



(51) International Patent Classification:
G06Q 20/00 (2012.01)

(21) International Application Number:
PCT/US2016/032147

(22) International Filing Date:
12 May 2016 (12.05.2016)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **DYNAMICS INC.** [US/US]; 493 Nixon Road, Cheswick, PA 15024 (US).

(72) Inventors; and

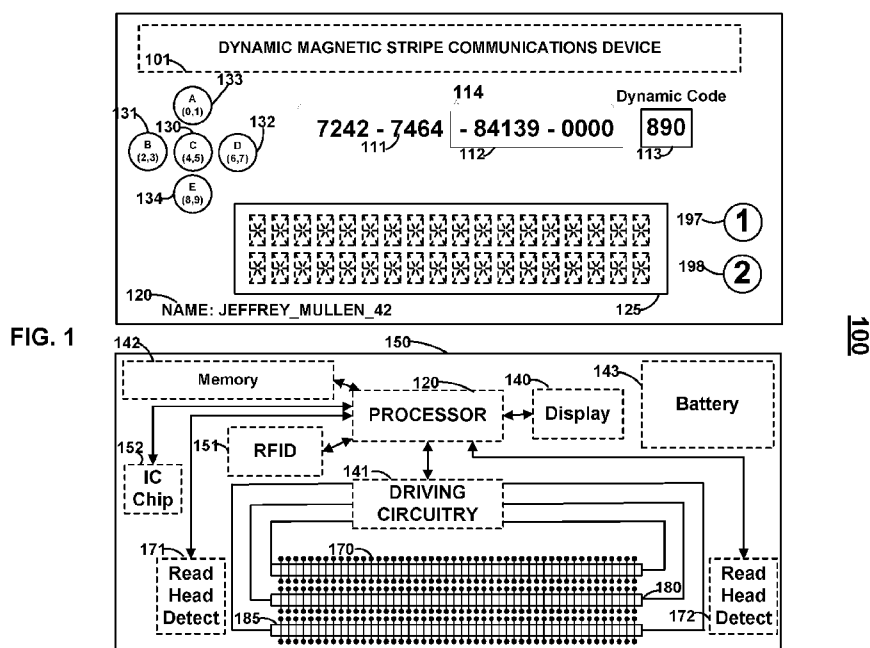
(71) Applicants (for US only): **MULLEN, Jeffrey, D.** [US/US]; 2212 Hassinger Lane, Glenshaw, PA 15116 (US).

BEAVER, Jonathan, L. [US/US]; 377 Wealdstone Road, Cranberry, PA 16066 (US).

(74) Agent: **GADDE, Sreekar, R.**; 493 Nixon Road, Cheswick, PA 15024 (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.

(54) Title: CARDS, DEVICES, SYSTEMS, METHODS AND DYNAMIC SECURITY CODES



(57) Abstract: A dynamic security code may be communicated to a verification entity by a payment device during a transaction. The verification entity may determine the validity of the dynamic security code. The determination may include comparing the dynamic security code to an expected value. In a case where the expected value is not received the dynamic security code may be compared to a valid dynamic code range. The range may include codes that immediately precede and succeed the expected code in order of expected receipt. A number of preceding codes may be different than a number of succeeding codes in the valid dynamic code range based on factors. A width of the valid dynamic code range may vary based on the factors. The factors may be based on, for example, transactional data, a transaction history, a transaction risk level, a trust relationship and/or a type of the transaction.

(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).

Declarations under Rule 4.17:

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

Published:

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

CARDS, DEVICES, SYSTEMS, METHODS
AND DYNAMIC SECURITY CODES

5 Cross-Reference To Related Application

[0001] This application claims the benefit of U.S. Provisional Patent Application No. 61/783,114, titled "CARDS, DEVICES, SYSTEMS, METHODS AND DYNAMIC SECURITY CODES," filed March 14, 2013 (Attorney Docket No. 10 D/144 PROV), which is hereby incorporated by reference herein in its entirety.

Background of the Invention

[0002] Example embodiments relate to magnetic cards, 15 devices and transaction systems.

Summary of the Invention

[0003] Systems and methods may be provided for securely processing a transaction and/or a payment of 20 goods with a payment card or other device (e.g., a mobile telephonic device, a tablet computer device, or another electronic device), and facilitating a user's selection of a service to be performed in addition to the transaction (e.g., the provision of a feature).

25 [0004] A card, or other device, may include one or more buttons. A user may associate a feature to a button of a card at any time and select the feature by pressing the button. At the time of purchase, information indicative of a dynamic security code, the type of 30 transaction and/or the button the user selected may be passed to a point-of-sale system as part of discretionary

- 2 -

data, along with a user's payment information. Such data may be, for example, communicated through a merchant acquirer's network to a processing facility.

[0005] The processing facility may, for example, authorize a payment transaction (e.g., based on a dynamic security code) and forward the information indicative of the type of transaction, the button a user selected and/or the identity of the user to a remote facility. The remote facility may be maintained by, for example, an ecosystem provider that provides an ecosystem associating payment cards, transaction types and feature providing applications, and facilitates the provision of features to users of the ecosystem. The remote facility may forward some/all of such information, and/or data based on such information, as well as additional information, to an application provider (e.g., a third party service provider) such that the application provider may enact a feature desired by the user.

[0006] A feature may include, for example, a game action in an online game by a game service provider, a check-in to a location by a check-in service provider, a coupon or voucher provided by a third party coupon provider, loyalty points provided by a third party loyalty service, an opportunity to rate a transaction or location provided by a rating service, any combination of such features, and/or any additional feature.

[0007] Selection of a feature may be facilitated, for example, by a Graphical User Interface (GUI) provided on a computing device (e.g., a mobile telephonic device) as a software application for that device or via the internet or an intranet through a web browser. The GUI may implement an application manager provided by an

- 3 -

application manger provider (that may be the same or different from an ecosystem provider).

[0008] Users may access an application manager via, for example, a website of the application manager provider and/or an issuer. The website may be accessed via, for example, a desktop and/or mobile browser. The user may use the application manager to manage features. For example, the user may activate applications, deactivate applications, assign applications to specific buttons (e.g., card buttons), assign applications to specific types of transactions, change application settings and/or view information with respect to individual applications via an application manager GUI.

[0009] Accordingly, for example, a user may receive a payment method compatible with the ecosystem (e.g., a powered card, or other device) in the mail and use his/her web browser to associate different features to different buttons. The user may then utilize the card in a store and press a button in order to select that feature

[0010] A facility such as a facility provided by an ecosystem provider may also receive information in addition to a dynamic security code, user identifier, a type of transaction and information indicative of the option selected by a user (or that the user made a payment). Such additional information may be, for example, the type of merchant (e.g., a retail merchant or a gas merchant), the location of a merchant (e.g., the zip code of a merchant), the origin of the transaction (e.g., online or in-store purchase), the name of the merchant (e.g., "Amazon.com," or "Walmart"), the amount of the transaction (e.g., \$10.25), identification of the commodities (e.g., services, goods, and/or the like) exchanged in the transaction, and any other information.

- 4 -

Such a facility may forward such information to an application provider (e.g., third party service provider) in addition to information generated by the facility (e.g., a second user identifier such that different
5 identifiers are used with the facility sending payment information and the application provider).

[0011] An application provider may communicate information to an ecosystem provider. Information received from an application provider may include, for
10 example, information indicative that the user was properly identified and a service was performed. Such information may be provided back to an issuing bank, processor, and/or other service provider such that the information may be displayed on a user's bill statement.
15 Additional information may also be provided that may change the way a transaction is authorized or settled.

[0012] Information indicative of a button press, a type of transaction and/or the use of a card, that triggers a feature, may be provided in and/or with a
20 payment message utilized at authorization or at settlement. Furthermore, the service provider may return information in a period of time that permits actions to be performed pre-authorization or pre-settlement.

[0013] The payment actions may be determined, for
25 example, via a user interaction with the card and/or use of a card reader. For example, a user may press a button on the card, from a group of buttons, that is associated with the application provider feature and/or use a card reader associated with the application provider feature.
30 Accordingly, a user may obtain the benefit of the whimsical and festive nature of a unique feature every time the user makes or accepts a payment.

- 5 -

[0014] A card may include a dynamic magnetic communications device. Such a dynamic magnetic communications device may take the form of a magnetic encoder or a magnetic emulator. A magnetic encoder may
5 change the information located on a magnetic medium such that a magnetic stripe reader may read changed magnetic information from the magnetic medium. A magnetic emulator may generate electromagnetic fields that directly communicate data to a magnetic stripe reader.
10 Such a magnetic emulator may communicate data serially to a read-head of the magnetic stripe reader.

[0015] All, or substantially all, of the front as well as the back of a card may be a display (e.g., bi-stable, non bi-stable, LCD, LED, or electrochromic display).
15 Electrodes of a display may be coupled to one or more capacitive touch sensors such that a display may be provided as a touch-screen display. Any type of touch-screen display may be utilized. Such touch-screen displays may be operable of determining multiple points
20 of touch. Accordingly, a barcode may be displayed across all, or substantially all, of a surface of a card. In doing so, computer vision equipment such as barcode readers may be less acceptable to errors in reading a displayed barcode.

[0016] A card may include a number of output devices to output dynamic information. For example, a card may include one or more RFIDs or IC chips to communicate to one or more RFID readers or IC chip readers, respectively. A card may include devices to receive
25 information. For example, an RFID and IC chip may both receive information and communicate information to an RFID and IC chip reader, respectively.
30

- 6 -

[0017] A device for receiving wireless information signals may be provided. A light sensing device or sound sensing device may be utilized to receive information wirelessly. A card may include a central processor that communicates data through one or more output devices simultaneously (e.g., an RFID, IC chip, and a dynamic magnetic stripe communications device). The central processor may receive information from one or more input devices simultaneously (e.g., an RFID, IC chip, dynamic magnetic stripe devices, light sensing device, and a sound sensing device). A processor may be coupled to surface contacts such that the processor may perform the processing capabilities of, for example, an EMV chip. The processor may be laminated over and not exposed such that such a processor is not exposed on the surface of the card.

[0018] A card may be provided with a button in which the activation of the button causes information to be communicated through a dynamic magnetic stripe communications device (e.g., the next time a read-head detector on the card detects a read-head). The information may be indicative of, for example, a feature (e.g., a payment feature) and/or a dynamic security code. A dynamic security code may be a security code that changes based on an event. For example, a dynamic security code may change upon each button press and/or each swipe of a device (e.g., powered card). According to at least one example embodiment, a device may include multiple buttons, at least one button immediately changing a dynamic code and a different button causing a current dynamic number to be displayed and to change upon a next swipe.

- 7 -

[0019] A processing server, such as a payment authorization server, may receive the information and may process a payment differently based on the received information. For example, the information may identify
5 a payment feature such that a purchase may be made with points, debit, credit, installment payments, or deferred payments, via a single payment account number (e.g., a credit card number) to identify a user and a payment feature code to select the type of payment a user desires
10 to utilize. As another example, the information may include a dynamic security code usable in an authorization decision.

[0020] A dynamic magnetic stripe communications device may include a magnetic emulator that comprises an
15 inductor (e.g., a coil). Current may be provided through this coil to create an electromagnetic field operable to communicate with the read-head of a magnetic stripe reader. The drive circuit may fluctuate the amount of current travelling through the coil such that a track of
20 magnetic stripe data may be communicated to a read-head of a magnetic stripe reader. A switch (e.g., a transistor) may be provided to enable or disable the flow of current according to, for example, a frequency/double-frequency (F2F) encoding algorithm. In doing so, bits
25 of data may be communicated.

[0021] Electronics may be embedded between two layers of a polymer (e.g., a PVC or non-PVC polymer). One or more liquid polymers may be provided between these two layers. The liquid polymer(s) may, for example, be
30 hardened via a reaction between the polymers (or other material), temperature, or via light (e.g., an ultraviolet or blue spectrum light) such that the

- 8 -

electronics become embedded between the two layers of the polymer and a card is formed.

[0022] A payment card or other device may receive information indicative of a feature desired by a user.

5 The payment card may communicate information indicative of the feature with payment card data associated with the card or a user selection. The payment data and feature information may be routed, for example, to an authorization server. The authorization server may

10 authorize payment and, based on the authorized payment, communicate the feature information to a remote server. The remote server may utilize this remote information to impact an application provider service. The feature information may, for example, be routed before the

15 payment card data reaches an authorization server. At merchant settlement, charge backs for a purchase associated with a feature may cause the feature to be reversed or a different feature to be implemented (e.g., a removal of rewards earned at authorization). The

20 feature may be implemented at settlement upon confirmation that, for example, no chargeback was associated with the payment transaction.

