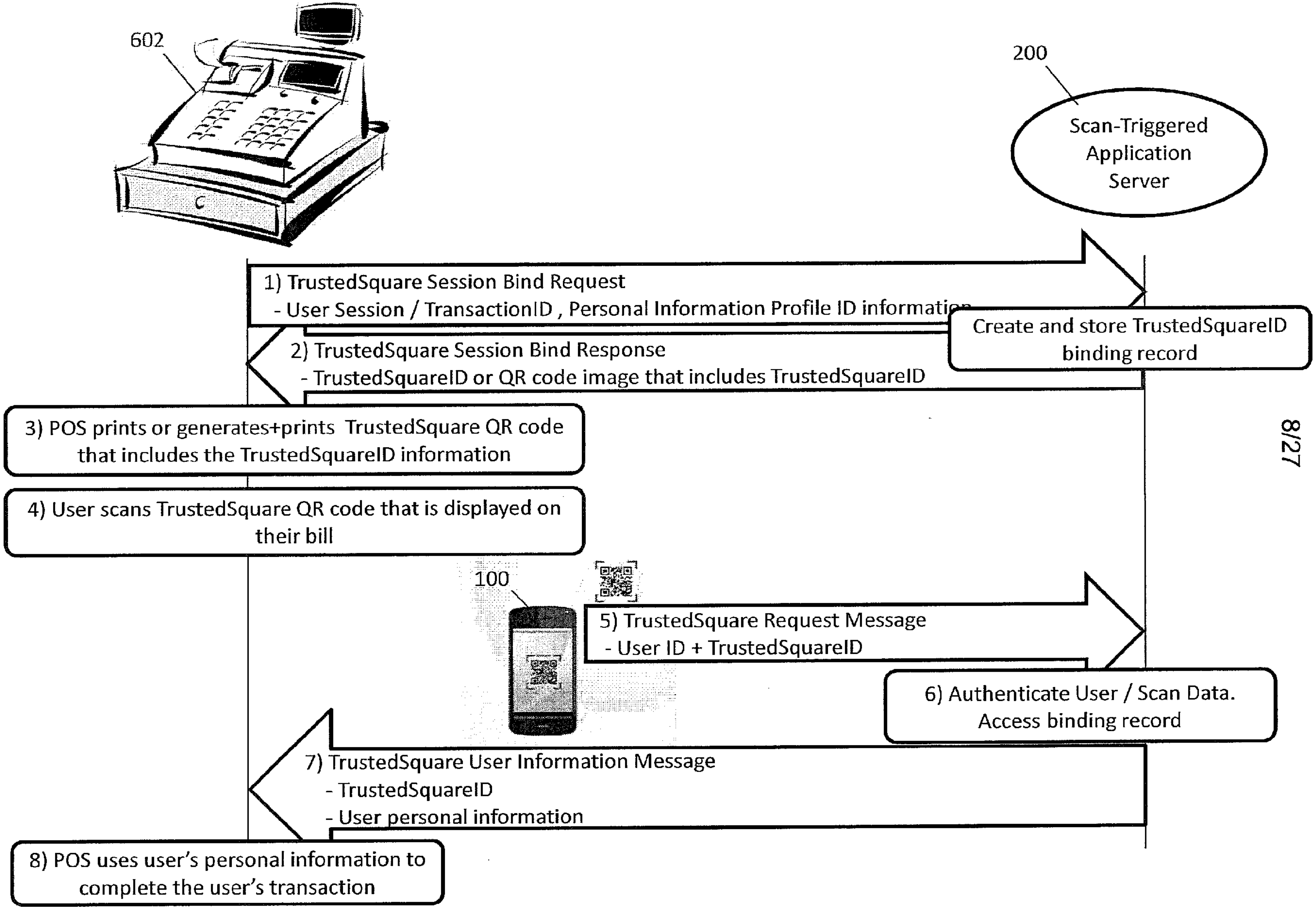

602
200
Scan-Triggered Application Server
1) TrustedSquare Session Bind Request
- User Session / TransactionID , Personal Information Profile ID informati
Create and store TrustedSquareID binding record
2) TrustedSquare Session Bind Response
- TrustedSquareID or QR code image that includes TrustedSquareID
3) POS prints or generates+prints TrustedSquare QR code that includes the TrustedSquareID information
4) User scans TrustedSquare QR code that is displayed on their bill
100
5) TrustedSquare Request Message
- User ID + TrustedSquareID
6) Authenticate User / Scan Data. Access binding record
7) TrustedSquare User Information Message
- TrustedSquareID
- User personal information
8) POS uses user's personal information to complete the user's transaction

