technology) -readable media (also referred to as computer-readable storage medium) including, but not limited to, attached storage media (e.g., hard disk drives, network disk drives, servers), internal storage media (e.g., RAM, ROM, EPROM, FLASH-EPROM, or any other memory chip or cartridge), removable storage media (e.g., CDs, DVDs, flash drives, memory cards, floppy disks, flexible disks), firmware, and/or other known or yet to be discovered storage media. Depending on its purpose, the memory may be transitory and/or non-transitory. Appropriate "messages," "communications," "signals," and/or "transmissions" (that includes various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof) over appropriate "communication paths," "transmission paths," and other means for signal transmission including any type of connection between two elements on the payment processing system (e.g., the adapter module 100, the mobile device 150, the payment accepting unit 120, hardware systems and subsystems, and memory) would be used as appropriate to facilitate controls and communications.

[0091] It should be noted that the terms "programs" and "subprograms" are defined as a series of instructions that may be implemented as software (i.e. computer program instructions or computer-readable program code) that may be loaded onto a computer to produce a "machine," such that the instructions that execute on the computer create structures for implementing the functions described herein or shown in the figures. Further, these programs and subprograms may be loaded onto a computer so that they can direct the computer to function in a particular manner, such that the instructions produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The programs and subprograms may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. The phrase "loaded onto a computer" also includes being loaded into the memory of the computer or a memory associated with or accessible by the computer. Separate, albeit interacting, programs and subprograms may be associated with the adapter modules 100, the server 130, and the mobile device 150 (including the mobile application 140) and these programs and subprograms may be divided into smaller subprograms to perform specific functions.

Petitioner Exhibit 1002-1220

[0092] The terms "messages," "communications," "signals," and/or "transmissions" include various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof. Appropriate technology may be used to implement the "communications," "signals," and/or "transmissions" including, for example, transmitters, receivers, and transceivers. "Communications," "signals," and/or "transmissions" described herein would use appropriate technology for their intended purpose. For example, hard-wired communications (e.g., wired serial communications) would use technology appropriate for hard-wired communications, short-range communications (e.g., Bluetooth) would use technology appropriate for close communications, and long-range communications (e.g., GSM, CDMA, Wi-Fi, or the like) would use technology appropriate for remote communications over a distance. Appropriate security (e.g., SSL or TLS) for each type of communication is included herein. The security units 755 and 955 include technology for securing messages. The security technology may be, for example, encryption/decryption technology (e.g., software or hardware). Although encryption/decryption is discussed primarily as being performed using a unique private key, alternative strategies include, but are not limited to encryption/decryption performed using public/private keys (i.e., asymmetric cryptography), or other encryption/decryption strategies known or yet to be discovered. Appropriate input mechanisms and/or output mechanisms, even if not specifically described, are considered to be part of the technology described herein. The communications unit 770 (shown in Figure 20) of the adapter module 100 is shown as including appropriate input and output mechanisms 772, 774 that may be implemented in association (e.g., directly or indirectly in functional communication) with male and female adapters 720, 730 of the adapter module 100. The communications unit 870 (shown in Figure 21) of the mobile device 150 includes mechanisms for both long-range communications (shown as the long-range communication capability 872 such as cellular and/or Wi-Fi mechanisms) for communicating with the server 130 and short-range communications (shown as the short-range communication capability 876 such as Bluetooth mechanisms) for communicating with the adapter module 100.

[0093] When used in relation to "communications," "signals," and/or "transmissions," the terms "provide" and "providing" (and variations thereof) are meant to include standard means of provision including "transmit" and "transmitting," but can also be used for non-traditional provisions as long as the "communications," "signals," and/or "transmissions" are "received" (that can also mean obtained). The terms "transmit" and

Petitioner Exhibit 1002-1221

"transmitting" (and variations thereof) are meant to include standard means of transmission, but can also be used for non-traditional transmissions as long as the "communications," "signals," and/or "transmissions" are "sent." The terms "receive" and "receiving" (and variations thereof) are meant to include standard means of reception, but can also be used for non-traditional methods of obtaining as long as the "communications," "signals," and/or "transmissions" are "obtained."

[0094] The term "associated" is defined to mean integral or original, retrofitted, attached, connected (including functionally connected), positioned near, and/or accessible by. For example, if the user interface (e.g., a traditional display 122 (Figure 19), a touch screen display 124 (Figure 19), a key pad 126 (Figure 19), buttons 126 (Figure 19, shown as part of the key pad 126), a keyboard (not shown), and/or other input or output mechanism) is associated with a payment accepting unit 120, the user interface may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120. Similarly, adapter modules 100 may be associated with payment accepting units 120 in that the adapter modules 100 may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120.

SYSTEM OVERVIEW

[0095] Figures 5, 6, and 7 together show major components of the mobile-device-to-machine payment system and the interactions there-between.

[0096] As shown, the adapter module 100 functionally connected bi-directionally to the payment accepting unit 120 via a wired serial connection such that no security is necessary. The adapter module 100 is also functionally connected bi-directionally to the mobile device 150 (and its installed mobile application 140) via short-range communication technology (e.g., a Bluetooth connection). Because the mobile device 150 is not a "trusted" link (e.g., it could be hacked by a user), only secured communications (transmissions) are passed between the adapter module 100 and the mobile device 150. This keeps communications secured and safe from hacking. The mobile device 150 (and its installed mobile application 140) is also functionally connected bi-directionally to a system management server 130 and/or a funding source server 160 via long-range communication technology (e.g., Wi-Fi or Cellular connection) that preferably has appropriate security (e.g., SSL security). Security between the mobile device 150 and the system management server

Petitioner Exhibit 1002-1222

130 has the advantage of protecting communications from the mobile device 150 to the system management server 130 that may include sensitive data and may not be encrypted. The system management server 130 and the funding source server 160 may be connected via a wired Internet connection with SSL security. The system management server 130 may be connected via a wired Internet connection with SSL security to an operators' server 170. Although not necessary to implement a purchase transaction, for other purposes (e.g., inventory), the operators' server 170 may be connected to the payment accepting unit 120 using a handheld computer sync or a cellular connection.

[0097] Also, a unique private key may be used to securely transmit encrypted messages between the adapter module 100 and the system management server 130 (although the encrypted transmissions would most likely be routed through the mobile device 150). The server 130 stores a private key for each adapter module 100, and this key is only known to the adapter module 100 and the server 130. No intermediary is privy to this key (especially not the mobile device 150). When the adapter module 100 and the server 130 communicate messages (e.g., AuthRequest and AuthGrant), the security unit 755 of the adapter module 100 encrypts the message with its private key and passes the message to the mobile device 150. The mobile device 150 (which preferably cannot decrypt the message) passes the encrypted message to the server 130. The server 130 is able to decrypt the message using the security unit 955 of the adapter module 100 and the unique private key. The security unit 955 of the server 130 uses this same unique private key to encrypt messages to the adapter module 100 and sends the message to the mobile device 150 to relay to the adapter module 100 that is able to decrypt the message using the security unit 755 of the adapter module 100 and the unique private key.

[0098] Figure 7 shows specific communications and messaging with a vending sequence (the numbers to the left of the communications and messaging) between the adapter module 100, the mobile device 150, and the system management server 130. These communications are discussed in more detail in the discussion pertaining to the schematic flow diagrams (Figures 8A-8G) and the flow charts (Figures 9A-9E).

[0099] It should be noted that Figures 5, 6, and 7 are examples, and are meant to help in the understanding of the mobile-device-to-machine payment system. For example, the shown long-range communications technology may be replaced with alternative long-range communications technology known or yet to be discovered, the shown short-range communication technology may be replaced with alternative short-range communication

Petitioner Exhibit 1002-1223

technology known or yet to be discovered, and the shown security may be replaced with alternative security known or yet to be discovered. The shown connections are meant to be examples, and there may be intermediaries that are not shown. The shown components have been simplified in that, for example, only one mobile device 150 (or machine 120, adapter module 100, or server 130) is shown where many may be included. Finally, the order of the steps may be changed and some steps may be eliminated.

ADAPTER MODULE

[00100] Figures 11-18 show views of adapter module 100a (referred to generally as adapter module 100). Adapter module 100 is a relatively low cost hardware component that is pre-configured to work with the industry standard multi-drop bus (MDB). On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g., cash).

[00101] The shown adapter modules 100 are preferably designed to be used as an in-line dongle for in-line insertion within, for example, a MDB of a machine 120. The wire used in MDB technology uses male and female connection ends or adapters to allow the attachment of peripherals. In the case of a vending machine, the wire with the connection ends or adapters would be present to allow the attachment of a payment receiving mechanism (e.g., a coin mechanism). The MDB male and female adapters 700, 710 may be separated (as shown in Figures 17-18). The adapter module 100a in Figures 11 and 17-18 has a male adapter 720 and a female adapter 730. The adapter module 100a may be plugged (inserted) in serial ("in-line") with the wire. For example, the MDB female adapter 710 may be connected to the male adapter 720 of the adapter module 100 and the MDB male adapter 700 may be connected to the female adapter 730 of the adapter module 100. The resulting in-line configuration is shown in Figure 19. It should be noted that the adapter modules 100 are designed to allow pass-through communications so that if the mobile-device-to-machine payment processing system is not enabled (e.g., for a particular purchase or simply turned off) the MDB functions as though the adapter module 100 is not there and the machine 120 can function normally.

HANDS-FREE MODE

[00102] Summarily, if it is available, a hands-free mode, from the user's perspective, would allow the user to approach a favorite payment accepting unit 120 and notice that the

Petitioner Exhibit 1002-1224

display (e.g., the displays 122 or 124 shown in Figure 19) associated with the payment accepting unit 120 shows funds available (e.g., the wallet balance), he would select the product or service using input mechanisms (e.g., buttons 126 or a touch screen display 124 shown in Figure 19) associated with the payment accepting unit 120, and he would retrieve his dispensed services or products.

[00103] During an initial handshake with the mobile device 150 (when the user is within range), the adapter module 100 reports to the mobile device 150 whether or not hands-free mode is available. If it is available, the installed mobile application 140 automatically connects to the payment accepting unit 120 without the user having to interact with the mobile device 150. The user observes that funds are available on the display 122, 124 of the payment accepting unit 120 and completes the purchase transaction as if cash was inserted in the machine 120 by inputting his selection on the payment accepting unit 120. The payment accepting unit 120 dispenses the product or service. After the selection is made, the change is returned to the mobile device 150.

[00104] Whether hands-free payment is available is determined by factors including, but not limited to whether if other mobile devices 150 are in range, if other adapter modules 100 are in range, if there are any alerts, if the payment trigger threshold is having wide variances and so deemed unstable, or if the payment accepting unit operator (e.g., a vending machine operator) has opted to disable hands-free mode for the payment accepting unit 120. In the latter instance, operators can disable via a maintenance mobile device 150, as well as through the operators' server 170 and/or the system management server 130.

[00105] Figure 3 is a table that shows considerations, conditions, or factors that may be used to determine whether the hands-free pay feature is available. Starting at the "Favorite?" column, this indicates whether the payment accepting unit 120 is a favorite machine. Preferably the hands-free pay feature is only available for use with "favorite" payment accepting units 120 (e.g., a vending machine at work or school). The "Alert" column has to do with whether there is some reason (e.g., there are too many users in range) that the hands-free pay feature should not work and, if there is such a reason, the user will be notified (alerted) and may be able to use the manual mode to resolve the alert and/or complete the transaction. Figure 3 shows situations in which a user is or is not able to make hands-free purchases from a machine 120 using a mobile application 140 on his mobile device 150. It should be noted that the shown interface is an example. For example, some of the features could be automated or pre-selected. (It should be noted that the left hand column, the "Tab"

Petitioner Exhibit 1002-1225

column, relates to whether the selected tab on the mobile application 140 is "all" or "favorite." Figures 10A-10D all show these tabs. Unlike the other columns in Figure 3, this column has more to do with the functionality and view of the application 140 than specifically with the hands-free feature. The tabs would allow a user to select whether he wanted to be alerted when he was in range of all payment accepting units 120 or just "favorite" payment accepting units 120 and the application 140 would show the appropriate view.)

[00106] Balance Display: An optional feature of the mobile-device-to-machine payment system that is particularly helpful in the hands-free mode (although it may be available in the manual mode and/or in a multiple-vend scenarios) is when the user's mobile device 150 sends "credit" to the payment accepting unit 120 (either via hands-free payment or through a manual swipe), the wallet balance is sent to the payment accepting unit 120 that is then displayed to the user on a display 122, 124 of the machine 120. This is particularly beneficial during hands-free mode when the user does not retrieve the mobile device 150 and, therefore, may not know the balance. Also, in a multiple-vend scenario the user would not have to calculate a remaining balance.

[00107] An example of a hands-free, multiple-vend scenario where a balance is displayed by the payment accepting unit 120, follows: The user has $5.00 in his/her virtual wallet as that is the amount that has been authorized (the AuthGrant being stored on the mobile device 150). The user walks up to the payment accepting unit 120 and $5.00 is displayed on the display 122, 124 of the payment accepting unit 120 since hands-free mode was enabled and credit was sent (e.g., via the short-range communication capability) to the payment accepting unit 120. The user makes a selection of $1.50 by interacting (e.g., pressing buttons) with the machine 120. The item (product or service) is dispensed and the "change" is "returned" (e.g., via the short-range communication capability) to the virtual wallet. But since the user is still standing in the payment zone 102, the remaining wallet balance of $3.50 is sent to the payment accepting unit 120 and displayed so that the user can now see that he/she has a $3.50 balance. (It should be noted that the authorized funds may remain on the machine 120 and not be transferred back to the mobile device 150 between transactions.) The user decides to purchase a $1.50 item, and the transaction is completed as usual (e.g., by interacting with the machine 120). Now the user is still standing in the payment zone 102 and he/she sees the wallet balance of $2.00 on the display 122, 124 of the payment accepting unit 120. The user decides that he/she does not wish to purchase anything else and simply walks

Petitioner Exhibit 1002-1226

away. As he/she walks out of the payment zone 102, the credit is cleared from the machine 120, but he/she is left with the knowledge that his wallet balance is $2.00 even though he/she never touched the mobile device 150. Communications between the payment accepting unit 120 and the adapter module 100 (via the mobile device 150) handle the accounting incidental to the transaction. The remaining balance ($2.00) is technically stored on the server 130, and may be reflected on the application 140 on the mobile device 150.

MULTIPLE DISTINCT ZONES

[00108] As shown in Figures 1-2, the functions performed by the adapter module 100 can be divided into distinct zones: a first "communication zone" (e.g., "Bluetooth range" 106), a second "authorization zone" 104, and a third "payment zone" 102. The payment zone 102 is smaller than or equal to (overlapping completely) the authorization zone 104. Put another way, the payment zone 102 is within or coextensive with the authorization zone 104. The payment zone 102 is a subset of the authorization zone 104 with a ratio of the payment zone 102 to the authorization zone 104 ranging from 0.01:1 to 1:1. It is not necessarily a fixed ratio and can vary between different payment accepting units 120, different mobile devices 150, different users, and over time. While the zones 102, 104, 106 are depicted as having a uniform shape, the zones may not necessarily be uniform (or constant over time) in that the shape can vary. For example, the shape of the Bluetooth range 106 may vary depending on environmental conditions such as obstacles in the room and payment accepting unit 120 door/wall materials.

[00109] Bluetooth Range 106 (sometimes also herein called the "communication zone"): The outermost range is the Bluetooth range 106 (shown in Figures 1-2). This is the area in which the adapter module 100 is able to broadcast its presence. In most situations, the Bluetooth range 106 is a passive range in that no actual data is exchanged between the mobile device 150 and the adapter module 100. While in the Bluetooth range 106, the mobile device 150 monitors the RSSI (Received Signal Strength Indicator).

[00110] Authorization Zone 104: The middle region is the authorization zone 104 (shown in Figures 1-2). This is a computed area based on the RSSI. As mentioned, the mobile device 150 monitors the RSSI while it is in the Bluetooth range 106. When the RSSI reaches a certain predetermined threshold based on In-Range Heuristics, the mobile device 150 can be considered to be in the authorization zone 104. In the authorization zone 104 the mobile device 150 establishes a connection to the adapter module 100 (e.g., a Bluetooth connection (Figure 5) with SSL protection (Figure 6)) and informs the adapter module 100 of its

Petitioner Exhibit 1002-1227

presence. After a successful handshake with the adapter module 100, the mobile device 150 registers the adapter module 100 and the adapter module 100 requests an authorization to the server 130 via the mobile devices' network connection (e.g., a Wi-Fi or cellular connection (Figure 5) with SSL protection (Figure 6)). It is important to note the mobile device 150 and the adapter module 100 have a non-exclusive relationship at this point. The adapter module 100 may collect registrations for all mobile devices 150 that are within the authorization zone 104.

[00111] An authorization occurs in preparation for when the user enters the payment zone 102 (shown in Figures 1-2). An authorization expires in a set period of time (for example, five minutes), so if the mobile device 150 is still in the authorization zone 104 at the time of expiration, the adapter module 100 submits for and receives another authorization. This will continue for a set number of times (for example, the limit may be three times to limit cases of numerous authorizations for a mobile device that may remain in the authorization zone 104 for an extended period of time without completing a transaction). Should authorization fail (for instance if the limit had been reached) prior to the user entering the payment zone 102, the adapter module 100 will request authorization when the mobile device 150 enters the payment zone 102 (which adds a few seconds to the experience).

[00112] Payment Zone 102: As a user enters the payment zone 102, the mobile device 150 establishes exclusive control of the adapter module 100. Once established, any other user in the payment zone 102 is put into a "waiting" status.

[00113] In the payment zone 102, the payment can be triggered automatically if the payment processing system has and is in hands-free mode. In such instances, the mobile device 150 is running the application 140 in background mode and will send credit to the payment accepting unit 120 without any explicit user interaction. The user completes the transaction on the payment accepting unit 120 in much the same manner as if cash had been inserted into the payment accepting unit 120 to establish credit. After the user completes the transaction (that may include one or more purchases), details of the transaction are preferably returned to the mobile device 150 and server 130 in separate messages. The message to the server 130 is preferably encrypted with the adapter module's 100 private key (Figure 6) to ensure data integrity. As shown in Figure 7, the "private key" coded message (Encrypted VendDetails) is preferably sent via the mobile device 150. The message to the mobile device 150 may be sent solely for the purpose of closing the transaction. The transaction history and balance are updated server-side via the encrypted message sent to the server 130.

Petitioner Exhibit 1002-1228

[00114] The other mode of operation is manual mode. In manual mode, the user launches the mobile device 150 and is able to swipe to send payment to the payment accepting unit 120. The user can also swipe back to cancel the payment. Like in hands-free mode, the purchase transaction is completed on the payment accepting unit 120 in the same manner as if cash were inserted into the payment accepting unit 120. The mobile device 150 is only used to send payment. Selection is made directly on the payment accepting unit 120.

[00115] Self-Calibrating Zone Threshold: A key, but optional feature, of the payment processing system is a self-calibrating payment zone RSSI threshold. Because RSSI can vary machine to machine, environment to environment, and device to device, having a fixed threshold at which payment is triggered can be problematic. The approach suggested herein is the creation of a self-calibrating threshold. When the user is interacting with the payment accepting unit 120 (such as when he makes his selection on the payment accepting unit 120), the payment accepting unit 120 notifies the adapter module 100 and the adapter module 100 logs the conditions such as RSSI, type of user mobile device 150, accelerometer data, and other information. It is at this point that it can be ascertained safely that the user is within arm's-length from the payment accepting unit 120 (by necessity the user is arm's-length because he is making some physical interaction with the payment accepting unit 120). This is the only point in the entire transaction in which it can be certain that the user is within arm's-length from the payment accepting unit 120.

[00116] Figure 4 shows a simplified set of steps involved when users enter the payment zone 102. Specifically, Figure 4 shows that credit is established 200 (this may have been done in the authorization zone 104, but if not it would be handled in the payment zone 102), that the user makes a selection using the machine 202, that the machine notifies the adapter module of the selection 204, that the adapter module (optionally) logs the RSSI 206, and that the purchase process(es) continues 208. Using the historically logged RSSI data, the adapter module 100 calculates one of several "average" RSSI using various mathematical models. This "average" could be a traditional average, a moving average, a weighted average, a median, or other similar summary function. The adapter module 100 could pre-process the historical data before running the function, such as to eliminate top and bottom data points, suspect data points, etc.

[00117] Optionally, during the handshake between the mobile device 150 and the adapter module 100, the information transmitted to the adapter module 100 may include, for example, the model of the mobile device 150. Using the received information pertaining to

Petitioner Exhibit 1002-1229

the mobile device models, the adapter module 100 can create multiple payment thresholds, one for each mobile device model. This allows for variances that may be inherent in different types of Bluetooth radios. An alternative to this method is for the adapter module 100 to broadcast a baseline payment zone threshold, and the mobile device 150 can use an offset from this baseline based on its specific model type. The payment zone thresholds (or baseline offsets) can be unique to specific types of mobile devices (e.g., by manufacturer, operating system, or component parts), models of mobile devices, or individual mobile devices (unique to each user).

[00118] In a typical scenario in which the payment zone threshold has been calibrated, the adapter module 100 advertises its presence along with the threshold at which it considers any mobile device 150 to be in the authorization zone 104. This is a one-way communication from adapter module 100 to mobile device 150. Once the mobile device 150 enters the authorization zone 104, there is a handshake that is established between the adapter module 100 and the mobile device 150. During this handshake, the mobile device 150 can share its model information with the adapter module 100, and the adapter module 100 can return the payment zone 102 threshold for that specific model.

[00119] Optionally, in addition to calibrating the payment zone threshold, the adapter module 100 can apply the self-calibrating model to the authorization zone 104 to calibrate the authorization zone threshold. As with the payment zone thresholds, the authorization zone thresholds can be unique to specific types of mobile devices, models of mobile devices, or individual mobile devices. In this scenario, the adapter module 100 would broadcast multiple thresholds by device type and the mobile device 150 would determine which threshold to apply (or alternatively broadcast a baseline and the mobile device 150 uses an offset based on its device model). Even in this scenario, the authorization zone 104 is a one-way communication.

[00120] Optionally, along with the threshold that is calculated (in the payment and/or the authorization zone(s)), a safety margin can be added to minimize scenarios in which a user is within range, but the mobile-device-to-machine payment processing system does not recognize it because the threshold may not have been reached. For example, if the calculated RSSI for an iPhone™ 5 on machine 4567 is -68 db, the mobile-device-to-machine payment processing system may add a safety margin of -5 db, and establish the threshold at -73 db. So when a user's phone is communicating with the adapter module 100 at an RSSI of -73 db or better, the mobile-device-to-machine payment processing system will allow the mobile

Petitioner Exhibit 1002-1230

device 150 to credit the payment accepting unit 120. The safety margin can be set on the server 130 and downloaded to the adapter module 100, or set on the mobile device 150, or set on the adapter module 100 itself.

[00121] Optionally, in the payment zone threshold, the mobile device 150 can use other data to determine when to cancel the exclusive control of the payment accepting unit 120, to identify when the user is moving out of the payment zone 102. External data could include accelerometer data from the mobile device 150. Using that data, the mobile device 150 can determine whether the user is standing relatively still in front of the payment accepting unit 120, or if the user is in motion – effectively walking away from the payment accepting unit 120.

SIGNAL UNAVAILABILITY ADAPTATION

[00122] The mobile-device-to-machine payment processing system described herein uses a mobile device's 150 short-range communication technology (e.g., Bluetooth mechanisms) (shown as short-range communication capability 876 in Figure 21) and a mobile device's 150 long-range communications technology (e.g., cellular and/or Wi-Fi mechanisms) (shown as long-range communication capability 872 in Figure 21). The short-range communication capability 876 communicates with the adapter module's 100 short-range communication technology (e.g., Bluetooth mechanisms) (shown as short-range communication capability 776 in Figure 20). The long-range communication capability 872 communicates with the server's 130 long-range communications technology (e.g., cellular and/or Wi-Fi mechanisms) (shown as long-range communication capability 972 in Figure 22). The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. This process is described herein and works properly if there is cellular or Wi-Fi coverage within the payment zone 102.

[00123] One option if there is no cellular or Wi-Fi coverage within the payment zone 102 is to determine whether there is cellular or Wi-Fi coverage within the authorization zone 104 or the Bluetooth range 106. If there is, then the sizes of the zones 102, 104, 106 could be adapted and the timing could be adapted. For example, if the mobile devices 150 detected problems with the cellular or Wi-Fi coverage within the payment zone 102, the user could carry his mobile device 150 into the other zones (or the mobile device 150 could use short-range communication technology to communicate with other mobile devices 150 within the authorization zone 104 or the Bluetooth range 106) to determine whether the zones have

Petitioner Exhibit 1002-1231

cellular or Wi-Fi coverage. If they do have coverage, communication between the mobile device 150 and the server 130 can be advanced (conducted earlier when the mobile device 150 is further from the machine 120) or delayed (conducted later when the mobile device 150 is further from the machine 120). This can be thought of as changing the size or shapes of the zones 102, 104, 106. The timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or Wi-Fi coverage again.

[00124] Another option if there is no cellular or Wi-Fi coverage within any of the zones 102, 104, 106 is for the user to obtain authorization while outside of the zones in a place with cellular or Wi-Fi coverage. This may occur, for example, if a user knows that he will be going to a place with a payment accepting unit 120 equipped with an adapter module 100 (perhaps to a favorite payment accepting unit 120) that does not have (or rarely has) cellular or Wi-Fi coverage. A user may also use the mobile application 140 to query payment accepting units 120 in a given range (e.g., within 50 miles) or at a given location (e.g., at a campground or in a particular remote city) to determine whether there is cellular or Wi-Fi coverage within the zones 102, 104, 106. The user can then obtain pre-authorization from the server 130 using the mobile application 140. Again, the timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or Wi-Fi coverage again. A mobile-device-to-machine payment system having the ability to implement this option would be able to accept cashless payments without requiring any network connection near the payment accepting unit 120. In some implementations, the mobile-device-to-machine payment processing systems described herein is located in a remote location where no signal is available, therefore, can accept cashless payments.

[00125] As an example of a situation in which there might be no cellular or Wi-Fi coverage within any of the zones 102, 104, 106 of a particular payment accepting unit 120, the user (a teenager) may be traveling to a remote location to attend summer camp where there is no cellular or Wi-Fi coverage. The camp may have several payment accepting units 120 (e.g., a machine that creates a dedicated "hot spot" that requires payment for use, vending machines, or machines for renting equipment such as bikes, kayaks, or basketballs). The camp facility might notify parents that the mobile-device-to-machine payment system is

Petitioner Exhibit 1002-1232

available. The parents, while at home, could obtain authorization for a particular amount (that could be doled out a certain amount per day or limited to type of machine or location) to be authorized and "loaded" into the user's mobile device 150 and specify that the authorization will not expire for a certain period or until a certain date. Thereafter, while at camp, the user could use the mobile application 140 on his mobile device 150 in a manner similar to those discussed elsewhere herein. Short-range communications may be used for communications between the adapter modules 100 (associated with the machines 120) and users' mobile devices 150.

[00126] One subtle but powerful component of the payment processing system described herein is that it requires a long-range communication capability (e.g., an Internet or cellular network connection) only in the authorization zone 104 and only for the time period required to send the AuthRequest and receive the AuthGrant. Once a valid AuthGrant is received by the mobile device 150, the long-range communication capability (e.g., an Internet or cellular network connection) is not required by either the mobile device 150 or the adapter module 100 in the payment zone 102 as long as the AuthGrant is valid (unexpired). This mechanism allows the system to seamlessly handle authenticated transactions in (temporary) offline mode, with the deferred acknowledgement and transaction messages performing the bookkeeping and cleanup when network connection is regained. The alternatives described above provide a unique way to artificially extend the authorization zone to include any location where the mobile device 150 can communicate with the server 130.

MULTIPLE USER RESOLUTION

[00127] As shown in Figure 2, in one practical scenario, multiple users are in the zones 102, 104, 106. As shown in Figure 2, users 1, 2, and 3 are in the payment zone 102 near the machine 120; users 5 and 6 are shown as positioned between the authorization zone 104 and the Bluetooth range 106; users 4 and 7 are in the Bluetooth range 106, user 10 is positioned on the edge of the Bluetooth range 106; and users 8 and 9 are positioned outside of Bluetooth range 106. In some implementations, the mobile-device-to-machine payment processing system manages and resolves issues pertaining to multiple users.

[00128] Users 4 and 7 are within the Bluetooth range 106 and the user 10 is either entering or leaving the Bluetooth range 106. Within the Bluetooth range 106 the users' mobile devices 150 are able to see the adapter module's 100 advertisement. In this zone, the mobile device 150 preferably does not initiate a connection. The adapter module 100 is preferably unaware of the users in the Bluetooth range 106. All the adapter module 100 is

Petitioner Exhibit 1002-1233

doing is advertising its presence to any multitude of users that may be in Bluetooth range 106.

[00129] The adapter module 100 begins to log users as the users (and their respective mobile devices 150) enter the authorization zone 104 (shown in Figure 2 as users 5 and 6). At this point, there is a non-exclusive connection initiated by the mobile device 150 to the adapter module 100. It does a handshake (e.g., to exchange information needed to obtain authorization and, optionally, to log information needed for a self-calibrating authorization zone threshold) and the mobile device 150 contacts the server 130 for an authorization (e.g., sending an AuthRequest and receiving an AuthGrant). The adapter module 100 registers all mobile devices 150 that have requested and received AuthGrants. The adapter module 100 continues communicating with any other mobile device 150 that enters the authorization zone 104. After initial contact, the adapter module 100 may provide the mobile device 150 with a deferral delay of when to check back in with the adapter module 100 allowing opportunity for other mobile devices 150 to communicate with the adapter module 100.

[00130] If there is only one user in the payment zone 102, a purchase transaction may be performed. If there are multiple users in the payment zone 102, the mobile-device-to-machine payment system must handle the situation.

[00131] One optional solution for handling the situation of the multiple users in the payment zone 102 is queuing users in the payment zone 102. Once any mobile device 150 enters the payment zone 102, it establishes exclusivity to a particular mobile device 150 (e.g., in a first-come-first-serve manner). Technically, however, the adapter module 100 is not establishing an exclusive connection to the mobile device 150. The adapter module 100 can still perform a round-robin poll and communicate with and advertise to other mobile devices 150. Instead, the adapter module 100 establishes a queue prioritized by RSSI and time (e.g., who was first and whether the authorization has expired) and it notifies (e.g., alerts) other mobile devices 150 to wait. The earliest valid (unexpired) authorization takes precedence when there is any tie in the RSSI. Otherwise, for example, the strongest average RSSI takes priority. Preferably the queue is not a static measure of the RSSI but an averaged measure over the period of time in the queue. This compensates for a scenario in which a user may be walking around in the queue and then shows up at the payment accepting unit 120 just as the previous user is finishing. If another user was also in the payment zone 102 and stood there the entire time, but may have newer authorization, he could win out.

Petitioner Exhibit 1002-1234

[00132] Anytime that the adapter module 100 cannot determine exactly which user is in the payment zone 102 in front of the payment accepting unit 120, the adapter module 100 will disable hands-free payment. The mobile device 150 will send an alert to the user and he can use swipe to pay (manual mode). All users in payment zone 102 will show "Connected" and the first to swipe payment to the payment accepting unit 120 then locks out other users.

MULTIPLE MODULE RESOLUTION

[00133] In the scenario where there are multiple modules present, determining which payment accepting unit 120 a user is in front of can be a challenge. In some implementations, the mobile-device-to-machine payment processing system described herein allows adapter modules 100 to communicate to other adapter modules 100 in range via Bluetooth. Each user receives authorization grants for specific payment accepting units 120. This means if there are multiple adapter modules 100 within the same authorization zone 104, there will be multiple authorization grants for the user. When the user enters the payment zone 102, it can be difficult to differentiate which payment accepting unit 120 the user is in front of if the payment zones 102 overlap.

[00134] To solve this problem, when the user enters the payment zone 102, the adapter modules 100 communicate with each other to determine the RSSI for the particular user (based on the signal from his mobile device 150) to triangulate which adapter module 100 (and the associated payment accepting unit 120) is closer to the user. Optionally, the inter-module communications can restrict the user to establishing an exclusive connection with only one payment accepting unit 120.

[00135] Optionally, when the user connects to a payment accepting unit 120, the mobile device 150 can send a communication to the payment accepting unit 120 for momentary display to the user on the display 122, 124 of the payment accepting unit 120. For example, the mobile device 150 can send a communication (e.g., "connected" or "Fred's Mobile Device Connected") to the payment accepting unit's display 122, 124 for a predetermined period of time (e.g., 1-3 seconds) so when the user is in payment zone 102, it is clear which payment accepting unit 120 the user is connected to prior to making a purchase (either in hands-free or manual mode).