[0023] A powered and/or device card may be provided with a visible number that changes periodically or

25 changes after each use. The number may be, for example, an account number, a CVV, CVV2, CVC2 and/or a CID. For dynamic credit cards that employ periodically changing numbers, a timing signal may be used. For example, a signal representative of time may be transmitted over an

30 area (e.g., the United States). Such a timing signal may be the U.S. atomic clock signal (e.g., the WWVB signal), a European timing signal (e.g., the DCF and MSF signals),

- 9 -

or a timing signal used in a locating/navigation system (e.g., a GPS signal).

[0024] A powered card and/or device card may have a number that is secure to the user. This secure number may then
5 be coded in a variety of ways. For example, the number may be coded utilizing a counter, timer, random number generator, or pseudorandom number generator to provide a coded number. If a counter is provided, the counter may be incremented periodically (or when the credit card is
10 used). The counter may be utilized in a coding function and this number may also be transmitted to an authorization facility when the dynamic credit card number is transmitted to the authorization facility.

[0025] A three or four digit card verification code
15 may be submitted as part of a credit card authorization process. A five or more digit card verification code may be submitted as part of a credit card authorization process. Such a security code may be dynamic and may be utilized to validate a transaction. A dynamic security
20 code may be provided on a display screen separate from the dynamic credit card number or the dynamic security code may be provided on the same display screen as the dynamic card number. According to some example embodiments, a dynamic card may be provided with a
25 dynamic security code and a static credit card number such that only the dynamic security code changes. Such embodiments may, or may not, include an encoder. Thus, a credit card may be provided that includes a dynamic security code. The dynamic security code may change
30 based on an event (e.g., a button press) and a credit card authorization facility may check to make sure the dynamic security code is valid. A dynamic security code may be validated by comparing the dynamic security code

- 10 -

to a listing of valid dynamic numbers and/or determining whether the dynamic security code is within a subset of solutions to an algorithm (e.g., time based subset).

[0026] Methods may be employed to generate dynamic security codes at a point-of-sale (e.g., by a card and/or device) and verification codes at a point-of-validation (e.g., by an authorization server), such that no synchronicity is required between the point-of-sale and the validation device. For example, a device may generate a dynamic code using a function and a timing signal, or by selecting a next code in a list of codes. The dynamic code may be communicated to a verification entity. The verification entity may determine whether the dynamic code is an expected code using the function and a timing signal, and/or the list of codes.

[0027] If the dynamic code matches the expected code, the dynamic code may be validated. If the dynamic code does not match the expected code, the dynamic code may be compared to all possible codes (past, present or future). If the dynamic code does not match a possible code the dynamic code may be invalidated and a text message sent to the user. If the dynamic code does match a possible code, a valid dynamic code range may be determined and/or the dynamic code may be compared to a valid dynamic code range. A valid dynamic code range may include temporally or sequentially adjacent codes to an expected code. If a code is received by a verification entity that corresponds to a code within the valid dynamic code range, the received code may be validated. Codes corresponding to codes within a valid dynamic code range may, for example, carry an acceptable risk of fraud for a transaction.

- 11 -

[0028] A dynamic code may not match an expected code for various reasons. For example, a payment device may dynamically change a security code each time a button is pressed by selecting a next code in a sequential list of codes. A verification entity may maintain an identical list and expect a next security code in the list each time a security code is received. The verification entity may not receive the expected security code, for example, due to asynchronicity between the payment device and the verification entity. Asynchronicity may arise where, for example, a user presses a button on the payment device multiple times prior to a transaction. As another example, two merchants may communicate purchase data at different rates such that dynamic security codes are received out of sequence. As yet another example, a card button may be depressed unintentionally, for example, in a user's wallet. As still another example, a communicated number may erroneously fail and another number may be communicated.

[0029] A valid dynamic code range may be used to authorize a transaction despite any asynchronicity between entities. For example, a valid dynamic code range may include codes that may be expected to be communicated within a particular time frame. The range may be determined based on transaction data, a user's transaction history, the transaction history of multiple users, a transaction risk level, whether a transaction is online or offline, whether a merchant is trusted, and any characteristics of a transaction that may lead to the receipt of an unexpected code by a verification entity.

- 12 -

[0030] Upon issuance of an account, a payment device (e.g., a powered card and/or the like) may be configured to include a dynamic security code list and/or algorithm.

5 Brief Description of the Drawings

[0031] Principles and advantages of the present invention can be more clearly understood from the following detailed description considered in conjunction with the following drawings, in which the same reference
10 numerals denote the same structural elements throughout, and in which:

[0032] FIG. 1 shows cards and architectures constructed in accordance with the principles of the present invention;

15 [0033] FIG. 2 shows devices constructed in accordance with the principles of the present invention;

[0034] FIG. 3 shows network topologies arranged in accordance with the principles of the present invention;

[0035] FIGS. 4 and 5 show transaction verification
20 methods performed in accordance with the principles of the present invention;

[0036] FIG. 6 shows methods of determining valid dynamic number ranges in accordance with the principles of the present invention; and

25 [0037] FIG. 7 shows dynamic number ranges in accordance with the principles of the present invention.

Detailed Description of the Invention

[0038] FIG. 1 shows cards and architectures according
30 to example embodiments. Referring to FIG. 1, card 100 may include, for example, dynamic magnetic stripe communications device 101, one or more displays (e.g., displays 112, 113 and 125), permanent information 120,

- 13 -

one or more buttons (e.g., buttons 130-134, 197 and 198) and/or dynamic number 114. Dynamic number 114 may include permanent portion 111. Permanent portion 111 may be, for example, printed, embossed and/or laser etched on card 100.

5 **[0039]** Multiple displays may be provided on card 100 for various purposes. For example, display 112 may be utilized to entirely, and/or partially display a dynamic number. Display 113 may be utilized to display a dynamic
10 code (e.g., a dynamic security code). Display 125 may display logos, barcodes and/or multiple lines of information. At least one of displays 112, 113 and 125 may be a bi-stable or non bi-stable display. A bi-stable display may be a display that maintains an image without
15 power.

[0040] Permanent information 120 may include, for example, information specific to a user (e.g., a user's name and/or username) and/or information specific to a card (e.g., a card issue date and/or a card expiration
20 date).

[0041] Buttons 131-134, 197 and 198 may be, for example, mechanical buttons, capacitive buttons, or a combination of mechanical and capacitive buttons. Buttons 131-134 may be used, for example, to enter
25 information (e.g., an access code) and/or to make a selection. For example, using buttons 131-134, a user may select options displayed on display 125 that instruct card 100 to communicate (e.g., via a dynamic magnetic stripe communications device, RFID and/or exposed IC
30 chip) a user's instructions to use a debit account, a credit account, a pre-paid account, and/or a point account for a transaction (e.g., a payment transaction). According to at least one example embodiment, more than

- 14 -

one account may be selected. For example, a transaction may be divided between accounts and card 100 may be utilized to indicate a user's desire to use a point account until the point account is exhausted and then to use a credit account.

5 **[0042]** Button 197 may be used, for example, to communicate information through dynamic magnetic stripe communications device 101 indicative of a user's desire to communicate a single track of magnetic stripe information. Persons skilled in the art will appreciate that pressing a button (e.g., button 197) may cause information to be communicated through device 101 when an associated read-head detector detects the presence of a read-head of a magnetic stripe reader. Button 198 may be utilized to communicate (e.g., after button 198 is pressed and after a read-head detects a read-head of a reader) information indicative of a user selection (e.g., to communicate two or more tracks of magnetic stripe data, to communicate different track data, to modify tracks of data and/or the like).

20 **[0043]** Button 197 and button 198 may each be used to associate a feature to a transaction. For example, button 197 and button 198 may be associated to different service provider applications. Each service provider application may be associated to a different service provider feature (e.g., rewards). A user may, for example, press one or more of buttons 197 and 198 to choose one or more features for a particular transaction.

25 **[0044]** A user may associate applications to buttons and/or features to applications, for example, on a graphical user interface (GUI) of a computing device. The graphical user interface may be, for example, an application manager provided by one or more entities

- 15 -

(e.g., an application manager provider). The associations may be changed, for example, at any time, periodically, and/or upon the occurrence of an event. According to some example embodiments, a user may
5 associate applications to buttons and/or features to applications by telephone, by electronic mail and/or any other communication method.

[0045] Associations between buttons and service provider applications may be maintained by an ecosystem
10 provider, for example, within an ecosystem of applications, transactional methods and types of transactions. When a transactional method (e.g., card 100) is used by a user, the ecosystem provider may receive transaction data and information indicative of a button
15 selected by the user. The ecosystem provider may determine the identity of an application associated to the button, and may communicate some or all of the information and/or transaction data to the application and/or the service provider. The service provider and/or
20 the application may provide a feature associated with the application based on the information and/or transaction data.

[0046] According to some example embodiments, a user may associate applications to buttons and/or features to
25 applications, for example, by pressing an associated button of card 100. For example, a user may select a third party feature from a list displayed to the user. The user may scroll through the list of features on the display (e.g., a display on the front of the card) using
30 buttons on card 100. The list of features may be displayed to the user individually, in groups and/or all features may be simultaneously displayed.

- 16 -

[0047] According to at least one example embodiment, a user may select a payment method (e.g., a type of payment on card 100) via manual input interfaces. The manual input interfaces may correspond to displayed
5 options (e.g., displayed on display 125) and/or may be independent buttons. Selected information may be communicated to a magnetic stripe reader via a dynamic magnetic stripe communications device. Selected information may also be communicated to a device (e.g.,
10 a mobile telephonic device) including a capacitive sensor and/or other type of touch sensitive sensor.

[0048] Different features may be provided based on the use of different payment methods and/or transaction types. For example, suppose a service provider provides
15 a reward feature based on the use of a particular payment method (e.g., a reward for using a particular credit card). A user may purchase an item using the particular payment method (e.g., may select a particular credit account using buttons 130-134 and display 125). When the
20 purchase is performed, the reward may be communicated to the user. As another example, suppose a service provider provides a reward feature based on a type of transaction. For example, a reward may be provided for a sale of a commodity using a particular transaction processor (e.g.,
25 issuer, acquirer and/or payment network). A user may sell a commodity using the particular transaction processor (e.g., the ecosystem provider) and upon completion of the sale a reward may be communicated to the user.

30 [0049] Selection of a feature may or may not have a cost associated with it. If a cost is associated with the feature, for example, the cost may be added to a customer's statement (e.g., added to a credit or debit

- 17 -

purchase) for a particular transaction. A fixed-fee and/or variable-fee (e.g., a percentage of the transaction) may then be removed from the fee charged to the user and distributed among particular parties, for example, distributed among a card issuer, application manager provider, ecosystem provider, device provider, service provider and/or one or more other entities. Persons skilled in the art in possession of example embodiments will appreciate that many different fee arrangements are possible, and that the various providers may be the same entities and/or different entities.

[0050] A cost may be associated to a feature selection, but may not be a cost to a user. For example, the cost may be a cost to a service provider (e.g., a third party service provider) and/or a merchant. The cost may be provided to other entities, for example, the device provider, card issuer, card processor, and/or any other entity (e.g., a card network).

[0051] Display 112 may display a dynamic number, for example, all or a portion of an account number (e.g., a credit and/or debit account number). Display 113 may display, for example, a dynamic verification code (e.g., a dynamic security code). The dynamic codes displayed on displays 112 and 113 may change according to various schemes as a security measure against fraudulent transactions. For example, dynamic numbers may change periodically and/or upon the occurrence of an event such that a previously recorded number may become unusable. Examples may include dynamic codes that change based on time, an algorithm (e.g., an encryption algorithm and/or hash table algorithm) and/or card usage.

[0052] Card 100 and/or a user may communicate a dynamic number to a processing facility, for example, a

- 18 -

dynamic number verification entity. The processing facility may validate the dynamic number. A user may purchase items using a dynamic card and a processing facility may authorize the purchases upon determining
5 that the dynamic number is valid.

[0053] Although example embodiments may be described with respect to numbers, the scope of example embodiments includes any representation of a security code and/or account, by any method. Characters, images, sounds,
10 signals, textures, braille, letters and/or any other distinguishable representations are contemplated by example embodiments.