Figure 3F

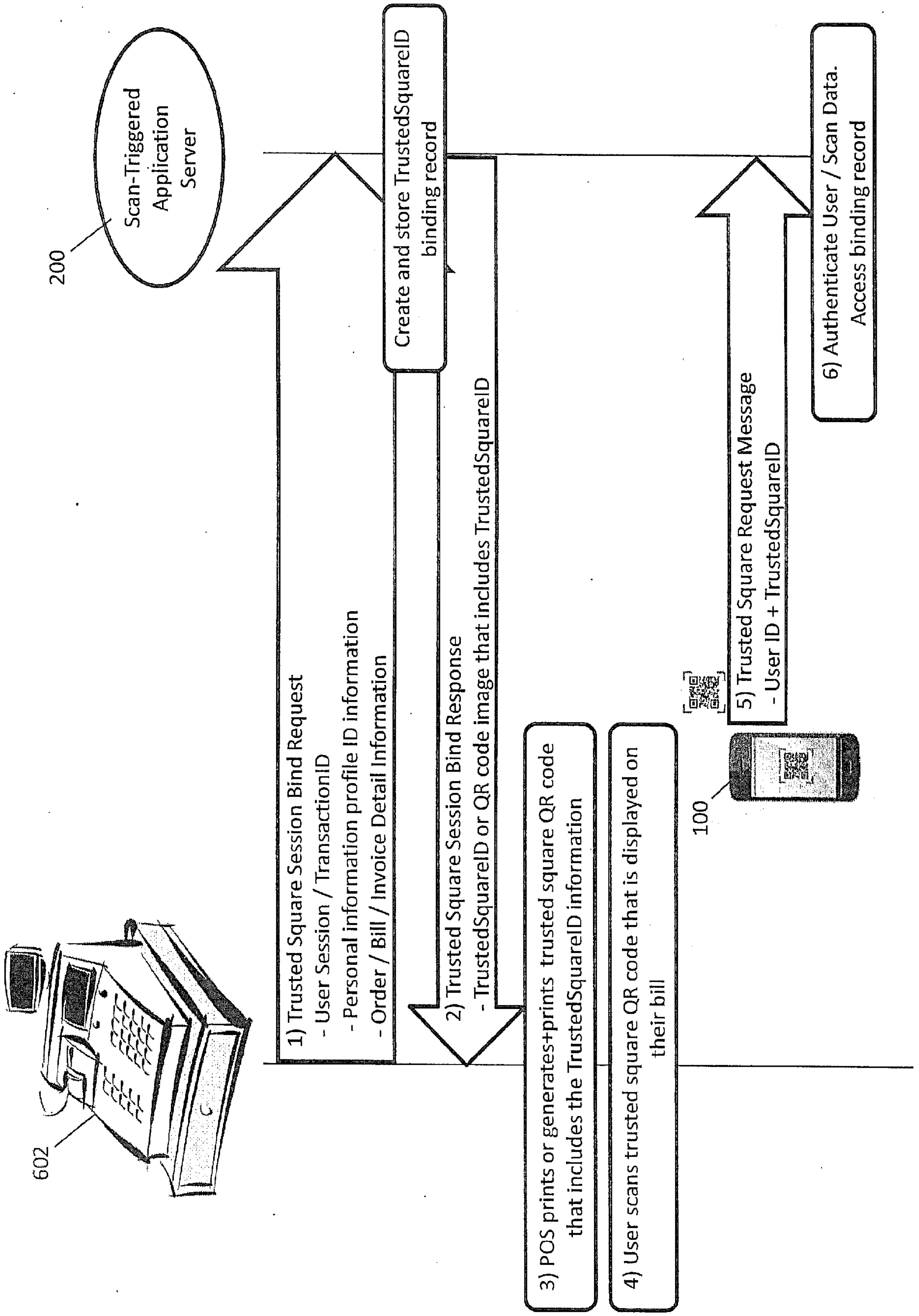

200
Scan-Triggered Application Server
602
1) Trusted Square Session Bind Request
- User Session / TransactionID
- Personal information profile ID information
- Order / Bill / Invoice Detail Information
Create and store TrustedSquareID binding record
2) Trusted Square Session Bind Response
- TrustedSquareID or QR code image that includes TrustedSquareID
3) POS prints or generates+prints trusted square QR code that includes the TrustedSquareID information
4) User scans trusted square QR code that is displayed on their bill
100
5) Trusted Square Request Message
- User ID + TrustedSquareID
6) Authenticate User / Scan Data.
Access binding record

Figure 3G

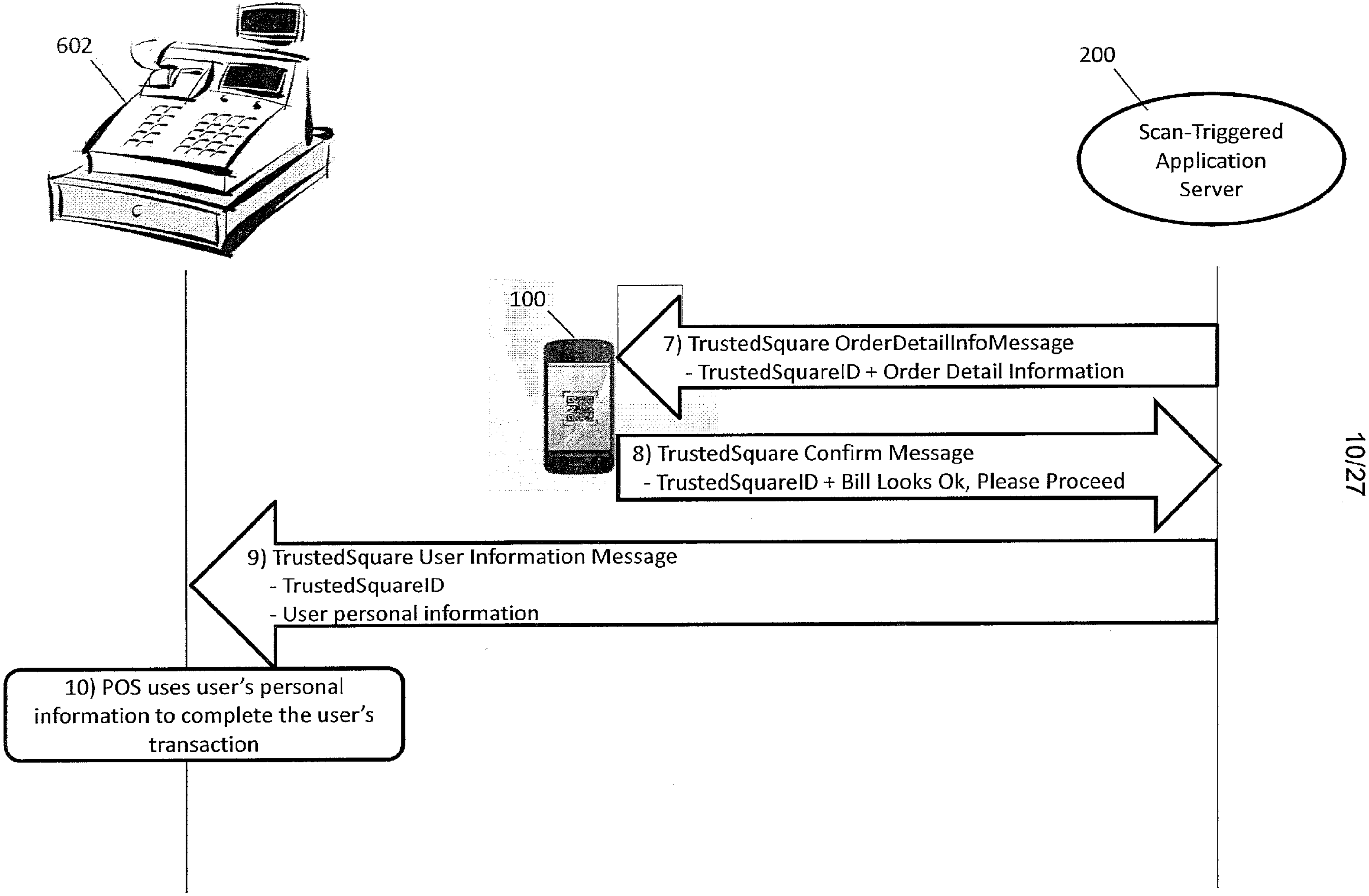

602
200
Scan-Triggered Application Server
100
7) TrustedSquare OrderDetailInfoMessage
- TrustedSquareID + Order Detail Information
8) TrustedSquare Confirm Message
- TrustedSquareID + Bill Looks Ok, Please Proceed
9) TrustedSquare User Information Message
- TrustedSquareID
- User personal information
10) POS uses user's personal information to complete the user's transaction

Figure 3H

Table 1

UserID (300)	User Name (302)
3245324	jsmith@gmail.com

Table 2

UserID (300)	User Full Name (304)	Shipping Address (306)	Billing Address (308)	Phone (310)
3245324	Joe L. Smith	12 Big St. Cary, NC 27510	10 Small St. Cary, NC 27510	9195551212

Table 3

UserID (300)	Credit Card Number (312)	Exp Date (314)	CCV (316)
3245324	1234123412341234	03/2015	657

Table 4

RequestingEntityID (318)	Requesting Entity Name (320)	IP Address/Port (322)	URL (324)	Secure Connection Credentials (326)
345	Bob's Online Store	3245324:10	www.bobsols.com	15154545

Table 5

TrustedSquareID (328)	RequestingEntityID (330)	Confirmation PIN (332)	External Confirmation Key (334)	Request Timestamp (336)	User Session/TransactionID (338)
87899	345	45645	2@#$565446	10/1/13 12:34:34	45645

Figure 3I

Table 6

TrustedSquareID (328)	PersonalInfoProfileID (340)
87899	3245324

Table 7A

TrustedSquareID (328)	UserID (340)	User Scan Timestamp (342)	User Provided Confirmation PIN (344)	External User Confirmation (346)	Granted RewardID (348)
87899	3245324	10/1/13 12:34:52	45645	2@#$565446	56578

Table 8A

PersonalInfoProfileID (350)	Personal Info Data Elements (352)
001	Full Name, Address, Phone,
002	Full Name, Billing Address, Zip Code, Credit Card number, CC expiration, CCV
003	Surgical History (e.g., surgery type, date, surgeon, medical facility, outcome data, etc.)
004	Academic history information (e.g., grades completed, universities attended, dates, etc.)