[00136] In addition, when the user is in manual mode, the mobile device 150 can display (e.g., on the touch screen 152 as shown in Figures 10A-10D) a visual indication of the payment accepting unit 120 (e.g., a picture and/or a payment accepting unit ID of the

Petitioner Exhibit 1002-1235

payment accepting unit 120) for visual confirmation. If the user is in manual mode, the user can manually change the payment accepting unit 120.

DESCRIPTIVE SCENARIO

[00137] Figure 7, Figures 8A-8G, and 9A-9E (as well as other figures) can be used to understand a detailed scenario of the mobile-device-to-machine payment processing system described herein. A flow of communications and steps are loosely described below with reference to these (and other figures). It should be noted that alternative scenarios could include, for example, a modified order of the steps performed.

[00138] Prior to vending transactions, a user downloads a mobile application 140 onto his mobile device 150, creates an account, and configures a funding source via, for example, a funding source server 160. A funding source may be, for example, a debit card, a credit card, campus cards, rewards points, bank accounts, payment services (e.g., PayPal™) or other payment option or combination of payment options known or yet to be discovered. The funding sources may be traditional and/or nontraditional payment sources that are integrated into the ecosystem described herein and then used indirectly as a source of funds. Funds from the funding source are preferably held on the server 130 such that when an AuthRequest is received by the server 130, the server 130 can send an AuthGrant authorizing funds for a purchase.

[00139] The user can specify one or more "favorite" adapter module(s) 100 (that has a one-to-one relationship to the payment accepting unit 120) that he may visit regularly, such as a vending machine at school or work. Favorite adapter modules 100 appear on a pre-filtered list and allow for additional rich features such as hands-free payment.

[00140] The payment accepting unit 120 may be equipped with an adapter module 100 that is constantly advertising its availability via Bluetooth (or other "signals," "communications," and/or "transmissions"). This ongoing advertising and scanning for adapter modules is shown in Figure 8A. As shown, the mobile device 150 is continuously scanning for any adapter module 100 within Bluetooth (or other "signal," "communication," and/or "transmission") range. When the user is within range of that adapter module 100, the mobile device 150 tracks and monitors the signal strength until a predetermined "authorization zone" threshold is achieved.

[00141] Figures 8B and 9A generally show that when the authorization zone threshold is reached, the mobile device 150 enters the authorization zone (block 302) and registers the adapter module 100. The mobile device 150 connects to the server 130 (block 304). The

Petitioner Exhibit 1002-1236

application 140 on the mobile device 150 creates a request for authorization (AuthRequest) and passes the AuthRequest to the server 130 using appropriate communication technology (e.g., GSM, CDMA, Wi-Fi, or the like) (block 306). The server 130 responds with an authorization grant (AuthGrant) encrypted with the specific adapter module's private key (block 306). This authorization token may minimally include the User identifier (ID), Apparatus ID (for the adapter module 100), authorization amount, and expiration time. The mobile device 150 receives the AuthGrant from the server 130, and retains it until the mobile device 150 is ready to issue payment to an adapter module 100. The mobile device 150 collects all pending AuthGrants that may be one or more depending on how many adapter modules 100 are in-range. Unused AuthGrants that expire are purged from the mobile device 150 and the server 130. It is important to note that the mobile device 150 is unable to read the AuthGrant because it is encrypted with the adapter module's unique private key that is only known to server 130 and adapter module 100. This provides a preferred key element of security in the system as the adapter module 100 only trusts AuthGrants that are issued by the server 130, and the AuthGrants cannot be read or modified by the mobile device 150 or any other party in between the server and the adapter module 100. Additional mobile devices 150 may enter the authorization zone 104 (block 308).

[00142] As the user approaches a specific adapter module 100, the user enters the payment zone 102 and an event threshold is triggered based on heuristics performed by the mobile device 150. Blocks 310 and 312 show the loop steps of waiting for a mobile device 150 from the authorization zone 104 to enter the payment zone 102. If the user leaves the authorization zone 104 without entering the payment zone 102, the adapter module 100 returns to advertising its presence (block 300).

[00143] Figures 8C and 9B generally show the user entering the payment zone. The mobile device 150 verifies that it has an unexpired and valid AuthGrant. If the AuthGrant is not good, it may be requested again, repeating the Authorization Request process (block 315). If the AuthGrant is good, the mobile device 150 sends the valid AuthGrant (including the wallet balance (block 322)) to the adapter module 100 to initiate a transaction. The mobile device 150 may issue the AuthGrant automatically without specific user interaction if the hands-free mode is supported (and the device is a favorite (block 318), there is only one device in the payment zone 102 (block 318), and (optionally) there is only one user in the authorization zone 104 (block 320). If any of these factors are not present, the mobile device 150 will prompt and/or wait for the user to begin the transaction manually (block 324).

Petitioner Exhibit 1002-1237

[00144] Figures 8D, 9C, and 9D generally show the transaction process. As shown in Figure 9C, the adapter module 100 runs through a series of questions to determine if there are any issues that would prevent vending including: has the user canceled in-app? (block 326), has the user walked away? (block 328), is the coin return pressed? (block 330), has more than a predetermined period of time elapsed? (block 332). If the answer to any of these questions is "yes," the transaction does not proceed. If the answers to all of these questions is "no," the user makes a selection (block 334) on the payment accepting unit 120 in the same or similar manner as compared to if cash or credit were presented to the payment accepting unit 120. If the machine 120 is able to vend (block 336), it attempts to release the product. If the vend fails (block 338) it is reported by the machine (block 340) and a credit is returned to the virtual wallet (block 342). If the vend is successful (block 338) it is reported by the machine (block 344). Put another way, after the transaction is complete, the adapter module 100 returns to the mobile device 150 the details of the transaction as well as an encrypted packet containing the vend details to be sent to the server 130 via the mobile device 150. Optionally, the adapter module 100 can pass additional information not directly related to the transaction such as payment accepting unit health, sales data, error codes, etc.

[00145] Figures 8D and 9E generally show the multi-vend function. If the machine has enabled multi-vend capabilities (block 350) and the multi-vend limit has not been reached, the process returns to the question of whether the user is in the payment zone (block 310 of Figure 9A). If the machine does not have enabled multi-vend capabilities (block 350) or the multi-vend limit has been reached, the wallet is decremented by the vend amount(s) and "change" is returned to the virtual wallet (block 354) and the process ends (block 356).

[00146] Figure 8E is a schematic flow diagram of an example login process. Figure 8F is a schematic flow diagram of an example boot-up process. Figure 8G is a schematic flow diagram of an example account check/update process.

[00147] Several of the figures are flow charts (e.g., Figures 9A-9E) illustrating methods and systems. It will be understood that each block of these flow charts, components of all or some of the blocks of these flow charts, and/or combinations of blocks in these flow charts, may be implemented by software (e.g., coding, software, computer program instructions, software programs, subprograms, or other series of computer-executable or processor-executable instructions), by hardware (e.g., processors, memory), by firmware, and/or a combination of these forms. As an example, in the case of software, computer program instructions (computer-readable program code) may be loaded onto a computer to

Petitioner Exhibit 1002-1238

produce a machine, such that the instructions that execute on the computer create structures for implementing the functions specified in the flow chart block or blocks. These computer program instructions may also be stored in a memory that can direct a computer to function in a particular manner, such that the instructions stored in the memory produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The computer program instructions may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. Accordingly, blocks of the flow charts support combinations of steps, structures, and/or modules for performing the specified functions. It will also be understood that each block of the flow charts, and combinations of blocks in the flow charts, may be divided and/or joined with other blocks of the flow charts without affecting the scope of the invention. This may result, for example, in computer-readable program code being stored in whole on a single memory, or various components of computer-readable program code being stored on more than one memory.

ADDITIONAL IMPLEMENTATIONS

[00148] Figure 23 illustrates a schematic flow diagram of a process 1000 of authenticating a user to perform a transaction in the payment processing system in accordance with some implementations. In some implementations, the payment processing system includes one or more payment modules 100 (e.g., each associated with a respective payment accepting unit 120 such an automatic retailing machine for dispensing goods and/or services), one or more mobile devices 150 (e.g., each executing the application 140 for the payment processing system either as a foreground or background process), and the server 130. The server 130 manages the payment processing system and, in some cases, is associated with an entity that supplies, operates, and/or manufactures the one or more payment modules 100. For brevity, the process 1000 will be described with respect to a respective payment module 100 and a respective mobile device 150 in the payment processing system.

[00149] The payment module 100 broadcasts (1002), via a short-range communication capability (e.g., BLE), a packet of information (sometimes also herein called "advertised information"). The packet of information at least includes an authorization code and an identifier associated with the payment module 100 (module ID). In some implementations,

Petitioner Exhibit 1002-1239

the packet of information further includes a firmware version of the payment module 100 and one or more status flags corresponding to one or more states of the payment module 100 and/or the payment accepting unit 120. The information included in the packet broadcast by the payment module 100 is further discussed below with reference to Figure 24A.

[00150] In some implementations, the payment module 100 sends out a unique authorization code every X seconds (e.g., 100 ms, 200 ms, 500 ms, etc.). In some implementations, the unique authorization codes are randomly or pseudo-randomly generated numbers. In some implementations, the payment module 100 stores broadcasted authorization codes until a received authorization grant token matches one of the stored authorization codes. In some implementations, the payment module 100 stores broadcasted authorization codes for a predetermined amount of time (e.g., Y minutes) after which time an authorization code expires and is deleted. In some implementations, the authorization code is encrypted with a shared secret key known by the server 130 but unique to the payment module 100. In some implementations, the payment module 100 initializes a random number and then the authorization codes are sequential counts from this random number. In such implementations, the payment module 100 stores the earliest valid (unexpired) counter without a need to store every valid authorization code. In some implementations, the authentication code included in the broadcast packet of information is a hash value of the randomly or pseudo-randomly generated number or the sequential number.

[00151] The mobile device 150 receives the broadcasted packet of information, and the mobile device 150 sends (1004), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), an authorization request to the server 130. For example, an application 140 that is associated with the payment processing system is executing as a foreground or background process on the mobile device 150. In this example, the application 140 receives the broadcasted packet of information when the mobile device 150 is within the communication zone of the payment module 100 (i.e., BLE range) and either automatically sends the authorization request to the server 130 or sends the authorization request to the server 130 when the mobile device 150 is within the authorization zone of the payment module 100. In some implementations, the broadcasted packet of information includes a baseline authorization zone threshold (i.e., an authorization zone criterion) indicating a baseline RSSI that the mobile device 150 (or the application 140) is required to observe before being within the authorization zone of the payment module 100. In some implementations, the mobile device 150 (or the application 140) offsets the baseline

Petitioner Exhibit 1002-1240

authorization zone threshold based on the strength and/or reception of the short-range communication capability (e.g., BLE radio/transceiver) of the mobile device 150. In some implementations, the authorization request at least includes the authorization code which was included in the broadcasted packet of information, an identifier associated with the user of the mobile device 150 or the user account under which the user of the mobile device 150 is logged into the application 140 (user ID), and the identifier associated with the payment module 100 (module ID). In some implementations, the authentication code included in authorization request is the hash value in cleartext. The authorization request is further discussed below with reference to Figure 24B.

[00152] After receiving the authorization request, the server 130 processes (1006) the authorization request. In some implementations, the server 130 decrypts the authorization code included in the authorization request with the shared secret key corresponding to the payment module 100. In some implementations, the server 130 determines whether the user associated with the user ID in the authorization request has sufficient funds in his/her account for the payment processing system to perform a transaction at the machine 120 that is associated with the payment module 100 corresponding to the module ID in the authorization request.

[00153] The server 130 sends (1008), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), an authorization grant token to the mobile device 150. In some implementations, the server 130 does not send the authorization grant token if the authorization code in the authorization request cannot be decrypted with the shared secret key corresponding to the payment module 100 (e.g., the authorization code is corrupted or hacked). In some implementations, the server 130 does not send the authorization grant token if the user associated with the user ID in the authorization request does not have sufficient funds in his/her account. In some implementations, in addition to the authorization grant token, the server 130 sends a message directly to the mobile device 150 which is not encrypted with the shared secret key corresponding to the payment module 100. After receiving the message, the mobile device 150 displays an appropriate message to the user such as insufficient balance or declined authorization. In some implementations, the server 130 sends an authorization grant token for an amount equal to zero; in which case, the payment module 100 interprets this as a declined or failed authorization which can result for any number of reasons including, but not limited to, insufficient balance or credit.

Petitioner Exhibit 1002-1241

[00154] The mobile device 150 receives the authorization grant token, and, subsequently, the mobile device 150 detects (1010) a trigger condition. In some implementations, the mobile device 150 (or the application 140) detects the trigger condition via the hand-free mode (e.g., upon entrance into the payment zone of the payment module 100) or manual mode (e.g., interacting with the user interface of the application 140 to initiate a transaction with the payment accepting unit associated with the payment module 100).

[00155] In some implementations, unused authorization grants (e.g., if there was no trigger condition or it expired) are canceled by the mobile device 150 by sending a cancellation message to the server 130 corresponding to the unused authorization grant. In some implementations, the server 130 denies or limits the number of authorization grants sent to the mobile device 150 until it has received transaction information or cancellation of authorization outstanding authorization grants sent to the mobile device 150.

[00156] In response to detecting the trigger condition, the mobile device 150 sends (1012), via a short-range communication capability (e.g., BLE), the authorization grant token to the payment module 100. Subsequently, the machine 120 displays credit to the user (e.g., via one of the displays 122 or 124 shown in Figure 19) and the user interacts with the input mechanisms of the machine 120 (e.g., via the buttons 126 or a touch screen display 124 shown in Figure 19) to purchase products and/or services.

[00157] Figure 24A illustrates a block diagram of a packet 1100 of information broadcast by the payment module 100 (e.g., in step 1002 of the process 1000 in Figure 23) in accordance with some implementations. In some implementations, the packet 1100 at least includes: module ID 1102 and authorization code 1104. In some implementations, the packet 110 additional includes: a firmware version 1106 and one or more status flags 1108.

[00158] In some implementations, the module ID 1102 is a unique identifier corresponding to the payment module 100 (sometimes also herein called the "adapter module 100") that broadcast the packet 1100.

[00159] In some implementations, the authorization code 1104 is a hash value in cleartext. In some implementations, the payment module 100 randomly or pseudo-randomly generates a number or determines a sequential number (*See* step 1002 of process 1000 in Figure 23) and performs a predetermined hash function (e.g., SHA-256) on the number to produce the hash value as the authorization code 1104. In some implementations, the authorization code 1104 is a unique code that is encrypted with a secret encryption key

Petitioner Exhibit 1002-1242

corresponding to the payment module 100. The secret encryption key is shared with the server 130, which enables the server 130 to decrypt the authorization code 1104 and encrypt the authorization grant token but not the mobile device 150. In some implementations, the encryption between server 130 and payment module 100 is accomplished by two pairs of public/private keys.

[00160] In some implementations, the firmware version information 1106 identifies a current firmware version 1112 of the payment module 100. In some implementations, the firmware version information 1106 also includes update status information 1114 indicating one or more packets received by the payment module 100 to update the firmware or one or more packets needed by the payment module 100 to update the firmware. In some implementations, the one or more status flags 1108 indicate a state of the payment module 100 and/or the payment accepting unit 120 associated with the payment module 100. In some implementations, the one or more status flags 1108 indicate a state of the payment module 100 such upload information indicator 1116 indicating that that the payment module 100 has information to be uploaded to the server 130 (e.g., transaction information for one or more interrupted transactions). In some implementations, upload information indicator 1116 triggers the mobile device 150 to connect to payment module 100 immediately (e.g., if it has interrupted transaction information to be uploaded to the server 130). In some implementations, the one or more status flags 1108 indicate a state of the payment accepting unit 120 including one or more of an error indicator 1118 (e.g., indicating that a bill and/or coin acceptor of the payment accepting unit 120 is experiencing a jam, error code, or malfunction), a currency level indicator 1120 (e.g., indicating that the level of the bill and/or coin acceptor reservoir of the payment accepting unit 120 is full or empty), and/or inventory level(s) indicator 1122 (e.g., indicating that one or more products of the payment accepting unit 120. In some implementations, the one or more status flags 1108 are error codes issued by payment accepting unit 120 over the MDB.

[00161] In some implementations, the zone criteria information 1110 specifies an authorization zone criterion 1124 (e.g., a baseline authorization zone threshold indicating a baseline RSSI that the mobile device 150 (or the application 140) is required to observe before being within the authorization zone of the payment module 100) and/or a payment zone criterion 1126 (e.g., a baseline payment zone threshold indicating a baseline RSSI that the mobile device 150 (or the application 140) is required to observe before being within the payment zone of the payment module 100). In some implementations, the baseline

Petitioner Exhibit 1002-1243

authorization zone threshold and the baseline payment zone threshold are default values determined by the server 130 or stored as variables by the application 140, in which case the authorization zone criterion 1124 and payment zone criterion 1126 are offsets to compensate for the strength and/or reception of the short-range communication capability (e.g., BLE radio/transceiver) of the payment module 100. Alternatively, zone criteria information 1110 includes a spread between the baseline authorization zone threshold and the baseline payment zone threshold. Thus, the mobile device 150 (or the application 140) determines the baseline authorization zone threshold and the baseline payment zone threshold based on the spread value and a default value for either the baseline authorization zone threshold or the baseline payment zone threshold. For example, the spread indicates -10 db and the default baseline payment zone threshold is -90 db; thus, the baseline authorization zone threshold is -80 db. Continuing with this example, after determining the baseline authorization zone threshold and the baseline payment zone threshold, the mobile device 150 (or the application 140) may further adjust the authorization zone threshold and/or the payment zone threshold based on the strength and/or reception of its short-range communication capability (i.e., BLE radio/transceiver).

[00162] Figure 24B is a block diagram of an authorization request 1130 sent by the mobile device 150 to the server 130 (e.g., in step 1004 of the process 1000 in Figure 23) in accordance with some implementations. In some implementations, the authorization request 1130 at least includes: a module ID 1102, a user ID 1134, and an authorization code 1104.

[00163] In some implementations, the module ID 1102 is a unique identifier corresponding to the payment module 100 that broadcast the 1100 that included the authorization code 1104.

[00164] In some implementations, the user ID 1134 is an identifier associated with the user of the mobile device 150 sending the authorization request 1130 to the server 130. In some implementations, the user ID 1134 is associated with the user account under which the user of the mobile device 150 is logged into the application 140.

[00165] In some implementations, the authorization code 1130 includes the authorization code 1104 included in the packet 1100 of information that was broadcast by the payment module 100.

[00166] Figure 24C is a block diagram of an authorization grant token 1140 sent by the server 130 to the mobile device 150 (e.g., in step 1008 of the process 1000 in Figure 23) in

Petitioner Exhibit 1002-1244

accordance with some implementations. In some implementations, in accordance with a determination that the authorization code 1136 included in the authorization request 1130 from the mobile device 150 is valid and that the user associated with the mobile device 150 has sufficient funds in his/her account for the payment processing system, the server 130 generates the authorization grant token 1140. In some implementations, the authorization grant token 1140 at least includes: a module ID 1102, a user ID 1134, an authorized amount 1146, (optionally) an expiration period offset 1148, and (optionally) the authorization code 1104.

[00167] In some implementations, the module ID 1102 is a unique identifier corresponding to the payment module 100 that broadcast the packet 1100 that included the authorization code 1104.

[00168] In some implementations, the user ID 1134 is an identifier associated with the user of the mobile device 150 that sent the authorization request 1130 to the server 130.

[00169] In some implementations, the authorized amount 1146 indicates a maximum amount for which the user of the mobile device 150 is authorized for a transaction using the authorization grant token 1140. For example, the authorized amount 1146 is predefined by the user of the mobile device 150 or by the server 130 based on a daily limit or based on the user's total account balance or based on a risk profile of the user correspond to the user ID 1134.

[00170] In some implementations, the expiration period 1148 offset indicates an offset to the amount of time that the payment module 100 holds the authorization grant token 1140 valid for initiation of a transaction with the machine 120 associated with the payment module 100. For example, the expiration period offset 1148 depends on the history and credit of the user of mobile device 150 or a period predefined by the user of mobile device 150.

[00171] In some implementations, the authorization grant token 1140 further includes the authorization code 1104 that was included in the authorization request 1130. In some implementations, when the authorization code 1104 is the hash value, the server 130 encrypts the authorization grant token 1140 including the hashed value with the shared secret encryption key associated with payment module 100. Subsequently, when mobile device 150 sends the authorization grant token 1140 to payment module 100 after detecting a trigger condition, the payment module 100 decrypts the authorization grant token 1140 using the secret key known only to server 130 and payment module 100 (which authenticates the

Petitioner Exhibit 1002-1245

message and the authorization grant), and then matches the hash value included in the decrypted authorization grant token 1140 to previously broadcast valid (unexpired) hash values (i.e., auth codes) to determine validity of the (which was known only by payment module 100).

[00172] Figure 24D illustrates a block diagram of transaction information 1150 generated by the payment module 100 (e.g., in step 1254 of the process 1250 in Figure 25B) in accordance with some implementations. In some implementations, the transaction information 1150 includes: a transaction ID 1152 for the respective transaction, a module ID 1154, a user ID 1156, (optionally) the authorization code 1158, transaction status information 1160, the transaction amount 1162, and other information 1164.

[00173] In some implementations, the transaction ID 1152 is a unique identifier corresponding to the respective transaction. In some implementations, the transaction ID 1152 is encoded based on or associated with the time and/or date on which and the location at which the respective transaction took place.

[00174] In some implementations, the module ID 1154 is a unique identifier corresponding to the payment module 100 that performed the respective transaction.

[00175] In some implementations, the user ID 1156 is an identifier associated with the user of the mobile device 150 that initiated the respective transaction.

[00176] In some implementations, the authorization code 1158 corresponds to the original authorization code (e.g., auth code 1104, Figures 24 A-24C) and/or authorization grant token (e.g., auth grant token 1140, Figure 24C) that was used to initiate the respective transaction. In some implementations, the authorization code 1156 is encrypted with a unique encryption key corresponding to the payment module 100.

[00177] In some implementations, the transaction status information 1160 includes an indication whether the respective transaction was completed, not-completed, or aborted. For example, the respective transaction is incomplete if a jam occurred at the payment accepting unit 120 and the user did not receive the product associated with the respective transaction. For example, if the user walks away from the payment accepting unit 120 after money was credited for the respective transaction, the respective transaction is aborted. In another example, if respective transaction times out after a predetermined time period because the user failed to select a product at the payment accepting unit 120, the respective transaction is

Petitioner Exhibit 1002-1246

aborted. In another example, if the user actuates a bill or coin return mechanism of the payment accepting unit 120, the respective transaction is aborted.

[00178] In some implementations, the transaction amount 1162 indicates the amount of the respective transaction or the amount of each of multiple transactions (e.g., in a multi-vend scenario). In some implementations, the transaction amount 1162 is encrypted with a unique encryption key corresponding to the payment module 100.

[00179] In some implementations, the other information 1164 includes other information related to the respective transaction such as the items dispensed by the payment accepting unit 120 and the type of transaction (e.g., coins, bills, credit card, manual mode, hands-free mode, etc.). In some implementations, the other information 1164 includes other information related to the payment module 100 and/or the payment accepting unit 120 associated with the payment module 100. For example, the other information 1164 includes a verification request to the server 130 in order to implement new firmware. In another example, the other information 1164 includes transaction information from one or more previous interrupted transactions. In another example, the other information 1164 includes transaction information for one or more transactions paid via bills and/or coins. In another example, the other information 1164 includes inventory information as to one or more products of the payment accepting unit 120.

[00180] Figure 25A illustrates a schematic flow diagram of a process 1200 for providing a representation of a machine event at a mobile device in accordance with some implementations. In some implementations, the payment processing system includes one or more payment modules 100 (e.g., each associated with a respective payment accepting unit 120 such an automatic retailing machine for dispensing goods and/or services), one or more mobile devices 150 (e.g., each executing the application 140 for the payment processing system either as a foreground or background process), and the server 130. The server 130 manages the payment processing system and, in some cases, supplies, operates, and/or manufactures the one or more payment modules 100. For brevity, the process 1200 will be described with respect to a respective payment module 100 associated with a respective payment accepting unit 120 (sometimes also herein called the "machine 120") and a respective mobile device 150 in the payment processing system.

[00181] In some implementations, the process 1200 occurs after the mobile device 150 sends the AuthGrant in Figure 8C. In some implementations, the process 1200 occurs after

Petitioner Exhibit 1002-1247

the mobile device 150 sends the authorization grant to the payment module 100 in operation 1012 of process 1000 in Figure 23.

[00182] The payment module 100 obtains (1202) an indication corresponding to an event at the machine 120. For example, after the process 1000 in Figure 23, the user of the mobile device 150 selects a product to purchase from the machine 120 by interacting with one or more input mechanisms of the machine 120 (e.g., buttons 126 or a touch screen display 124 shown in Figure 19), and the machine 120 dispenses the selected product. Continuing with this example, after the product is dispensed, the transaction is complete and the payment module 100 obtains an indication from the machine of the completed transaction. In some implementations, the indication includes the amount of the transaction and (optionally) machine status information associated with the machine 120 such as inventory information as to one or more products of the payment accepting unit 120 and/or the like. In some implementations, the indication includes status information indicating that the transaction was aborted (e.g., via actuation of a coin return mechanism at the machine 120) or that there was an error with the transaction (e.g., a vending jam or other malfunction with the machine 120).

[00183] After obtaining the indication corresponding to completion of the first transaction, the payment module 100 generates (1204) a notification corresponding to the event at the machine 120.

[00184] The payment module 100 sends (1206), via a short-range communication capability (e.g., BLE), the notification to the mobile device 150. In some embodiments, in addition to the notification corresponding to the event at machine 120, the payment module 100 sends a promotion or advertisement to the mobile device 150 that is targeted to the user of the mobile device 150 based on the transaction or the user ID included in the AuthGrant or authorization grant token that initiated the transaction. In some embodiments, in addition to the notification corresponding to the event at machine 120, the payment module 100 sends a pseudo randomly selected promotion or advertisement to the mobile device 150 that is selected from a set of promotions or advertisements stored by the payment module 100. For example, the promotion is a coupon for a free soda following the purchase of ten sodas from the machine 120 by the user of the mobile device 150. For example, the promotion is a random 50% off coupon or free soda coupon. For example, the transaction corresponds to a vended soda and the advertisement corresponds to a new soda from the same company that produces the vended soda.

Petitioner Exhibit 1002-1248

[00185] The mobile device 150 provides (1208) a representation of the notification. For example, in Figure 26A, the mobile device 150 displays user interface 1302 on touch screen 152 with a message 1306 that indicates that the first transaction is complete. For example, in Figure 26C, the mobile device 150 displays user interface 1320 on touch screen 152 with a message 1322 that indicates that the transaction was aborted. For example, in Figure 26D, the mobile device 150 displays user interface 1330 on touch screen 152 with a message 1332 that indicates that there was an error with the transaction. For example, the mobile device 150 also displays a representation of the promotion of advertisement on the user interface for the application 140.

[00186] Figure 25B illustrates a schematic flow diagram of a process 1250 for processing acknowledgement information in accordance with some implementations. In some implementations, the payment processing system includes one or more payment modules 100 (e.g., each associated with a respective payment accepting unit 120 such an automatic retailing machine for dispensing goods and/or services), one or more mobile devices 150 (e.g., each executing the application 140 for the payment processing system either as a foreground or background process), and the server 130. The server 130 manages the payment processing system and, in some cases, supplies, operates, and/or manufactures the one or more payment modules 100. For brevity, the process 1250 will be described with respect to a respective payment module 100 associated with a respective payment accepting unit 120 (machine 120) and a respective mobile device 150 in the payment processing system.

[00187] In some implementations, the process 1250 occurs after the mobile device 150 sends the AuthGrant in Figure 8C. In some implementations, the process 1250 occurs after the mobile device 150 sends the authorization grant to the payment module 100 in operation 1012 of process 1000 in Figure 23.

[00188] The payment module 100 obtains (1252) an indication corresponding to completion of a first transaction from the machine 120. For example, after the process 1000 in Figure 23, the user of the mobile device 150 selects a product to purchase from the machine 120 by interacting with one or more input mechanisms of the machine 120 (e.g., buttons 126 or a touch screen display 124 shown in Figure 19), and the machine 120 dispenses the selected product. Continuing with this example, after the product is dispensed, the transaction is complete and the payment module 100 obtains an indication from the machine of the completed transaction. In some implementations, the indication includes the amount of the transaction and (optionally) machine status information associated with the

Petitioner Exhibit 1002-1249

machine 120 such as inventory information as to one or more products of the payment accepting unit 120 and/or the like.

[00189] After obtaining the indication corresponding to completion of the first transaction, the payment module 100 generates (1254) a first notification with first transaction information based on the indication, and the payment module 100 stores the first transaction information. In some implementations, the first transaction information includes a transaction ID for the first transaction, a module ID corresponding to payment module 100, a user ID corresponding to the mobile device 150, transaction status information indicating that the first transaction is complete, and the transaction amount indicated by the indication. In some implementations, the payment module 100 retains the authorization code included in the original broadcasted packet and/or the authorization grant token and includes the authorization code in the first transaction information. In some implementations, the authorization code is encrypted with a secret key corresponding to the payment module 100, which is shared with the server 130 but not the mobile device 150. In some implementations, the first transaction information further includes other information such as the machine status information included in the first notification or transaction information corresponding to previous interrupted transaction(s). See Figure 24D and the accompanying text for further discussion regarding transaction information 1150.

[00190] The payment module 100 sends (1256), via a short-range communication capability (e.g., BLE), the first notification with first transaction information to the mobile device 150. In some embodiments, in addition to first transaction information corresponding to completion of the first transaction at machine 120, the first notification includes a promotion or advertisement to the mobile device 150 that is targeted to the user of the mobile device 150 based on the transaction or the user ID included in the AuthGrant or authorization grant token that initiated the transaction. In some embodiments, in addition to first transaction information corresponding to completion of the first transaction at machine 120, the first notification includes a pseudo randomly selected promotion or advertisement to the mobile device 150 that is selected from a set of promotions or advertisements stored by the payment module 100. For example, the promotion is a coupon for a free soda following the purchase of ten sodas from the machine 120 by the user of the mobile device 150. For example, the promotion is a random 50% off coupon or free soda coupon. For example, the transaction corresponds to a vended soda and the advertisement corresponds to a new soda from the same company that produces the vended soda.

Petitioner Exhibit 1002-1250

[00191] The mobile device 150 provides (1258) a representation of the first notification. For example, in Figure 26A, the mobile device 150 displays user interface 1302 on touch screen 152 with a message 1306 that indicates that the first transaction is complete. For example, the mobile device 150 also displays a representation of the promotion of advertisement on the user interface for the application 140.

[00192] The mobile device 150 sends (1260), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), the first transaction information to the server 130.

[00193] The server 130 processes (1262) the first transaction information. For example, the server 130 debits the account of the user associated with the user ID in the first transaction information in the amount indicated by the first transaction information.

[00194] The server 130 sends (1264), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), first acknowledgment information to the mobile device 150. In some implementations, the first acknowledgment information acknowledges that the server 130 received the first transaction information. In some implementations, the first acknowledgment information includes the user ID, the module ID, the transaction ID, and (optionally) the authorization grant included in the transaction information (e.g., auth grant 1158, Figure 24D).

[00195] After receiving the first acknowledgement information, the mobile device 150 sends (1266), via a short-range communication capability (e.g., BLE), the first acknowledgment information to the payment module 100.

[00196] After receiving the first acknowledgment information, the payment module 100 deletes (1268) the stored first transaction information.

[00197] Attention is now directed towards implementations of user interfaces and associated processes that may be implemented on the mobile device 150 with zero or more speakers, zero or more microphones, and a display. For example, the display is a touch screen (sometimes also herein called a "touch screen display") enabled to receive one or more contacts and display information (e.g., media content, websites and web pages thereof, user interface for the application 140, and/or user interfaces for applications). Figures 26A-26D illustrate example user interfaces for providing a representation of a machine event at a mobile device in accordance with some implementations.

Petitioner Exhibit 1002-1251

[00198] Figures 26A-26D show user interfaces displayed on mobile device 150 (e.g., a mobile phone); however, one skilled in the art will appreciate that the user interfaces shown in Figures 26A-26D may be implemented on other similar computing devices. The user interfaces in Figures 26A-26D are used to illustrate the processes described herein, including the process described with respect to Figures 25A-25B and 27A-27B.

[00199] For example, a user of the mobile device 150 approaches a machine 120 (e.g., vending machine 78x928 as shown in Figures 10A-10D) and executes application 140 on the mobile device 150 so as to perform an electronic transaction with the machine 120. For example, with reference to Figures 10C-10D, the user of the mobile device 150 initiates a transaction with the machine 120 (e.g., vending machine 78x928) by performing a swipe gesture at a location corresponding to the representation of the dollar bill (e.g., a substantially vertical swipe gesture from a location corresponding to the representation of the dollar bill to the top edge of the mobile device 150).