[0054] Generation of a dynamic number and the functionality needed to verify the dynamic number at a processing/authorization facility may be accomplished in
15 a variety of ways. For example, a private key (or equation, hash table function and/or the like) and a secure card number (e.g., a private number) may be known to both the dynamic card (e.g., stored in memory 142 of
20 a card 100) and the processing/authorization facility. A signal may be received or generated by the dynamic card (e.g., a counter signal, a randomly generated signal, a timing signal, etc.) and the dynamic card may produce a dynamic number based on the signal, the private key
25 and/or the private card number. The processing facility may utilize the private key, private card number, the dynamic number, and/or the signal (or a different signal) to verify that the dynamic number is correct. The private key may be unique to a user or common to multiple users.

30 **[0055]** As one non-limiting example, a processing facility may receive a time stamp with a dynamic number and other information received from a dynamic card (e.g., account identification information and expiration date).

- 19 -

The processing facility may use the time stamp, the received dynamic card information (and any other received information), the private key, and the private number to verify that the dynamic number is correct for that period of time (or a string of consecutive periods of time that include, and are located near, the time stamp). A time stamp may be utilized, for example, to authorize online purchases and/or telephonic purchases that are not immediately processed. A time stamp may be indicative of, for example, a particular time or period of time. According to at least one example embodiment, a timing may be independently determined by a dynamic card and a processing facility (e.g., using a same time source and/or different timing sources) and a time stamp may not be communicated.

[0056] Persons skilled in the art will appreciate that a dynamic card number may be produced without the need for a private number such as a private credit card number or security code, for example, a number stored in both a credit card and a remote facility. For example, a timing signal may be encoded based on a private key (or equation) and the resultant encoded number utilized as a dynamic credit card number.

[0057] A private key may be an equation or formula that uses one or more other variables (e.g., a random number) to generate a coded number (e.g., a dynamic number). Persons skilled in the art will appreciate that one or more private keys (e.g., an equation or formula) may be utilized to code different numbers for a dynamic card. For example, one private key may be utilized to code a dynamic card number while another private key may be utilized to code a dynamic security code. As another

- 20 -

example, different private keys may be used for different magnetic stripe data tracks

[0058] A number of private keys (and/or private numbers) may be stored in a credit card and such private
5 keys (and/or private numbers) may be changed periodically (e.g., every day or week). A similar number of private keys (and/or private numbers) may be stored in a remote facility (e.g., a remote server), the selection of which may be determined by a particular time (e.g., a
10 particular day or a particular week). A processing/authorization facility, or any device/facility, may receive the dynamic card number and decode the dynamic number based on a replica of the private key and/or private number of the card that is
15 stored at, or accessible by, the facility (e.g., stored on a database and/or server).

[0059] Persons skilled in the art in possession of example embodiments will appreciate that synchronization between a payment device and a processing facility may
20 not occur. For example, a merchant may generate a time stamp for a transaction at a different time than a dynamic number is generated by a payment device. As another example, timing signals used by a payment device and a processing facility may be based on different clocks.

[0060] A valid dynamic number range may be used to
25 validate a dynamic number despite any asynchronicity. As an example, card 100 may generate a dynamic number and may increment a counter each time card 100 is used (e.g., swiped). If information does not reach a processing
30 facility a counter used by the processing facility may not also increment. The processing facility may authorize dynamic numbers that are valid within a range to avoid declining transactions that are otherwise valid

- 21 -

(e.g., non-fraudulent). For example, if a dynamic number is recognized for another value of a counter within a range (e.g., backwards or forwards within 10 increments of the counter from the value of the counter at the processing facility), the processing facility may authorize a transaction. The processing facility may adjust the counter based on the received valid dynamic number and/or a history of received valid dynamic numbers. An algorithm and/or transaction history may be maintained to determine if non-synchronized validations exceed an expected error level. If the error level is exceeded, transactions may be declined.

[0061] According to example embodiments, a range of valid dynamic numbers at a processing facility may vary, for example, in symmetry and/or width. A symmetric valid dynamic number range may include an equal number of valid dynamic numbers before and after an expected dynamic number. A non-symmetric range may include fewer valid dynamic numbers before an expected dynamic number than after, or fewer valid dynamic numbers after an expected dynamic number than before. A range width may be the total number of valid dynamic numbers within the range.

[0062] According to example embodiments, a range of valid dynamic numbers at a processing facility may vary (in symmetry and/or width) based on a variety of factors. The factors may be associated with, for example, the characteristics of a transaction, the characteristics of a user (or multiple users), a user transaction history and/or a multiple-user transaction history.

[0063] For example, a range of valid dynamic numbers may vary based on transaction data and/or data derived from transaction data (collectively "transaction data"). Transaction data may include, for example, a merchant

- 22 -

name, a type of merchant, a date/time stamp, a season, a location, a monetary value, a name of a merchant acquirer, a type of a merchant acquirer, a name of an issuer, a type of an issuer, a name of an issuer processor, a type of an issuer processor, a name of a payment network, a type of a payment network, a stage of a transaction (e.g., authorization, adjustment and/or settlement), a name of a product and/or a type of product. Transaction data may include, for example, any data generated and/or received during a transaction.

[0064] As another example, a range of valid dynamic numbers may vary based on the characteristics of a user, for example, a user credit score and/or the like. As yet another example, a range of valid dynamic numbers may vary based on a user transaction history, for example, previously received transaction data (e.g., including previously used dynamic numbers and/or previously used dynamic number ranges). As still another example, a range of valid dynamic numbers may vary based on multiple-user characteristics and/or multiple-user transaction histories. Data from multiple users may be processed to, for example, identify trends, identify indicators of fraud, and/or perform other probability analyses.

[0065] As still yet other examples, a range of valid dynamic numbers may vary based on track data (e.g., which of three magnetic stripe tracks are communicated) and/or whether a transaction is performed online or in person.

[0066] The characteristics of a transaction, the characteristics of a user (or multiple users), a user transaction history and/or a multiple-user transaction history may be used to determine a risk level associated with a transaction. The risk level may be user specific,

- 23 -

transaction specific and/or based on a payment method. A user specific risk level may be based on, for example, a user transaction history. For example, card users whose transaction history indicates that the user's account has been compromised in the past may be assigned a higher risk level than users without such a history, and a valid dynamic number range may be decreased or eliminated. A transaction specific risk level may be based on, for example, transaction data and/or a transaction history. For example, transaction data and a transaction history may include a location and time stamp for each of two transactions by a user. If the distance between locations and the difference between the time stamps indicates that the authorized card user may not have made both purchases (e.g., purchases in the U.S. and Japan, 10 minutes apart), the risk level assigned to the transaction may be increased, and a valid dynamic number range may be decreased or eliminated. A payment method risk level may be, for example, based on the type of payment method used for a transaction or the card network associated with the payment method. For example, different tiers of cards may be associated to different acceptable user annoyance levels and acceptable risk levels. A valid dynamic number range may be modified to align the probability of a declined transaction with each card tier. As another example, a valid dynamic number range may be based on the payment network associated with the payment method (e.g., Visa™, MasterCard™, etc.). A particular payment network may be preferred, trusted and/or associated with fewer fraudulent transactions.

[0067] A valid dynamic number range may either include or exclude previously used dynamic numbers. A valid dynamic number range may include a previously used

- 24 -

dynamic number within the range for purposes of defining the width of the range but exclude the previously used dynamic number for purposes of validating a received number (e.g., in a case where repeat dynamic numbers are not permitted).

[0068] A range of valid dynamic numbers may be applied according to different standards. For example, valid dynamic number ranges may be applied less rigorously to trusted merchants than to unknown or distrusted merchants. A trusted merchant may be, for example, a preferred partner, a merchant rated highly by a rating entity (e.g., the Better Business Bureau®), by a consumer protection agency and/or by consumers. A trusted merchant may be identified based on, for example, transaction data (e.g., a merchant type code, merchant id and/or merchant name). A trusted merchant may be permitted, for example, to use a single dynamic number a greater number of times than a nontrusted merchant and/or a wider dynamic number range width. A nontrusted merchant may be any merchant that is not a trusted merchant (e.g., an unknown or poorly rated merchant).

[0069] According to at least one example embodiment, a range of valid dynamic numbers may be calculated using the risk level determined from one or more of the factors. For example, each possible risk level may be associated to one of a plurality of algorithms used to determine a valid dynamic number range. The algorithms may use one or more of the factors in determining the range.

[0070] If a communicated dynamic number is recognized (e.g., by an authorization facility) as a value within a valid dynamic number range, but the dynamic number is not the expected value, the processing facility may authorize a transaction and set the counter at the processing

- 25 -

facility to match the expected counter value at card 100. For example, a card may, at the push of a button on a dynamic card, generate a new number (e.g., from a list of stored numbers). A remote facility may determine if a
5 future valid dynamic number matches the generated new number and, if a future number is valid, the remote facility may invalidate some (or all) numbers located before the newly validated number. At the next transaction, the dynamic facility may, for example,
10 attempt to validate the received number with the number located after the newly validated number. A table may store, for example, a dynamic number and a pointer to the next entry. A processor may read a dynamic number and utilize the pointer to determine the location of the next
15 expected dynamic number. A valid dynamic number range may be determined based on the expected dynamic number (e.g., centered on the expected dynamic number). Persons of ordinary skill in the art will appreciate that similar strategies may be used for schemes employing an
20 algorithm.

[0071] Where an algorithm is used to determine a dynamic number, a remote processing/authorization facility may, for example, perform the same process as the dynamic card and compare the facility's dynamic
25 number with the received dynamic number for verification. For example, a remote facility may include any equations and signals needed by the dynamic card to generate a dynamic number and may perform an operation similar to the one performed by the dynamic card to generate its own
30 dynamic number. The remote facility may then compare the received dynamic number to the generated dynamic number to determine if the two numbers are the same and/or within an expected degree of similarity. A valid dynamic number

- 26 -

range may be based on, for example, a subset of possible solutions to an equation. For example, the valid dynamic number range may include all solutions to an equation based on a portion of a timing signal (e.g., a temporal window).

5 [0072] A remote processing/authorization facility may decode a dynamic number using an equation and/or a private key (which may be an equation itself or a variable) to obtain a resultant number and compare this number against a private number for approval. If the decoded number matches or is sufficiently similar to the private number (which may, or may not, be the same private number stored in the credit card), then the dynamic number may be validated.

10 [0073] A dynamic card may be utilized using traditional infrastructure and may be utilized for online (or telephonic) purchases and purchases that require the card to be swiped (or entered manually into a credit card reader). A dynamic number may be decoded at any point in a transaction (e.g., point-of-sale, routing, authorization, adjustment and/or settlement). For example, an online store may include the components (e.g., hardware and/or software) necessary to decode the dynamic number such that a decoded number (e.g., a credit/debit card number) may be transmitted to a card processing facility.

20 [0074] A processing facility, or any device decoding a number, may utilize an identification number to identify the account/card that produced the dynamic number. The identification number may then be utilized to look up, for example, the private key and/or private number of the account/card such that a dynamic number can be generated from the retrieved information (and compared

25

30

- 27 -

to the received dynamic number) and/or the retrieved information can be utilized to decode the dynamic number such that the card may be validated and/or a transaction authorized. Multiple users may utilize the same dynamic number at any one time and the identity of the account/card can still be determined (e.g., by using the identification information).

[0075] Identification information may be utilized to identify a credit card. Multiple users may be utilizing the same dynamic number (e.g., a dynamic credit card number or a dynamic verification code) at any time. The identification information may be utilized to identify a credit card such that a dynamic number can be, for example, retrieved/generated for a particular period of time (and/or a particular transaction) for the identified credit card and compared to the received dynamic number.

[0076] The dynamic card number may be transformed into a particular credit card format so that a dynamic number may be verified as having the appropriate format before, for example, the number is transmitted to a credit card processing/authorization facility. For example, a coding equation may be utilized that always produces numbers that fit a particular format.

[0077] A dynamic card system may allow multiple users to have the same dynamic number at any particular time. Additional information may be transmitted to identify the user. For example, an account number and/or name may be utilized. According to at least one example embodiment, a traditional credit card number may be written on a traditional magnetic stripe. Such a credit card number may be used for identifying the user. A dynamic security code (e.g., a four digit security code such as a verification code) may then be provided that changes

- 28 -

periodically. Such dynamic information (e.g., the dynamic security code) may be written to a portion of the magnetic stripe that does not have the traditional credit card number and/or the dynamic information (e.g., the dynamic security code) may be displayed to a user.