Table 9A

RewardID (354)	Reward Description (356)	Reward Entity (357)	Reward Expiration Date (358)
56578	$1 off	Bob's Online Store	11/2/2013

Figure 3J

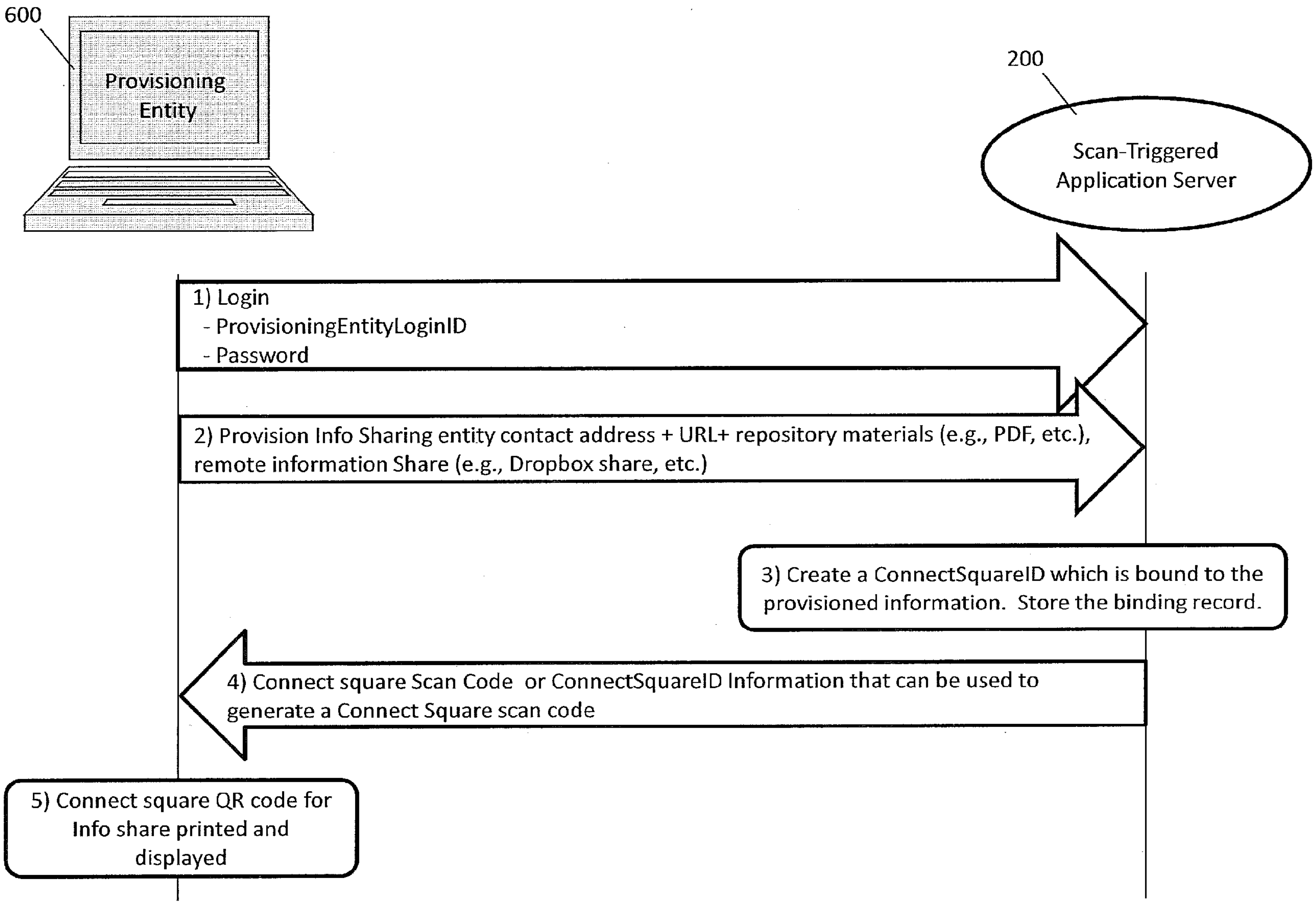

600
Provisioning Entity
200
Scan-Triggered Application Server
1) Login
- ProvisioningEntityLoginID
- Password
2) Provision Info Sharing entity contact address + URL+ repository materials (e.g., PDF, etc.), remote information Share (e.g., Dropbox share, etc.)
3) Create a ConnectSquareID which is bound to the provisioned information. Store the binding record.
4) Connect square Scan Code or ConnectSquareID Information that can be used to generate a Connect Square scan code
5) Connect square QR code for Info share printed and displayed

Figure 4A

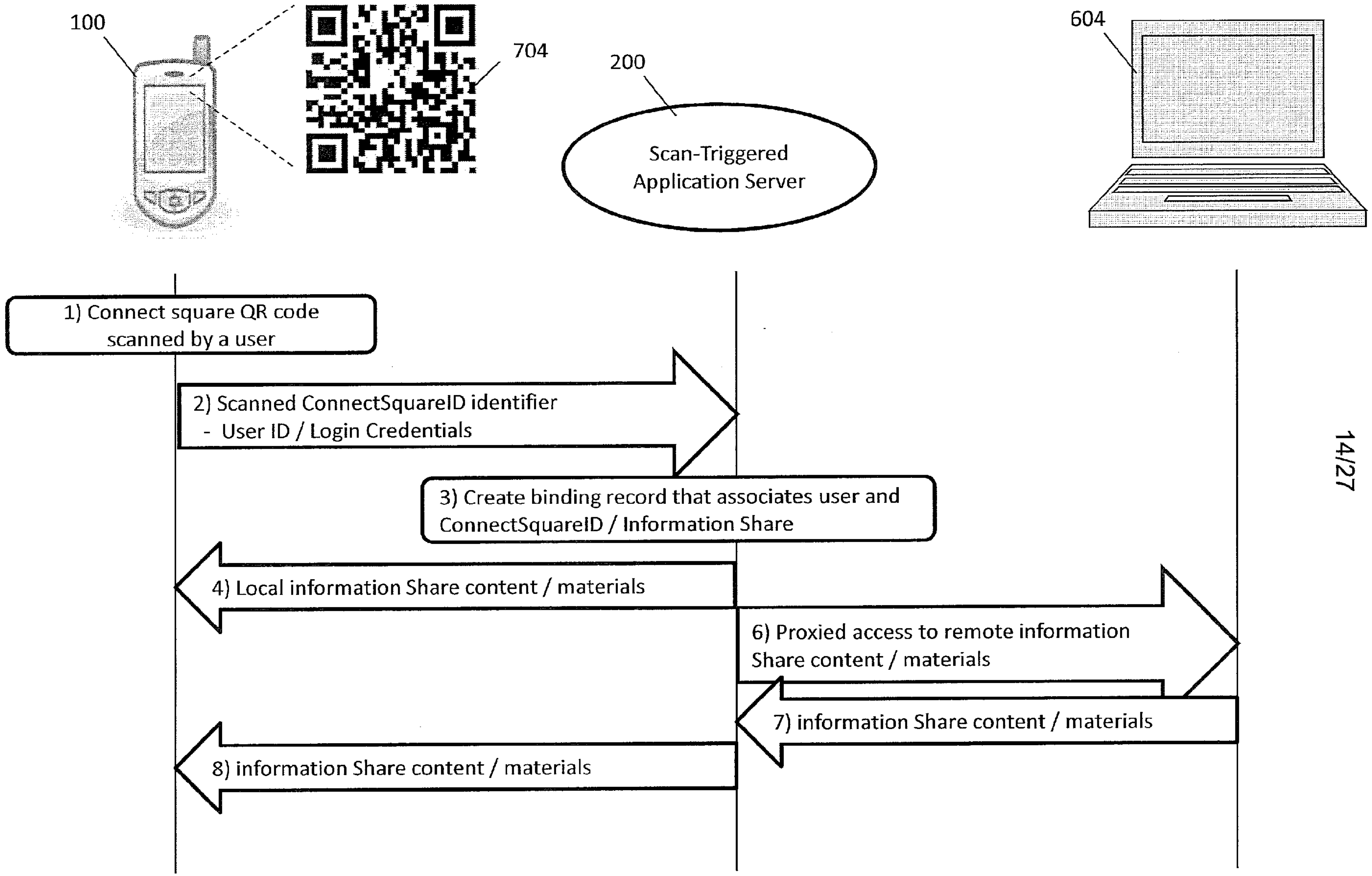

100
704
200
Scan-Triggered Application Server
604
1) Connect square QR code scanned by a user
2) Scanned ConnectSquareID identifier
- User ID / Login Credentials
3) Create binding record that associates user and ConnectSquareID / Information Share
4) Local information Share content / materials
6) Proxied access to remote information Share content / materials
7) information Share content / materials
8) information Share content / materials