[00200] Figure 26A illustrates the mobile device 150 displaying a user interface 1302 of the application 140 on touch screen 152 after the user of the mobile device 150 initiates and performs a transaction with the machine 120. In Figure 26A, the user interface 1302 includes prepaid balance 1304 which indicates that $1.00 has been deducted from the prepaid balance after performing a transaction with the machine 120 as compared to the prepaid balance in Figure 10C-10D (i.e., $9.00 in Figures 10C-10D and $8.00 in Figure 26A). In Figure 26A, the user interface 1302 also includes a message 1306 indicating that the transaction with the machine 120 is complete.

[00201] Figure 26B illustrates the mobile device 150 displaying a user interface 1310 of the application 140 on touch screen 152 after the user of the mobile device 150 initiates a transaction with the machine 120 and an error with the transaction occurs or the transaction is aborted. In Figure 26B, the user interface 1310 shows the representation of the dollar bill sliding onto the touch screen 152 (e.g., in a substantially top to bottom manner). In Figure 26B, the interface 1310 includes prepaid balance 1312 which indicates that no money has been deducted from the prepaid balance after performing a transaction with the machine 120 as compared to the prepaid balance in Figure 10C-10D (i.e., $9.00 in Figures 10C-10D and $9.00 in Figure 26B).

[00202] Figure 26C illustrates the mobile device 150 displaying a user interface 1320 of the application 140 on touch screen 152 after the representation of the dollar bill slides onto the touch screen 152 in Figure 26B due to the transaction being aborted. For example,

Petitioner Exhibit 1002-1252

the user aborts the transaction by actuating a coin return mechanism of the machine 120. In another example, the user aborts the transaction by selection an abort affordance on the interface of the application 140 (not shown). In Figure 26C, the user interface 1320 includes a message 1322 indicating that the transaction with the machine 120 was aborted and that the user's account was not debited for the aborted transaction.

[00203] Figure 26D illustrates the mobile device 150 displaying a user interface 1330 of the application 140 on touch screen 152 after the representation of the dollar bill slides onto the touch screen 152 in Figure 26B due to the occurrence of an error with the transaction. For example, a malfunction with the machine 120 (e.g., a vending jam or stuck item) causes the error to occur. In Figure 26D, the user interface 1330 is associated with the application 140 executed on the mobile device 150. In Figure 26D, the user interface 1330 includes a message 1332 indicating that an error occurred during the transaction with the machine 120 and that the user's account was not debited for the transaction.

[00204] Figures 27A-27B illustrate a flowchart diagram of a method 1400 of presenting representations of payment accepting unit events in accordance with some implementations. In some implementations, the method 1400 is performed by a device with one or more processors, memory, one or more output devices, and two or more communication capabilities. For example, in some implementations, the method 1400 is performed by the mobile device 150 (Figures 5 and 21) or a component thereof (e.g., the application 140). In some implementations, the method 1400 is governed by instructions that are stored in a non-transitory computer readable storage medium (e.g., the memory 860, Figure 21) and the instructions are executed by one or more processors (e.g., the processing unit 850, Figure 21) of the device. Optional operations are indicated by dashed lines (e.g., boxes with dashed-line borders).

[00205] After sending a request to a payment module via a first communication capability transaction to initiate a transaction with a payment accepting unit (e.g., an offline-payment operated machine such as a vending machine or kiosk) associated with the payment module, the mobile device obtains (1402) a notification from the payment module via the first communication capability, where the notification indicates an event at the payment accepting unit associated with the payment module. In some implementations, method 1400 occurs after the mobile device 150 sends the AuthGrant in Figure 8C. In some implementations, method 1400 occurs after the mobile device 150 sends the authorization grant to the payment module 100 in operation 1012 of process 1000 in Figure 23. Operation

Petitioner Exhibit 1002-1253

1206 of Figure 25A, for example, shows the mobile device 150 receiving a notification sent by the payment module 100 (e.g., the adapter module 100, Figures 5 and 20) sent via the first communication capability (e.g., a short-range communication technology/protocol such as BLE). The notification indicates an event at the payment accepting unit (e.g., the payment accepting unit 120, Figures 5 and 19) (sometimes also herein called "machine 120") associated with the payment module 100.

[00206] In some implementations, the first communication capability corresponds (1404) to a short-range communication protocol. As described above, the short-range communication protocols include BLE, NFC, and/or other protocols utilizing non-persistent communication channels.

[00207] In response to obtaining the notification, the mobile device provides (1406) a representation of the notification to a user of the mobile device via the one or more output devices of the mobile device. For example, in Figure 26A, the mobile device 150 displays user interface 1302 on touch screen 152 with a message 1306 that indicates that the first transaction is complete. For example, in Figure 26C, the mobile device 150 displays user interface 1320 on touch screen 152 with a message 1322 that indicates that the transaction was aborted. For example, in Figure 26D, the mobile device 150 displays user interface 1330 on touch screen 152 with a message 1332 that indicates that there was an error with the transaction.

[00208] In some implementations, the one or more output devices of the mobile device include (1408) at least one of: a display, one or more speakers, one or more LEDs, and a vibration mechanism. For example, the mobile device 150 includes one or more of a display (e.g., the touch screen 152, Figures 10A-10D), one or more speakers, one or more LEDs, and a vibration mechanism.

[00209] In some implementations, the representation of the notification is at least one of (1410): a message displayed on the display of the mobile device; a banner notification displayed on a display of the mobile device; a vibration alert from the vibration mechanism of the mobile device; an aural alert from the one or more speakers of the mobile device; and a visual alert from the one or more LEDs of the mobile device. For example, in Figures 26B-26D, the representation of the notification includes messages 1306, 1322, and 1332 displayed on the touch screen 152 of the mobile device 150. In another example, the representation of the notification is a predefined sequence of vibrations provided by the vibration mechanism of the mobile device 150. In another example, the representation of the notification is a

Petitioner Exhibit 1002-1254

predefined sequence of tones provided by the one or more speakers of the mobile device 150. In another example, the representation of the notification is a predefined sequence of blinking LEDs of the mobile device 150.

[00210] In some implementations, the notification indicates (1412) abortion of a transaction initiated by the user of the mobile device. In Figure 26C, for example, the user interface 1320 includes the message 1322 indicating that the transaction has been aborted. For example, the user aborts the transaction by actuating a coin return mechanism of the machine 120. In another example, the user aborts the transaction by selection an abort affordance on the interface of the application 140 (not shown).

[00211] In some implementations, the notification indicates (1414) completion of a transaction between the user of the mobile device and the payment accepting unit. In Figure 26A, for example, the user interface 1302 includes the message 1306 indicating that completion of the transaction with the machine 120 initiated by the user of the mobile device 150.

[00212] In some implementations, the notification indicating completion of the transaction at least includes (1416) an amount of the completed transaction. In Figure 26A, for example, the user interface 1302 includes prepaid balance 1304 which indicates that $1.00 has been deducted from the prepaid balance after performing a transaction with the machine 120 as compared to the prepaid balance in Figure 10C-10D (i.e., $9.00 in Figures 10C-10D and $8.00 in Figure 26A).

[00213] In some implementations, the mobile device sends (1418) at least a portion of the notification to a server via a second communication capability distinct from the first communication capability. Operation 1260 of Figure 25B, for example, shows the mobile device 150 sending first transaction information to the server 130 for a completed transaction via the second communication capability (e.g., a long-range communication protocols such as Wi-Fi, CDMA, GSM, and/or the like). For example, the first transaction information at least includes the amount of the first completed transaction.

[00214] In some implementations, the first communication capability corresponds (1420) to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol. For example, the first communication capability of the mobile device 150 is a radio/transceiver means for communicating via one or more short-range communication protocols such as BLE, NFC, and/or the like (i.e., a non-

Petitioner Exhibit 1002-1255

persistent communication channel). For example, the second communication capability of the mobile device 150 is a radio/transceiver means for communicating via one or more long-range communication protocols such as Wi-Fi, CDMA, GSM, and/or the like.

[00215] In some implementations, the notification indicates (1422) failure of a transaction initiated by the user of the mobile device or a malfunction associated with the payment accepting unit. In Figure 26D, for example, the user interface 1330 includes the message 1332 indicating that there was an error with the transaction. For example, the transaction fails due to a vending jam or other malfunction. In another example, the payment accepting unit experiences a malfunction due to an open door or the like. In some implementations, at least a portion of the failure/malfunction notification is sent to the sever 130 and an alert is subsequently sent to the operator of the payment accepting unit (e.g., the machine 120) by the server 130.

[00216] It should be understood that the particular order in which the operations in Figures 27A-27B have been described is merely for example purposes and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to other methods described herein are also applicable in an analogous manner to the method 1400 described above with respect to Figures 27A-27B.

[00217] Figure 28A illustrates a block diagram of an offline-payment operated machine 1500 in accordance with some implementations. For example, the offline-payment operated machine 1500 (e.g., a form of the machine 120) is an electro-mechanical machine capable of accepting currency (e.g., coins), which is not connected to any networks (e.g., telephone, cellular, or Wi-Fi). For example, the offline-payment operated machine 1500 is a washer or dryer at a laundromat, a parking meter, a car wash payment kiosk, a video gaming console (i.e., a coin-operated arcade game), a coin-operated pool table, a coin-operated dart machine, a coin-operation vacuum or air pump (such as those commonly found at gas stations), or other offline-payment operated machine that dispenses goods (e.g., products stocked by the machine 1500) and/or provides services (e.g., allows a user to use the services, such as playing a video game, using the washer or dryer, etc.). Offline-payment operated machines are, in some circumstances, unattended in the sense that no operator is physically near the machine while the machine is operating normally. Therefore, these machines are

Petitioner Exhibit 1002-1256

also referred to herein as "unattended machines," "unattended coin-operated machines," and "unattended offline-payment operated machines."

[00218] In Figure 28A, the offline-payment operated machine 1500 includes a microswitch 1502, a control unit 1506, a power supply 1508, a transistor 1510, and an operation unit 1512. The components of the offline-payment operated machine 1500 in Figure 28A are examples and one of skill in the art will appreciate that various other components may be included in or excluded from the offline-payment operated machine 1500.

[00219] In Figure 28A, the microswitch 1502 is a leveraged microswitch with lever 1504. For example, the microswitch 1502 is a CHERRY BRAND™ microswitch with a normally open terminal ("NO"), a normally closed terminal ("NC"), and a common terminal. For example, the lever 1504 is incorporated into a coin slot of the offline-payment operated machine 1500 and is depressed whenever a coin slides down the coin slot into a coin reservoir of the offline-payment operated machine 1500 (not shown). For example, when the lever 1504 is depressed and the microswitch 1502 is wired in the NO configuration as shown in Figure 28A, the switch is closed. Continuing with this example, when the switch is closed, control unit 1506 receives a pulse (i.e., a payment acceptance signal) from the common terminal of the microswitch 1502 indicating depression of the lever 1504 from the reception of a US quarter (i.e., $0.25) or coin of another value.

[00220] In some implementations, when the control unit 1506 receives a preset sequence of payment acceptance signals indicative of a preset number of coins being received by the microswitch 1502, the control unit 1506 initiates the operation of the offline-payment operated machine 1500. For example, after receiving the preset sequence of payment acceptance signals (e.g., three pulses indicating reception of three US quarters), the control unit 1506 initiates operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512. For example, the operation unit 1512 is a motor of a dryer which begins spinning once current flows from the power supply 1508.

[00221] In Figure 28A, payment module 1520 (e.g., a form of the adapter module 100, Figures 5 and 20) is configured to be installed in the offline-payment operated machine 1500 so as to retrofit the offline-payment operated machine 1500 to be able to accept electronic payments. In some implementations, the payment module 1520 is referred to herein as a pulse-providing device 1520 (as discussed below in reference to Figures 31-33). In some

Petitioner Exhibit 1002-1257

implementations, the payment module 1520 includes all or some of the components included in adapter module 100 in Figure 20 such as processing unit 750, memory 760, a security unit 755, and a communications unit 770. In some implementations, the payment module 1520 also includes a first interface module 1522, a second interface module 1524, and a lead 1536 for drawing power from power supply 1508 of the offline-payment operated machine 1500.

[00222] In Figure 28A, the first interface module 1522 is configured to sample payment acceptance signals from the microswitch 1502 (e.g., a coin receiving switch) via lead 1532 of the offline-payment operated machine 1500. For example, the payment acceptance signals are indicative of a coin being received by the microswitch 1502 which depress lever 1504. In Figure 28A, the second interface module 1524 is configured to sample control signals from the control unit 1506 of the offline-payment operated machine 1500 via lead 1534 that initiates an operation of the offline-payment operated machine (e.g., the application of current to the gate of the transistor 1510) in response to receiving a preset sequence of payment acceptance signals from the microswitch 1502 (e.g., the coin receiving switch) indicative of the preset number of coins.

[00223] In some implementations, even though a particular unattended machine (e.g., 1500, Figure 28A) is not connected to any network and an operator is not located in proximity to the particular unattended machine, the unattended machine is still able accept remotely-configured options (e.g., multi-credit pricing options) that are configured at a server and sent to the pulse-providing device 1520 that is coupled with the particular unattended machine via an encrypted exchange of information with a mobile phone. In some implementations, the encrypted exchange of information includes instructions or data that allow the pulse-providing device 1520 to provide electric pulses that are determined in accordance with a remotely-configured option that is selected by a user of mobile device (e.g., via a user interface display in an application 140, as pictured in Figure 32). Additional details are also provided below in reference to Figures 31-33.

[00224] Figure 28B illustrates signals sampled by the payment module 1520 in accordance with some implementations. In Figure 28B, sample 1550 represents a preset sequence of payment acceptance signals sampled by the first interface module 1522 via lead 1532 that are sent from the microswitch 1502 to the control unit 1506. For example, the preset sequence of payment acceptance signals indicative of the preset number of coins include pulses (i.e., payment acceptance signals) 1552, 1554, 1556, and 1558. For example, the leading edges of pulses 1552, 1554, 1556, and 1558 at times 1582, 1584, 1586, and 1588

Petitioner Exhibit 1002-1258

indicate reception of a coin by microswitch 1502 which causes the switch to close when wired in the NO configuration as shown in Figure 28A. In Figure 28B, sample 1570 represents a control signal sampled by the second interface module 1524 via lead 1534 that is sent from the control unit 1506 to transistor 1510. In Figure 28B, the sample 1570 includes a pulse 1572 that is sent from the control unit 1506 to transistor 1510 at time 1590 after receiving the preset sequence of payment acceptance signals from the microswitch 1502 (i.e., pulses 1552, 1554, 1556, and 1558).

[00225] Figures 29A-29B illustrate a flowchart diagram of a method of retrofitting an offline-payment operated machine to accept electronic payments in accordance with some implementations. In some implementations, the method 1600 is performed by a payment module with one or more processors and memory. In some implementations, the payment module also includes a short-range communication capability corresponding to a short-range communication protocol (e.g., a non-persistent communication channel such as BLE, NFC, and/or the like), where the short-range communication capability is configured to communicate with one or more mobile devices, where each of the one or more mobile devices is configured with a complimentary short-range communication capability and a long-range communication capability corresponding to a long-range communication protocol (e.g., Wi-Fi, CDMA, GSM, and/or the like).

[00226] In some implementations, the payment module is coupled with an offline-payment operated machine (e.g., the payment accepting unit 120, Figures 5 and 19 (sometimes also herein called "machine 120"), or the offline-payment operated machine 1500, Figure 28A) such as dryer or washer in a laundromat, a parking meter, a car wash payment kiosk, or the like. In some implementations, the offline-payment operated machine includes a coin receiving switch (e.g., the microswitch 1502, Figure 28A) and a control unit (e.g., the control unit 1506, Figure 28A). In some implementations, the payment module further includes: (A) a first interface module (e.g., the first interface module 1522, Figure 28A) configured to sample payment acceptance signals from the coin receiving switch of the offline-payment operated machine, where the signals are indicative of a coin being received by the coin receiving switch; and (B) a second interface module (e.g., the second interface module 1524, Figure 28A) configured to sample control signals from the control unit of the offline-payment operated machine that initiate an operation of the offline-payment operated machine in response to receiving a preset sequence of payment acceptance signals from the coin receiving switch indicative of the preset number of coins. By sampling and storing these

Petitioner Exhibit 1002-1259

signals, the payment module 1520 is able to simulate operation of a respective coin receiving switch in response to receiving the correct/preset number of coins so as to trigger operation of the offline-payment operated machine in response to completion of an electronic payment.

[00227] For example, in some implementations, the method 1600 is performed by the adapter module 100 (Figures 5 and 20) or payment module 1520 (Figure 28A). In some implementations, the method 1600 is governed by instructions that are stored in a non-transitory computer readable storage medium (e.g., the memory 760, Figure 20) and the instructions are executed by one or more processors (e.g., the processing unit 750, Figure 20) of the payment module. Optional operations are indicated by dashed lines (e.g., boxes with dashed-line borders).

[00228] In some implementations, the payment module detects (1602), via the first interface module, a preset sequence of payment acceptance signals from the coin receiving switch that causes the control unit to initiate the operation of the offline-payment operated machine, where the preset sequence of payment acceptance signals are indicative of a preset number of coins received by the coin receiving switch. For example, with reference to Figures 28A-28B, the first interface module 1522 of the payment module 1520 samples payment acceptance signals via lead 1532 from the microswitch 1502 to the control unit 1506. For example, each of the payment acceptance signals is indicative of reception of a coin by the microswitch 1502. Continuing with this example, the second interface module 1524 of the payment module 1520 samples control signals via lead 1534 from the control unit 1506 to the transistor 1510. The payment module 1520 detects a preset sequence of payment acceptance signals from the microswitch 1502 that causes the control unit 1506 to apply a current to the gate of the transistor 1510 (e.g., the control signals). For example, the preset sequence of payment acceptance signals is indicative of a preset number of coins received by the microswitch 1502 to cause operation of the offline-payment operated machine 1500. For example, the application of current to the gate of the transistor 1510 allows current to flow from the power supply 1508 to the operation unit 1512 so that the operation. For example, the operation unit 1512 is a motor of a dryer which begins spinning once current flows from the power supply 1508.

[00229] In some implementations, the payment module determines (1604) the predefined signal sequence to emulate the preset sequence of payment acceptance signals from the coin receiving switch. In some implementations, after detecting the preset sequence of payment acceptance signals that causes the control unit 1506 to initiate the operation of the

Petitioner Exhibit 1002-1260

offline-payment operated machine 1500, the payment module 1520 determines a predefined signal sequence to emulate the preset sequence of payment acceptance signals. In some implementations, the money value associated with each pulse in the preset sequence of payment acceptance signals from the microswitch 1502, indicative of the preset number of coins to initiate the operation of the offline-payment operated machine 1500, is a default currency (e.g., USD) and amount (e.g., $0.25) set in the firmware of the payment module 1520. In some implementations, the money value associated with the each pulse in the preset sequence of payment acceptance signals from the microswitch 1502, indicative of the preset number of coins to initiate the operation of the offline-payment operated machine 1500, is set by the server 130 and can be changed remotely by using the mobile device 150 as a communications bridge to send information indicating the value of a pulse from the server 130 to the mobile device 150 via the second communication capability (e.g., GSM, CDMA, or Wi-Fi) and forwarding the information from the mobile device to the payment module 1520 via the first communication capability (e.g., BLE). For instance, in most cases, each pulse is US $0.25. Additional details regarding remotely configuring options for offline-payment operated machines are also provided below in reference to Figures 31-33.

[00230] In some implementations, determining the predefined signal sequence includes (1606) at least one of: identifying a count of pulses in the present sequence of payment acceptance signals; identifying amplitude of pulses in the present sequence of payment acceptance signals; identifying shape of pulses in the present sequence of payment acceptance signals; and identifying an interval between pulses. In some implementations, after detecting the preset sequence of payment acceptance signals (e.g., the sample 1550, Figure 28B), the payment module 1520 determines a predefined signal sequence to emulate the preset sequence of payment acceptance signals by identifying a count of pulses in the preset sequence of payment acceptance signals, an interval between pulses in the preset sequence of payment acceptance signals, the shape of pulses in the preset sequence of payment acceptance signals, and an amplitude of pulses in the preset sequence of payment acceptance signals.

[00231] The payment module receives (1608) a request via the short-range communication capability from a respective mobile device to perform an operation of the offline-payment operated machine. For example, with reference to Figure 8C, the payment module 1520 (Figure 28A) receives the AuthGrant from the mobile device 150 via the short-range communication capability (e.g., BLE) indicating that the user of the mobile device 150

Petitioner Exhibit 1002-1261

wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A). For example with reference to operation 1012 in Figure 23, the payment module 1520 (Figure 28A) receives an authorization grant token from the mobile device 150 via the short-range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A).

[00232] The payment module validates (1610) the request. Validation of the request indicates (1612) that the respective mobile device is authorized to initiate payment for the operation by a remote server via the long-range communication capability. In some implementations, the payment module 1520 validates the request from the mobile device 150 by determining whether the AuthGrant or the authorization grant token includes a valid authorization code.

[00233] In accordance with a determination that the request is valid, the payment module causes (1614) the payment operated machine to perform the operation by issuing a predefined signal sequence to the control unit, where the predefined signal sequence emulates a signal sequence that would be issued by the coin receiving switch in response to receiving a preset number of coins. For example, with reference to Figure 28B, the payment module 1520 issues a predefined signal sequence with first interface module 1522 to the control unit 1506 that emulates sample 1550 in Figure 28B. Continuing with this example, in response to receiving the predefined signal sequence from the payment module 1520 control unit 1506 causes initiation of the operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512. In some implementations, the control unit 1506 causes initiation of the operation by setting a timer to an amount of time corresponding to the preset number of coins whereby current flows to the gate of the transistor 1510 for the set amount of time. For example, the preset number of coins is a number of a coins required to run the offline-payment operated machine 1500 by for a default amount of time and subsequent coins may be added to extend the amount of time that the offline-payment operated machine 1500 by will run. In some implementations, the preset number of coins is a number of a coins required to cause the offline-payment operated machine 1500 to dispense a purchased item, such as laundry detergent.

[00234] Alternatively, in some implementations, in accordance with a determination that the request is valid, the offline-payment operated machine 1500 displays credit to the user (e.g., via one of the displays 122 or 124 shown in Figure 19) and the user interacts with

Petitioner Exhibit 1002-1262

the input mechanisms of the offline-payment operated machine 1500 120 (e.g., via the buttons 126 or a touch screen display 124 shown in Figure 19) to perform the operation of the machine. For example, if the offline-payment operated machine 1500 is a dryer, the user of the mobile device 150 selects the appropriate spin cycle via input mechanisms of the dryer, and when the user of the mobile device 150 selects a start/run input mechanism of the dryer, control unit 1506 of the dryer causes initiation of the operation of the dryer (e.g., starting a motor that corresponds to operation unit 1512 in Figure 28A).

[00235] In some implementations, instead of issuing the predefined signal sequence to the control unit, the pulse-providing device 1520 issues a remotely-configured signal sequence (i.e., configured remotely by an operator and sent to the pulse-providing device 1520 via the mobile device with the authorization grant) that corresponds to payment provided by the user via the mobile device. In some implementations, the remotely-configured signal sequence does not correspond to the predefined signal sequence for an equivalent number of coins. For example, if the user chooses to send a payment of one dollar to the unattended machine (via the pulse-providing device 1520), the predefined signal sequence observed by the pulse-providing device 1520 may indicate that four predefined pulses are to be provided (in order to simulate pulses provided in response to the receipt of four quarters by the unattended machine, but instead of providing those four predefined pulses, the pulse-providing device 1520 instead might sent five remotely-configured pulses. In this way, operators are able to easily configure new pricing options, without having to physically interacted with their remotely-located unattended machines. Additional details are provided below in reference to Figures 31-33.

[00236] In some implementations, prior to sending the operation information and after causing the offline-payment operated machine to perform the operation by issuing the predefined signal sequence to the control unit, the payment module obtains (1616) a notification from the offline-payment operated machine indicating initiation of the operation of the offline-payment operated machine and the preset number of coins. For example, after issuing the preset signal sequence to control unit 1506, the payment module 1520 (Figure 28A) obtains a notification indicating that the control unit 1506 sent control signals to initiate operation of the offline-payment operated machine 1500 in response to receiving the predefined signal sequence. For example, the notification is obtained by the second interface module 1524 (e.g., the sample 1570, Figure 28B) sampling controls signals sent by control

Petitioner Exhibit 1002-1263

unit 1506 (e.g., application of current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512).

[00237] In response to receiving the notification, the payment module (1618): generates the operation information based at least in part on the notification; and stores the generated operation information in the memory. For example, after obtaining the notification, the payment module 1520 (Figure 28A) generates operation information corresponding to performance of the operation and the preset number of coins associated with the predefined signal sequence (e.g., the amount required to initiate operation of the offline-payment operated machine 1500) and stores the operation information in memory local to the payment module 1520 (e.g., the memory 760, Figure 20).

[00238] In some implementations, the payment module sends (1620) operation information corresponding to the operation to the respective mobile device via the short-range communication capability. For example, after operation 1618, the payment module 1520 (Figure 28A) sends the operation information to the mobile device 150 via the first communication capability of the mobile device 150 such as a radio/transceiver means for communicating via one or more short-range communication protocols such as BLE, NFC, and/or the like (i.e., a non-persistent communication channel)

[00239] It should be understood that the particular order in which the operations in Figures 29A-29B have been described is merely for example purposes and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein (e.g., by including details from the method 1700 in Figure 30 and/or the method 3200 of Figure 32). Additionally, it should be noted that details of other processes described herein with respect to other methods described herein (e.g., the method 1700 in Figure 30 or the method 3200 of Figure 32) are also applicable in an analogous manner to the method 1600 described above with respect to Figures 29A-29B.

[00240] Figure 30 illustrates a flowchart diagram of a method 1700 of enabling a payment operated machine to accept electronic payments in accordance with some implementations. In some implementations, the method 1700 is performed by an offline-payment operated machine (e.g., the payment accepting unit 120, Figures 5 and 19 (sometimes also herein called "machine 120"), or the offline-payment operated machine 1500, Figure 28A) such as dryer or washer in a laundromat, a parking meter, a car wash payment kiosk, or the like.

Petitioner Exhibit 1002-1264

[00241] In some implementations, the offline-payment operated machine includes a control unit (e.g., the control unit 1506, Figure 28A), memory, and a coin receiving switch (e.g., the microswitch 1502, Figure 28A). In some implementations, the offline-payment operated machine also includes a short-range communication capability corresponding to a short-range communication protocol (e.g., a non-persistent communication channel such as BLE, NFC, and/or the like), where the short-range communication capability is configured to communicate with one or more mobile devices, where each of the one or more mobile devices is configured with a complimentary short-range communication capability and a long-range communication capability corresponding to a long-range communication protocol (e.g., Wi-Fi, CDMA, GSM, and/or the like). For example, in some implementations, the method 1700 is performed by the machine 120, (Figures 5 and 19). In some implementations, the method 1700 is governed by instructions that are stored in a non-transitory computer readable storage medium and the instructions are executed by the control unit of the offline-payment operated machine.

[00242] The offline-payment operated machine receives (1702) a request via a short-range communication capability from a respective mobile device to perform an operation of the offline-payment operated machine. For example, with reference to Figure 8C, the payment module 1520 (Figure 28A) receives the AuthGrant from the mobile device 150 via the short-range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A). For example with reference to operation 1012 in Figure 23, the payment module 1520 (Figure 28A) receives an authorization grant token from the mobile device 150 via the short-range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A).

[00243] The offline-payment operated machine validates (1704) the request. Validation of the request indicates (1706) that the respective mobile device is authorized to initiate payment for the operation by a remote server via the long-range communication capability. In some implementations, the payment module 1520 validates the request from the mobile device 150 by determining whether the AuthGrant or the authorization grant token includes a valid authorization code.

[00244] In accordance with a determination that the request is valid, the offline-payment operated machine performs (1708) the operation by issuing a predefined signal

Petitioner Exhibit 1002-1265

sequence to the control unit, where the predefined signal sequence emulates a preset number of coins received by the coin receiving switch. For example, in accordance with a determination that the request is valid, the offline-payment operated machine or a component thereof issues a predefined signal sequence to the control unit 1506 that emulates sample 1550 in Figure 28B. Continuing with this example, in response to receiving the predefined signal sequence from the payment module 1520, control unit 1506 causes initiation of the operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512. In another example, in accordance with a determination that the request is valid, the control unit 1506 causes initiation of the operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512.

[00245] It should be understood that the particular order in which the operations in Figure 30 have been described is merely for example purposes and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein (e.g., by including details from the method 1600 or the method 3200). Additionally, it should be noted that details of other processes described herein with respect to other methods described herein (e.g., the method 1600 in Figures 29A-29B and the method 3200 of Figure 32) are also applicable in an analogous manner to the method 1700 described above with respect to Figure 30.

[00246] Figure 31 is a schematic flow diagram of a process 3100 for determining electric pulses to provide to an unattended machine based on remotely configured options for the unattended machine, in accordance with some implementations.

[00247] In some implementations, the process 3100 for determining electric pulses to provide to an unattended machine is performed via one or more components of the payment processing systems described herein. As shown in Figure 31, the one or more components include an unattended machine 1500 (Figure 28A), a module (e.g., a pulse-providing device 1520 that is coupled with the unattended machine via an internal interface of the unattended machine), an application 140 (e.g., a mobile payment application) that is executing on a mobile device 150, and a server 130.

[00248] In some implementations, the application 140 is in communication with the pulse-providing device 1520 (e.g., via transmission of bluetooth signals, such as bluetooth

Petitioner Exhibit 1002-1266

low energy signals (BLE)) that is coupled with the unattended machine 1520. The pulse-providing device 1520 advertises an authorization code (3102) and the application 140 receives the advertised broadcast from the pulse-providing device 1520. The application 140 then requests authorization from the server 130 (3104). In some implementations, the server 130 creates an authorization grant using a default pricing option for the machine, encrypts the authorization grant, and transmits it to the mobile device (3106). Authorization requests and the creation of authorization grants are explained in detail above and, in particular, in reference to Figures 8A-8G.

[00249] The user at this time can chose to either send a payment amount that corresponds to the default pricing option to the pulse-providing device 1520, or alternatively, select from another pricing option (3108) that was received from the server. In some implementations, the application 140 executing on the mobile device 150 also displays a user interface that allows for selecting from the pricing options received from the server (an example user interface is shown in Figure 32).

[00250] The user, for example, may select a third option that is displayed within the user interface (e.g., the option for "4 credit: $1:00," pictured in Figure 33). The application 140 then causes the mobile device 150 to send a new authorization request to the server this time accompanied by the index value 3 (3110). Upon receiving the authorization request, the server determines the value of the pricing option with index 3 for that particular machine, creates a new authorization grant, and sends that to the mobile device (3112).

[00251] In some implementations, payment is then sent to the unattended machine 1520 after satisfaction of a trigger condition (3114) (e.g., a proximity-based trigger condition based on proximity of the mobile device 150 to the pulse-providing device 1520 or a user-input-based trigger condition that is based on user input (such as a swipe gesture) that is received within the application 140). In some implementations, the authorization grant that is sent to the payment module (3116) includes pricing for the amount of the pricing referenced by index value 3.

[00252] Additionally, the authorization grant also includes information for the number of pulses (and, in some instances, characteristics of the pulses, such as pulse width that are explained above) that the pulse-providing device 1520 should send to the unattended machine 1520. The pulse-providing device 1520 decrypts the authorization grant and retrieves the information for the number of pulses to provide and then provides pulses to the unattended machine in accordance with the retrieved information (3118). The user is then able to

Petitioner Exhibit 1002-1267

interact with the unattended machine (e.g., to have as many plays at a video game console as the user paid for, to be able to use a coin-operated laundry machine a number of times based on payment provided by the user, and the like based on the type of unattended machine 1520).

[00253] In order to ensure that the user's account is debited properly, the process 3100 also includes sending transaction completion information and uploading that information to the server 130 (3122-3124). Details regarding the processing and sending of transaction completion information (also referred to as operation information) are provided above in reference to operations 1616-1620 of Figure 29B.

[00254] In some implementations, a data structure is utilized that decouples the pricing and pulses to create a variety of pricing options. More specifically, a pricing table as follows can be possible: 25 cents = 1 pulse = 1 credit; 50 cents = 2 pulses = 2 credits; 1.00 = 5 pulses = 5 credits; and 2.00 = 12 pulses = 12 credit.