5 **[0078]** A signal may be utilized to produce a key that is used in an equation to manipulate a credit card number. The signal may be a timing signal, a counter signal, a random number generator signal (e.g., that operates similar to a random number generator in a processing facility) and/or the like. Such a counter number (or random number) may be provided to a processing facility so that the processing facility may decode (or perform the same function as the dynamic card and compare the results). A credit card number may be invalidated at the facility if, for example, any particular number is used more than a particular number of times (e.g., more than 10 times). Such a counter may be increased after every purchase (e.g., after a user presses a button to change the number). As per another example, if a counter is used and the counter is increased when a number is used (or the credit card believes that a number has been used), the number of transactions operable of being made may be limited by the storage capacity of the counter.

25 **[0079]** Architecture 150 may be utilized with any card (e.g., any card 100). Architecture 150 may include, for example, processor 120, display 140, driving circuitry 141, memory 142, battery 143, radio frequency identification (RFID) 151, integrated circuit (IC) chip 152, electromagnetic field generators 170, 180, and 185, and read-head detectors 171 and 172.

30 **[0080]** Processor 120 may be any type of processing device, for example, a central processing unit (CPU)

- 29 -

and/or a digital signal processor (DSP). Processor 120 may be, for example, an application specific integrated circuit (ASIC). Processor 120 may include on-board memory for storing information (e.g., drive code). Any
5 number of components may communicate to processor 120 and/or receive communications from processor 120. For example, one or more displays (e.g., display 140) may be coupled to processor 120. Persons skilled in the art will appreciate that components may be placed between
10 particular components and processor 120. For example, a display driver circuit may be coupled between display 140 and processor 120.

[0081] Memory 142 may be coupled to processor 120. Memory 142 may store data, for example, data that is
15 unique to a particular card. Memory 142 may store any type of data. For example, memory 142 may store a list of numbers, a function, base variables, a function determination value, a key, and/or the like, used to generate a dynamic number. As another example, memory
20 142 may store discretionary data codes associated with buttons of card 100. Discretionary data codes may be recognized by remote servers to effect particular actions. For example, a discretionary data code may be stored in memory 142 and may be used to cause a third
25 party service feature to be performed by a remote server (e.g., a remote server coupled to a third party service such as an online voucher and/or coupon provider).

[0082] Architecture 150 may include any number of reader communication devices. For example, architecture
30 150 may include at least one of IC chip 152, RFID 151 and a magnetic stripe communications device. IC chip 152 may be used to communicate information to an IC chip reader (not illustrated). IC chip 152 may be, for example, an

- 30 -

EMV chip. RFID 151 may be used to communicate information to an RFID reader. RFID 151 may be, for example, a RFID tag. A magnetic stripe communications device may be included to communicate information to a magnetic stripe reader. For example, a magnetic stripe communications device may provide electromagnetic signals to a magnetic stripe reader.

[0083] Different electromagnetic signals may be communicated to a magnetic stripe reader to provide different tracks of data. For example, architecture 150 may include electromagnetic field generators 170, 180 and 185 to communicate separate tracks of information to a magnetic stripe reader. Electromagnetic field generators 170, 180, and 185 may include a coil (e.g., each may include a coil) wrapped around one or more materials (e.g., a soft-magnetic material and/or a non-magnetic material). Each electromagnetic field generator may communicate information, for example, serially and/or in parallel to a receiver of a magnetic stripe reader for a particular magnetic stripe track.

[0084] Architecture 150 may include read head detectors 171 and 172. Read-head detectors 171 and 172 may be configured to sense the presence of a magnetic stripe reader (e.g., a read-head housing of a magnetic stripe reader). Information sensed by the read-head detectors 171 and 172 may be communicated to processor 120 to cause processor 120 to communicate information serially from electromagnetic generators 170, 180, and 185 to magnetic stripe track receivers in a read-head housing of a magnetic stripe reader.

[0085] According to at least one example embodiment, a magnetic stripe communications device may change the information communicated to a magnetic stripe reader at

- 31 -

any time. Processor 120 may, for example, communicate user-specific and card-specific information through RFID 151, IC chip 152, and/or electromagnetic generators 170, 180, and 185 to card readers coupled to remote
5 information processing servers (e.g., purchase authorization servers). Driving circuitry 141 may be utilized by processor 120, for example, to control electromagnetic generators 170, 180 and 185.

[0086] FIG. 2 shows devices according to example
10 embodiments. Referring to FIG. 2, device 200 may be, for example, a mobile telephonic device and/or other device (e.g., portable computer such as a portable tablet computer). Device 200 may include, for example, housing 202, display 210, device card 220, virtual buttons 230
15 and 231, keyboard 240, selections 250-280, and/or dynamic code 290.

[0087] Display 210 may include, for example, light-sensitive and/or touch-sensitive elements. Device 200 may communicate information to a card reader, for
20 example, via a contactless signal (e.g., an RFID signal) and/or a contact-based signal (e.g., a USB connection). Any of multiple different communication technologies may be used to communicate information to, for example, a card reader.

[0088] Device 200 may include a device card 220 and/or virtual buttons 230 and 231. Device card 220 may be a virtual representation of a card and/or any information identifying a payment method (e.g., credit account
25 number). Persons skilled in the art will appreciate that
30 any physical card described herein may be provided as a device card on, for example, a computing system (e.g., a mobile telephonic device and/or a computer). Physical buttons of a physical card may, for example, correspond

- 32 -

to virtual buttons of a device card. Likewise, any device card may be provided as a physical card. Virtual buttons of a device card may, for example, correspond to physical buttons of a physical card.

5 **[0089]** Virtual button 230 may, for example, correspond to one feature (e.g., an automatic association of a coupon to a purchase) from one service provider. Virtual button 231 may, for example, correspond to another feature (e.g., a product of the month feature) from the same or a different service provider.

10 **[0090]** All features associated to a card may be utilized, for example, with a particular payment account (e.g., a credit account) such that a payment transaction with that payment account is performed if any feature is selected. As another example, one or more features may be associated with a payment account (e.g., a credit account) while an additional one or more features may be associated with a different payment account (e.g., a debit account). Accordingly, a selected feature associated with a credit account may be utilized to make a purchase with credit and may perform an additional action associated with that feature. A different selected feature associated with a debit account may be utilized to make a purchase with debit and may perform an additional action associated with that different feature.

20 **[0091]** Selection 250 may be, for example, a link to an application for a new card provided by, for example, an ecosystem provider, application manager provider, card manufacturer and/or the like. Upon activation of selection 250 a user may be directed to an application form. Selection 260 may be, for example, a link to an application for an upgrade to a new card provided by, for

- 33 -

example, an ecosystem provider, application manager provider, card manufacturer and/or the like. Upon activation of selection 260 a user may be directed to an application form. According to at least one example
5 embodiment, selections 250 and 260 may only appear upon availability to a user and may not require an application process (e.g., may be based on preapproval).

[0092] Selection 270 may be, for example, activate an alert feature indicating that a card user requires
10 immediate assistance. Upon activation of selection 270 information may be automatically communicated to one or more responsible parties, for example, local authorities (e.g., a 911 call center coordinating emergency services). Selection 280 may be, for example, a link
15 used to display a GUI. Upon activation of selection 280 an application manager used to associate features to virtual buttons, and virtual buttons to payment methods, may be displayed.

[0093] Dynamic code 290 may be, for example, a credit
20 card number, CVV, CVV2, CVC2, a CID, an extended length code and/or the like). Dynamic code 290 may change based on an event, for example, based on a change in time, a button press, a counter and/or the like. Dynamic code 290 may change based on a transaction using, for example,
25 a table and/or algorithm. For example, dynamic code 290 may change every transaction, every number of transactions, for a type of transaction (e.g., greater than \$100 and/or using a debit card) and/or the like.

[0094] FIG. 3 shows network topologies according to
30 example embodiments. Referring to FIG. 3, network topology 300 may be a logical topology of a transactional network including multiple network elements. The network elements may include, for example, mobile device 305,

- 34 -

card reader 310, card 315, network access infrastructure 325, wireless access point 335, mobile network 330, IP network 340, payment network 355, device 370, contactless device 380, issuer 360, application providers 365, ecosystem provider 345, application manager provider 350 and/or verification server 390.

[0095] Mobile device 305 may be, for example, a mobile telephonic device, a personal digital assistant (PDA), an electronic tablet, a laptop, a global positioning system (GPS), an MP3 player, a smartphone and/or the like. Mobile device 305 may be used by any transactional entity, for example, a user, a merchant, a biller, an enterprise, a government, a non-profit organization and/or the like. Card reader 310 may be, for example, a data input device configured to read data from a storage medium (e.g., card 315). For example, card reader 310 may receive data from a magnetic stripe, EMV chip, contactless (e.g., RFID) technology and/or the like. Card reader 310 may connect to mobile device 305 via, for example, interface 320. Interface 320 may be an input to, for example, any one of multiple ports of a mobile device 305, for example, an input to a universal serial bus (USB) port, MicroUSB port, 32-pin connector, a headphone jack, an Ethernet port and/or the like.

[0096] Ecosystem provider 345 may be an entity providing one or more ecosystems of applications and transactional methods, and may be, for example, a transaction processor (e.g., an issuer, a merchant acquirer, an acquirer processor, a payment network and/or the like). Application providers 365 may be, for example, entities providing and/or maintaining applications compatible with one or more ecosystems. Issuers 360 may be issuer processors and/or issuers of

- 35 -

transactional methods compatible with one or more ecosystems (e.g., issuing financial institutions). Application manager provider 350 may be, for example, an entity providing an interface (e.g., a graphical user interface (GUI)), used to associate applications to payment methods and/or transaction types, within an ecosystem provided by ecosystem provider 345. Payment network 355 may be, for example, an entity routing transactional information between, for example, ecosystem provider 345 and issuers 360. Verification server 390 may be, for example, a remote processing facility verifying dynamic codes (e.g., dynamic card numbers and/or security codes) communicated during a transaction. According to example embodiments, verification of dynamic codes is not limited to a verification server and be performed at any network element.

[0097] Ecosystem provider 345, application providers 365, application manager provider 350, issuers 360, payment network 355, and/or verification server 390 may be connected by, for example, IP network 340, mobile network 330, private networks, trusted networks, encryption networks, sub-networks and/or the like. Connections between network elements may be wired and/or wireless.

[0098] Mobile device 305 may include one or more transceivers, receivers and/or transmitters that may communicate with one or more wired networks (e.g., IP network 340 and/or payment network 355) and/or one or more wireless networks (e.g., mobile network 330). Mobile device 305 may, for example, communicate with a cellular station over a wireless radio interface (e.g., a global system for mobile communications (GSM) air

- 36 -

interface and/or the like) that may be used by mobile device 305 to communicate information (e.g., voice and data) to cellular network access infrastructure 325 (e.g., one or more GSM base transceiver stations, base station controllers and mobile switching centers). Persons skilled in the art will appreciate that cellular network access infrastructure 325 may utilize any access architecture, for example, a code-division multiple access architecture and/or a time-division multiple access architecture.

[0099] Mobile device 305 may, for example, communicate with wireless access point 335 over a wireless interface (e.g., a Bluetooth interface, Wi-Fi interface and/or the like). Mobile device 305 may, for example, access one or more wired networks (e.g., IP network 312 and/or payment network 314) and/or one or more wireless networks (e.g., mobile network 310) without the need to first gain access to cellular network access infrastructure 325.

[0100] Mobile device 305 may initiate a financial transaction with one or more network entities and/or devices. Transactional information (e.g., a dynamic payment account number, a dynamic security code and/or a card expiration date of a purchaser) may be used to process the financial transaction. The transactional information may be communicated to mobile device 305 from, for example, card 315 via card reader 310.

[0101] For example, a financial transaction may include a purchase of items for sale by a user. A purchaser's request to purchase the items may be initiated by a browser of mobile device 305 via an access point, for example, wireless access point 335 and/or cellular network access infrastructure 325. Mobile device 305 may obtain payment information via card reader

- 37 -

310 (e.g., when card 315 is swiped through card reader 310), and may communicate the payment information to one or more network elements for transactional processing. For example, payment information may be communicated to
5 issuer 360 (e.g., a bank)

[0102] Transactional processing may include multiple transactional events and associated transactional communication flows. Examples of transactional events may include authorizations, verifications, settlements,
10 statement debits (e.g., piggyback events), statement credits, returns, partial returns, voids, adjustments and/or chargebacks. Examples of transactional communication flows may include authorization, batching, clearing and funding.