Figure 4B

Table 7B

UserID *(400)*	User Name (402)	Zip (404)
3245324	jsmith@gmail.com	27516

Table 8B

ConnectSquareID *(406)*	*Information Sharer Name* Info (408)	Resource URL (410)	Contact Email / Address (412)	Contact Phone (414)
001	Bob's Furniture	www.bobsfurniture.com	Bob@gmail.com	9195551212

Table 9B

ConnectSquareID *(406)*	*RewardID* (416)	Reward Description (418)	Reward Entity (419)	Reward Expiration Date (420)
001	87899	$2 off	Bob's Furniture	11/2/2013

Table 10

UserID *(422)*	*ConnectSquareID* (424)	Scan Date (426)	Granted RewardID (428)	Feedback / Rating (429)
3245324	001	10/24/2013	87899	"Awful service"

Table 11

ConnectSquareID *(406)*	*Share Provider* (430)	Share Resource URL (432)	Share Access Credentials (434)	Share Duration (436)
001	Dropbox	www.dropbox.com/demo/	#%$r34323@#@#434	1 day

Figure 4C

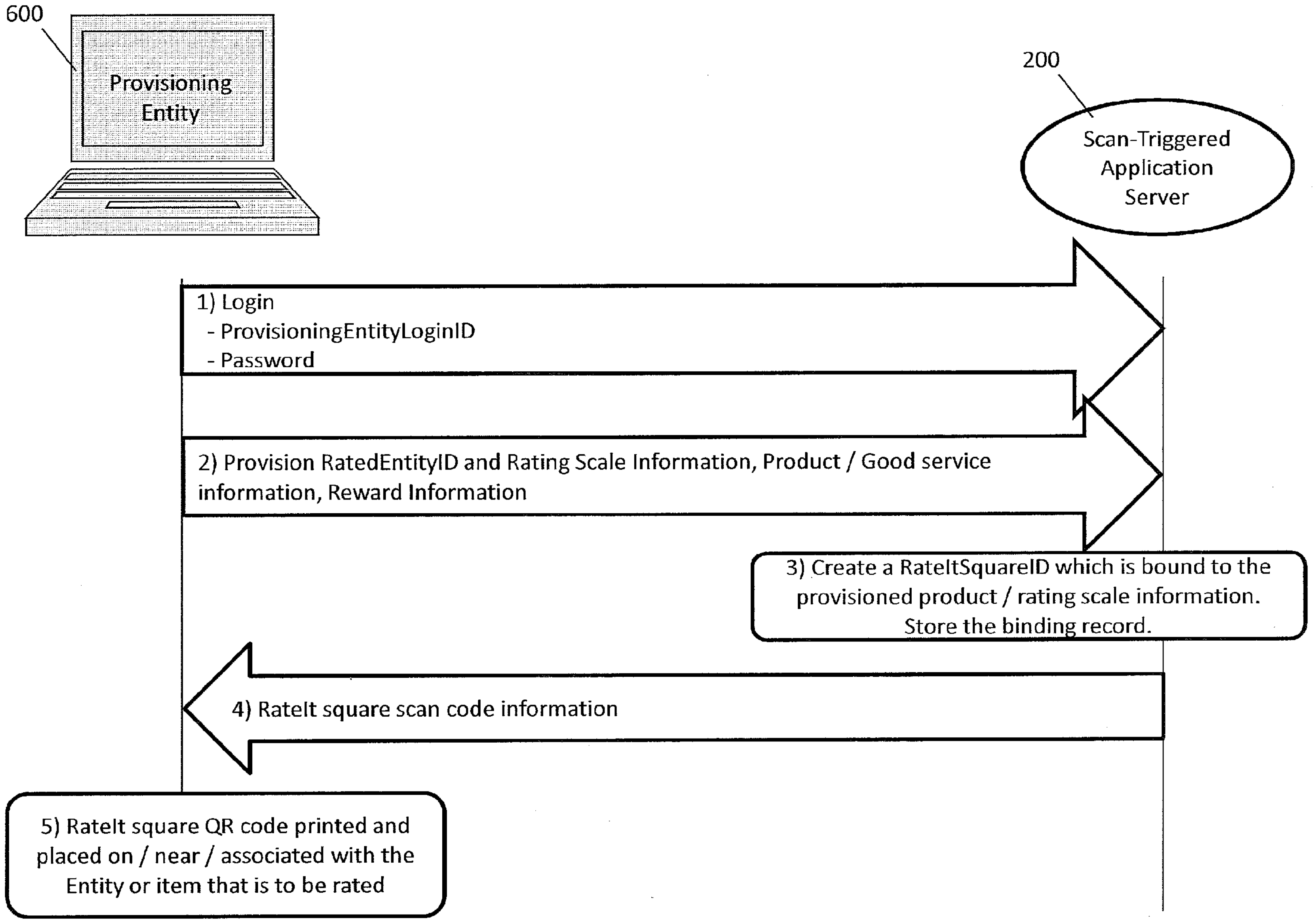

600
Provisioning Entity
200
Scan-Triggered Application Server
1) Login
- ProvisioningEntityLoginID
- Password
2) Provision RatedEntityID and Rating Scale Information, Product / Good service information, Reward Information
3) Create a RateItSquareID which is bound to the provisioned product / rating scale information. Store the binding record.
4) RateIt square scan code information
5) RateIt square QR code printed and placed on / near / associated with the Entity or item that is to be rated