[00255] In some implementations, the mobile device 150 and the application 140 are not trusted to tell the unattended machine how many credits it is to receive. These components are also not trusted to determine the amount of credits. In some implementations, all that information is instead configured at the server 130. The user has access to information about the pricing matrix including number of credits (as presented in a user interface shown in the application 140, such as that shown in Figure 32), and while it appears to user that the selection is being made at the mobile app, in some implementations the user is simply selecting an index value. In some implementations, the index value is sent to the server 130 where it looks up the pricing and credits, encrypts the details, and sends back to the application 140 (e.g., as an authorization grant) with an encryption key that can only be read by the particular pulse-providing device 1520 that is coupled with that particular unattended machine (for which the authorization grant was generated).

[00256] In some implementations, authorizations for all pricing options can be sent down to the application (from the server 130) at the time of the original authorization request (e.g., at the time when the requested authorization for a default authorization grant is received by the server 130, such as 3104 in Figure 31). In some implementations, when an index value is subsequently selected via a user interface that is provided to the user within the application 140 (e.g., that shown in Figure 32), an appropriate indexed authorization grant is then sent to the pulse-providing device 1520. In some implementations, all authorization grants have the same authorization code, so once an authorization grant with the same

Petitioner Exhibit 1002-1268

authorization code is sent to the pulse-providing device 1520, the remaining authorization grants are invalidated since the pulse-providing device 1520 will accept only one authorization grant with the same authorization code (as explained in detail above in reference to Figures 8A-8G).

[00257] In some implementations, the amount and number of pulses are dissociated and be in any number independent of the value of pulse.

[00258] In some implementations, pulse lengths (widths) can be different for each credit amount, and the pulses can be in an array (for example when sending three pulses in one swipe: first pulse is 10ms, second is 50ms, third is 10ms).

[00259] In some implementations, when there is an entire machine offer, instant authorization can be provided to a user (e.g., after receiving an authorization request from a mobile device) and an appropriate authorization grant can be sent to the unattended machine 1500 (via the mobile device and the pulse-providing device) without requiring the user to pay first (have a balance).

[00260] In this way and by using the process 3100, various pricing options can be selected by a user without creating a trusted relationship between the application 140, the user, and the pulse-providing device 1520. The user cannot make a free-form input in number of credits (these are predefined at the server 130) and the user is simply selecting index values that are then interpreted by the server 130 in order to then send credit/ pulsing data that is associated with the selected index value to the pulse-providing device (i.e., the mobile device 150 is merely used as a communication medium to route the credit/ pulsing data from the server 130 to the pulse-providing device 1520).

[00261] Figure 32 illustrates an example of a user interface on a mobile device that is used for selecting one of the remotely configured options for the unattended machine, in accordance with some implementations.

[00262] As shown in Figure 32, in some implementations, the user interface includes a number of pricing options for the unattended machine. As explained above in reference to Figure 31, the pricing options are received from a server 130 in response to an authorization request from a user of the mobile device 150. In some implementations, the pricing options are configured by an operator of the unattended machine via a web-based interface (so that the operator does not need to be in physical proximity to the unattended machine in order to create and make available new pricing options for the unattended machine). As also

Petitioner Exhibit 1002-1269

explained above, the user interface provides no details regarding electric pulses that will be provided to the unattended machine after the user selects one of the pricing options.

[00263] In some implementations, the user interfaces is a machine-specific card (e.g., machine-specific card 3202) that also includes details regarding special promotions or offers for the unattended machine (e.g., as shown in Figure 32, there is an available offer of "Buy 7 get 1 FREE"). After the user selects the available offer, the user is able to provide payment equivalent to 7 coin-operated credits, but will receive 8 plays instead of just 7. This is because, the server 130 stores information indicating that 8 pulses are to be provided to the unattended machine (via the pulse-providing device 1520) in response to the receipt of payment equivalent to 7 coin-operated credits.

[00264] In some implementations, the available offer that is highlighted is selected for inclusion on the front of the machine-specific card by the operator and additional offers are also available by flipping over the machine-specific card. Flipping over the machine-specific card is performed in response to a user selection of the "special offers" tab and the back of the machine-specific card is then revealed showing one or more additional offers for the unattended machine.

[00265] In some implementations, the user interface also includes a label for the unattended machine that is being interacted with (e.g., a label of "Street Fighter" is shown in a top portion of the user interface, Figure 32). In some implementations, the user interface also includes a representation of the unattended machine (e.g., a photo of the unattended machine that is taken by an operator and then uploaded to the server 130 for subsequent presentation to users via the application 140).

[00266] As also shown in Figure 32, portions of machine-specific cards for other unattended machines are also illustrated (e.g., machine-specific cards 3204 and 3206). Swiping in a lateral direction over the machine-specific card allows the user to access machine-specific cards for the other unattended machines. After accessing a new machine-specific card for one of the other unattended machines, then authorization requests are then submitted to the server 130 in order to receive available pricing options and authorization grants that correspond to the available pricing options for these other unattended machines (as explained above regarding process 3100, Figure 31). In some implementations, default authorization grants for each of the other unattended machines are received before the user swipes in the appropriate lateral direction (in this way, the default pricing information is pre-

Petitioner Exhibit 1002-1270

loaded and specific pricing data for other indexes can be later obtained if the user selects one of the other indexes for the other unattended machines).

[00267] Figure 33 is a flow diagram of a method of determining electric pulses to provide to an unattended machine based on remotely configured options for the unattended machine, in accordance with some implementations. For convenience, the method 3300 is described below as performed by an application (e.g., the application 140 described above) that is executing on a mobile device (e.g., the mobile device 150 described above).

[00268] The method 3300 allows for determining electric pulses to provide to an unattended machine based on remotely-configured options for the unattended machine. As explained above, unattended machines cannot accept real-time or configurable pricing options because they are hard-wired to accept only specific coins at specific credit values. By retro-fitting an unattended machine with a pulse-providing device 1520 (described above), operators of unattended machines are able to establish new pricing options and make those available to users via the application 140. In this way, by implementing method 3300, the functioning of unattended machines is improved, user experiences at the unattended machines is improved, and operators can open up new revenue streams.

[00269] As shown in Figure 33, the method 3300 begins when the application detects (3302), based on a broadcast received from a pulse-providing device that is coupled with the unattended machine, presence of the unattended machine in proximity to a mobile device. For example, the broadcast is a bluetooth low energy (BLE) transmission sent by the pulse-providing device and that transmission includes an authentication code (discussed in detail about in reference to Figures 8A-8G.

[00270] After detecting the presence of the unattended machine, the application receives (3304), from a server (e.g., server 130 described above), information about a first set of remotely-configured options for interacting with the unattended machine. In some implementations, the server 130 is not capable of communicating directly with the unattended machine, because the unattended machine does not have a network connection.

[00271] In some implementations, the remotely-configured options are pricing options. In some implementations, the remotely-configured options are pricing options that are determined according to a predefined pricing schedule. In some implementations, the predefined pricing schedule is determined based on a current time of day at the server (in this way, time of day or timezone information received or communicated via the mobile device is

Petitioner Exhibit 1002-1271

not trusted and only such timing information from the server 130 is utilized, in order to avoid or mitigate potential malicious behavior). In some implementations, the remotely-configured options are configured by an operator of the unattended machine without requiring any physical interactions with the unattended machine (e.g., the operator need only configure options through the server, such as via a web-based interface and need not physically change any operation or interface of the unattended machine).

[00272] In some implementations, the remotely-configured options are distinct from those pricing options that are available via mechanical interaction with the unattended machine (via insertion of coins into the unattended machine). For example, an operator can establish 2-for-1 deals, time-based deals (discounts for using the machine after, before, or during a certain time of day), loyalty deals (discounts for using the unattended machine on multiple days in a row), deals based on last activity (discounts for returning to use an unattended machine that has not been used for more than a predetermined inactivity period), and the like and these options are not available unless a user interacts with the unattended machine via the application 140 and the pulse-providing device 1520 (because these options must be dynamically conveyed to the unattended machine through communications with the server 130, as explained herein).

[00273] In response to receiving the information about the first set of remotely-configured options, the application displays (3306), within the application while it is executing on the mobile device, user interface objects that allow for selection of respective options in the first set of remotely-configured options. An example user interface is shown in Figure 32 (and described above in reference to Figures 31 and 32).

[00274] The application also detects (3308) a selection of a first user interface object that corresponds to a first option in the first set of remotely-configured options. After (or in response to) detecting the selection of the first user interface object, the application receives (3310), from the server, information that includes an authorization grant for the first option at the unattended machine, wherein the information includes specifications regarding electric pulses to be provided to the unattended machine by the pulse-providing device in accordance with the first option. In accordance with a determination that a trigger condition has been satisfied, the applicant sends (3312) the information that includes the authorization grant and the specifications to the pulse-providing device. After sending the authorization grant and the pulse information to the pulse-providing device, the application receives (3314) an indication (such as a transaction completion or operation information, as explained above in reference to

Petitioner Exhibit 1002-1272

Figure 31), from the pulse-providing device, that the electric pulses were provided to the unattended machine according to the specifications.

[00275] In some implementations, the application receives a second indication from the server that the remotely-configured options are no longer current. For example, the server compares a first hash value that is associated with the remotely-configured options (such as the first set) to a second hash value that is associated with the most current remotely-configured options available at the server. If the hash values do not match, then the server sends (to the application 140), the indication. In response to receiving the second indication from the server, the application receives an updated set of remotely-configured pricing options that is distinct from the first set of remotely-configured pricing options. In some implementations, any payment that was sent by the user to the unattended machine based on the first set of remotely-configured options (now out-of-date) is canceled and the user is provided with user interface objects that allow for selection of a new option that is now provided via the updated set of remotely-configured options.

[00276] One of ordinary skill in the art will recognize that the operations of method 3300 may be re-arranged, replaced, or modified based on the operations of other methods described herein (e.g., methods 1600 and 1700).

[00277] It should be noted that relative terms are meant to help in the understanding of the technology and are not meant to limit the scope of the invention. Similarly, unless specifically stated otherwise, the terms used for labels (e.g., "first," "second," and "third") are meant solely for purposes of designation and not for order or limitation. The term "short" in the phrase "short-range" (in addition to having technology specific meanings) is relative to the term "long" in the phrase "long-range."

[00278] The terms "may," "might," "can," and "could" are used to indicate alternatives and optional features and only should be construed as a limitation if specifically included in the claims.

[00279] It should be noted that, unless otherwise specified, the term "or" is used in its nonexclusive form (e.g., "A or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, "and/or" is used similarly (e.g., "A and/or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, the terms "includes" and "has" mean "comprises"

Petitioner Exhibit 1002-1273

(e.g., a device that includes, has, or comprises A and B contains A and B, but optionally may contain C or additional components other than A and B). It should be noted that, unless otherwise specified, the singular forms "a," "an," and "the" refer to one or more than one, unless the context clearly dictates otherwise.

[00280] It is to be understood that the inventions, examples, and implementations described herein are not limited to particularly exemplified materials, methods, and/or structures. It is to be understood that the inventions, examples, and implementations described herein are to be considered preferred inventions, examples, and implementations whether specifically identified as such or not.

[00281] The terms and expressions that have been employed in the foregoing specification are used as terms of description and not of limitation, and are not intended to exclude equivalents of the features shown and described. While the above is a complete description of selected implementations of the present invention, it is possible to practice the invention using various alternatives, modifications, adaptations, variations, and/or combinations and their equivalents. It will be appreciated by those of ordinary skill in the art that any arrangement that is calculated to achieve the same purpose may be substituted for the specific embodiment shown. It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described and all statements of the scope of the invention that, as a matter of language, might be said to fall therebetween.

Petitioner Exhibit 1002-1274

What is claimed is:

1. A method of determining electric pulses to provide to an unattended machine based on remotely-configured options for the unattended machine, the method comprising:

at an application executing on a mobile device:

detecting, based on a broadcast received from a pulse-providing device that is coupled with the unattended machine, presence of the unattended machine in proximity to the mobile device;

after detecting the presence of the unattended machine, receiving, from a server, information about a first set of remotely-configured options for interacting with the unattended machine;

in response to receiving the information about the first set of remotely-configured options, displaying, in the application, user interface objects that allow for selection of respective options in the first set of remotely-configured options;

detecting a selection of a first user interface object that corresponds to a first option in the first set of remotely-configured options;

after detecting the selection of the first user interface object, receiving, from the server, information that includes an authorization grant for the first option at the unattended machine, wherein the information includes specifications regarding electric pulses to be provided to the unattended machine by the pulse-providing device in accordance with the first option;

in accordance with a determination that a trigger condition has been satisfied, sending the authorization grant and the pulse information to the pulse-providing device; and

after sending the information that includes the authorization grant and the specifications to the pulse-providing device, receiving an indication, from the pulse-providing device, that the electric pulses were provided to the unattended machine according to the specifications.

2. The method of claim 1, wherein the remotely-configured options are pricing options.

3. The method of claim 1, wherein the remotely-configured options are pricing options that are determined according to a predefined pricing schedule.

4. The method of claim 3, wherein the predefined pricing schedule is determined based on a current time of day at the server.

Petitioner Exhibit 1002-1275

5. The method of claim 1, wherein the remotely-configured options are configured by an operator of the unattended machine without requiring any physical interactions with the unattended machine.

6. The method of any one of claims 1-5, further comprising:

receiving a second indication from the server that the remotely-configured options are no longer current; and

in response to receiving the second indication from the server, receiving an updated set of remotely-configured pricing options that is distinct from the first set of remotely-configured pricing options.

7. The method of any one of claims 1-6, wherein a short-range transceiver of the mobile device receives the broadcast from the pulse-providing device.

8. The method of any one of claims 1-7, wherein a long-range wireless transceiver of the mobile device receives the information about the first set of remotely-configured options for interacting with the unattended machine from the remote server.

9. The method of any one of claims 1-8, wherein a short-range wireless transceiver of the mobile device transmits the authorization grant and the pulse information is transmitted to the pulse-providing device.

10. The method of any one of claims 1-9, wherein a short-range wireless transceiver of the mobile device receives the indication from the pulse-providing device.

11. A mobile device comprising:

one or more processors and memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for performing the method of any one of claims 1-10.

12. A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a mobile device with one or more processors, cause the mobile device to perform the method of any one of claims 1-10.

13. A method of determining electric pulses to provide to an unattended machine based on remotely-configured options for the unattended machine, the method comprising:

Petitioner Exhibit 1002-1276

at a pulse-providing device that is coupled with the unattended machine:

receiving, from an application executing on a mobile device, an authorization grant that includes specifications regarding electric pulses to be provided to the unattended machine by the pulse-providing device in accordance with a pricing option selected by a user at the application executing on the mobile device, wherein the pricing option is specific to the unattended machine;

in response to receiving the authorization grant, determining whether the authorization grant is valid;

in accordance with a determination that the authorization grant is valid, providing electric pulses to the unattended machine according to the specifications; and

after providing the electric pulses to the unattended machine, sending, to the application executing on the mobile device, an indication that the electric pulses were provided to the unattended machine according to the specifications.

14. The method of claim 13, wherein the pricing option is not available to users that interact with the unattended machine via mechanical insertion of coins.

15. The method of claim 13, wherein the pricing option is remotely configured and received from a remote server via the mobile device.

16. The method of claim 13, wherein the pricing option is remotely configured and determined according to a predefined pricing schedule.

17. The method of claim 13, wherein the pricing option is configured by an operator of the unattended machine without requiring any physical interactions with the unattended machine.

18. The method of any one of claims 13-17, further comprising:

receiving a second indication from the server that the pricing options is no longer current; and

in response to receiving the second indication from the server, receiving an updated pricing option that is distinct from the pricing option.

19. A pulse-providing device comprising:

Petitioner Exhibit 1002-1277

one or more processors and memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for performing the method of any one of claims 13-18.

20. A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a pulse-providing device with one or more processors, cause the pulse-providing device to perform the method of any one of claims 13-18.

21. A system for determining electric pulses to provide to an unattended machine based on remotely-configured options for the unattended machine, the system comprising:

a pulse-providing device that is coupled with the unattended machine, wherein the pulse-providing device is configured to:

perform operations described in the method of any one of claims 13-18; and

an application that is executing on a mobile device, wherein the application is configured to:

perform operations described in the method of any one of claims 1-10; and

a server that is in communication with the application that is executing on the mobile device, wherein the server is configured to:

perform operations including retrieving specifications for electric pulses that are associated with selected pricing options and sending those retrieve specifications to the mobile device.

Petitioner Exhibit 1002-1278

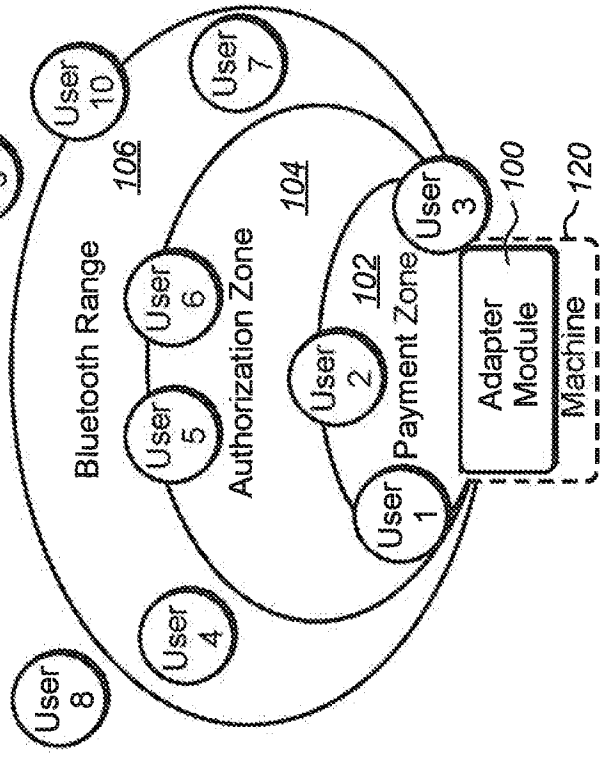


Figure 2

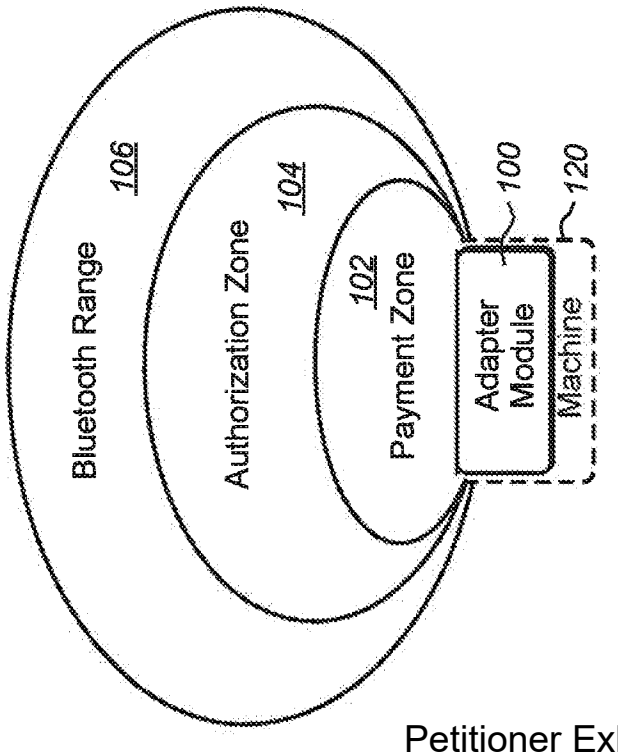


Figure 1

Tab	Favorite?	Alert	View to User
All	Yes	No	User can make Hands-free Credit with the connected vending machine
All	No	Yes	User needs to launch Mobile Device and then swipe to make transaction manually
Favorite	Yes	No	Hands-free transaction will be available to the user via vending machine
Favorite	No	No	User is not alerted for the vending machine which is not a favorite machine. Hands-free mode will not work, manual swipe for transaction required by user.
Either All or Favorite	Yes	Yes	BUT Hands-free Credit is not available (disable by module, expired AuthGrant, insufficient balance, or other issue), then user will get an alert so that user can swipe credit manually.

Figure 3

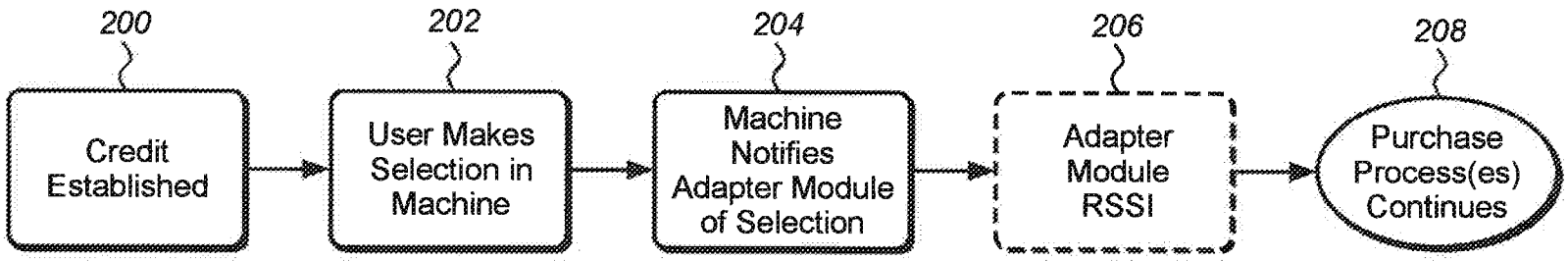


Figure 4

Petitioner Exhibit 1002-1280

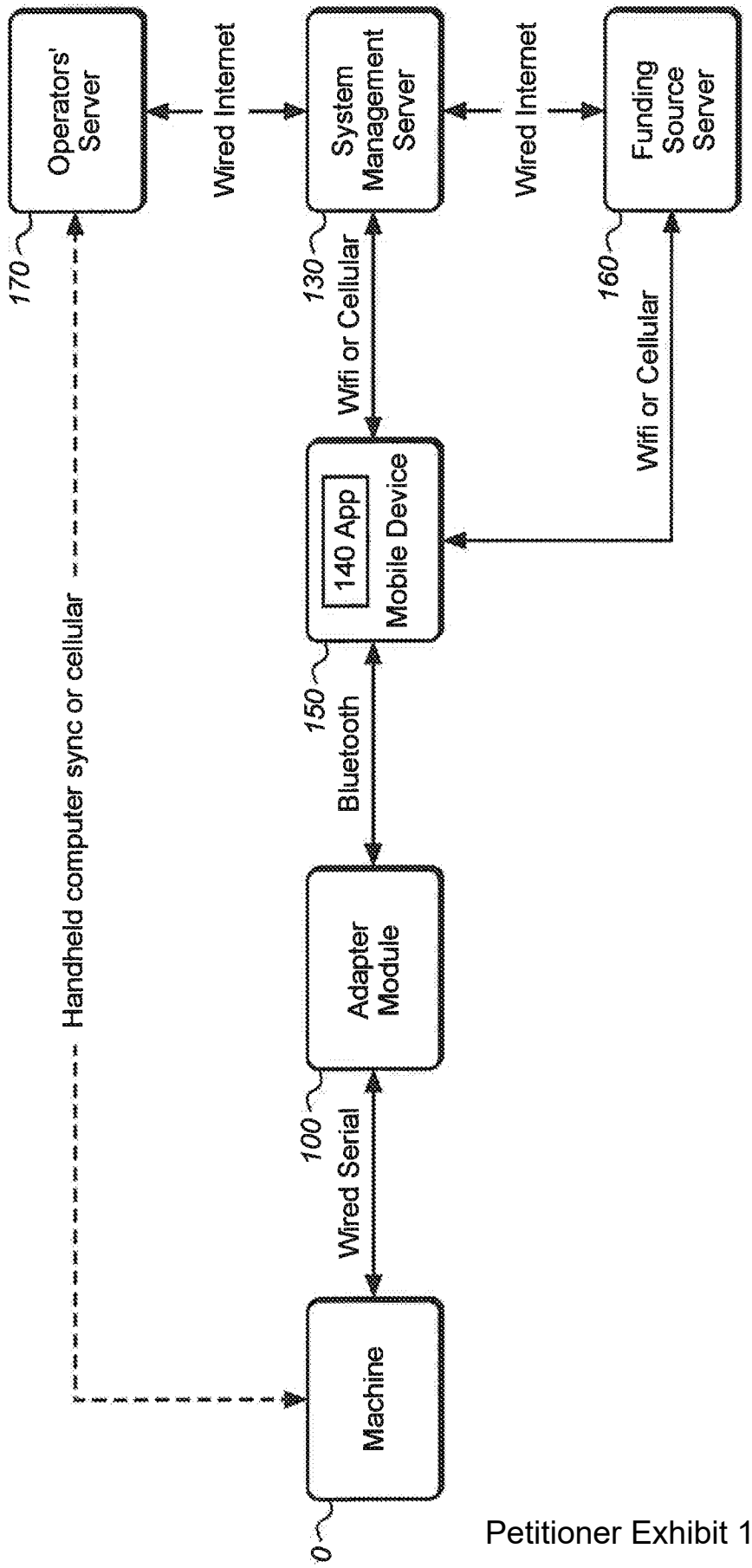

Operators' Server
Wired Internet
System Management Server
Wired Internet
Funding Source Server
170
130
Wifi or Cellular
160
Wifi or Cellular
140 App
Mobile Device
150
Bluetooth
Handheld computer sync or cellular
Adapter Module
100
Wired Serial
Machine
0

Figure 5

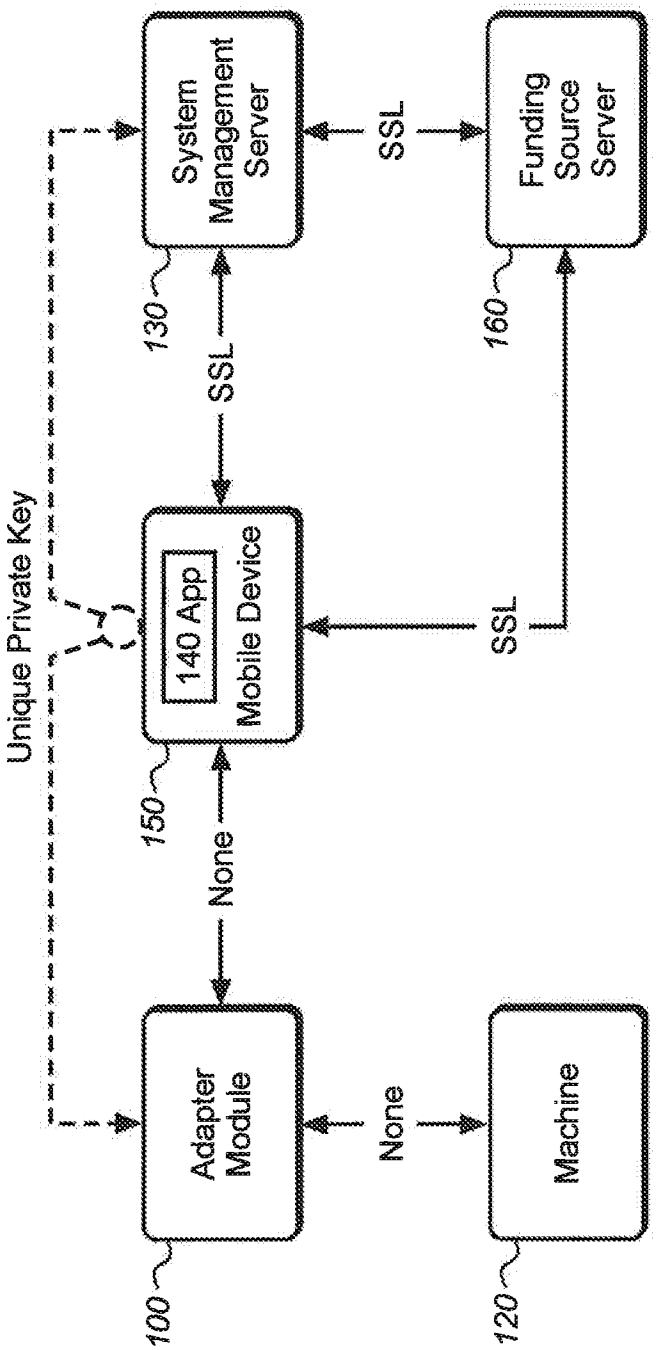

System Management Server
130
SSL
SSL
Funding Source Server
160
Unique Private Key
140 App
Mobile Device
150
None
SSL
Adapter Module
100
None
Machine
120

Figure 6

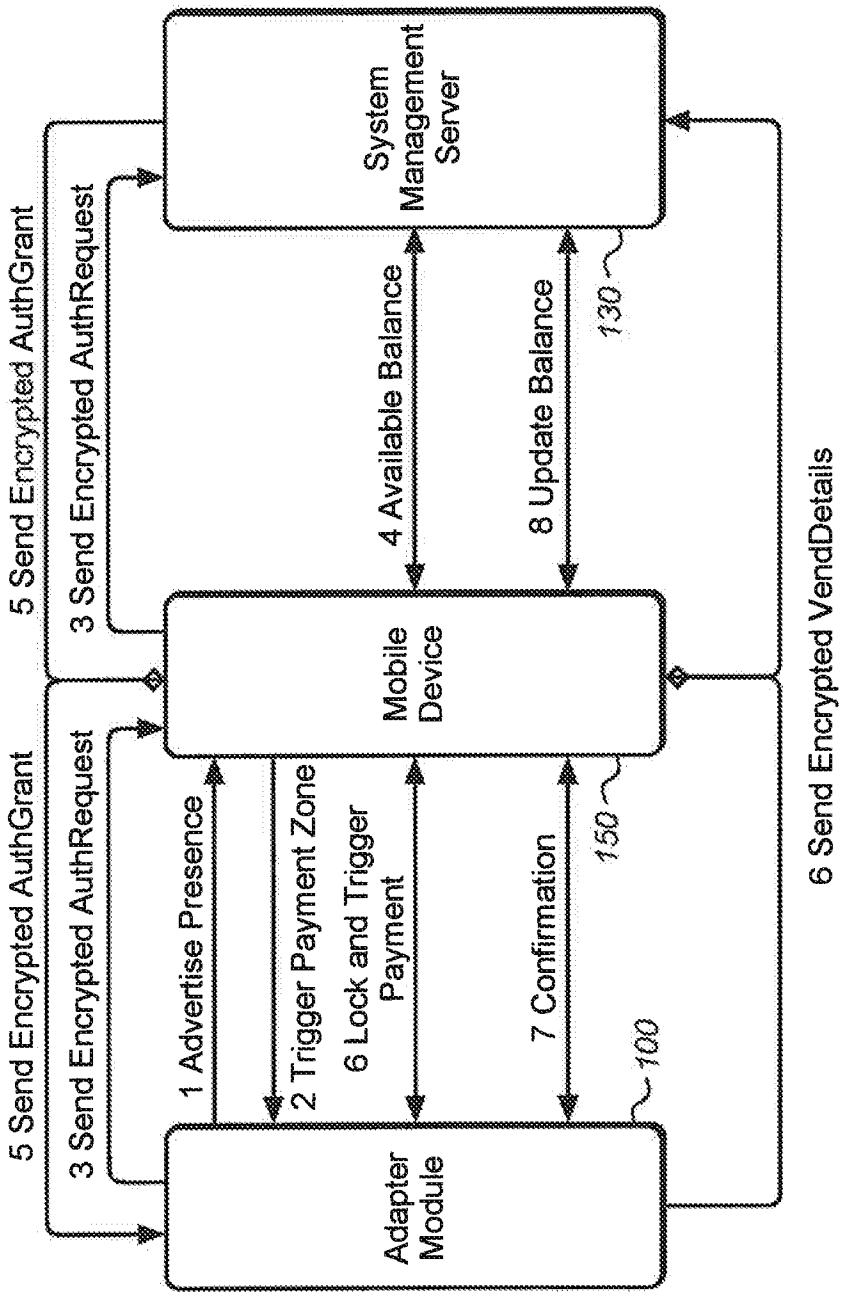

System Management Server
Mobile Device
Adapter Module
5 Send Encrypted AuthGrant
3 Send Encrypted AuthRequest
5 Send Encrypted AuthGrant
3 Send Encrypted AuthRequest
1 Advertise Presence
2 Trigger Payment Zone
6 Lock and Trigger Payment
4 Available Balance
8 Update Balance
7 Confirmation
6 Send Encrypted VendDetails
130
150
100