[0103] Authorization of a purchase may include mobile
15 device 305 communicating transactional information to issuer 360. Based on the transactional information, issuer 360 may communicate some or all of the transaction data to ecosystem provider 345. Ecosystem provider 345
20 may communicate a portion of the transactional information, all of the transactional information and/or information related to the user to one or more of application providers 365 for provision of one or more features. In response to receiving transactional
25 information and/or user information from ecosystem provider 345, the one or more application providers 365 may, for example, communicate a request for a statement credit and/or statement debit (e.g., a piggyback charge) to ecosystem provider 345. For example, a feature
30 provided by an application provider 365 may include providing a rebate (e.g., statement credit) to a purchaser buying an item and/or a monetary value to the user (e.g., statement credit) for using card 315. Issuer

- 38 -

345 (and/or a merchant acquirer) may authorize the purchase, the statement credit and/or the statement debit, and/or request authorization from one or more of issuers 360. Authorization may include verifying that a
5 dynamic code (e.g., an account number, CVV, CVV2, CVC2 and/or a CID) included in transactional information is valid using verification server 390. The authorizing entity may, for example, communicate authorization of the purchase to mobile device 305 and/or decline to authorize
10 the purchase.

[0104] According to some example embodiments, a dynamic code may be unique to a user. According to other example embodiments, a dynamic code may not be unique to the user and authorization verification server 390 may
15 use other transaction information to perform a verification.

[0105] Upon authorization of a purchase, payment transaction information may be recorded onto a receipt that may be delivered to mobile device 305 via any one
20 or more delivery options (e.g., via a short messaging service of mobile network 330 and/or an email delivery service of IP network 340). A payment receipt may, for example, be provided to mobile device 305 as a proof-of-purchase object (e.g., a barcode) that may be provided
25 to a display of mobile device 305 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation.

[0106] Authorized transactions may be batched (e.g., aggregated) by mobile device 305, a merchant acquirer
30 and/or by another network element. The batched transactions may be cleared by communicating (e.g., daily) the batched transactions to one or more of issuers 360 (routed by, for example, payment network 314),

- 39 -

debiting the purchaser's account and communicating a monetary value from one or more of issuers 360 to, for example, a merchant acquirer. For example, where ecosystem provider 345 acts as a merchant acquirer, funding may include ecosystem provider 345 notifying mobile device 305 that funding has occurred and/or communicating the monetary value to mobile device 305 (and/or a financial institution associated with mobile device 305 in a case where ecosystem 345 is not the merchant's bank). Various fees may be deducted from the monetary value and paid to various entities during transactional processing.

[0107] Application providers 365 may provide features to a user at any one of the various stages of transactional processing. In some cases, a transaction may be reversed (e.g., a void or credit) after a user and/or purchaser receives a reward based on the transaction. For example, a user may sell an item to a purchaser, receive a statement credit and then the purchaser may return the purchased item. According to example embodiments, one or more of application providers 365 (and/or an entity providing a feature to an application provider 365) may be notified by ecosystem provider 345 that a transaction has been reversed. The one or more application providers 365 (and/or the entity providing a feature to an application provider 365) may take action based on the notification. For example, the one or more application providers 365 may reclaim a reward, add a charge to a user's and/or purchaser's statement, remove user authorization to use an application and/or the like.

[0108] Persons skilled in the art in possession of example embodiments will appreciate that many

- 40 -

transactional models with different communication flows may be applied to example embodiments (e.g., closed or open loop) and transactions may be routed in various ways. For example, verification of a dynamic code may
5 be performed at any stage of processing by various entities (e.g., payment network 355, issuers 360 and/or the like). As another example, although transactional processing of transaction data may be performed by ecosystem provider 345 as a merchant acquirer, according
10 to other example embodiments, ecosystem provider 345 may perform none, some or all of the functions of other network elements.

[0109] Persons skilled in the art in possession of example embodiments will appreciate that features may be
15 provided by ecosystem provider 345 and or application providers 365 in various ways. For example, although some example embodiments may include application providers 365 requesting the addition of a debit or credit to a transaction prior to authorization, according
20 to other example embodiments, statement debit and/or credit requests from application providers 365 may be separate from transactional communication flows (e.g., separate from authorization, batching, clearing and/or funding) or at different points within a transactional
25 communication flow.

[0110] Device 370 may be, for example, a server, a laptop computer, a PDA, a desktop computer, a mobile device, a stand-alone piece of electronic equipment (e.g., a card reader), and/or the like. Contactless
30 device 380 may be, for example, a powered card and/or a non-powered card (e.g., a powered payment card and/or a non-powered payment card). Device card 375 may be a virtual representation of contactless device 380 or may

- 41 -

be an independent device card. Device 370 may include a contactless interface that may initiate, sustain, and/or terminate communication channel 385 between contactless device 380 and device 370. Contactless device 380 and
5 device 370 may communicate via channel 385 using any number of contactless mediums, which may include for example, visible, audible, capacitive, electromagnetic (e.g., RF), magnetic, and/or RF mediums.

[0111] Contactless device 380 may communicate
10 transactional information to device 370 to initiate a financial transaction (e.g., a purchase) using, for example, an IC chip, RFID tag and/or a magnetic stripe communications device. Transactional information may be communicated from contactless device 380 to device 370
15 in support of, for example, processing of the financial transaction. For example, device 370 may communicate transactional information and a purchase amount to ecosystem provider 345 (or an independent merchant acquirer). Ecosystem provider 345 may authorize the
20 transaction and/or may obtain authorization from one or more of issuers 360. Authorization may include verifying that a dynamic code (e.g., an account number, CVV, CVV2, CVC2 and/or a CID) included in transactional information is valid using verification server 390. Ecosystem
25 provider 345 may communicate the authorization to device 370. The user may be provided a receipt upon authorization of the financial transaction.

[0112] Device 370 may batch the authorized transaction with other transactions and communicate the batched
30 transactions to ecosystem provider 345, and/or ecosystem provider 345 may batch the transactions. Ecosystem provider 345 may request payment from one or more of issuers 360. The one or more issuers 360 may communicate

- 42 -

a monetary value to ecosystem provider 345 and debit the user's account. Ecosystem provider 345 may communicate the monetary value to device 370 and/or notify device 370 that funding has occurred. Various fees may be deducted
5 from the monetary value and paid to various entities during transactional processing.

[0113] Ecosystem provider 345 may associate transactional information to an application and/or an application provider 365 (e.g., one or more of
10 application providers 365). Ecosystem provider 345 may communicate some or all of the transactional information to the application and/or application provider 365 associated to the transactional information. The application and/or an application provider 365 may
15 communicate a request to ecosystem provider 345 (e.g., a request for a statement debit and/or credit). Ecosystem provider 345 may authorize the request, and/or communicate the request to one or more of issuers 360. A monetary value may be communicated to the application
20 provider 365, for example, in exchange for provision of a feature. The feature may include, for example, providing a reward to a user of contactless device 380 and/or device 370 as either a purchaser and/or merchant.

[0114] FIG. 4 shows transaction verification methods
25 according to example embodiments. Referring to FIG. 4, a verification entity may receive a number (e.g., a security code) as part of transaction processing (e.g., as in 405). The verification entity may, for example, compare the received number to all possible dynamic
30 numbers that may occur in a verification scheme (e.g., as in 410). For example, the verification entity may determine whether the received number is a solution to an algorithm used to generate dynamic numbers. As

- 43 -

another example, the verification entity may maintain a table storing, for example, a sequential list of possible dynamic numbers. The verification entity (e.g., a server) may determine whether the received number corresponds to
5 a table entry. If the number is not a possible dynamic number, the verification entity may determine that the received number is invalid (e.g., as in 425).

[0115] If the number is a possible dynamic number within the verification scheme, the verification entity
10 may determine whether the received number is an expected number (e.g., as in 415). As one example, an expected number may be based on a solution to an algorithm using a signal (e.g., a timing signal). As another example, a verification scheme may include sequentially selecting
15 numbers listed in a table based on, for example, card use (e.g., successful card communications and/or transaction events). A currently selected number in the table may be identified as the expected number.

[0116] A received number may be valid even though the
20 received number does not match the expected number due to, for example, asynchronicity between the sender and receiver. For example, a timing signal used by a payment device (e.g., a powered card and/or mobile computing device) to generate a number during a transaction may be
25 asynchronous to a timing signal used by a verification entity (e.g., even if intended to be synchronous). As another example, a payment device may change a dynamic number each time a button is pressed on the payment device and a verification entity may not receive notice of each
30 button press. For example, a user may press a button on a payment device multiple times before communicating with a card reader. The verification entity may expect a number corresponding to the first button press, but may

- 44 -

receive a number corresponding to the last button press. As yet another example, a card button may be depressed unintentionally, for example, in a user's wallet. As still another example, a generated or communicated number
5 may erroneously fail and another number may be communicated.

[0117] If the received number is an expected number, the verification entity may determine that the received number is a valid dynamic number (e.g., as in 430). If
10 the received number is not an expected number, the verification entity may determine a valid dynamic number range and determine whether the received number is a number included in the valid dynamic number range (e.g., as in 420 and 423). A valid dynamic number range may be
15 a subset of all possible dynamic numbers within the verification scheme. For example, the valid dynamic number range may include all solutions to an algorithm within a period of time (e.g., a week). As another example, the valid dynamic number range may include a
20 subset of numbers (e.g., 100 numbers) within a table, and may include numbers immediately before and after an expected number.

[0118] If the received number is included in the valid dynamic number range, the verification entity may
25 determine that the received number is a valid dynamic number (e.g., as in 430). If the received number is not included in the valid dynamic number range, the verification entity may determine that the received number is invalid (e.g., as in 425).

30 [0119] A determination of whether or not a received number is a valid dynamic number may be used in a determination of whether or not to authorize a transaction. The validity determination may be used as

- 45 -

one factor in an authorization determination or may be the sole factor in an authorization determination.

[0120] If the received number is a valid dynamic number, a valid dynamic number range may be updated (e.g., as in 435). For example, a table including possible dynamic numbers may include a pointer indicating an expected number. If the received number is the expected number, the pointer may be moved to the next dynamic number in a sequential listing of dynamic numbers. If the received number is not the expected number but is included in a valid dynamic number range, the pointer may be moved to the next dynamic number after the received number and/or an algorithm may be used to determine the expected number. The algorithm may be based on a variety of factors. For example, the algorithm may determine the expected number based on transaction data and a transaction history (e.g., sequential positions in the table of previously received valid dynamic numbers).

[0121] Example embodiments may be described with respect to numbers for ease of explanation. However, the scope of example embodiments includes any distinguishing representation of a security code and/or account, by any sensory method. Characters, images, sounds, textures, signals, braille, letters and/or any other distinguishable representations are contemplated by example embodiments.

[0122] Persons of ordinary skill in the art in possession of example embodiments will appreciate that the transaction verification method of FIG. 4 is not limited by the illustrated sequence, which is provided for purposes of explanation. Steps 405-435 are not temporally constrained with respect to each other and

individual steps need not take place at all. For example, a transaction verification method may include only steps 405, 423, 425 and 430. As another example, step 420 may be performed prior to the method of FIG. 4 (e.g., a range
5 may be static or periodically determined, for example, based on multiple, different payment device users).

[0123] FIG. 5 shows transaction verification methods according to example embodiments. Referring to FIG. 5, a verification entity may receive a number (e.g., a
10 security code) and other transaction data as part of transaction processing (e.g., as in 505). The verification entity may, for example, determine a risk level associated with the transaction (e.g., as in 507).

[0124] A risk level associated with a transaction may
15 be, for example, user specific, transaction specific and/or payment method specific. A user specific risk level may be based on, for example, a user transaction history. For example, card users whose transaction history indicates that their account has been used for
20 fraudulent transactions in the past may be assigned a higher risk level than users without such a history. A payment method risk level may be, for example, based on an underwriting class of the payment method (e.g., based on credit score) and/or the card network associated with
25 the payment method. A transaction specific risk level may be based on, for example, transaction data and/or a transaction history. For example, transaction data used in conjunction with a transaction history may indicate that a current purchase is one of multiple purchases
30 (e.g., 10) from the same merchant in a relatively short period of time (e.g., 5 minutes), and may indicate a fraudulent transaction.