Figure 5A

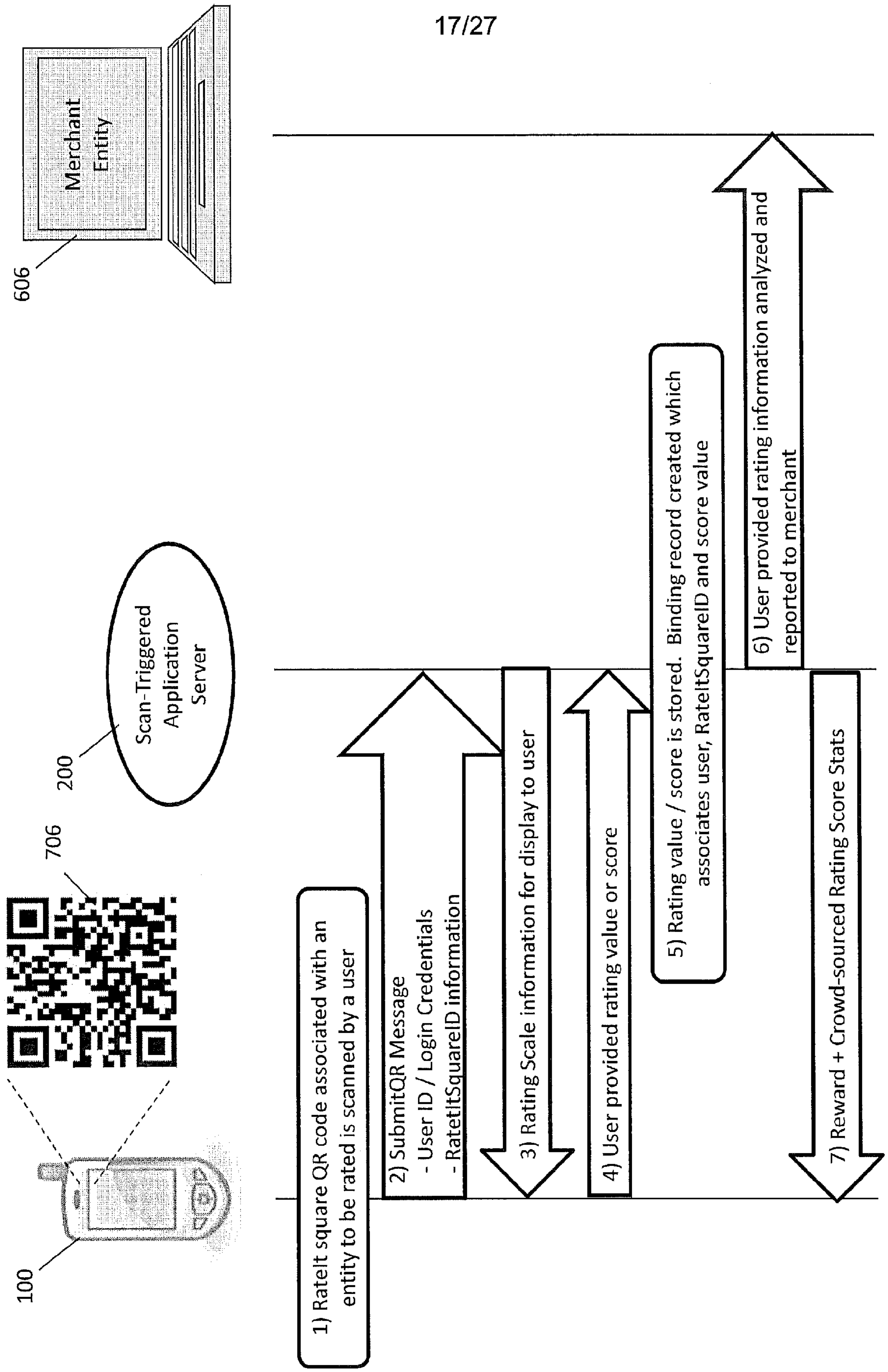

100
706
200
Scan-Triggered Application Server
606
Merchant Entity
1) RateIt square QR code associated with an entity to be rated is scanned by a user
2) SubmitQR Message
- User ID / Login Credentials
- RateItSquareID information
3) Rating Scale information for display to user
4) User provided rating value or score
5) Rating value / score is stored. Binding record created which associates user, RateItSquareID and score value
6) User provided rating information analyzed and reported to merchant
7) Reward + Crowd-sourced Rating Score Stats

Figure 5B

Table 12

UserID *(400)*	User Name (402)	Zip (404)
3245324	jsmith@gmail.com	27516

Table 13

RateItSquareID *(450)*	*RateIt Entity* *ID* (452)	RateIt Scale & Resolution (454)	MerchantID (456)	Merchant Name (458)	Location (460)
001	"Bottle #1"	1 – 10, .5 units	2342	Big Wines	Store #12
002	"Bottle #2"	Great, Ok, Poor, Awful	2584	Big Wines	Store #14

Table 14

RateItSquareID *(450)*	*RewardID* (462)	Reward Description (464)	Reward Entity (465)	Reward Expiration Date (466)
001	87899	$2 off	Big Wines	11/2/2013

Table 15

UserID *(468)*	*RateItSquareID* (470)	RateIt Value (472)	Scan Date (474)	Granted RewardID (476)
345325	001	4	10/24/2013	87899

Figure 5C

Table 16

RateItSquareID (450)	*RateIt Entity ID* (452)	Rating Category (478)	RateIt Scale & Resolution (480)	MerchantID (482)	Merchant Name (484)
001	“HoppyIPA”	Bitterness	1 (worst) – 10 (best), .5 units	524	CraftBrew
001	“HoppyIPA”	Malt Aroma	Strong, Mild, Weak	524	CraftBrew

Table 17

UserID (468)	*RateItSquareID* (486)	Rating Category (488)	RateIt Value (490)	Scan Date (492)
345325	001	Bitterness	4	10/24/2013
345325	001	Malt Aroma	Mild	10/24/2013