Figure 7

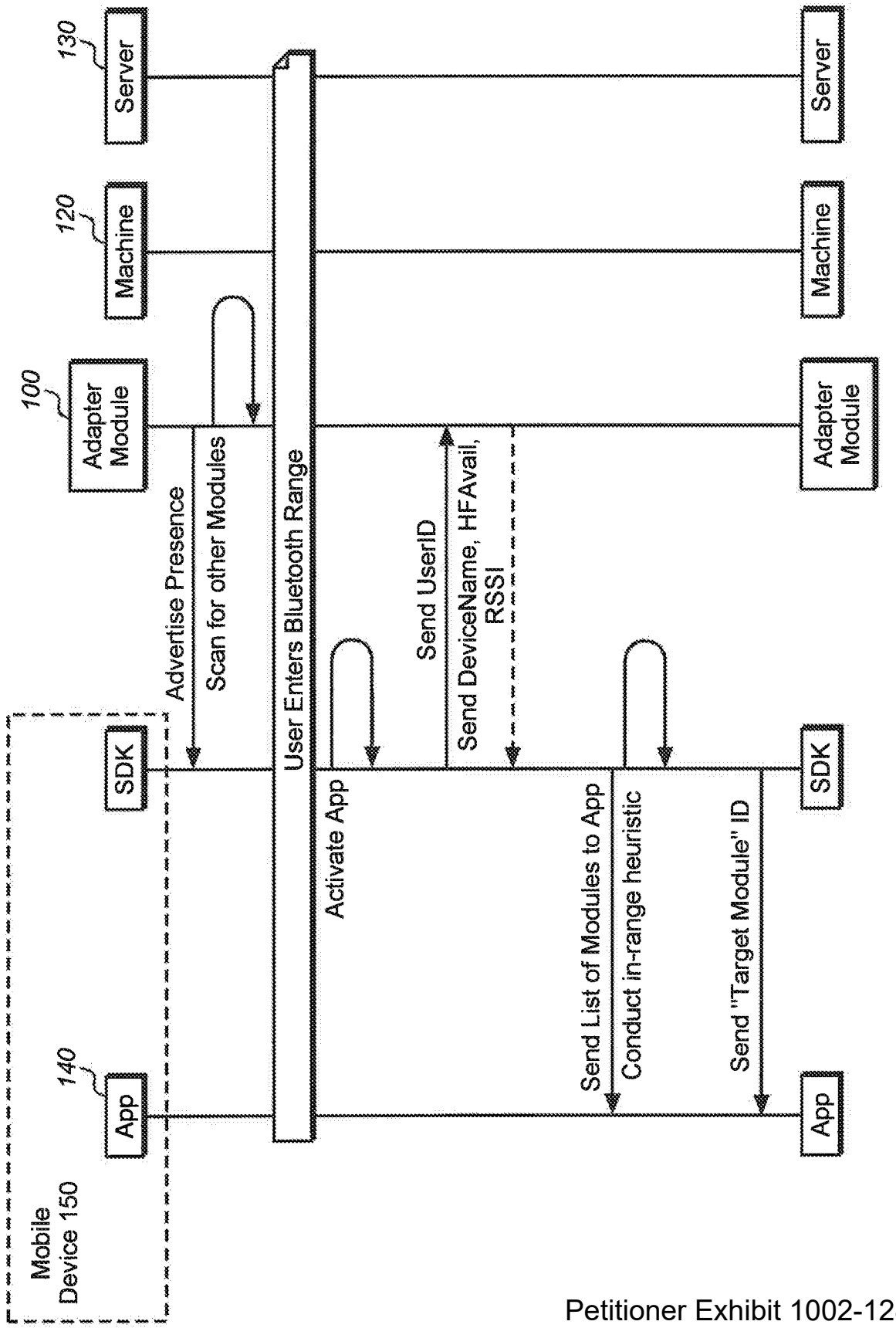

Mobile Device 150
App
140
SDK
Adapter Module
100
Machine
120
Server
130
Advertise Presence
Scan for other Modules
User Enters Bluetooth Range
Activate App
Send UserID
Send DeviceName, HFAvail, RSSI
Send List of Modules to App
Conduct in-range heuristic
Send "Target Module" ID
Server
Machine
Adapter Module
SDK
App

Figure 8A

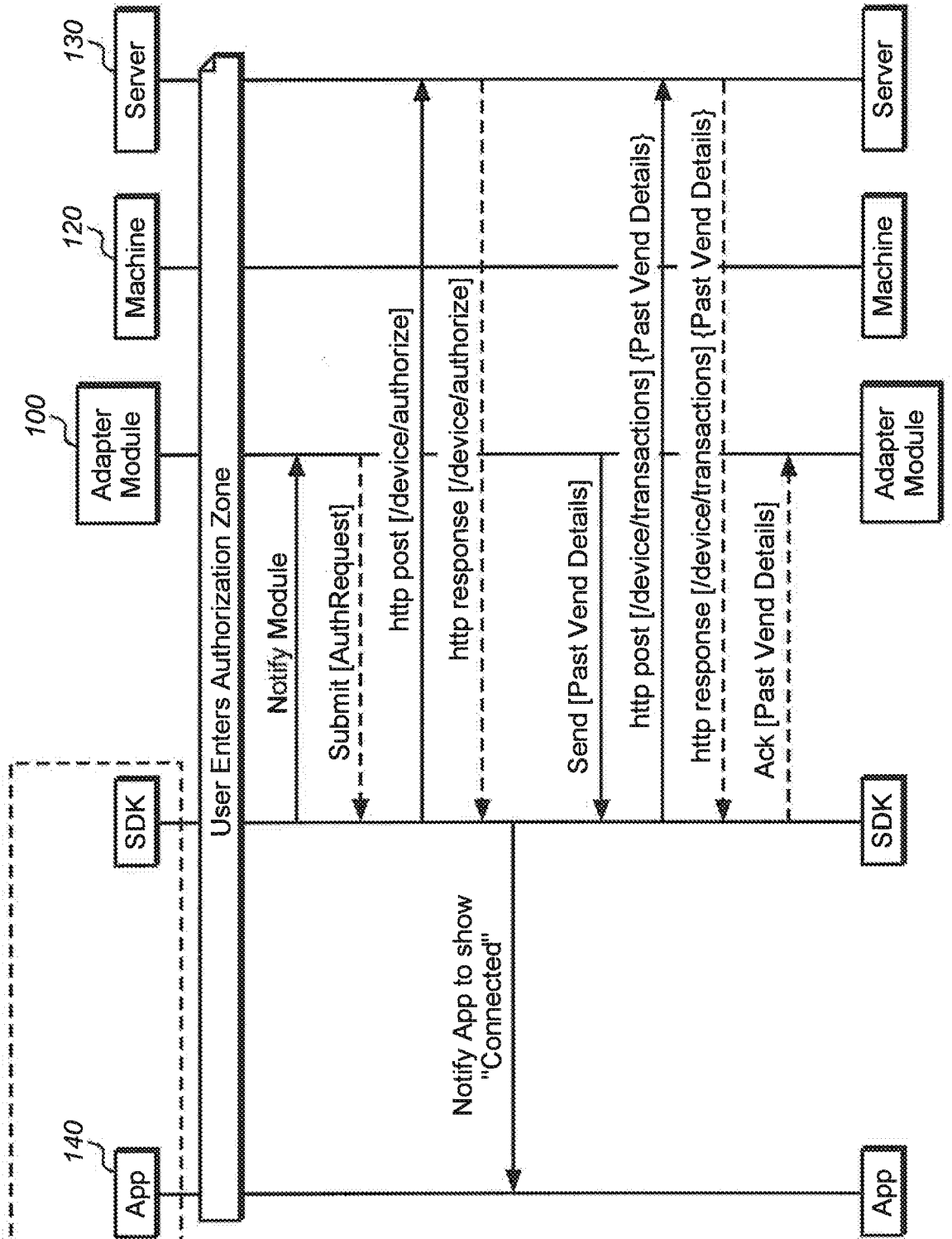

Mobile Device 150
140
App
SDK
100
Adapter Module
120
Machine
130
Server
User Enters Authorization Zone
Notify Module
Submit [AuthRequest]
http post [/device/authorize]
http response [/device/authorize]
Send [Past Vend Details]
http post [/device/transactions] {Past Vend Details}
http response [/device/transactions] {Past Vend Details}
Ack [Past Vend Details]
Notify App to show "Connected"
App
SDK
Adapter Module
Machine
Server

Figure 8B

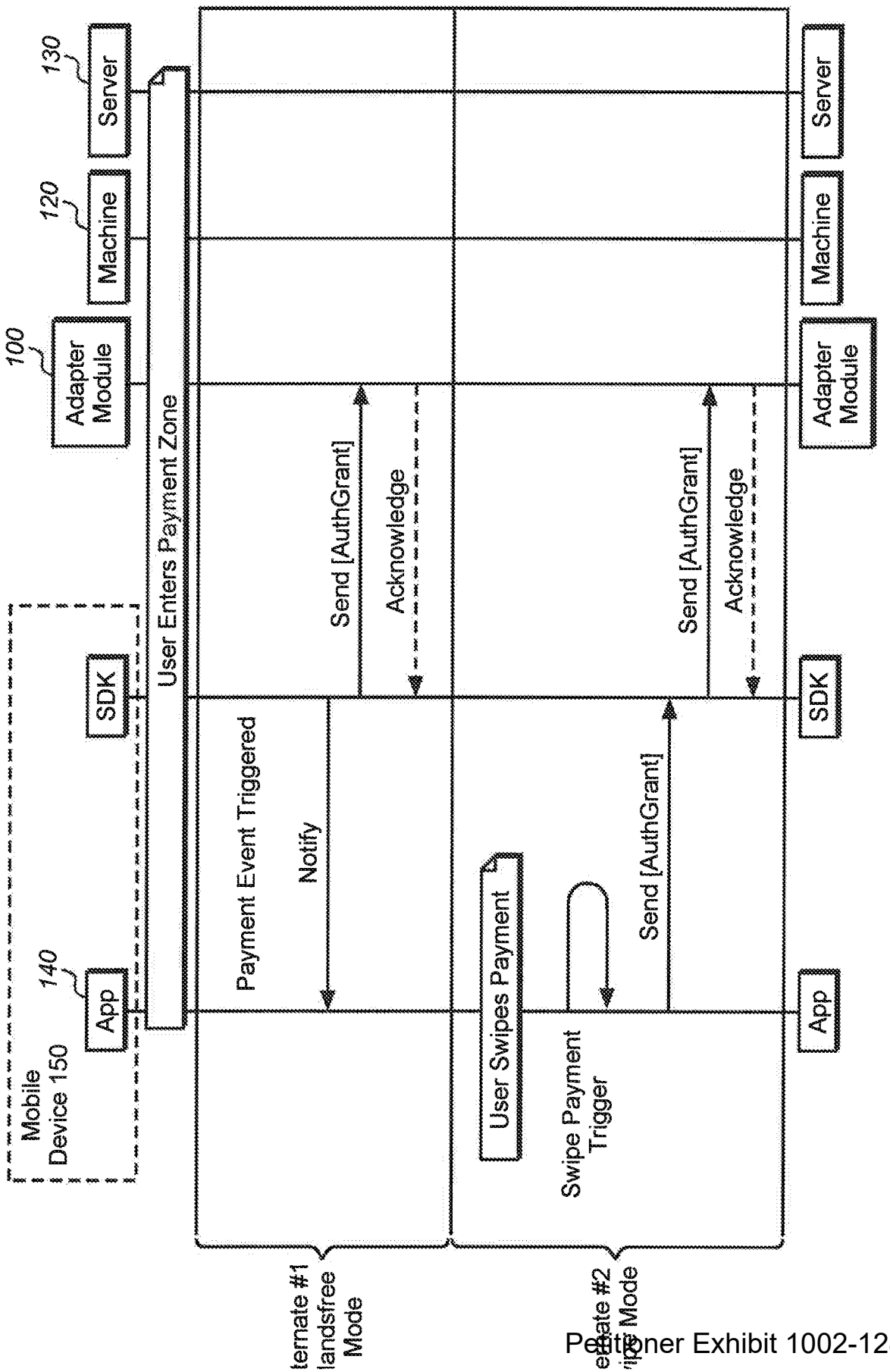

Mobile Device 150
App
140
SDK
Adapter Module
100
Machine
120
Server
130
User Enters Payment Zone
Payment Event Triggered
Notify
Send [AuthGrant]
Acknowledge
User Swipes Payment
Swipe Payment Trigger
Send [AuthGrant]
Acknowledge
Send [AuthGrant]
SDK
Adapter Module
Machine
Server
App
ternate #1
landsfree Mode
ernate #2
ipe Mode

Figure 8C

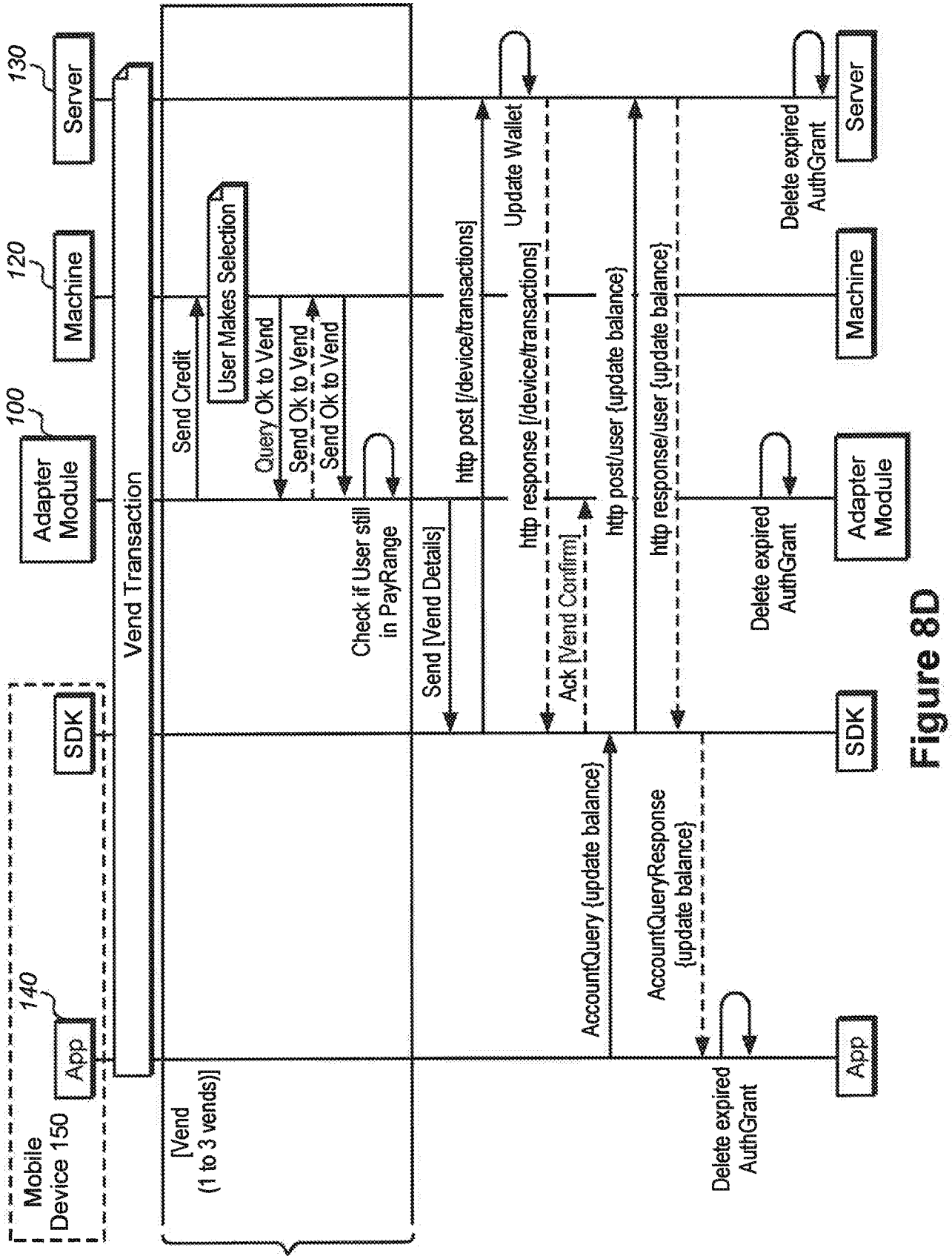

Mobile Device 150
App
140
SDK
Adapter Module
100
Machine
120
Server
130
Vend Transaction
Send Credit
User Makes Selection
Query Ok to Vend
Send Ok to Vend
Send Ok to Vend
Check if User still in PayRange
Send [Vend Details]
http post [/device/transactions]
Update Wallet
http response [/device/transactions]
Ack [Vend Confirm]
http post/user {update balance}
http response/user {update balance}
Delete expired AuthGrant
Delete expired AuthGrant
Delete expired AuthGrant
AccountQuery {update balance}
AccountQueryResponse {update balance}
[Vend (1 to 3 vends)]
oop for
ultiple
/ends

Figure 8D

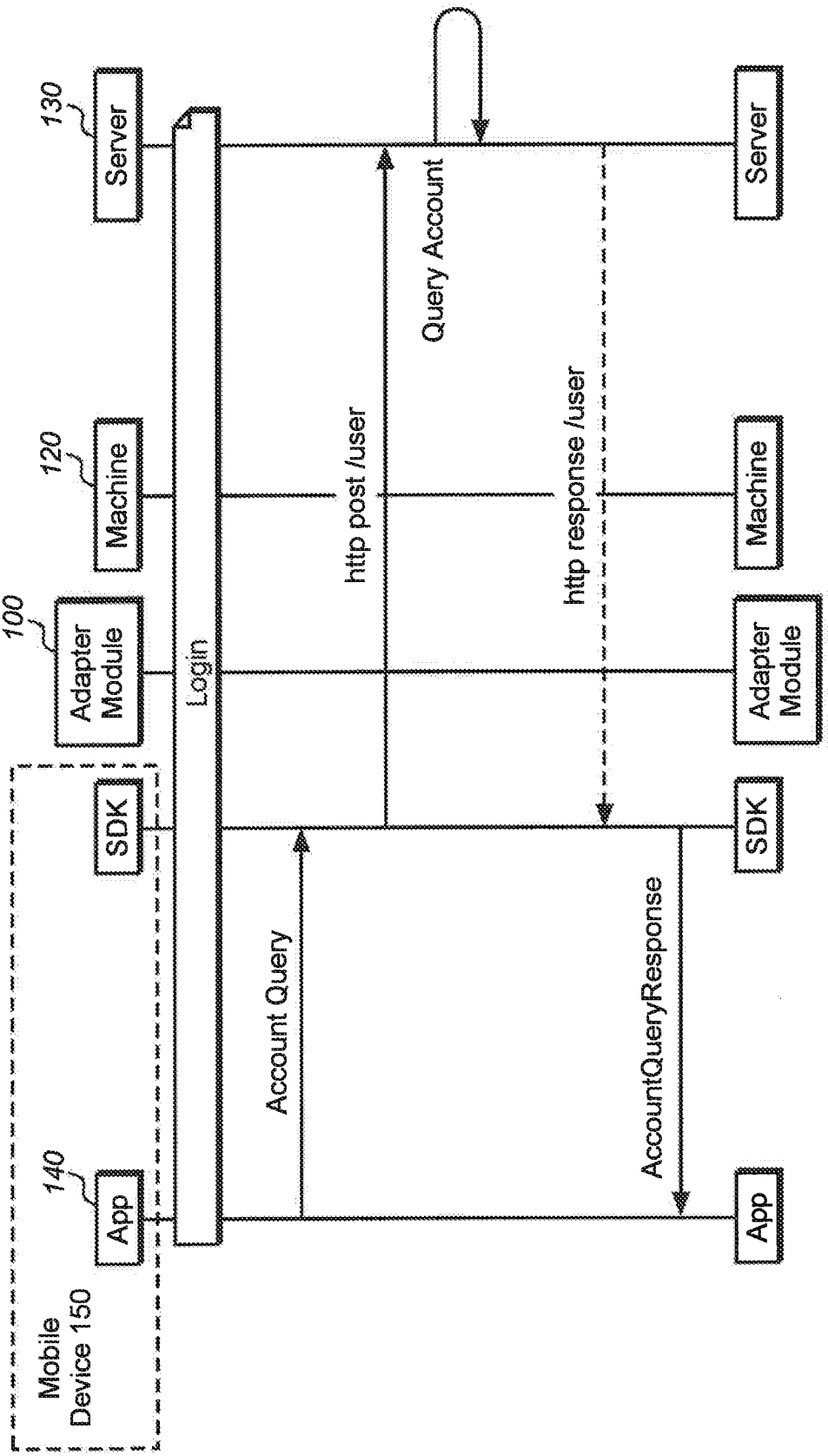

Mobile Device 150
140
App
100
Adapter Module
SDK
120
Machine
130
Server
Login
Account Query
AccountQueryResponse
http post /user
http response /user
Query Account
App
Adapter Module
SDK
Machine
Server

Figure 8E

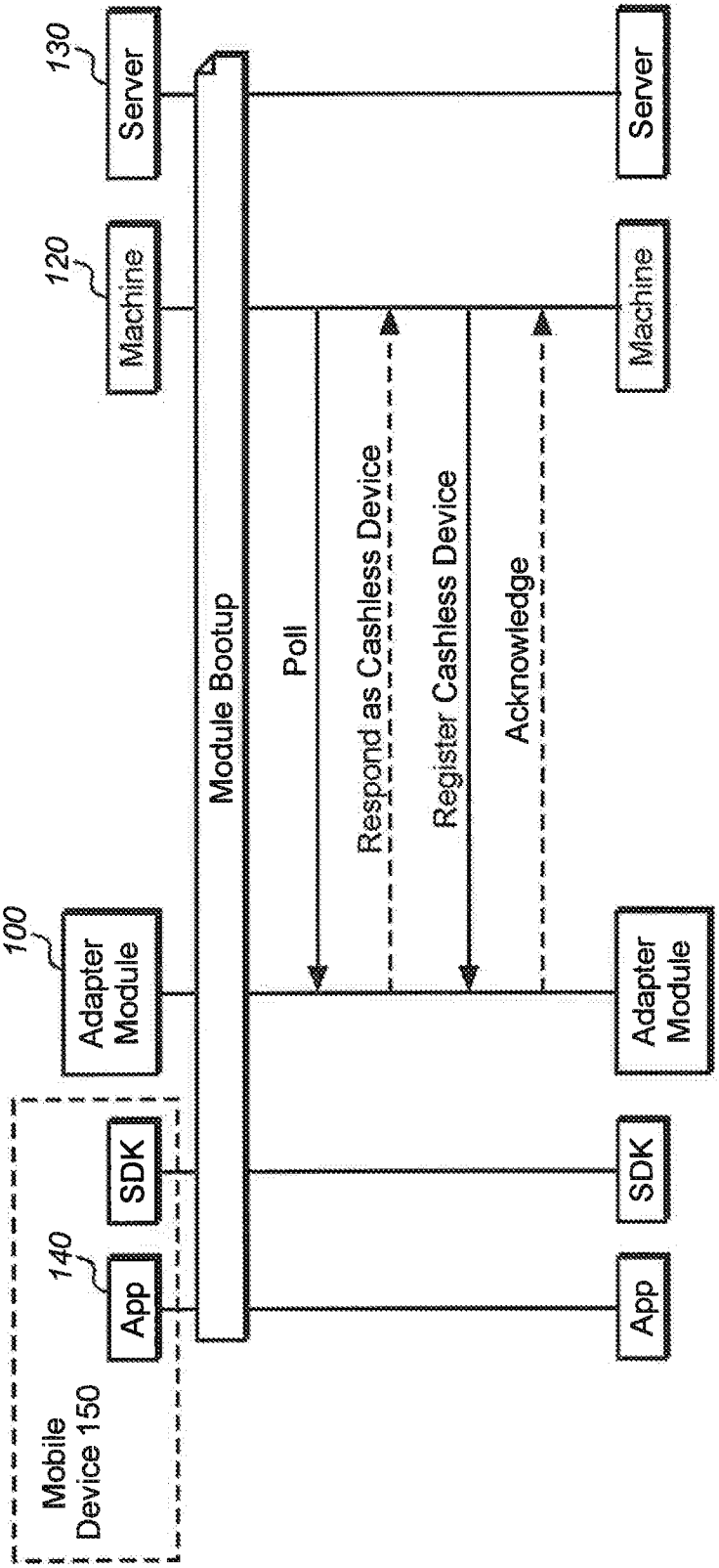

Mobile Device 150
App
140
SDK
Adapter Module
100
Machine
120
Server
130
Module Bootup
Poll
Respond as Cashless Device
Register Cashless Device
Acknowledge
App
SDK
Adapter Module
Machine
Server

Figure 8F

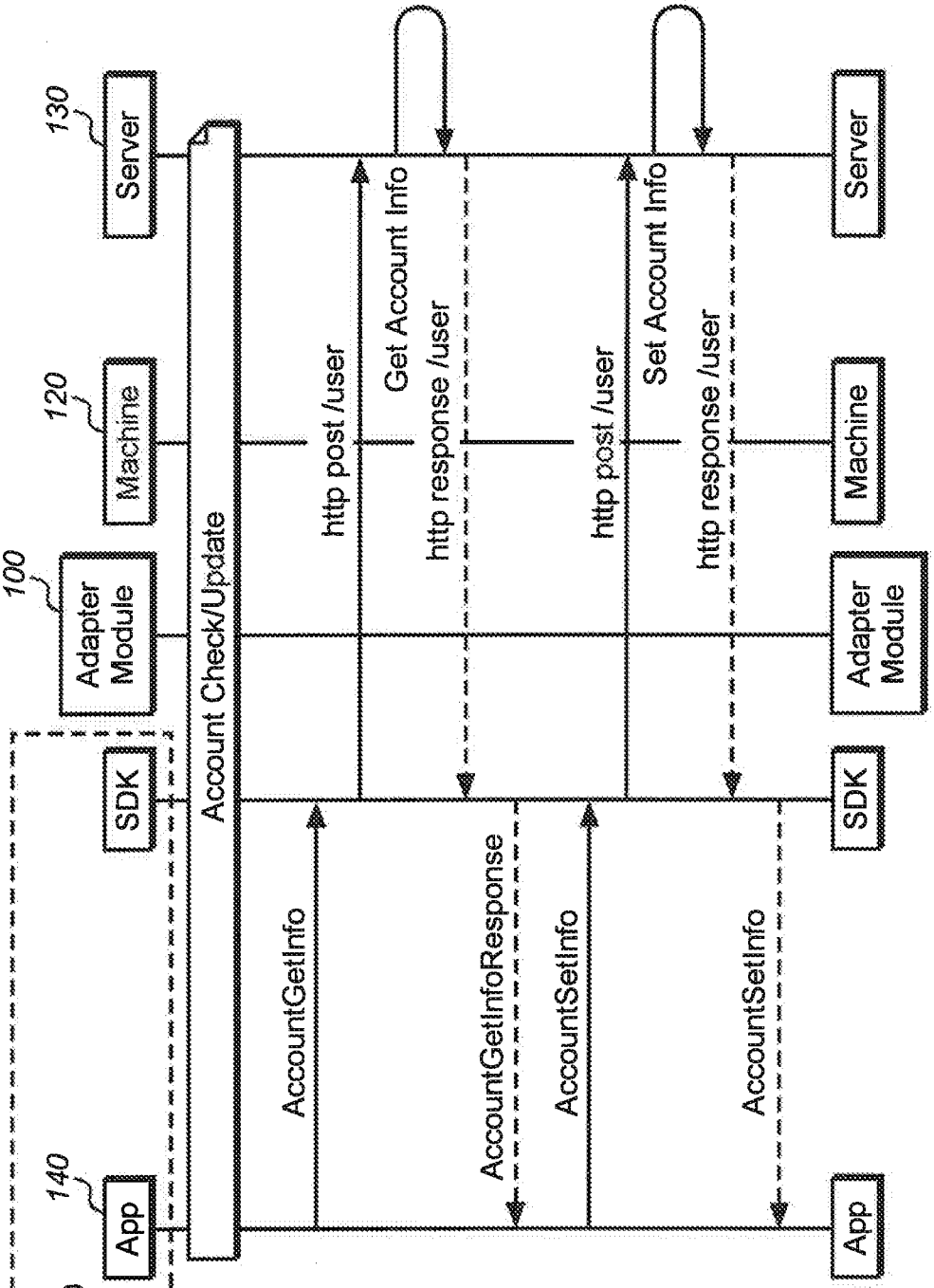

Mobile Device 150
App
140
SDK
Adapter Module
100
Machine
120
Server
130
Account Check/Update
AccountGetInfo
http post /user
Get Account Info
http response /user
AccountGetInfoResponse
AccountSetInfo
http post /user
Set Account Info
http response /user
AccountSetInfo
SDK
Adapter Module
Machine
Server
App

Figure 8G

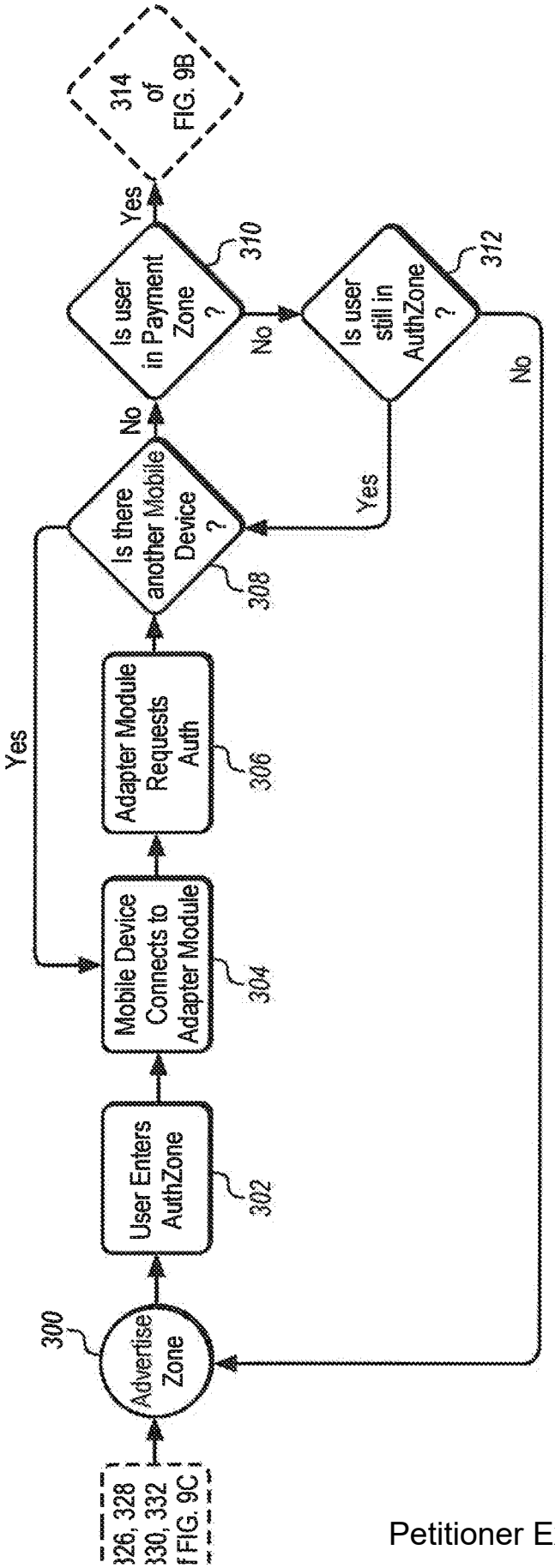

326, 328
330, 332
of FIG. 9C
300
Advertise Zone
User Enters AuthZone
302
Mobile Device Connects to Adapter Module
304
Adapter Module Requests Auth
306
Is there another Mobile Device ?
308
Is user in Payment Zone ?
310
Is user still in AuthZone ?
312
314 of FIG. 9B
Yes
No
Yes
No
Yes
No

Figure 9A

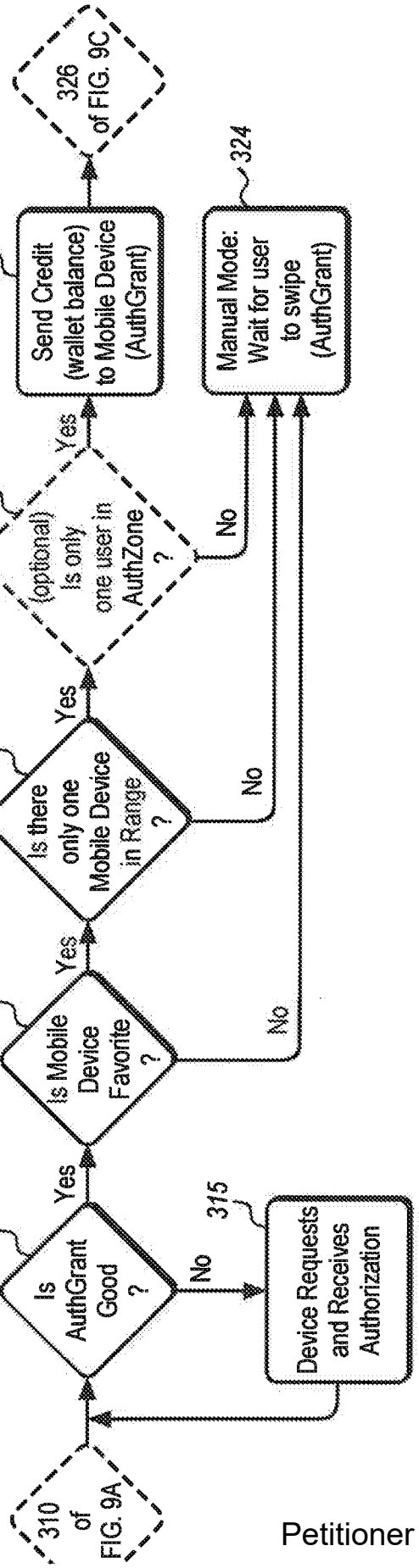

310 of FIG. 9A
314
Is AuthGrant Good ?
No
315
Device Requests and Receives Authorization
Yes
316
Is Mobile Device Favorite ?
No
Yes
318
Is there only one Mobile Device in Range ?
No
Yes
320
(optional) Is only one user in AuthZone ?
No
Yes
322
Send Credit (wallet balance) to Mobile Device (AuthGrant)
324
Manual Mode: Wait for user to swipe (AuthGrant)
326 of FIG. 9C