[0125] Other transaction specific indicators of risk may include, for example, an authorization request for: a larger than user-average monetary value; a purchase of multiple items of the same type; a purchase of an item
5 at a location separated by a distance from a previous purchase, where the distance between purchase locations is not traversable in a time indicated by a difference in time stamps; a purchase included in a larger than user-average volume of purchases; a purchase including
10 overnight shipping charges; and/or an international purchase.

[0126] The verification entity may determine whether or not a transaction associated with the transaction data is an online transaction (e.g., as in 510). An online
15 transaction may be, for example, a transaction by a user that is performed remotely from a merchant via a communication network and/or may be a transaction in which a payment method is not used to communicate data (e.g., no card swipe).

20 [0127] If the transaction is not an online transaction, the verification entity may determine if a merchant associated with the transaction is a trusted merchant (e.g., as in 530). If the merchant is not a trusted merchant, the verification entity may determine
25 a valid dynamic number range using an algorithm (e.g., as in 535). The algorithm may use multiple, different factors to determine the valid dynamic number range. For example, the algorithm may consider transaction data, transaction history and risk level.

30 [0128] Transaction data may include magnetic stripe track data and/or other data included in a transaction authorization communication flow, and/or information derived from such data. For example, transaction data

- 48 -

may include a merchant name, a type of merchant, a date/time stamp, a season, a location, a monetary value, a name of a merchant acquirer, a type of a merchant acquirer, a name of an issuer, a type of an issuer, a name of an issuer processor, a type of an issuer processor, a name of a payment network, a type of a payment network, a product and/or a type of product. Transaction data may include, for example, any data generated and/or received during a transaction. An example of the use of transaction data in determining a valid dynamic number range may include, for example, varying the range based on a type of merchant. For example, if the type of merchant is a hotel, where credit card data may be recorded at check-in, and the payment transaction completed at check-out, the algorithm may increase the valid dynamic number range relative to, for example, where the type of merchant is a retail store and transactions are quickly processed.

[0129] Transaction history may include, for example, prior valid dynamic number ranges applied to a particular user. Prior valid dynamic ranges may be used, for example, as part of a regressive algorithm. The regressive algorithm may consider past and current data to tailor a valid dynamic range to a user over time.

[0130] If the offline merchant is a trusted merchant, the verification entity may determine a valid dynamic number range using an algorithm and associated offline modifications for a trusted merchant (e.g., as in 540). The algorithm used for trusted merchants may be the same as the algorithm used for untrusted merchants. The associated offline modifications may be used to modify the valid dynamic number range and/or change the application of the valid dynamic range based on

- 49 -

characteristics of trusted, offline transactions. For example, the valid dynamic number range may be modified where a trusted, offline merchant is trusted due to rigorous in-store verifications, for example, signature and/or identification verifications. The valid dynamic number range may be increased. As another example, the application of the valid dynamic range may be changed for offline trusted merchants by, for example, permitting a greater number of repeat uses of a dynamic number (e.g., 5) than permitted for a nontrusted, offline merchant (e.g., 0).

[0131] If the transaction is an online transaction, the verification entity may determine if an online merchant associated with the transaction is a trusted online merchant (e.g., as in 515). If the merchant is not a trusted, online merchant, the verification entity may determine a valid dynamic number range using an algorithm and associated modifications for online merchants (e.g., as in 525). The algorithm used for untrusted, online merchants may be the same as the algorithm used for offline merchants. The associated online modifications may be used to modify the valid dynamic number range and/or change the application of the valid dynamic range based on characteristics of online transactions. For example, online modifications may include disregarding missing magnetic stripe track data and/or negating risk factors. A risk factor may be negated based on the characteristics of online transactions. For example, a purchase location may not be relevant as an indicator of fraud where transaction data may indicate the principal place of business of an online merchant as the transaction location.

- 50 -

[0132] If the merchant is a trusted, online merchant, the verification entity may determine a valid dynamic number range using an algorithm, associated online modifications and associated trusted, online modifications (e.g., as in 525). The algorithm used for trusted, online merchants may be the same as the algorithm used for offline merchants. The associated online modifications may be the same as for untrusted, online merchants. The associated trusted, online modifications may be used to modify the valid dynamic number range and/or change the application of the valid dynamic range based on characteristics of trusted, online transactions. For example, the valid dynamic range may be modified where a trusted, online merchant is trusted due to user ratings. The valid dynamic number range may be increased. As another example, the application of the valid dynamic range may be changed for online, trusted merchants by, for example, permitting a greater number of repeat uses of a dynamic number than permitted for a other merchants merchant. For example, a trusted, online merchant may be a music provider and/or virtual mall where that maintains user payment account details for an extended period of time (e.g., months or years).

[0133] Persons of ordinary skill in the art in possession of example embodiments will appreciate that the transaction verification method of FIG. 5 is not limited by the illustrated sequence, which is provided for purposes of explanation. Steps 505-540 are not temporally constrained with respect to each other and individual steps need not take place at all. For example, a transaction verification method may not include step 507. Further, other variations are contemplated. For example, in addition or alternatively to the use of an

- 51 -

algorithm and modifications, a different algorithm may be determined for each type of merchant (e.g., offline, online, trusted) and/or a subset of merchants. As another example, in addition or alternatively to the use
5 of an algorithm, a table of numbers may be used to determine a valid dynamic number range. According to at least one example embodiment, a single algorithm without modifications may be used for one or more transactions. According to some example embodiments, combinations of
10 these examples may be used.

[0134] FIG. 6 shows methods of determining valid dynamic number ranges according to example embodiments. Referring to FIG. 6, a verification entity may receive a number (e.g., an account number) and other transaction
15 data as part of transaction processing (e.g., as in 605). The verification entity may, for example, determine an expected number for the transaction associated to the transaction data (e.g., as in 607). For example, the verification entity may maintain a list of all possible
20 number in sequential order and maintain a pointer to the expected number.

[0135] The verification entity may determine a backward valid dynamic range based on the expected number (e.g., as in 610). A backward valid dynamic number range
25 may include numbers that have or should have been received prior to the expected number. The backward valid dynamic number range may be static and may include, for example, numbers immediately prior to the expected number (e.g., 25). Previously received numbers may be
30 counted for purposes of determining the width of the backward valid dynamic number range even if the previously received numbers may not be valid for the current transaction. According to some example

embodiments, previously received numbers may not be considered in determining the backward valid dynamic number range.

5 **[0136]** The backward dynamic valid range may not be static. For example, the backward dynamic valid range may be determined using a regressive algorithm. The regressive algorithm may consider past and current data to tailor a valid dynamic range to a user over time (e.g., equilibrium). For example, past valid dynamic ranges for
10 a user and current data may be used in the determination. Past valid dynamic ranges may be weighted differently from current data. For example, past valid dynamic ranges may be assigned an 80% weight and current data may be assigned a 20% weight, and/or vice versa.

15 **[0137]** The verification entity may determine a forward valid dynamic range based on the expected number (e.g., as in 610). A forward valid dynamic number range may include numbers that will or should be received subsequent to the expected number. The forward valid
20 dynamic number range may be static and may include, for example, numbers immediately following the expected number (e.g., 100).

25 **[0138]** The forward dynamic valid range may not be static. For example, the forward dynamic valid range may be determined using a regressive algorithm. The regressive algorithm may consider past and current data to tailor a valid dynamic range to a user over time (e.g., equilibrium). For example, past valid dynamic ranges for
30 a user and current data may be used in the determination. Past valid dynamic ranges may be weighted differently from current data.

[0139] According to example embodiments, a valid dynamic number range may include the expected number, the

backward dynamic range and the forward dynamic range, and may be asymmetric. For example, the backward valid dynamic number range may include a different number of valid dynamic numbers than the forward valid dynamic range. As another example, the backward valid dynamic range may exclude previously received numbers and may be asymmetric in sequence. According to other example embodiments, the valid dynamic number range may be symmetric and include the same number of valid dynamic numbers before and after the expected number.

[0140] FIG. 7 shows dynamic number ranges according to example embodiments. Referring to FIG. 7, dynamic number range 705 may illustrate a symmetric dynamic number range. For example, in dynamic number range 705, three numbers immediately precede and immediately follow an expected number. Dynamic number range 710 may illustrate an asymmetric dynamic number range. For example, in dynamic number range 710, two numbers immediately precede and five numbers immediately follow an expected number. Although example embodiments may describe more numbers in a forward valid dynamic range than in a backward valid dynamic range, persons of ordinary skill in the art will appreciate that fewer numbers may be in a forward valid dynamic range than in a backward valid dynamic range. Dynamic number range 720 may illustrate a sequentially asymmetric dynamic range. For example, in dynamic number range 720, three dynamic numbers precede and three dynamic numbers immediately follow an expected number. However, one of the numbers ("762") preceding the expected number is invalid. For example, number 762 may be a previously received valid dynamic number that may not be valid for more than a single transaction.

- 54 -

[0141] Persons of ordinary skill in the art will appreciate that variations of the dynamic number ranges shown in FIG. 7 are contemplated. For example, a dynamic number range may be asymmetric as well as sequentially
5 symmetric. Further, example embodiments apply to dynamic numbers generally, whether security codes, account numbers and/or the like.

[0142] Persons skilled in the art will appreciate that various elements of different example embodiments may be
10 combined in various ways. Disclosure with respect to one figure may be used in example embodiments described with respect to a different figure. Persons skilled in the art will also appreciate that the present invention is not limited to only the embodiments described. Instead,
15 the present invention more generally involves dynamic information. Persons skilled in the art will also appreciate that the apparatus of the present invention may be implemented in other ways than those described herein. All such modifications are within the scope of
20 the present invention, which is limited only by the claims that follow.

Embodiments

[0143] Embodiment 1 is a method, comprising:
25 receiving a code;
determining that the code is valid; and
authorizing a transaction based on the code.

[0144] Embodiment 2 is a method according to
30 embodiment 1, further comprising:
determining a valid dynamic code range.

- 55 -

[0145] Embodiment 3 is a method according to embodiment 1, further comprising:

5 determining a valid dynamic code range,
wherein the valid dynamic code range is
asymmetric.

[0146] Embodiment 4 is a method according to embodiment 1, further comprising:

determining a valid dynamic code range using an
algorithm.

10 [0147] Embodiment 5 is a method according to embodiment 1, further comprising:

receiving transaction data; and
determining a valid dynamic code range using an
algorithm,
15 wherein the algorithm is based on the transaction
data.

[0148] Embodiment 6 is a method according to embodiment 1, further comprising:

receiving transaction data; and
20 determining a valid dynamic code range using an
algorithm,
wherein the algorithm is based on the transaction
data and a user transaction history.

[0149] Embodiment 7 is a method according to embodiment 1, further comprising:

receiving transaction data; and
25 determining a valid dynamic code range using a
weighted algorithm,
wherein the algorithm is based on prior valid
30 dynamic code ranges and transaction data.

- 56 -

[0150] Embodiment 8 is a method according to
embodiment 1, further comprising:

receiving transaction data,
wherein the determining the code is valid includes
5 comparing the code to a listing of codes.

[0151] Embodiment 9 is a method according to
embodiment 1, further comprising:

receiving transaction data;
determining a risk level; and
10 determining a valid dynamic code range.

[0152] Embodiment 10 is a method according to
embodiment 1, further comprising:

receiving transaction data;
determining a risk level;
15 determining that a transaction associated with the
transaction data is an online transaction; and
determining a valid dynamic code range.

- 57 -

What is claimed is:

1. A method, comprising:
receiving a code;
determining that the code is valid; and
authorizing a transaction based on the code.
2. The method of claim 1, further comprising:
determining a valid dynamic code range.
3. The method of claim 1, further comprising:
determining a valid dynamic code range,
wherein the valid dynamic code range is
asymmetric.
4. The method of claim 1, further comprising:
determining a valid dynamic code range using an
algorithm.
5. The method of claim 1, further comprising:
receiving transaction data; and
determining a valid dynamic code range using an
algorithm,
wherein the algorithm is based on the transaction
data.
6. The method of claim 1, further comprising:
receiving transaction data; and
determining a valid dynamic code range using an
algorithm,

- 58 -

wherein the algorithm is based on the transaction data and a user transaction history.