Figure 5D

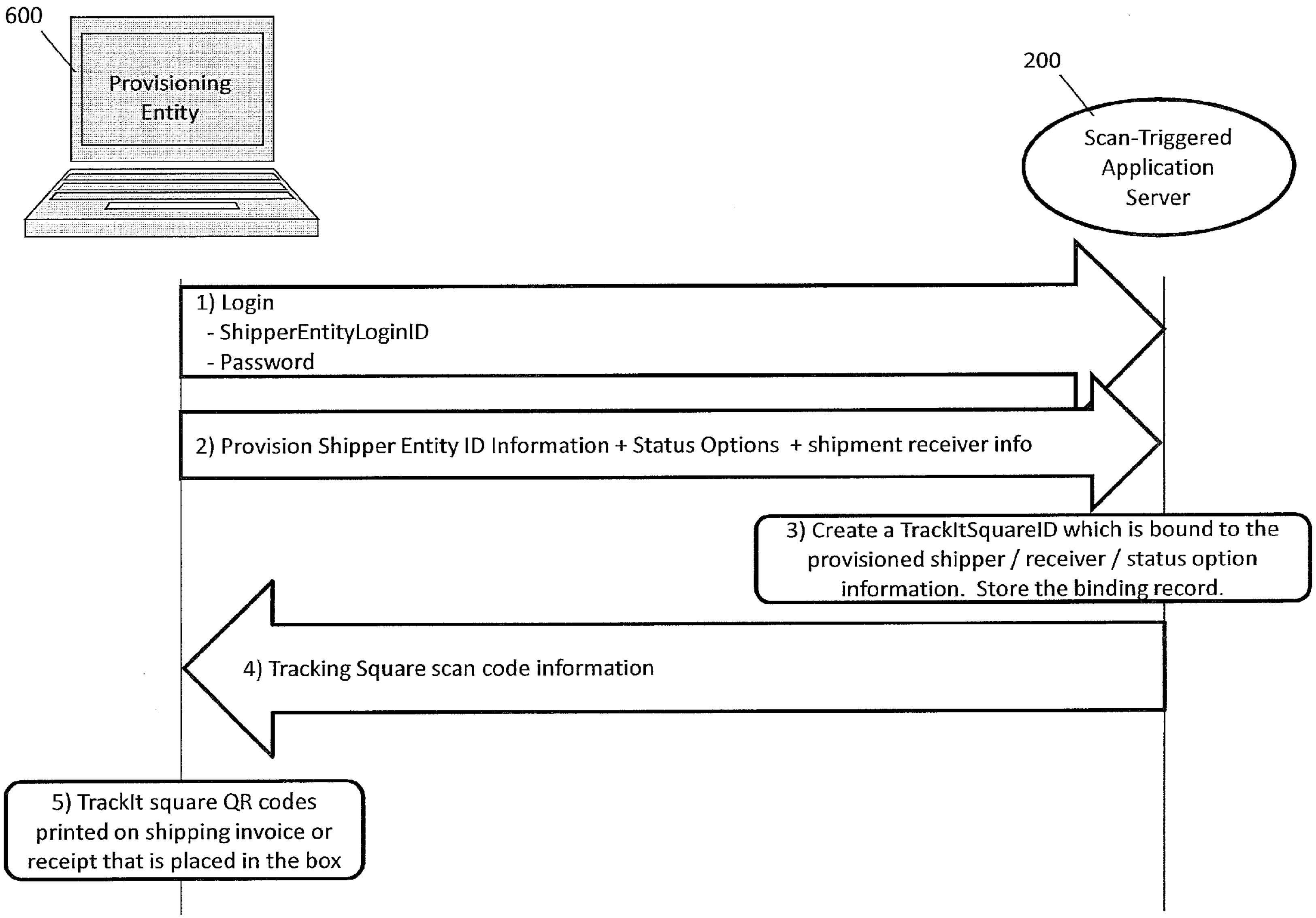

600
Provisioning Entity
200
Scan-Triggered Application Server
1) Login
- ShipperEntityLoginID
- Password
2) Provision Shipper Entity ID Information + Status Options + shipment receiver info
3) Create a TrackItSquareID which is bound to the provisioned shipper / receiver / status option information. Store the binding record.
4) Tracking Square scan code information
5) TrackIt square QR codes printed on shipping invoice or receipt that is placed in the box

Figure 6A

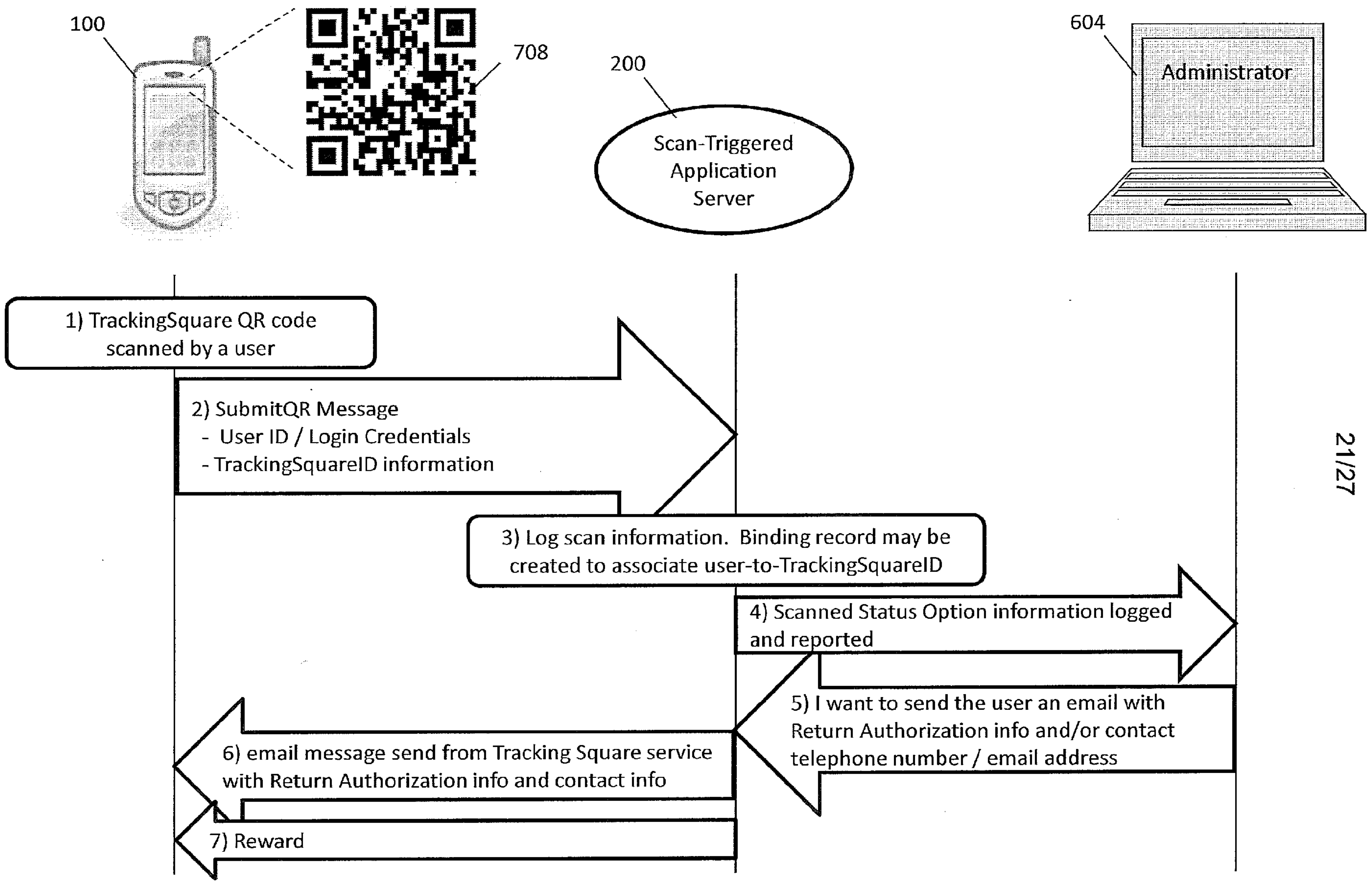

100
708
200
604
Administrator
Scan-Triggered Application Server
1) TrackingSquare QR code scanned by a user
2) SubmitQR Message
- User ID / Login Credentials
- TrackingSquareID information
3) Log scan information. Binding record may be created to associate user-to-TrackingSquareID
4) Scanned Status Option information logged and reported
5) I want to send the user an email with Return Authorization info and/or contact telephone number / email address
6) email message send from Tracking Square service with Return Authorization info and contact info
7) Reward