Figure 9B

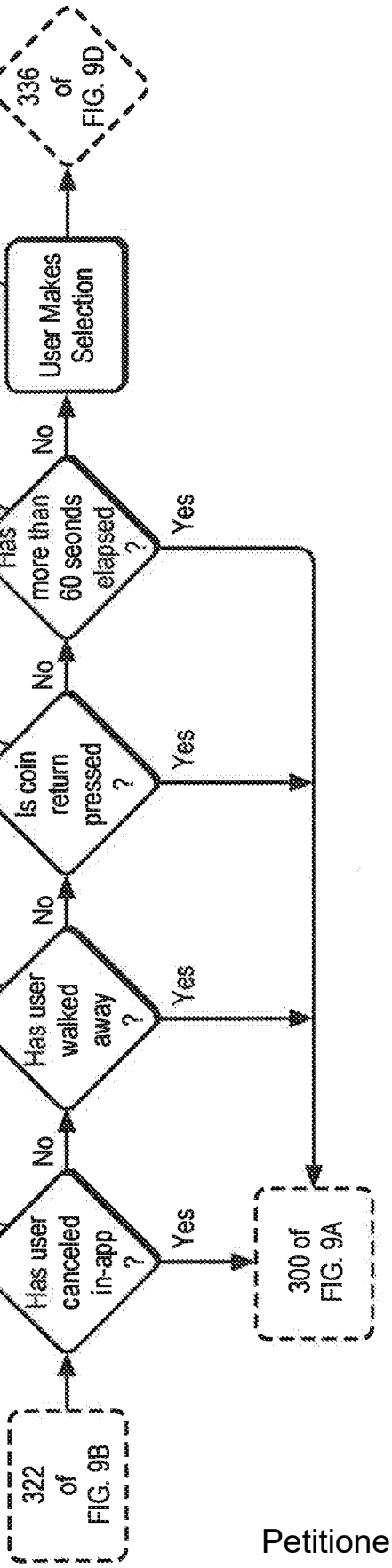

322 of FIG. 9B
326
Has user canceled in-app ?
No
Yes
300 of FIG. 9A
328
Has user walked away ?
No
Yes
330
Is coin return pressed ?
No
Yes
332
Has more than 60 seonds elapsed ?
No
Yes
334
User Makes Selection
336 of FIG. 9D

Figure 9C

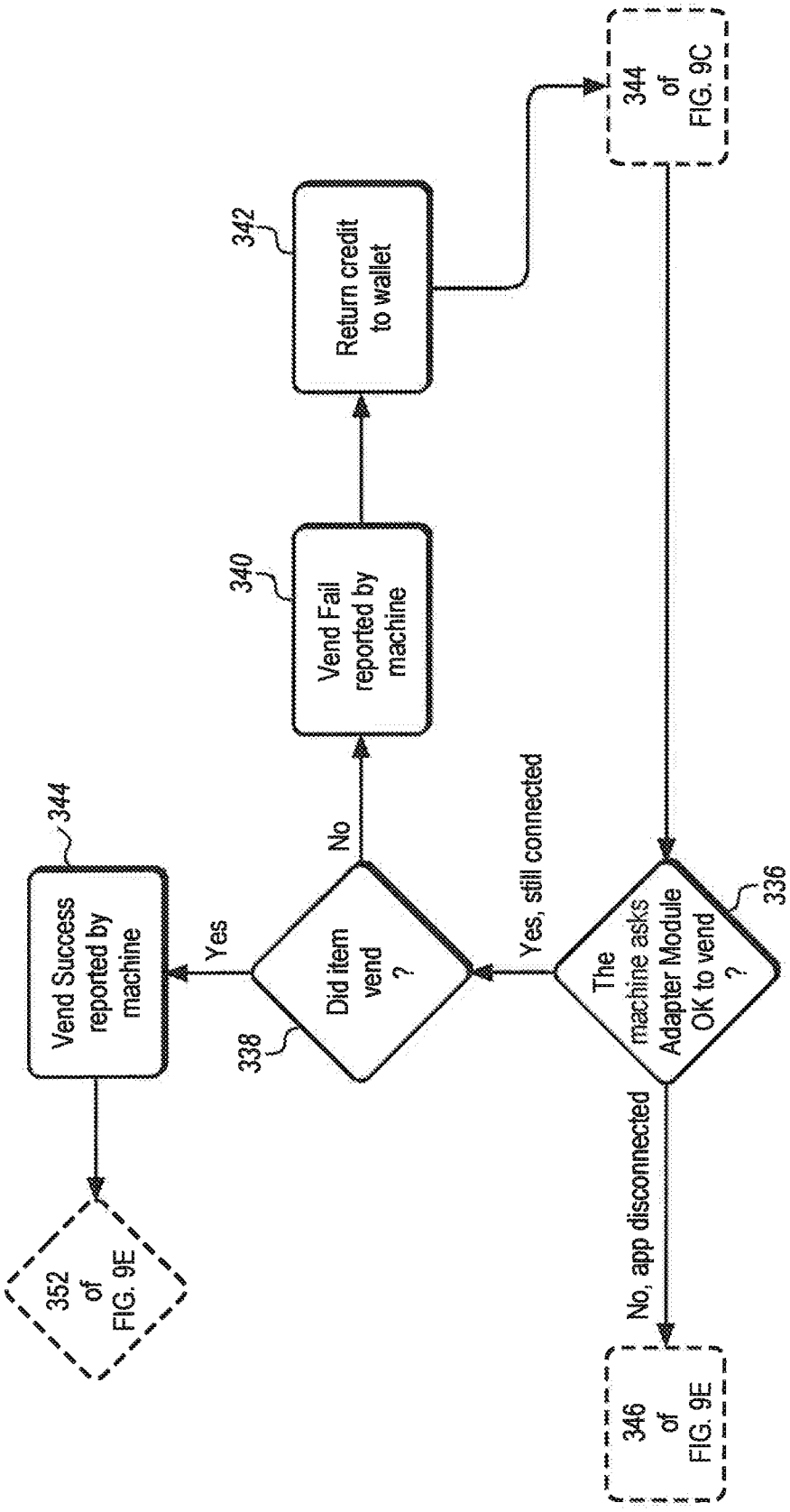

344 of FIG. 9C
342
Return credit to wallet
340
Vend Fail reported by machine
No
338
Did item vend ?
Yes
344
Vend Success reported by machine
352 of FIG. 9E
Yes, still connected
The machine asks Adapter Module OK to vend ?
336
No, app disconnected
346 of FIG. 9E

Figure 9D

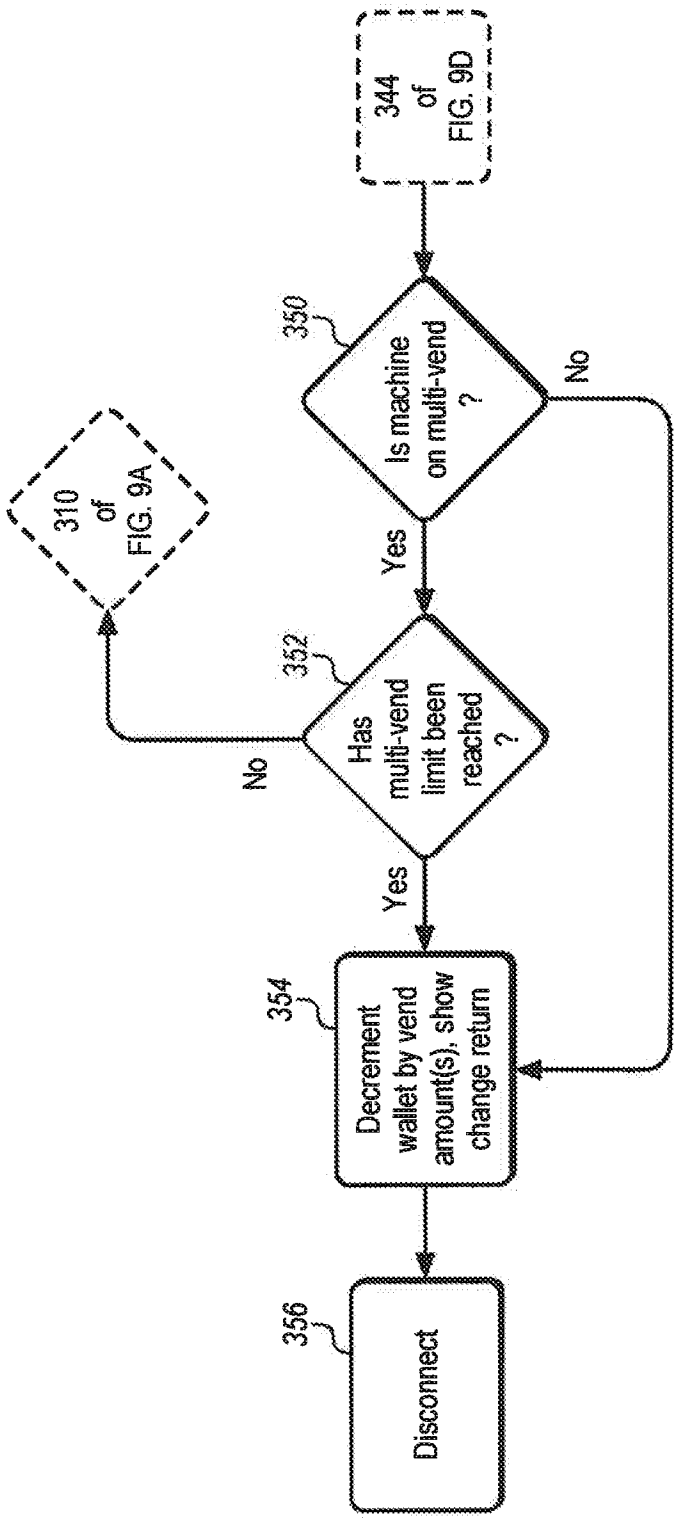

344 of FIG. 9D
350
Is machine on multi-vend ?
No
Yes
310 of FIG. 9A
352
Has multi-vend limit been reached ?
No
Yes
354
Decrement wallet by vend amount(s), show change return
356
Disconnect

Figure 9E

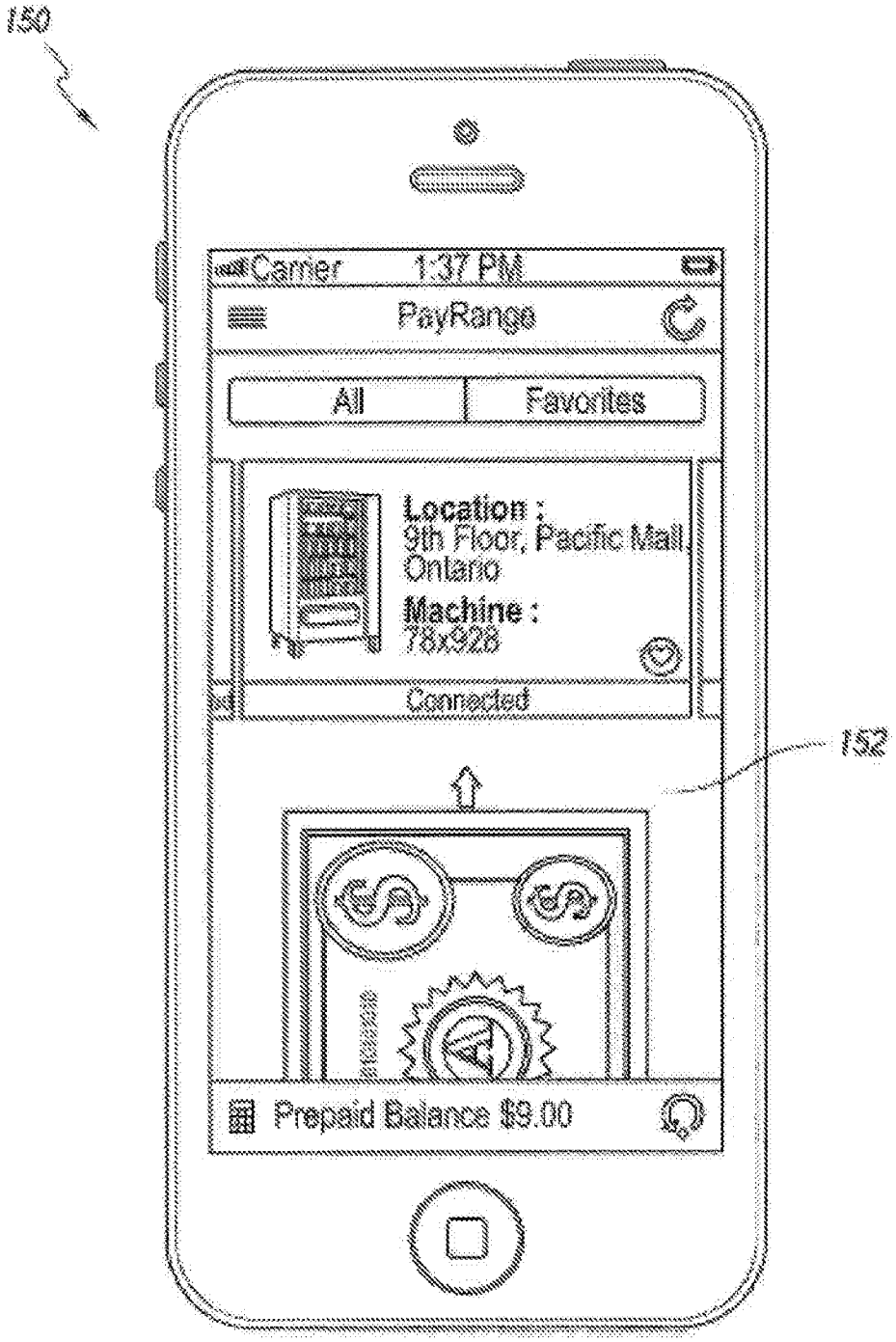

150
Carrier
1:37 PM
PayRange
All
Favorites
Location :
9th Floor, Pacific Mall
Ontario
Machine :
78x928
Connected
152
Prepaid Balance $9.00

Figure 10A

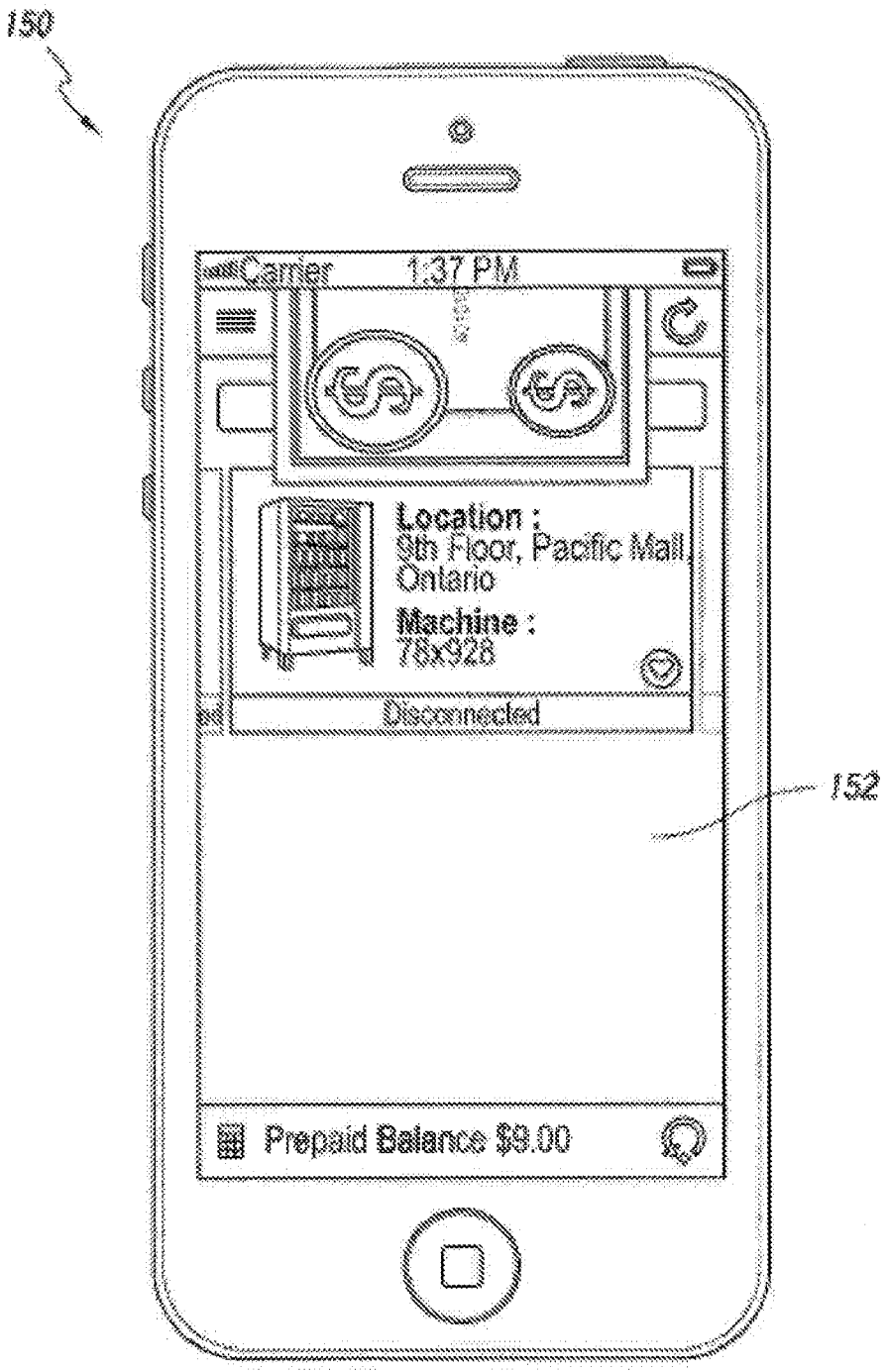


Figure 10B

Petitioner Exhibit 1002-1297

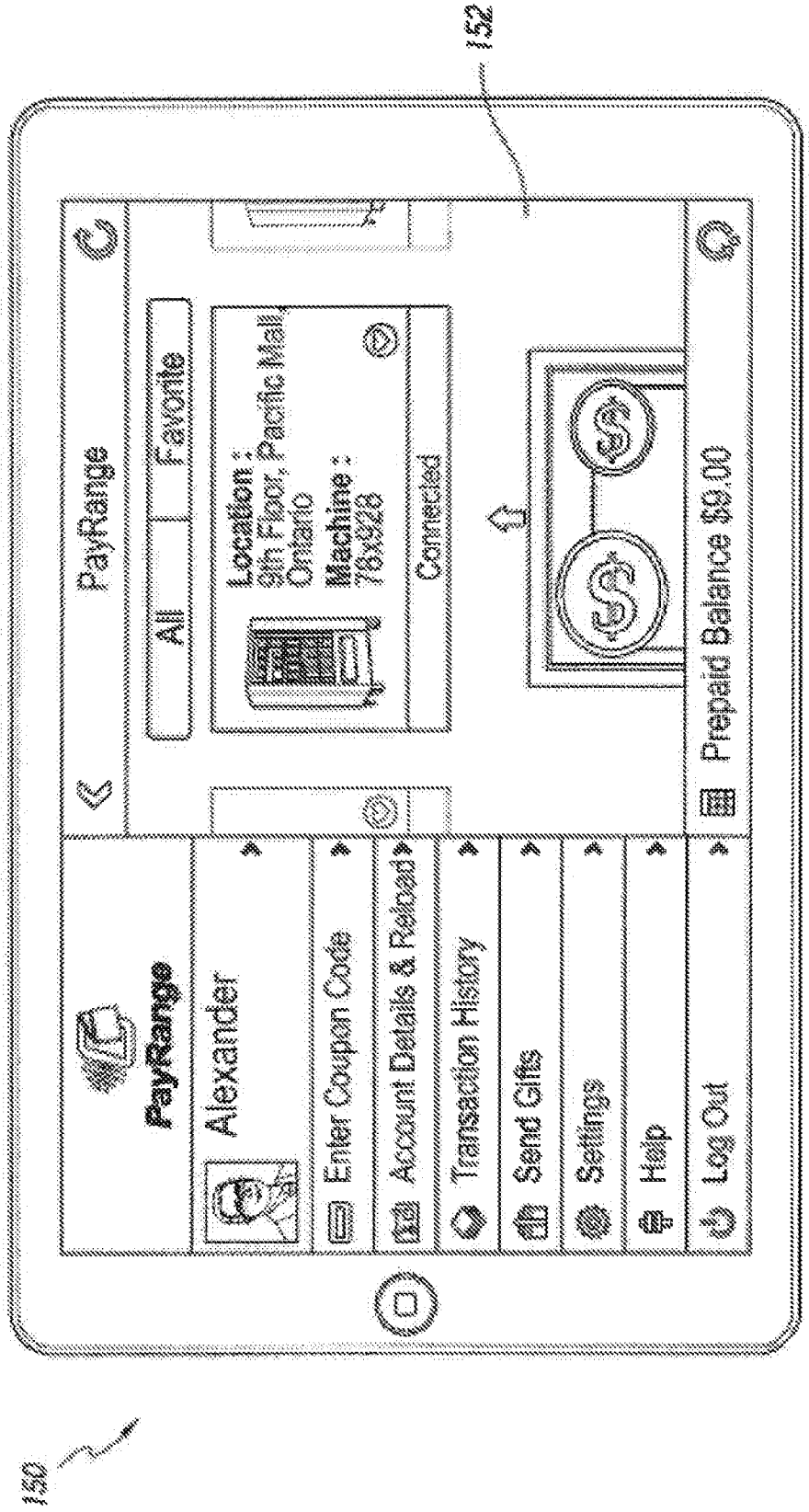

150
152
PayRange
Alexander
Enter Coupon Code
Account Details & Reload
Transaction History
Send Gifts
Settings
Help
Log Out
PayRange
All
Favorite
Location :
9th Floor, Pacific Mall,
Ontario
Machine :
78x928
Connected
Prepaid Balance $9.00

Figure 10C

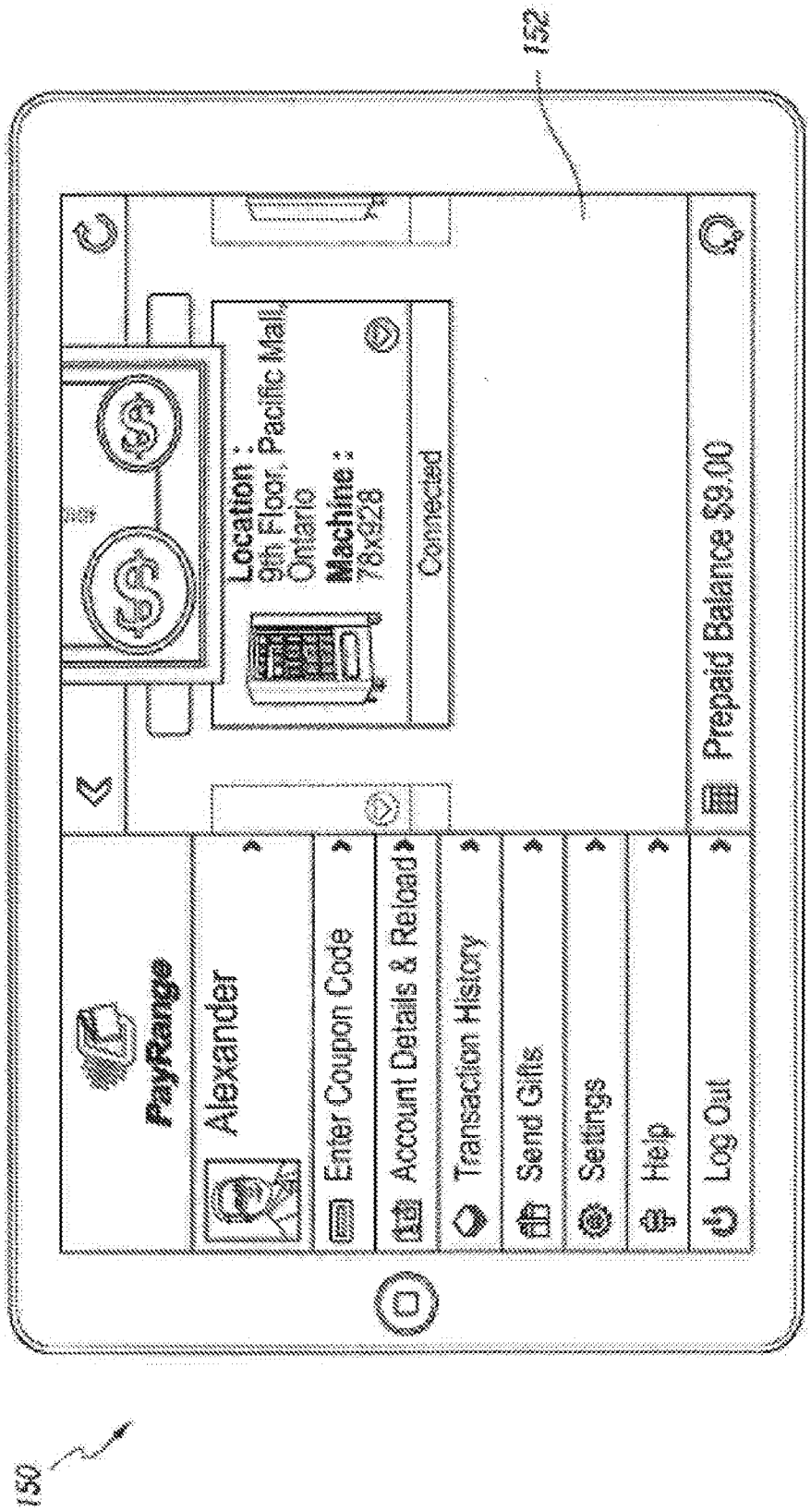

150
152
PayRange
Alexander
Enter Coupon Code
Account Details & Reload
Transaction History
Send Gifts
Settings
Help
Log Out
Location :
9th Floor, Pacific Mall,
Ontario
Machine :
78x928
Connected
Prepaid Balance $9.00