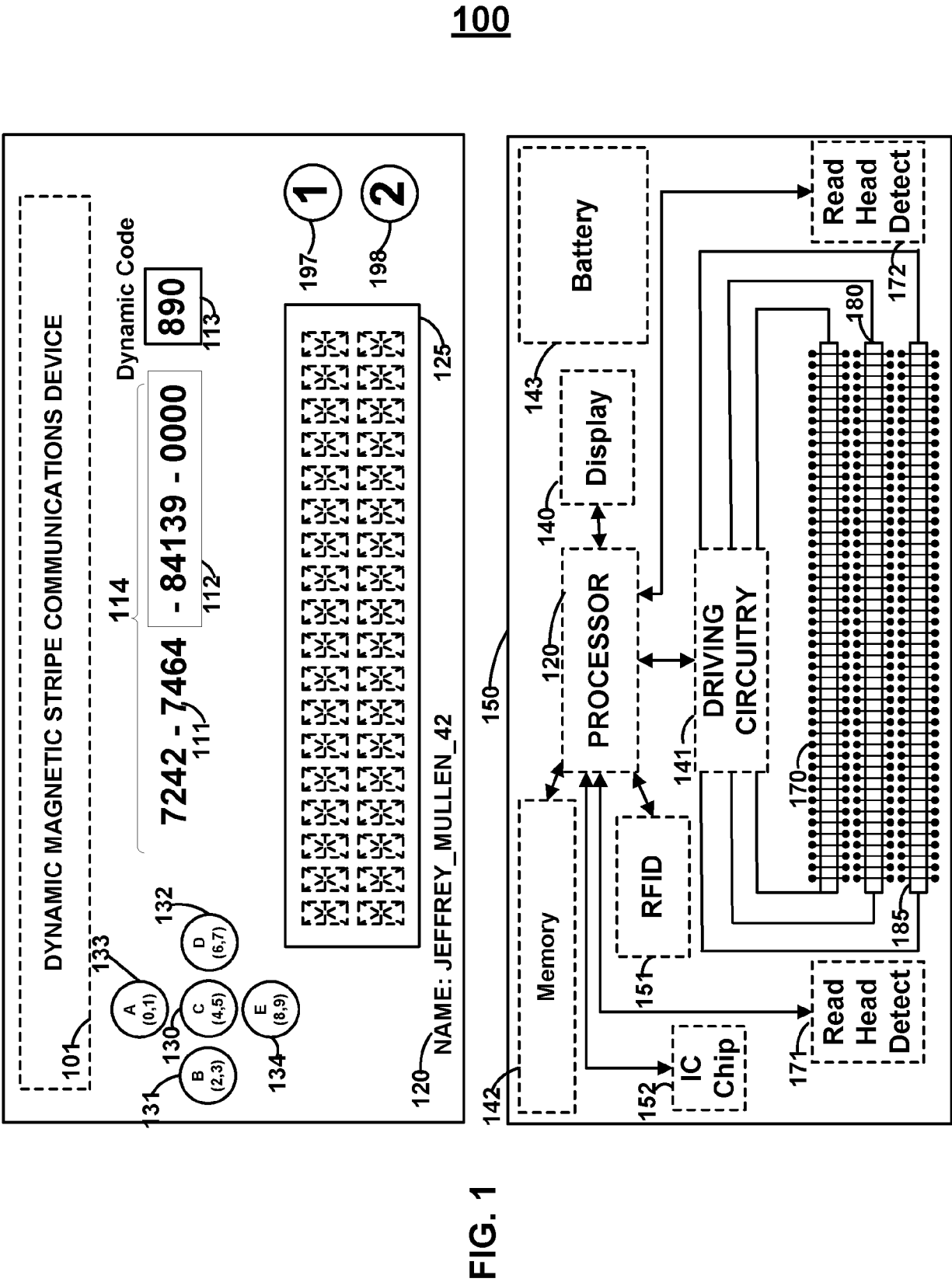
7. The method of claim 1, further comprising:
receiving transaction data; and
determining a valid dynamic code range using a weighted algorithm,

wherein the algorithm is based on prior valid dynamic code ranges and transaction data.

8. The method of claim 1, further comprising:
receiving transaction data,
wherein the determining the code is valid includes comparing the code to a listing of codes.

9. The method of claim 1, further comprising:
receiving transaction data;
determining a risk level; and
determining a valid dynamic code range.

10. The method of claim 1, further comprising:
receiving transaction data;
determining a risk level;
determining that a transaction associated with the transaction data is an online transaction; and
determining a valid dynamic code range.



200

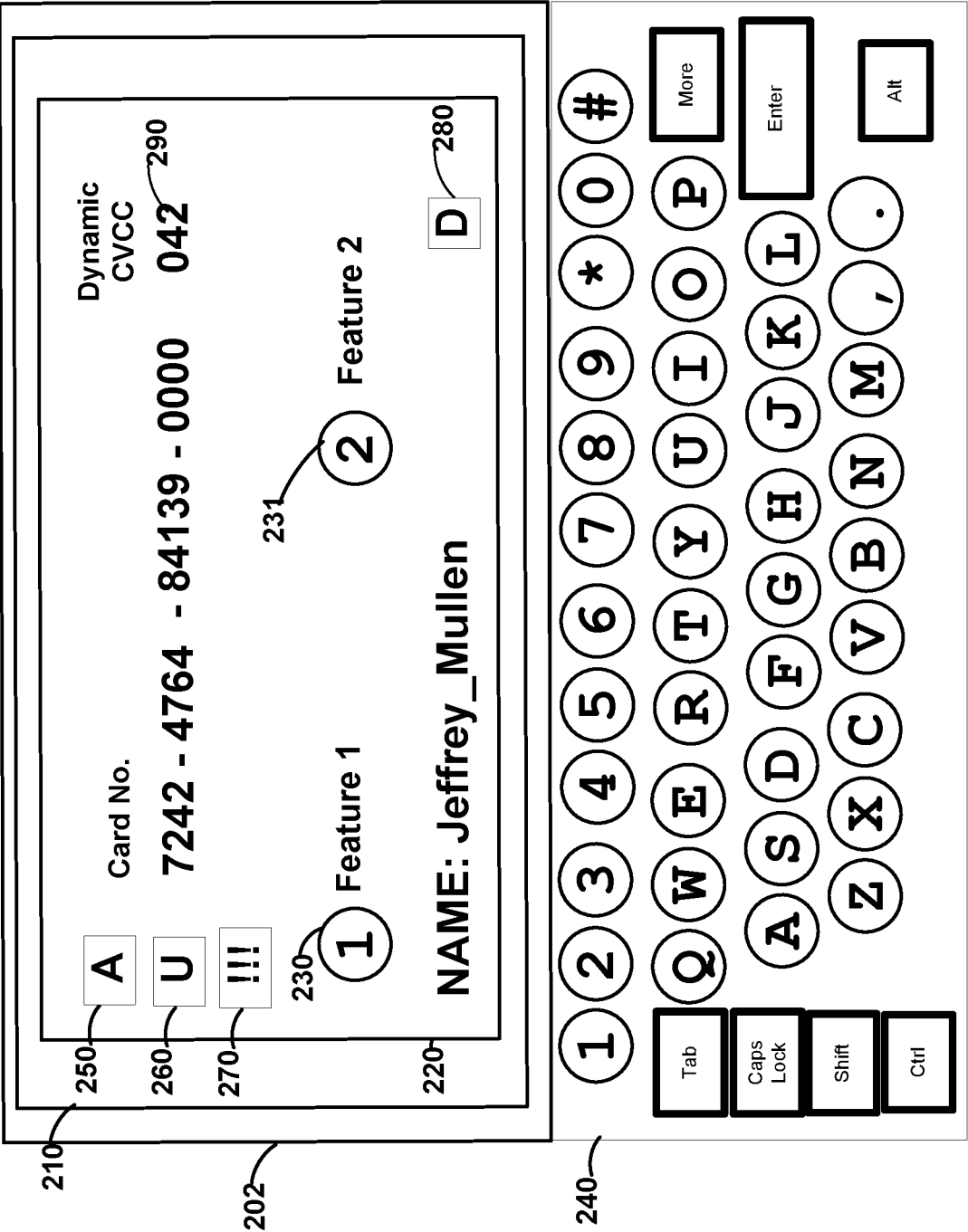
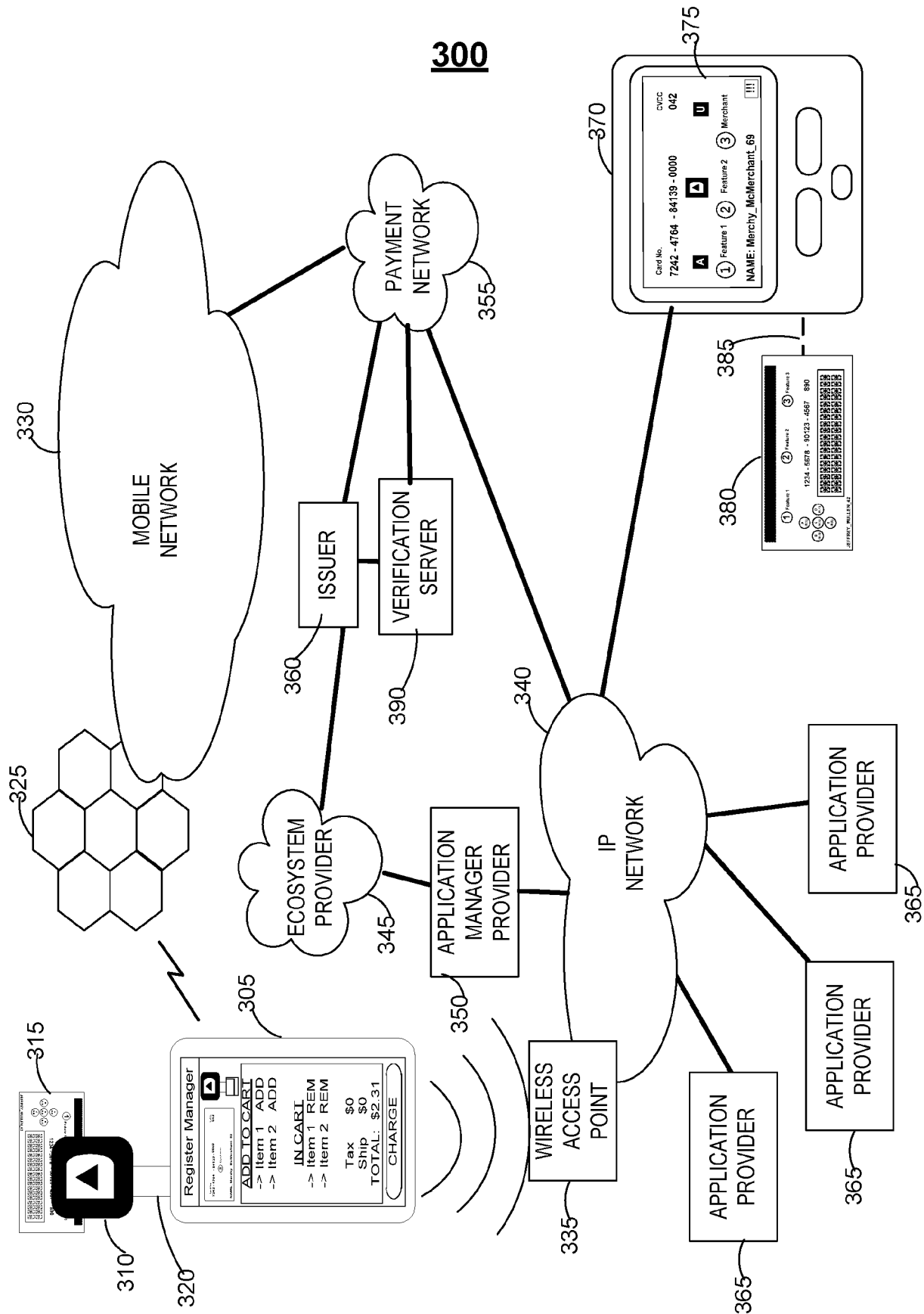