Figure 6B

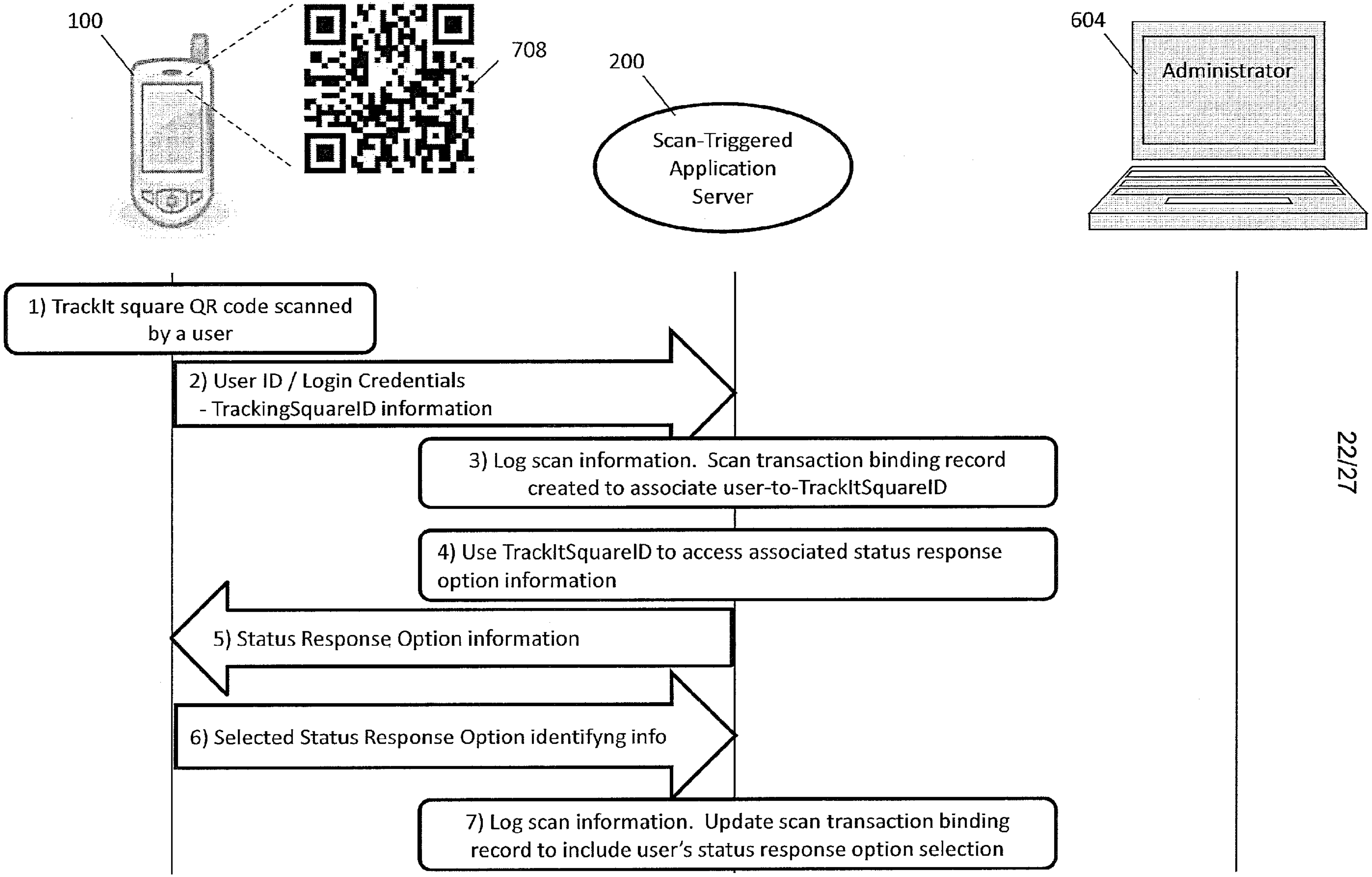

100
708
200
Scan-Triggered Application Server
604
Administrator
1) TrackIt square QR code scanned by a user
2) User ID / Login Credentials
- TrackingSquareID information
3) Log scan information. Scan transaction binding record created to associate user-to-TrackItSquareID
4) Use TrackItSquareID to access associated status response option information
5) Status Response Option information
6) Selected Status Response Option identifyng info
7) Log scan information. Update scan transaction binding record to include user's status response option selection

Figure 6C

Table 18

UserID (300)	User Name (302)	Zip (304)
3245324	jsmith@gmail.com	27516

Table 19

TrackingSquareID (500)	*Status Requesting EntityID* (502)	StatusResponse OptionID (504)	Status Response Option Description (506)	Merchant Order ID (508)	Receiver Info (509)
001	Fred's Glassware	103944	"arrived broken"	458487	CustomerID, etc.

Table 20

RewardID (510)	Reward Description (512)	Reward Entity (513)	Reward Expiration Date (514)
87899	$2 off your next order	Fred's Glassware	11/2/2013

Table 21

UserID (516)	TrackingSquareID (518)	Scan Timestamp (520)	Return Authorization (522)	Granted RewardID (524)
345325	001	10/1/13 @ 8:23:45pm	Return43234	87899

Table 22

UserID (516)	TrackingSquareID (518)	StatusResponseOptionID (526)	Scan Timestamp (520)	Return Authorization (522)	Granted RewardID (524)
345325	001	103944	10/1/13 @ 8:23:45pm	Return43234	87899

Figure 6D

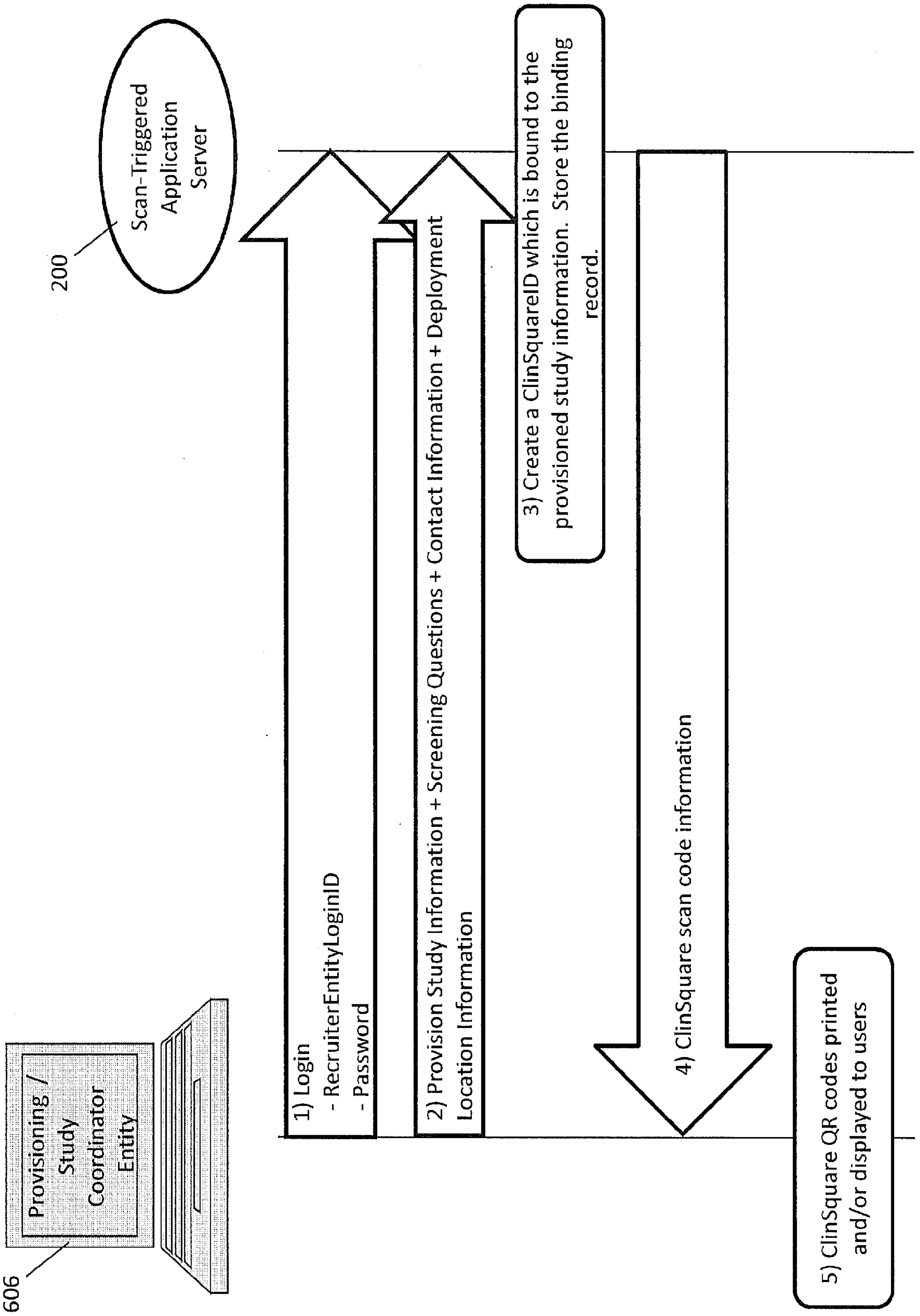

200
Scan-Triggered Application Server
606
Provisioning / Study Coordinator Entity
1) Login
- RecruiterEntityLoginID
- Password
2) Provision Study Information + Screening Questions + Contact Information + Deployment Location Information
3) Create a ClinSquareID which is bound to the provisioned study information. Store the binding record.
4) ClinSquare scan code information
5) ClinSquare QR codes printed and/or displayed to users