Figure 10D

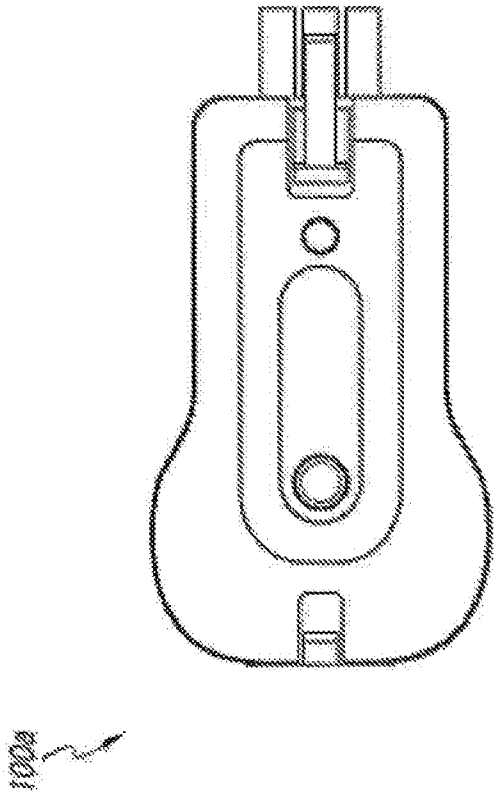


Figure 12

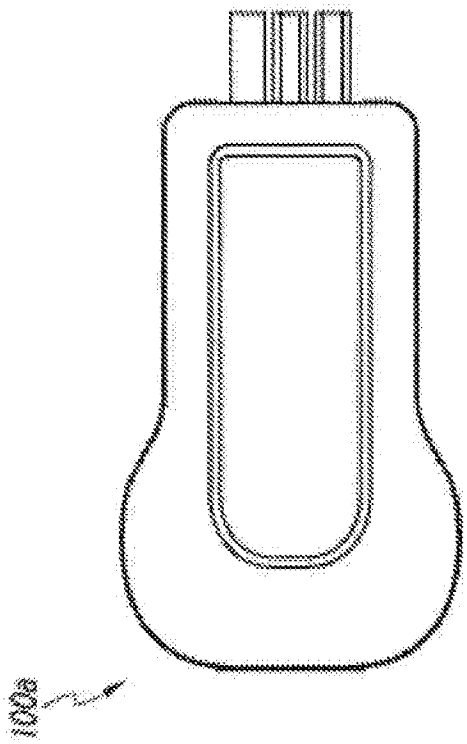


Figure 13

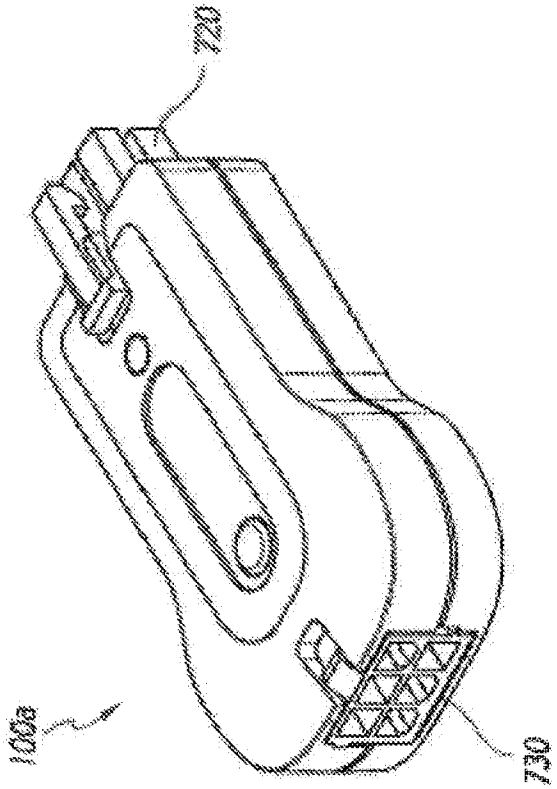


Figure 11

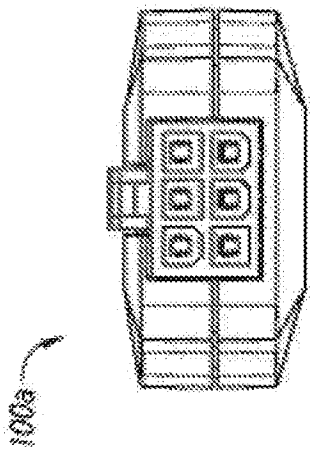


Figure 16

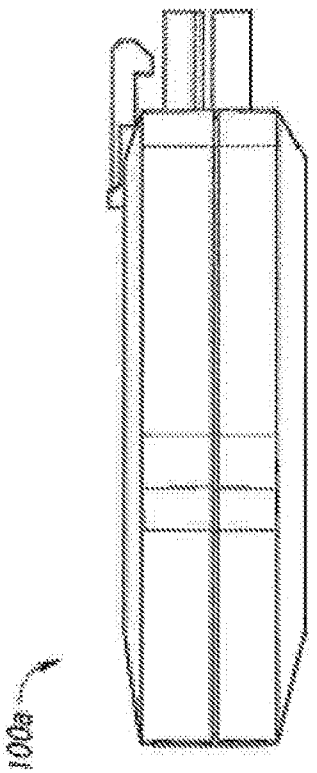


Figure 14

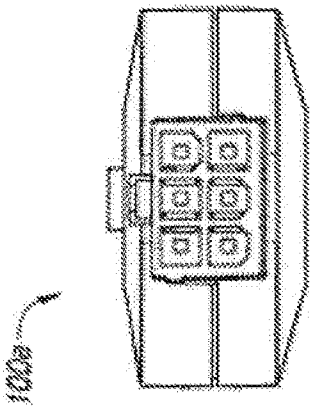


Figure 15

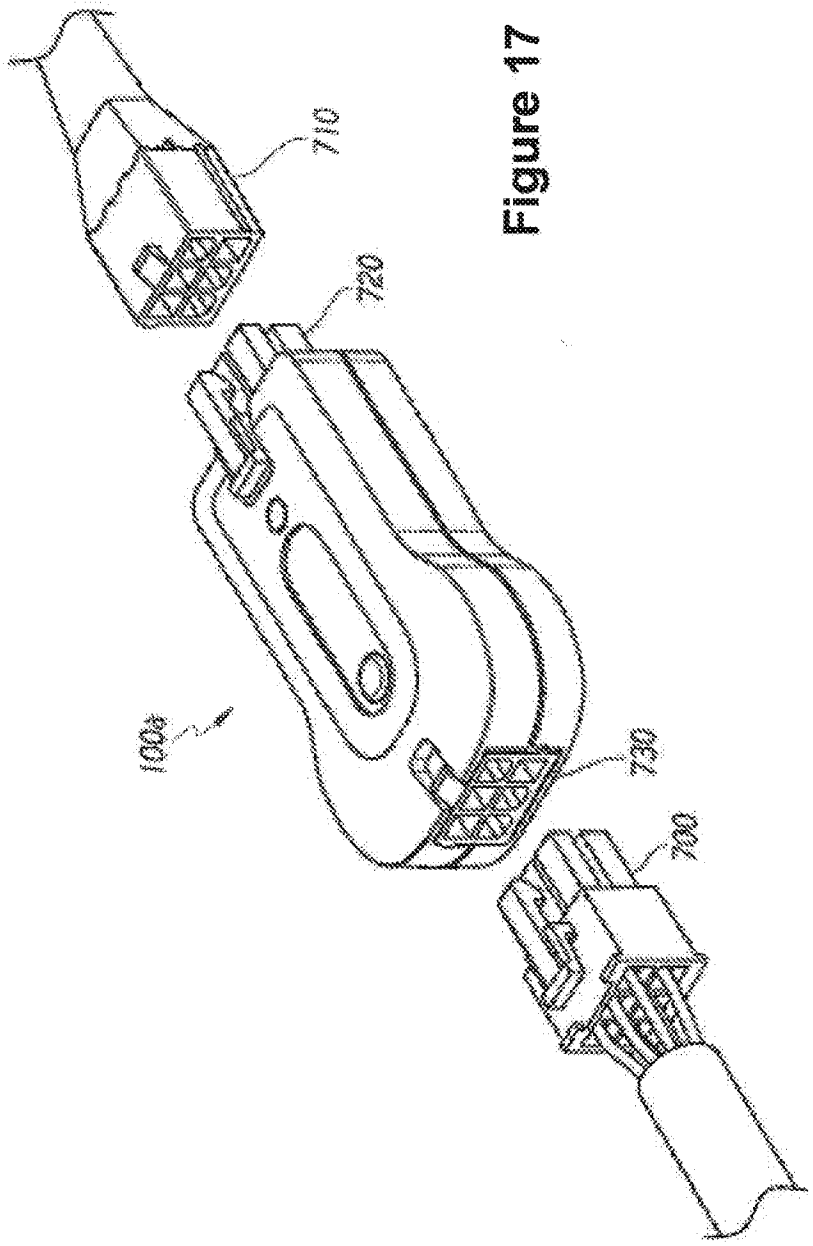


Figure 17

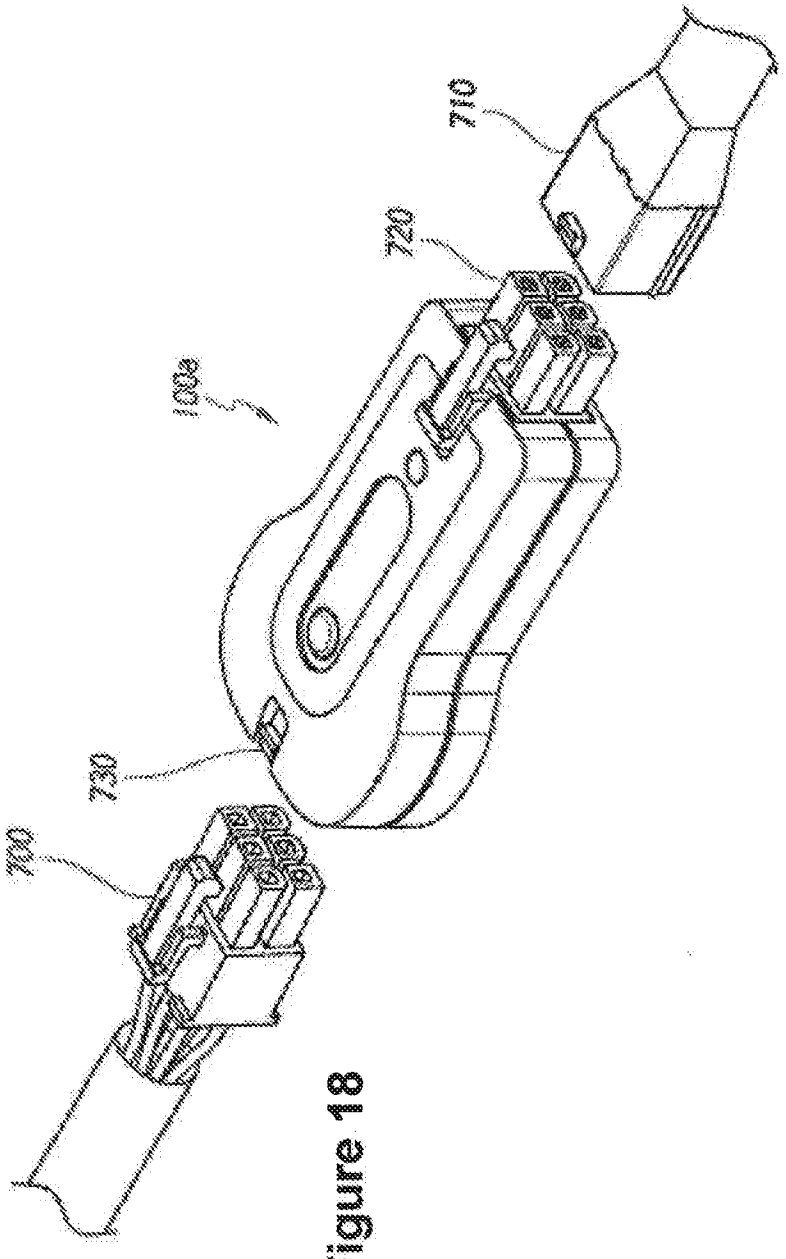


Figure 18

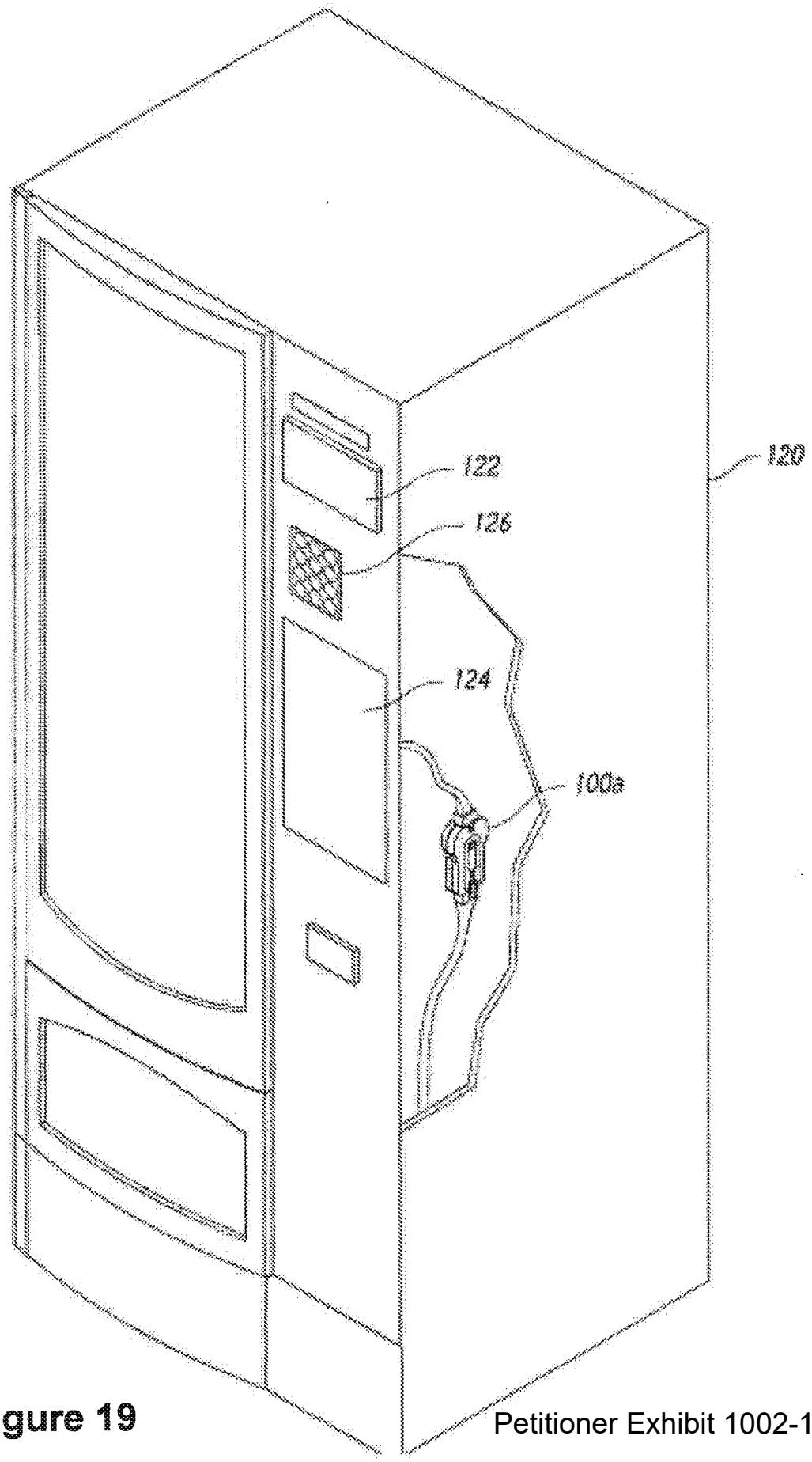


Figure 19

Petitioner Exhibit 1002-1303

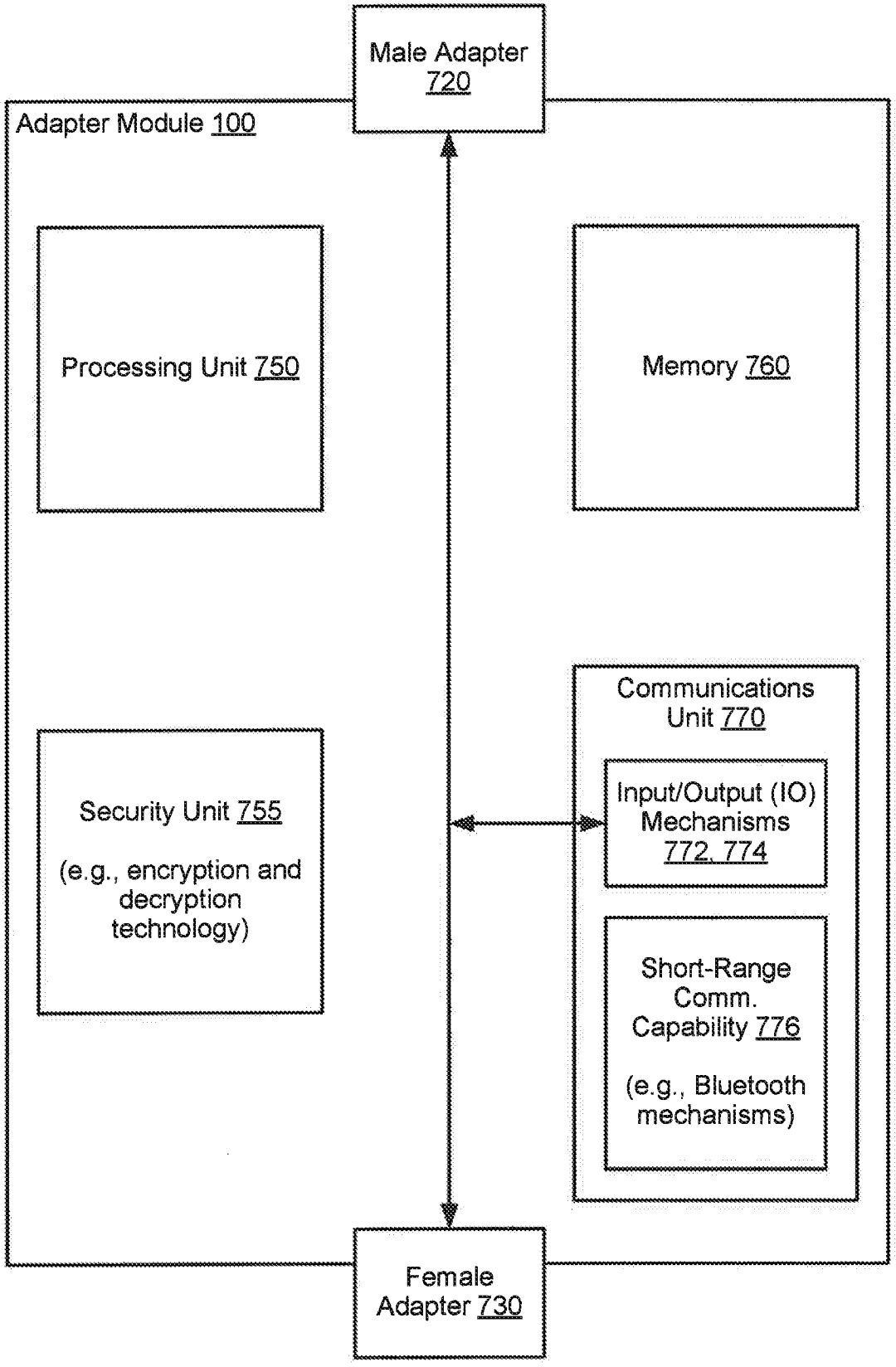


Figure 20 Petitioner Exhibit 1002-1304

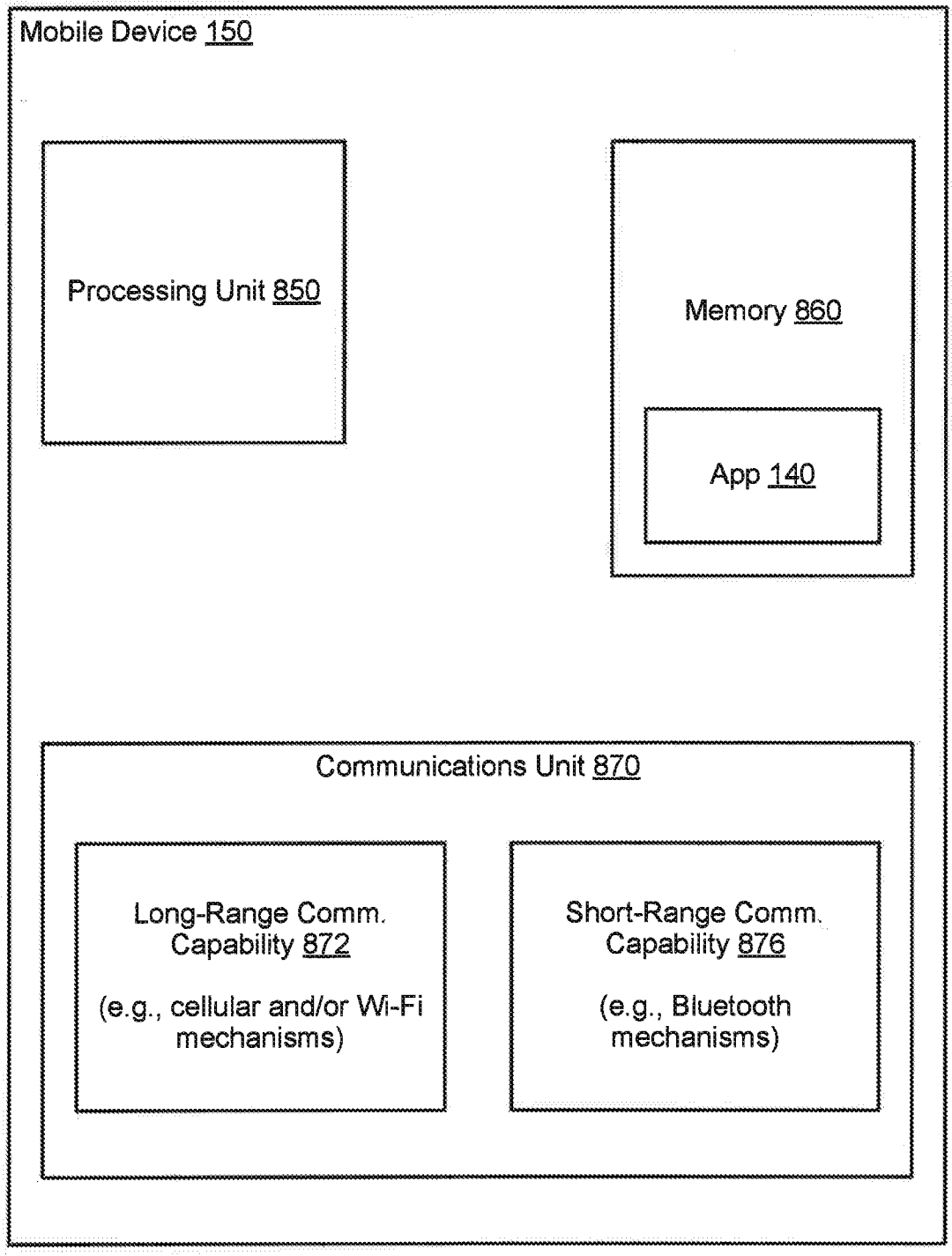

Mobile Device 150
Processing Unit 850
Memory 860
App 140
Communications Unit 870
Long-Range Comm. Capability 872
(e.g., cellular and/or Wi-Fi mechanisms)
Short-Range Comm. Capability 876
(e.g., Bluetooth mechanisms)

Figure 21

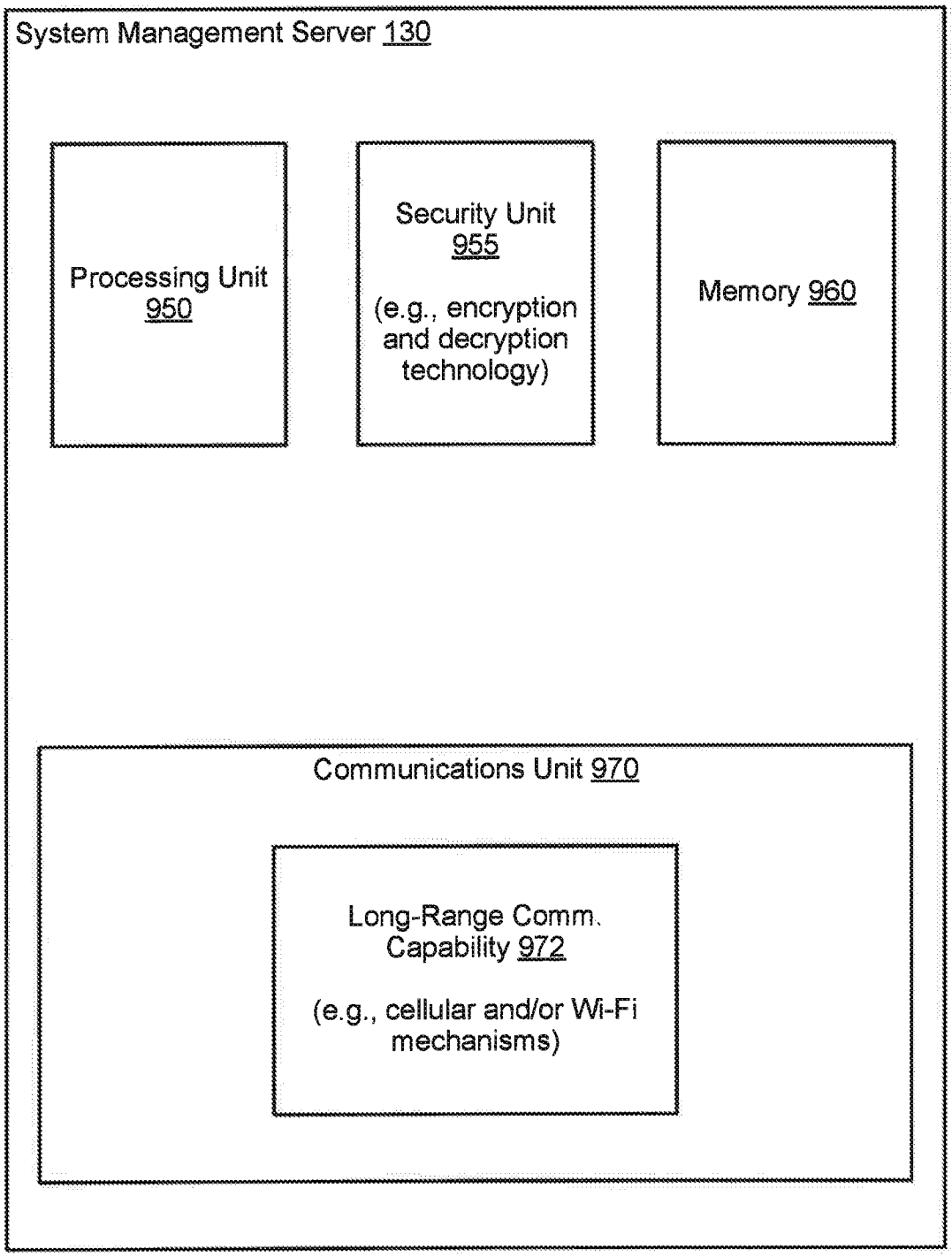

System Management Server 130
Processing Unit 950
Security Unit 955
(e.g., encryption and decryption technology)
Memory 960
Communications Unit 970
Long-Range Comm. Capability 972
(e.g., cellular and/or Wi-Fi mechanisms)

Figure 22

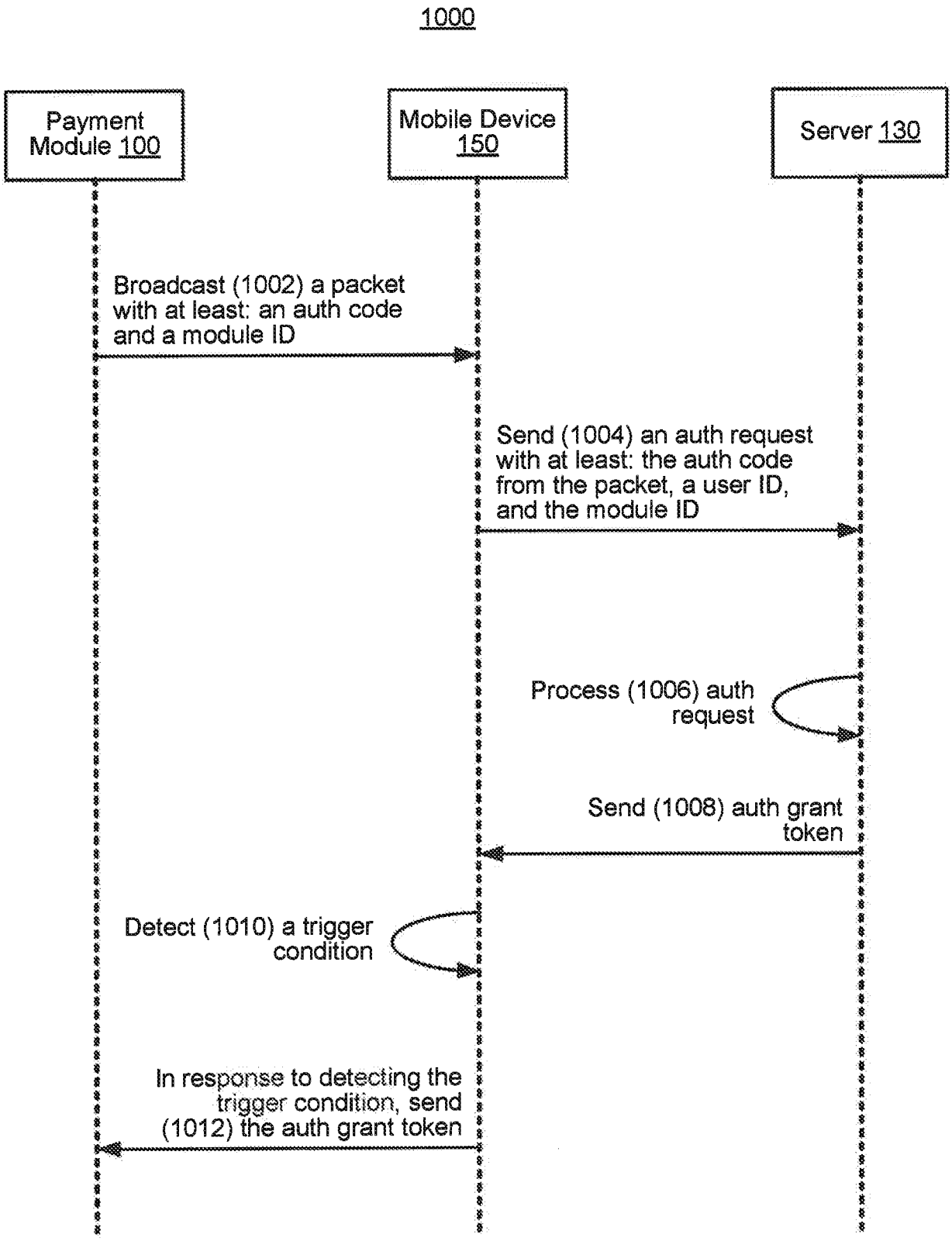

1000
Payment Module 100
Mobile Device 150
Server 130
Broadcast (1002) a packet with at least: an auth code and a module ID
Send (1004) an auth request with at least: the auth code from the packet, a user ID, and the module ID
Process (1006) auth request
Send (1008) auth grant token
Detect (1010) a trigger condition
In response to detecting the trigger condition, send (1012) the auth grant token

Figure 23

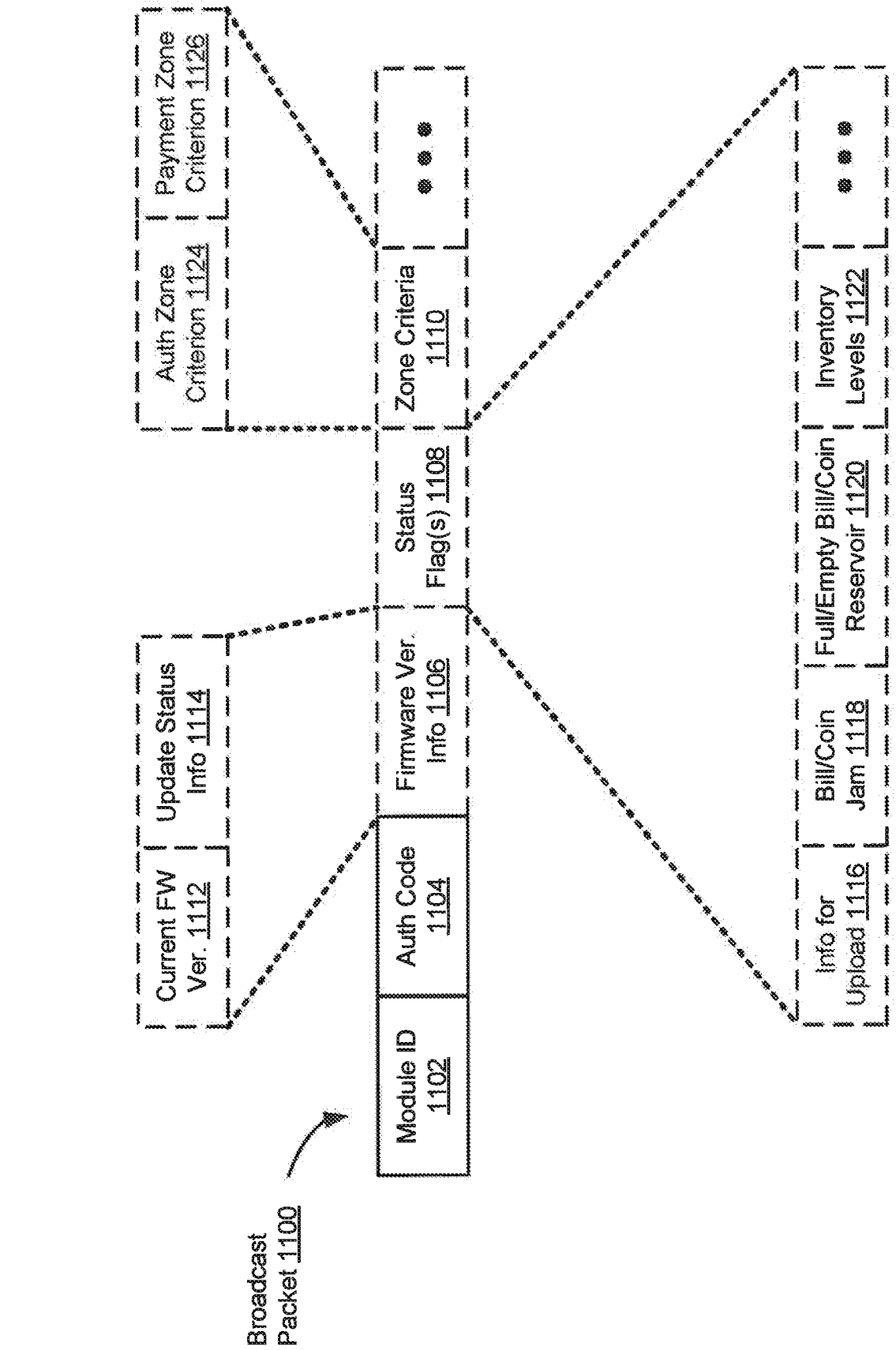

Broadcast Packet 1100
Module ID 1102
Auth Code 1104
Firmware Ver. Info 1106
Status Flag(s) 1108
Zone Criteria 1110
Current FW Ver. 1112
Update Status Info 1114
Auth Zone Criterion 1124
Payment Zone Criterion 1126
Info for Upload 1116
Bill/Coin Jam 1118
Full/Empty Bill/Coin Reservoir 1120
Inventory Levels 1122

Figure 24A

Figure 24B

Figure 24C

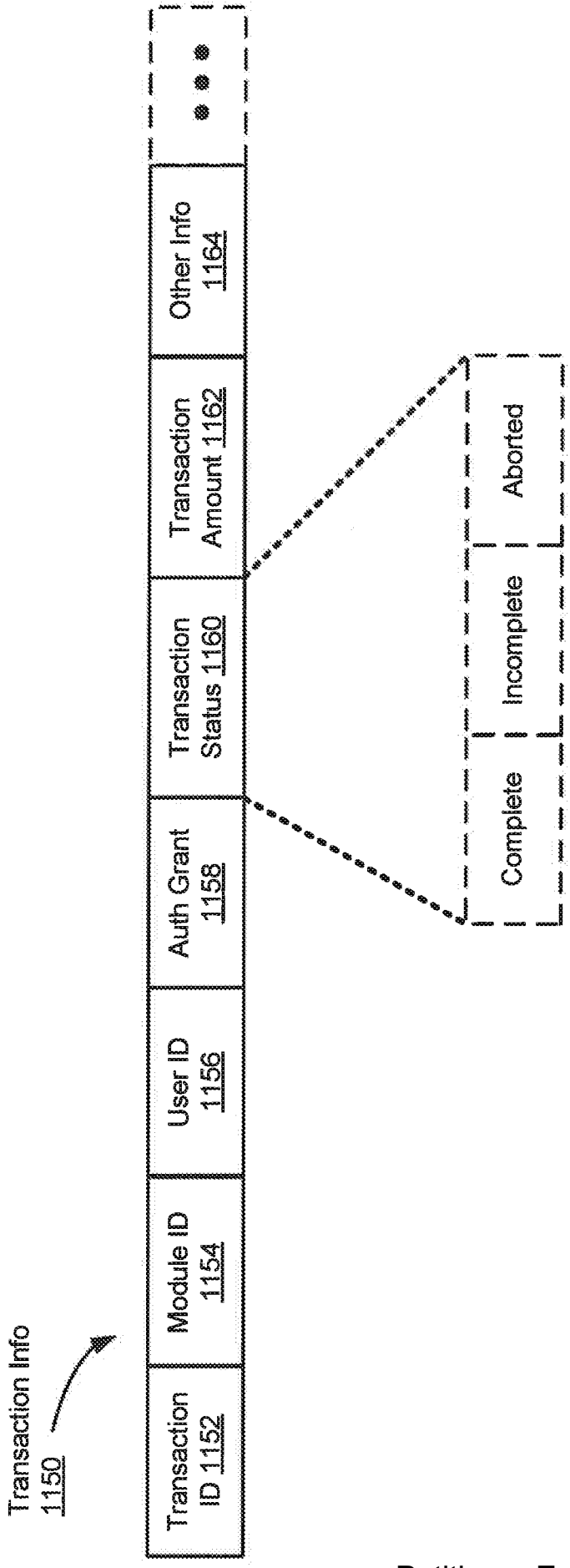

Transaction Info 1150
Transaction ID 1152
Module ID 1154
User ID 1156
Auth Grant 1158
Transaction Status 1160
Transaction Amount 1162
Other Info 1164
Complete
Incomplete
Aborted