FIG. 2



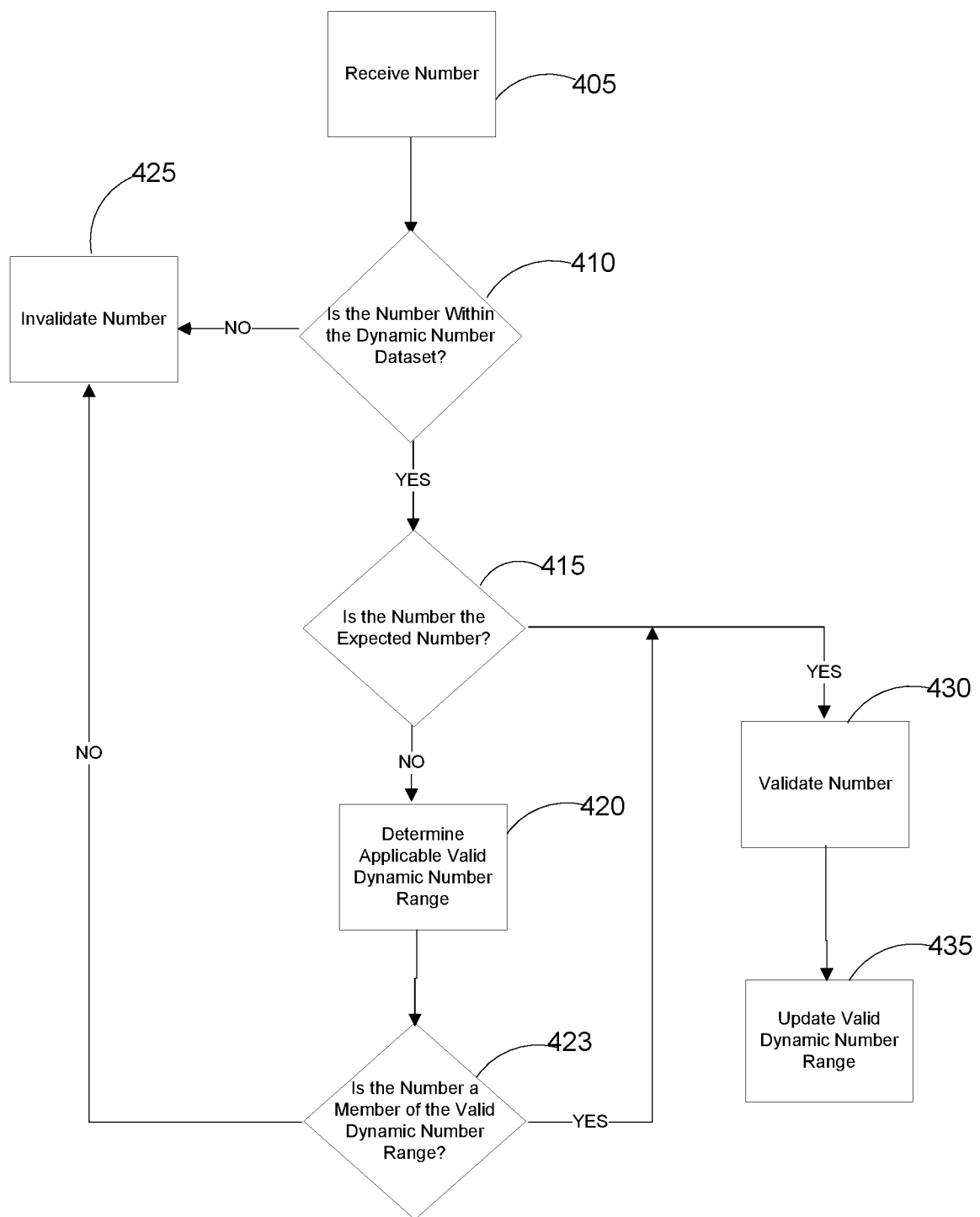


FIG. 4

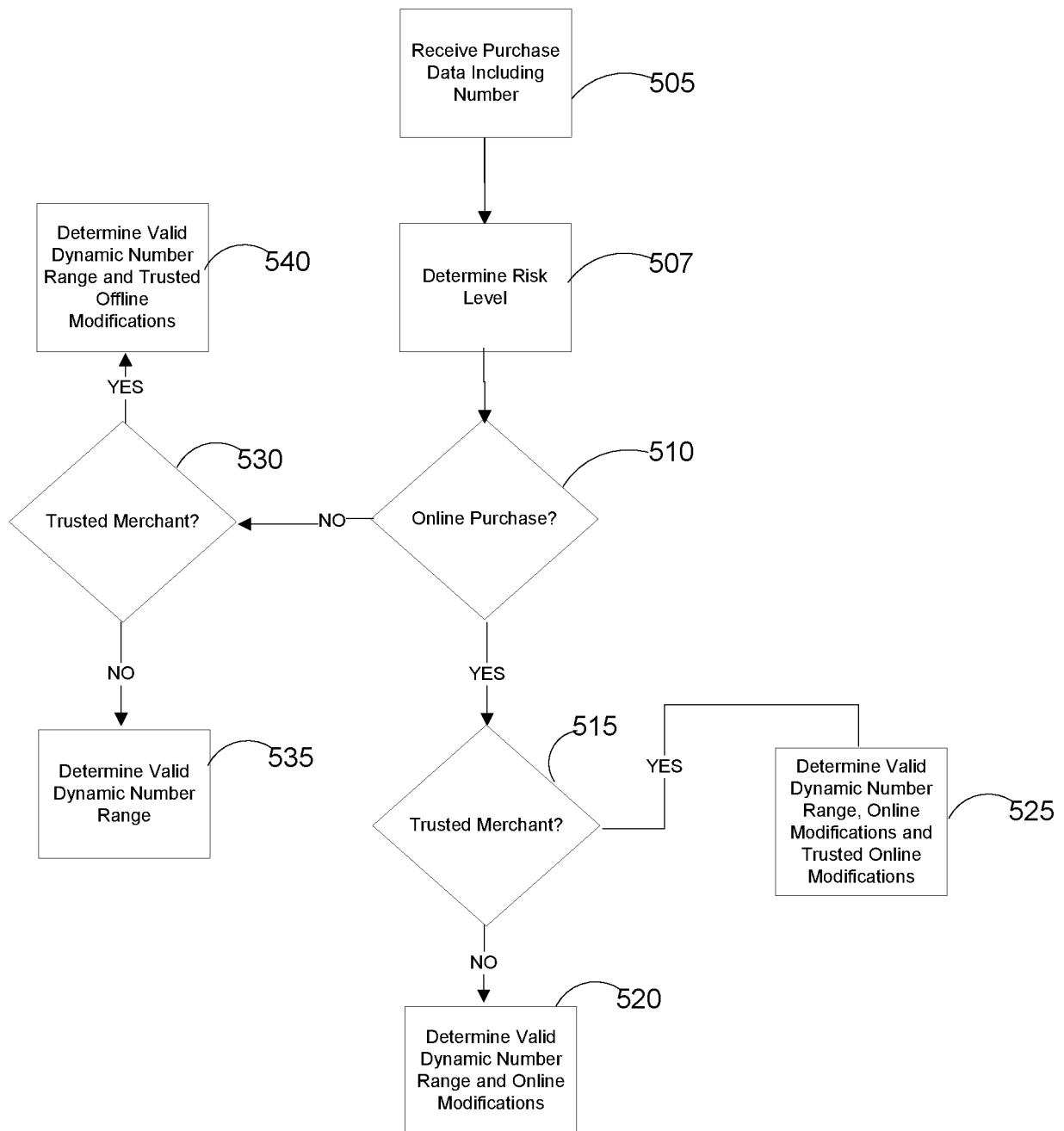
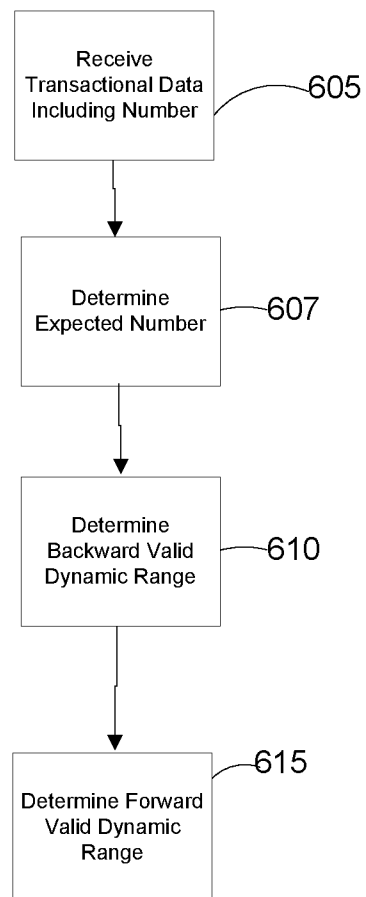
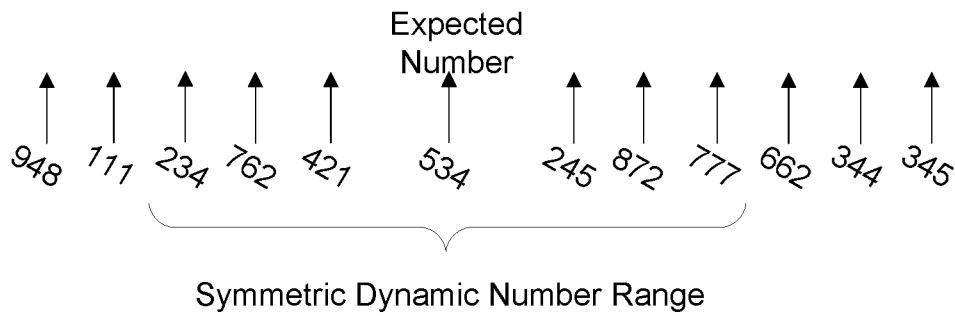
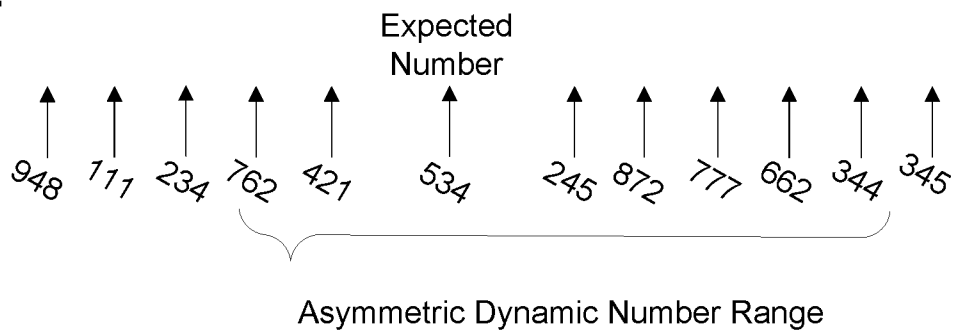
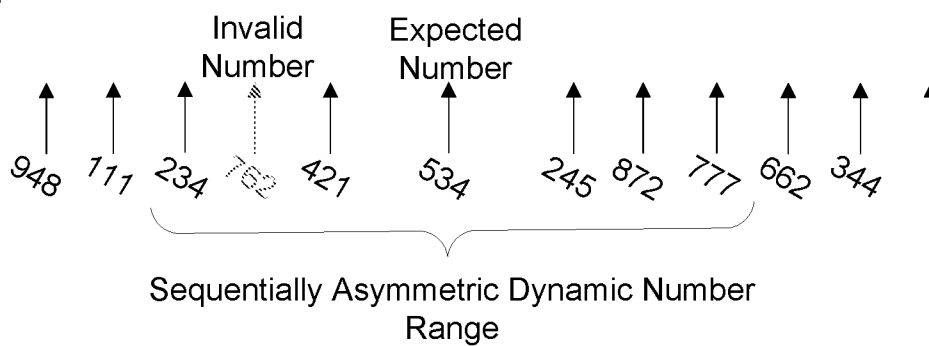


FIG. 5

**FIG. 6**

705**710****720****FIG. 7**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 16/32147

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06Q 20/00 (2016.01)

CPC - G06Q 20/00

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):G06Q 20/00 (2016.01)

CPC: G06Q 20/00

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

CPC: G06Q 20/38, G06Q 20/385, H04L 9/00 (Keyword limited search below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PatBase, Google Scholar, Google Patents; Search Terms: dynamic, code, transaction, approv*, authenticat*, autoriz*, asymmetric*, risk, algorithm, Dynamics, Mullen, Beaver

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/0272307 A1 (BUER) 25 October 2012 (25.10.2012) entire document especially Abstract, para [0021], para [0036]-[0037], para [0049]-[0051], para [0057]-[0058], para [0067]	1-10
A	US 9,033,218 B1 (Batra) 19 May 2015 (19.05.2015) entire document	1-10

☐ 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

12 July 2016

Date of mailing of the international search report

16 AUG 2016

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. 571-273-8300

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774