Figure 7A

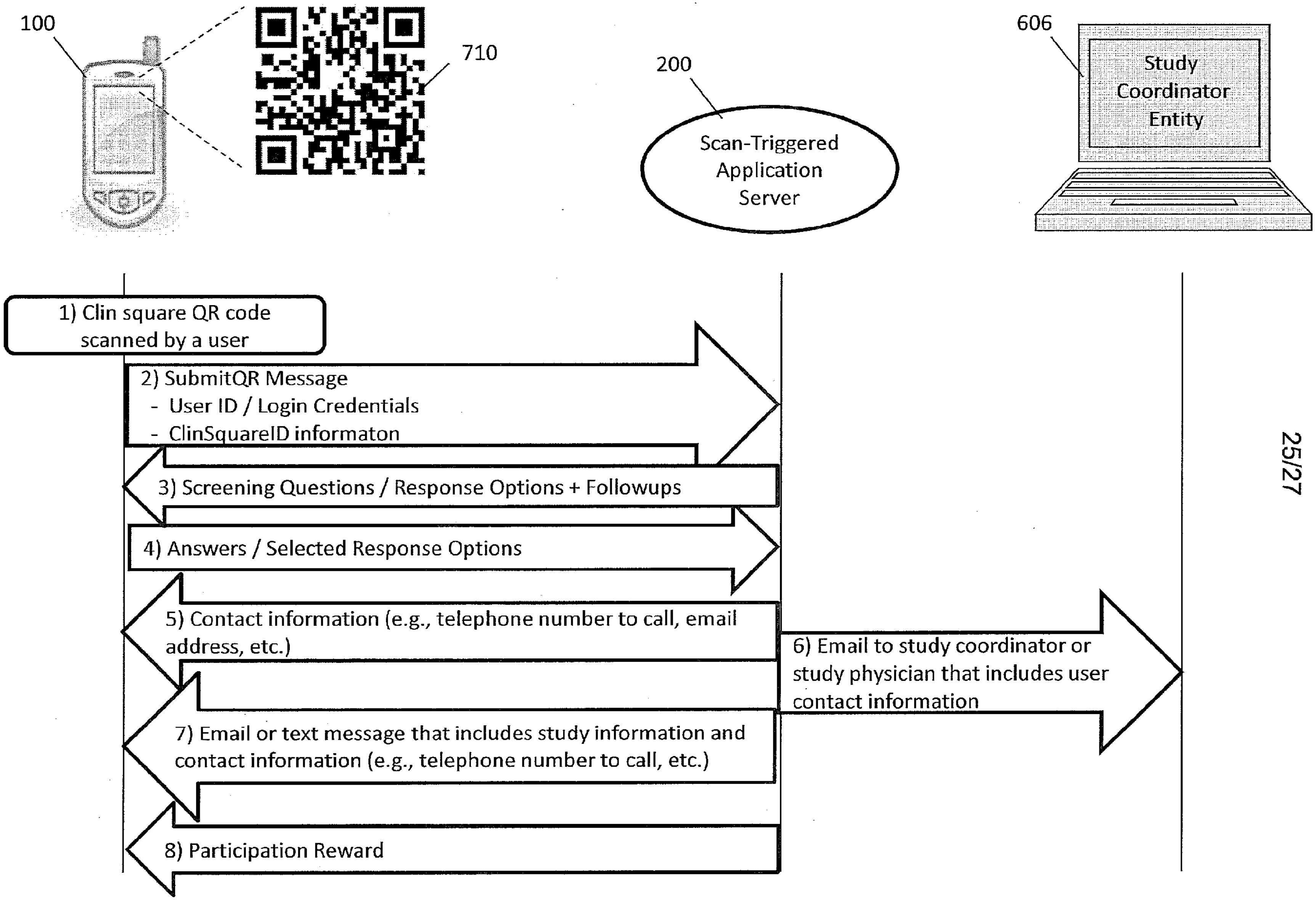

100
710
200
Scan-Triggered Application Server
606
Study Coordinator Entity
1) Clin square QR code scanned by a user
2) SubmitQR Message
- User ID / Login Credentials
- ClinSquareID informaton
3) Screening Questions / Response Options + Followups
4) Answers / Selected Response Options
5) Contact information (e.g., telephone number to call, email address, etc.)
6) Email to study coordinator or study physician that includes user contact information
7) Email or text message that includes study information and contact information (e.g., telephone number to call, etc.)
8) Participation Reward

Figure 7B

Table 22

UserID *(300)*	User Name (302)	Zip (304)
3245324	jsmith@gmail.com	27516

Table 23

ClinSquareID *(530)*	*StudyID* *(532)*	*StudyCoordinatorID* (534)	Study Description (536)
001	001	The Clinical Trial Store	High Blood Pressure Study

Table 24

StudyID (532)	*Contact Info* (538)	Location / Zipcode (540)
001	1-800-234-3243	*
002	1-919-469-5758	27510

Table 25

StudyID *(532)*	*Screening* *QuestionID* (544)	Screening Question (546)	Response Options (547)	Pass Criteria (548)
001	1	"What is your age?"	18,19,20,21,22,23,24,25,26,27	>=23 AND <=25
001	2	"What is your gender?"	Male, Female	Male

Figure 7C

Table 26

ClinSquareID *(530)*	Deployment EntityID (550)	Deployment Entity (552)	Deployment LocationID (554)	Deployment Location Description (556)
001	9485	CVS Pharmacy	321	Store #1435
002	9485	UNC Hospitals	514	Main Hospital, Chapel Hill, NC

Table 27

RewardID (558)	Reward Description (560)	Reward Entity (561)	Reward Expiration Date (562)
87899	$2 off your next prescription	Walgreen's	11/2/2013

Table 28

UserID *(564)*	ClinSquareID (566)	ClinSquare Scan Timestamp (568)	Granted RewardID (570)
345325	001	10/1/13 @ 8:23:45pm	87899

Table 29

UserID *(564)*	*ClinSquareID* *(566)*	*Screening QuestionID* (568)	Respondent Answer (572)	Evaluation (574)
345325	001	1	32	Fail
345325	001	2	Male	Pass

Figure 7D

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US14/55644

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G09G 5/24, 5/377; G06T 11/20 (2014.01)
CPC - G06T 11/60, 11/80, 11/206
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)
IPC(8)-G09G 5/24, 5/377; G06T 11/20 (2014.01);
CPC-G06T 11/60, 11/80, 11/206; USPC-345/440, 441, 469

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)
MicroPatent (US-G, US-A, EP-A, EP-B, WO, JP-bib, DE-C,B, DE-A, DE-T, DE-U, GB-A, FR-A); Google Patent/Google Scholar; IP.com; IEEE.org; collect* track, monitor, rate, ratable, scan*, read, client, QR code, RFID, client, mobile, rank, inventory, identify*, reward, goods, wharehouse, QR, smart tag, wine, track*1, bar code, score, grade, bottle, item, stock, consumer, trend, collect*, NFC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 2013/0187926 A1 (SILVERSTEIN, T et al.) July 25, 2013, paragraphs [0076]-[0080], [0306],[0337]- [0339], [0349]	1-2, 6-8, 12-14, and 18 -------------------------------- 3-5, 9-11, 15-17
Y	US 2007/0187266 A1 (PORTER, G et al.) August 16, 2007, paragraphs [0070]-[0080]	3-5, 9-11, 15-17

□ Further documents are listed in the continuation of Box C. □

* 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 17 November 2014 (17.11.2014)	Date of mailing of the international search report 08 DEC 2014
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774