Figure 24D

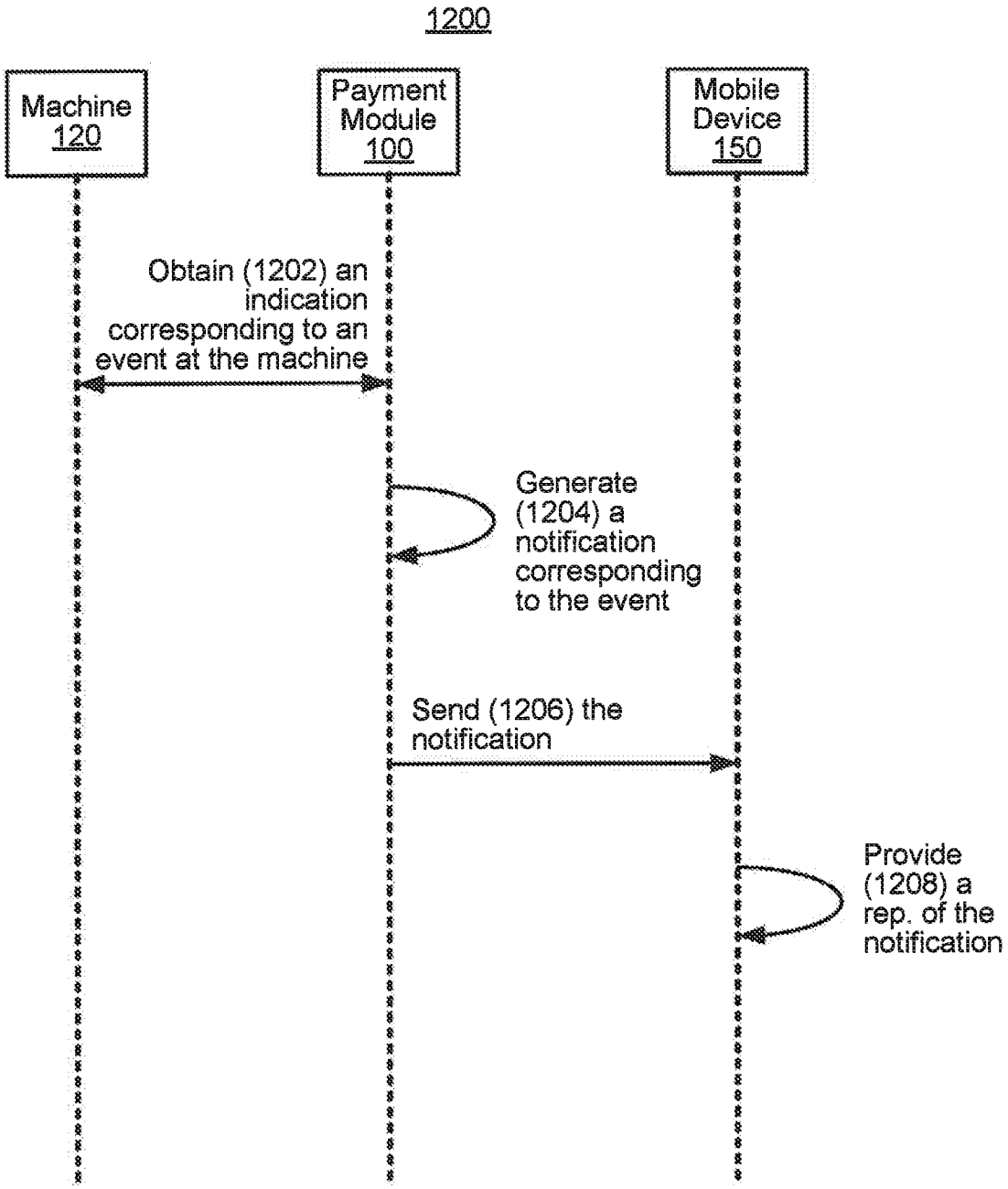
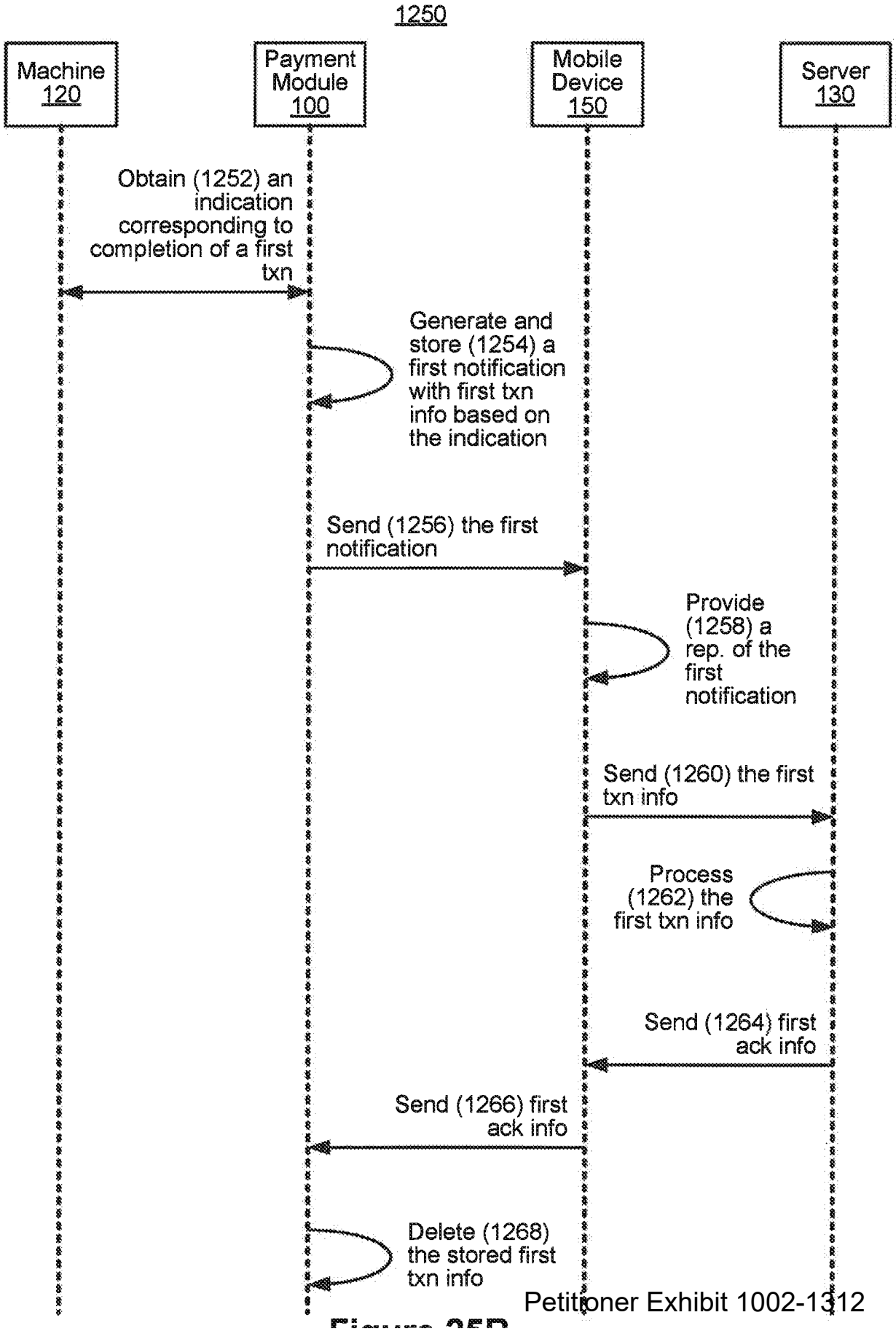

1200
Machine 120
Payment Module 100
Mobile Device 150
Obtain (1202) an indication corresponding to an event at the machine
Generate (1204) a notification corresponding to the event
Send (1206) the notification
Provide (1208) a rep. of the notification

Figure 25A



Petitioner Exhibit 1002-1312

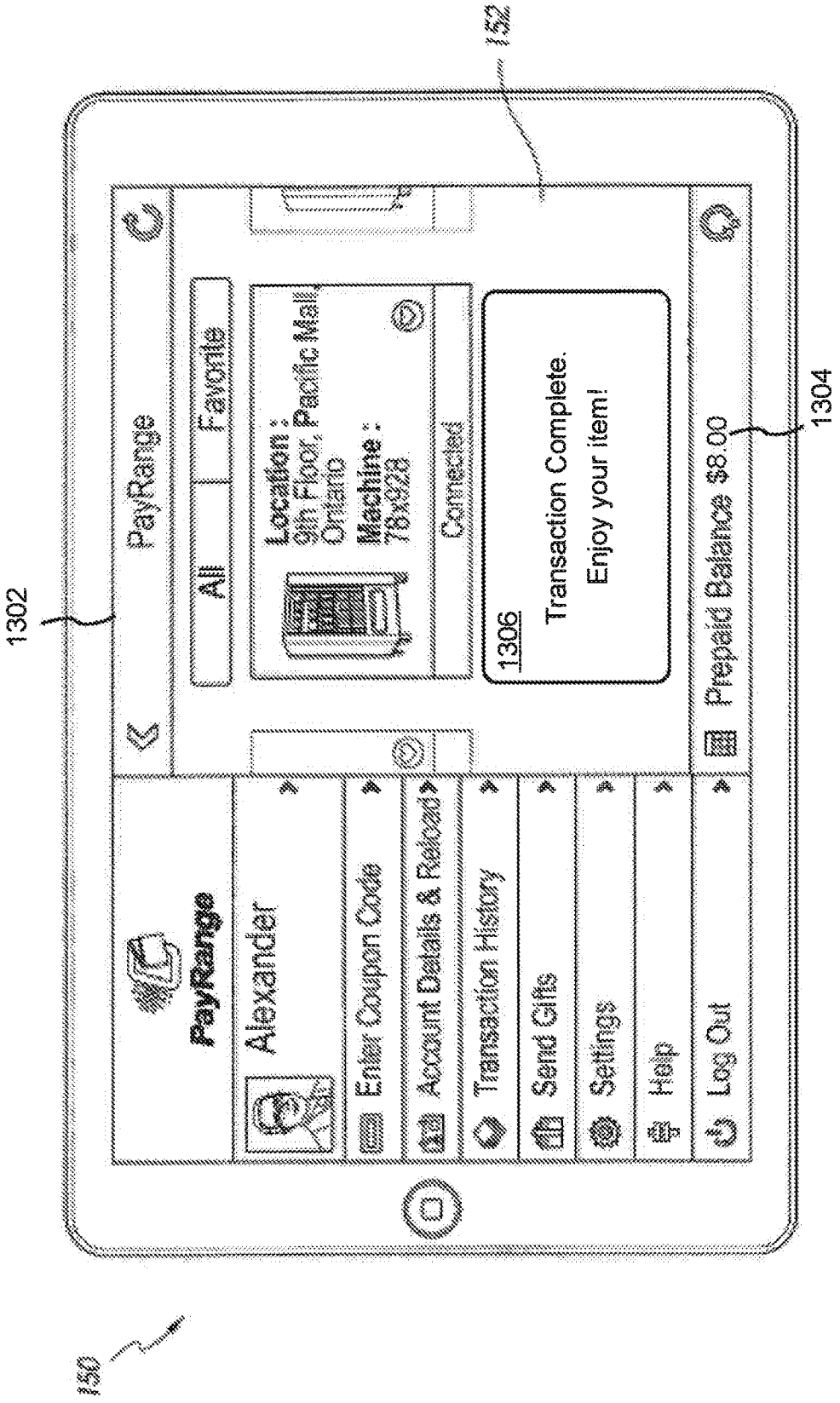

150
1302
152
1304
PayRange
Favorite
All
Location :
9th Floor, Pacific Mall
Orlando
Machine :
78x928
Connected
1306
Transaction Complete.
Enjoy your item!
Prepaid Balance $8.00
PayRange
Alexander
Enter Coupon Code
Account Details & Reload
Transaction History
Send Gifts
Settings
Help
Log Out

Figure 26A

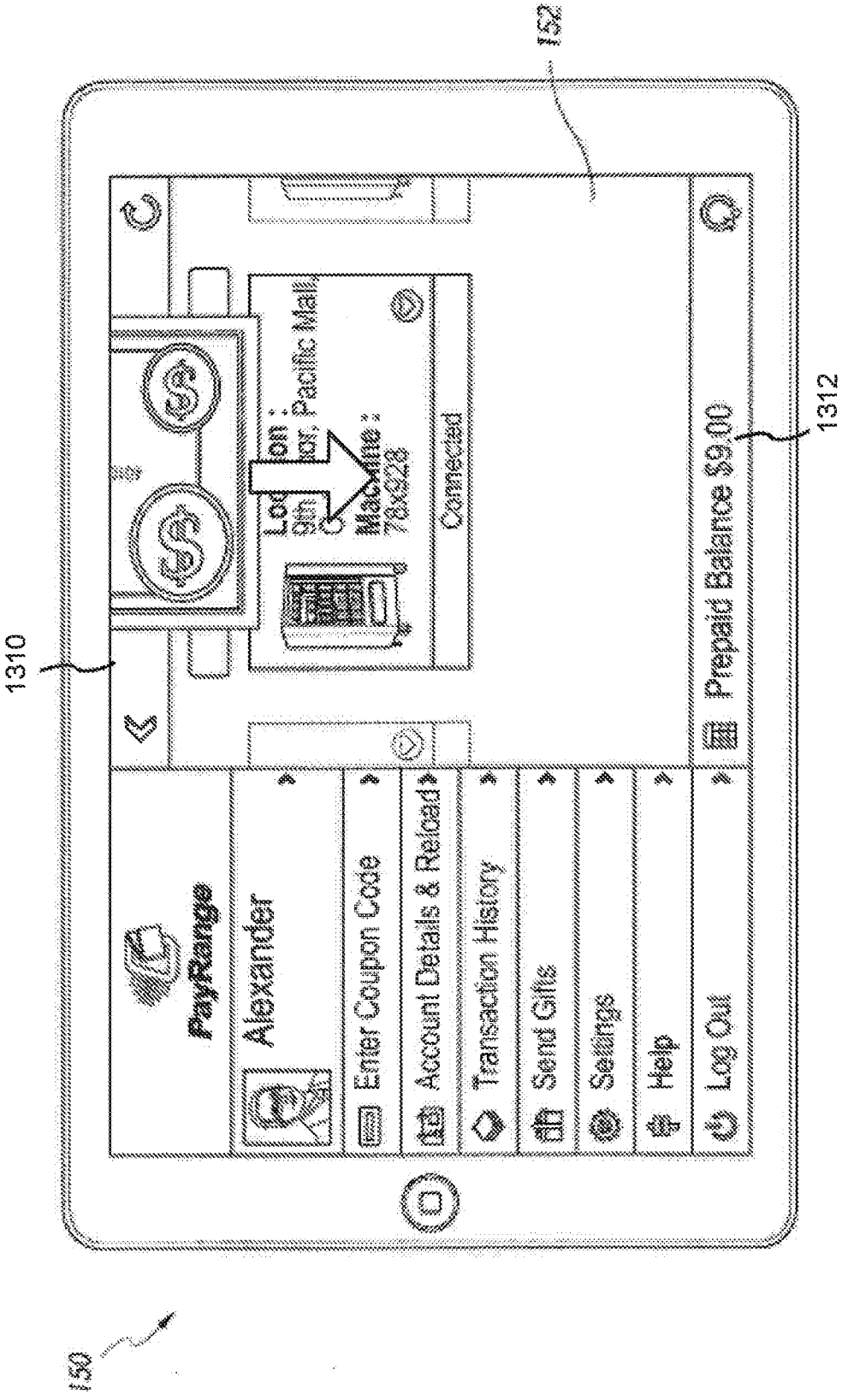

150
152
1310
1312
PayRange
Alexander
Enter Coupon Code
Account Details & Reload
Transaction History
Send Gifts
Settings
Help
Log Out
Prepaid Balance $9.00
Connected
Machine :
78x628

Figure 26B

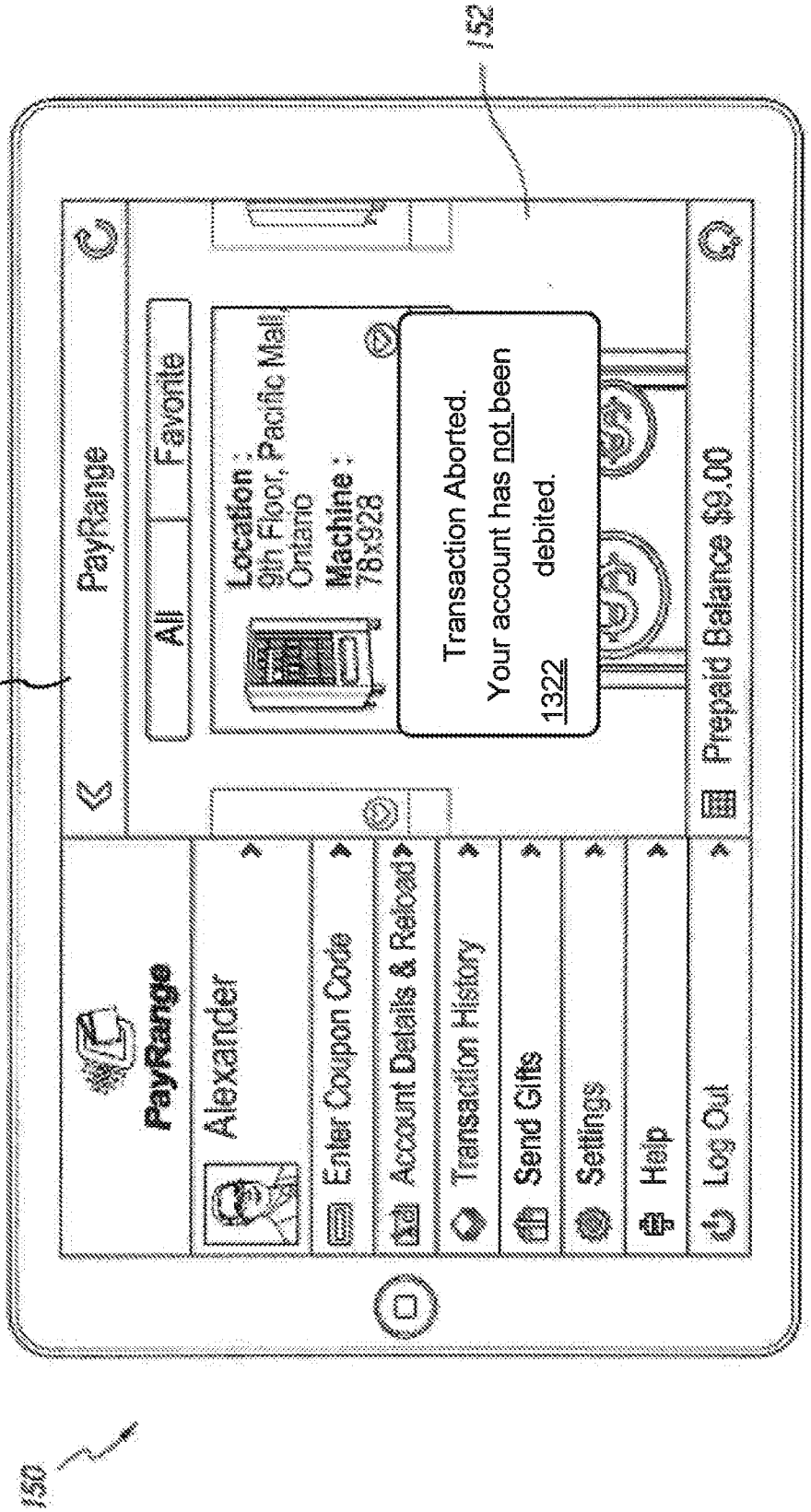

150
152
1320
PayRange
Alexander
Enter Coupon Code
Account Details & Reload
Transaction History
Send Gifts
Settings
Help
Log Out
All
Favorite
Location :
9th Floor, Pacific Mall
Ontario
Machine :
78x928
Transaction Aborted.
Your account has not been
debited.
1322
Prepaid Balance $9.00

Figure 26C

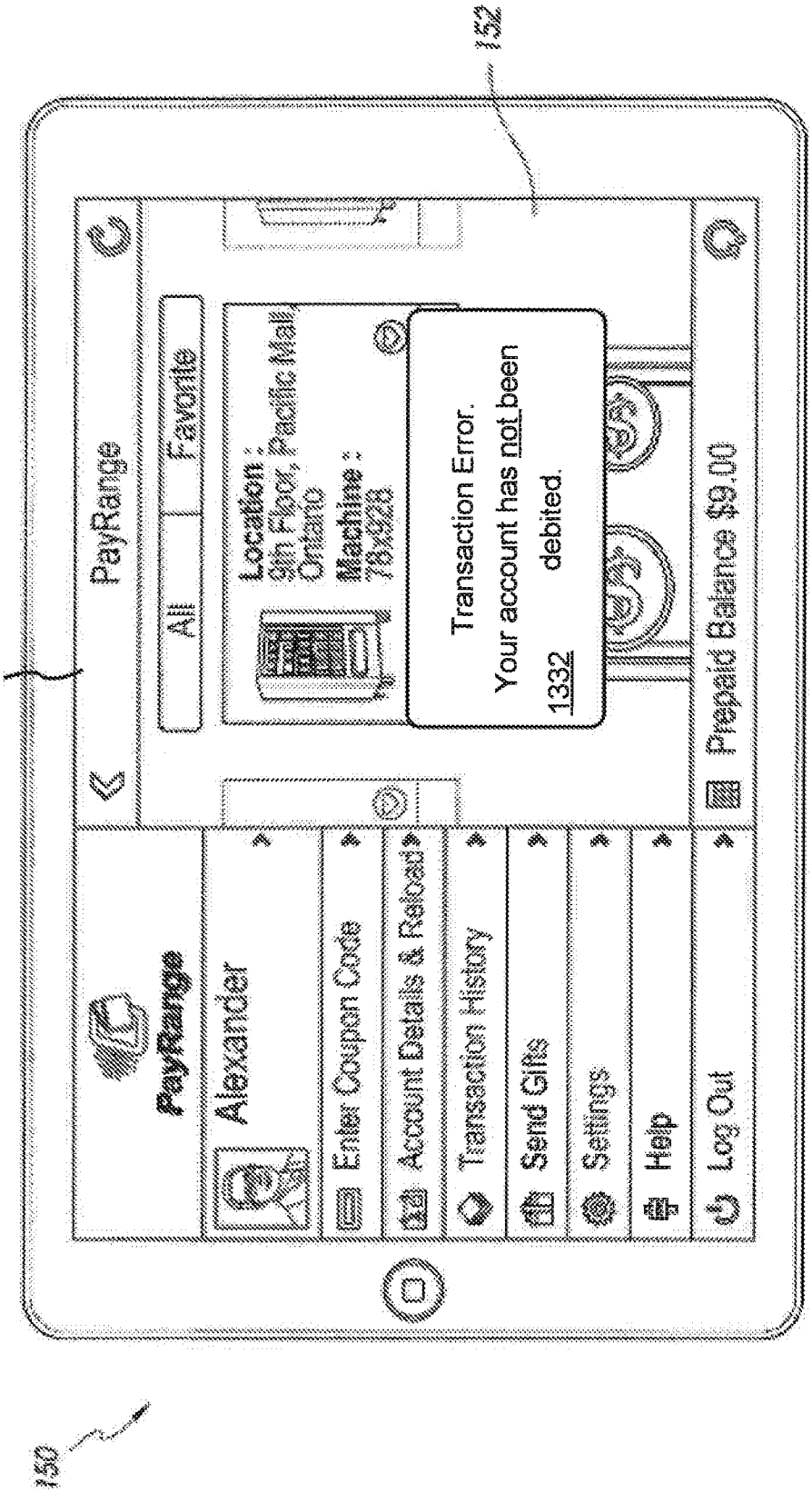

150
152
1330
PayRange
Alexander
Enter Coupon Code
Account Details & Reload
Transaction History
Send Gifts
Settings
Help
Log Out
All
Favorite
Location :
9th Floor, Pacific Mall,
Ontario
Machine :
78x928
Transaction Error.
Your account has not been
debited.
1332
Prepaid Balance $9.00

Figure 26D

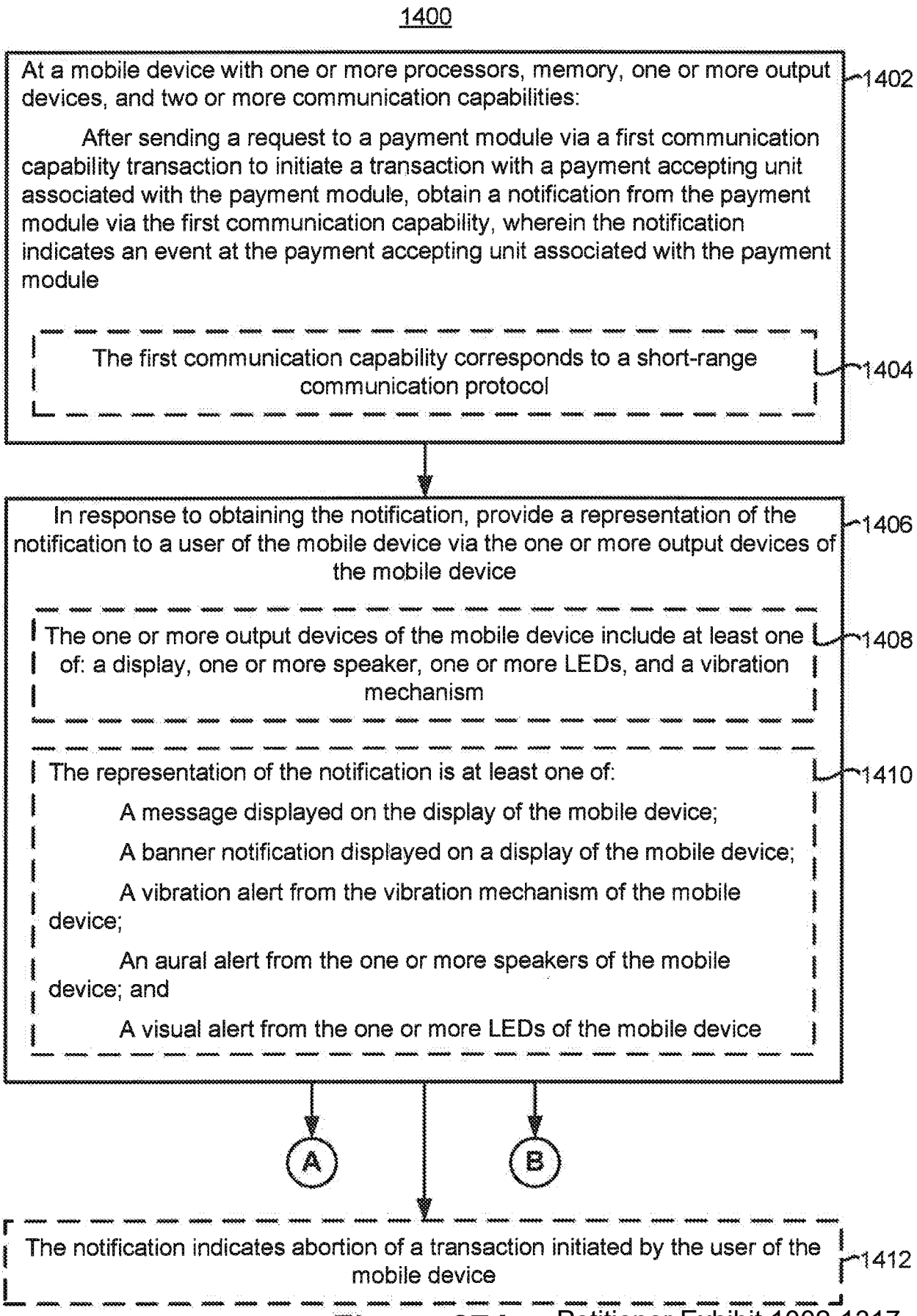


Figure 27A

Petitioner Exhibit 1002-1317

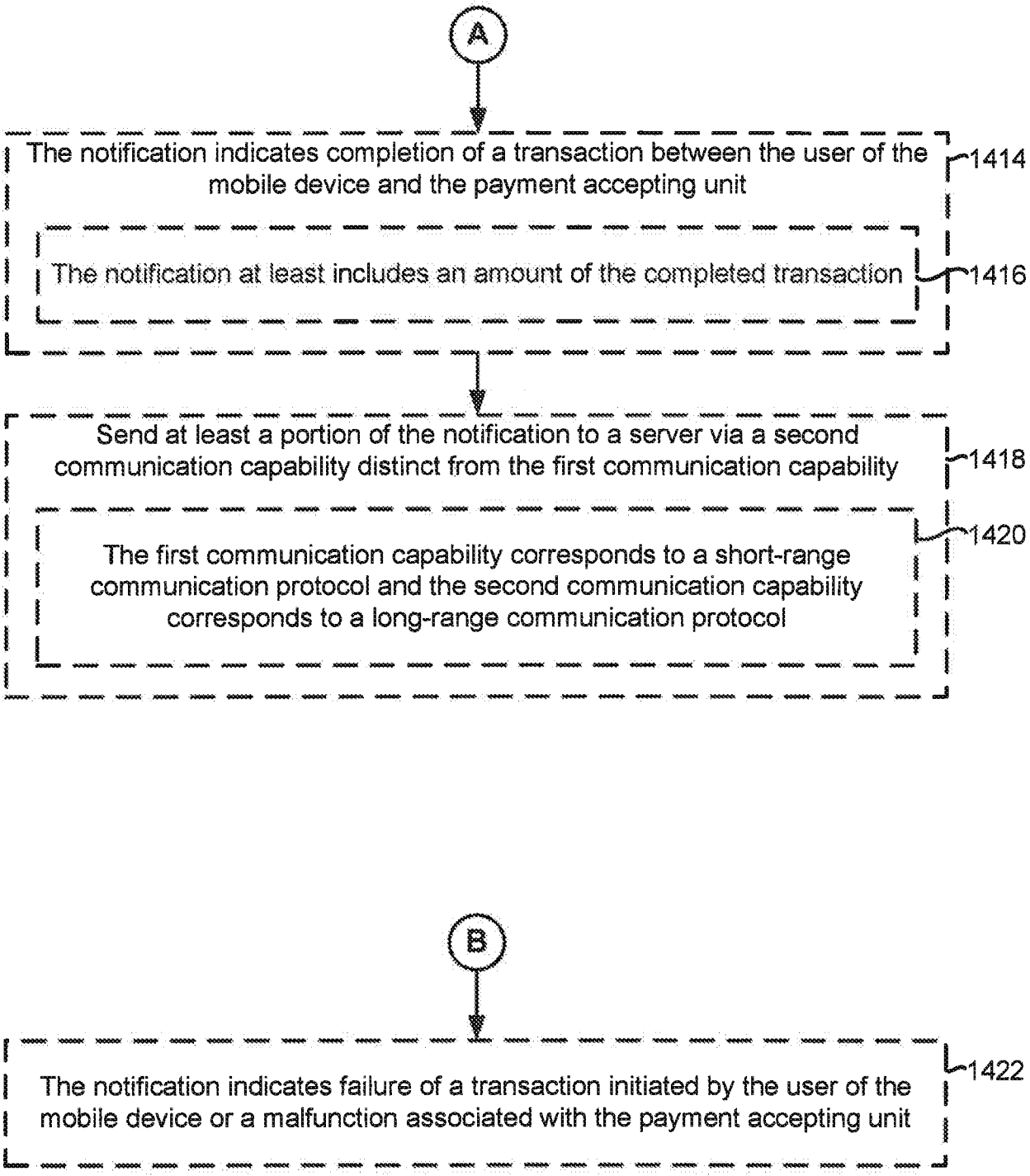

A
The notification indicates completion of a transaction between the user of the mobile device and the payment accepting unit
1414
The notification at least includes an amount of the completed transaction
1416
Send at least a portion of the notification to a server via a second communication capability distinct from the first communication capability
1418
The first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol
1420
B
The notification indicates failure of a transaction initiated by the user of the mobile device or a malfunction associated with the payment accepting unit
1422

Figure 27B

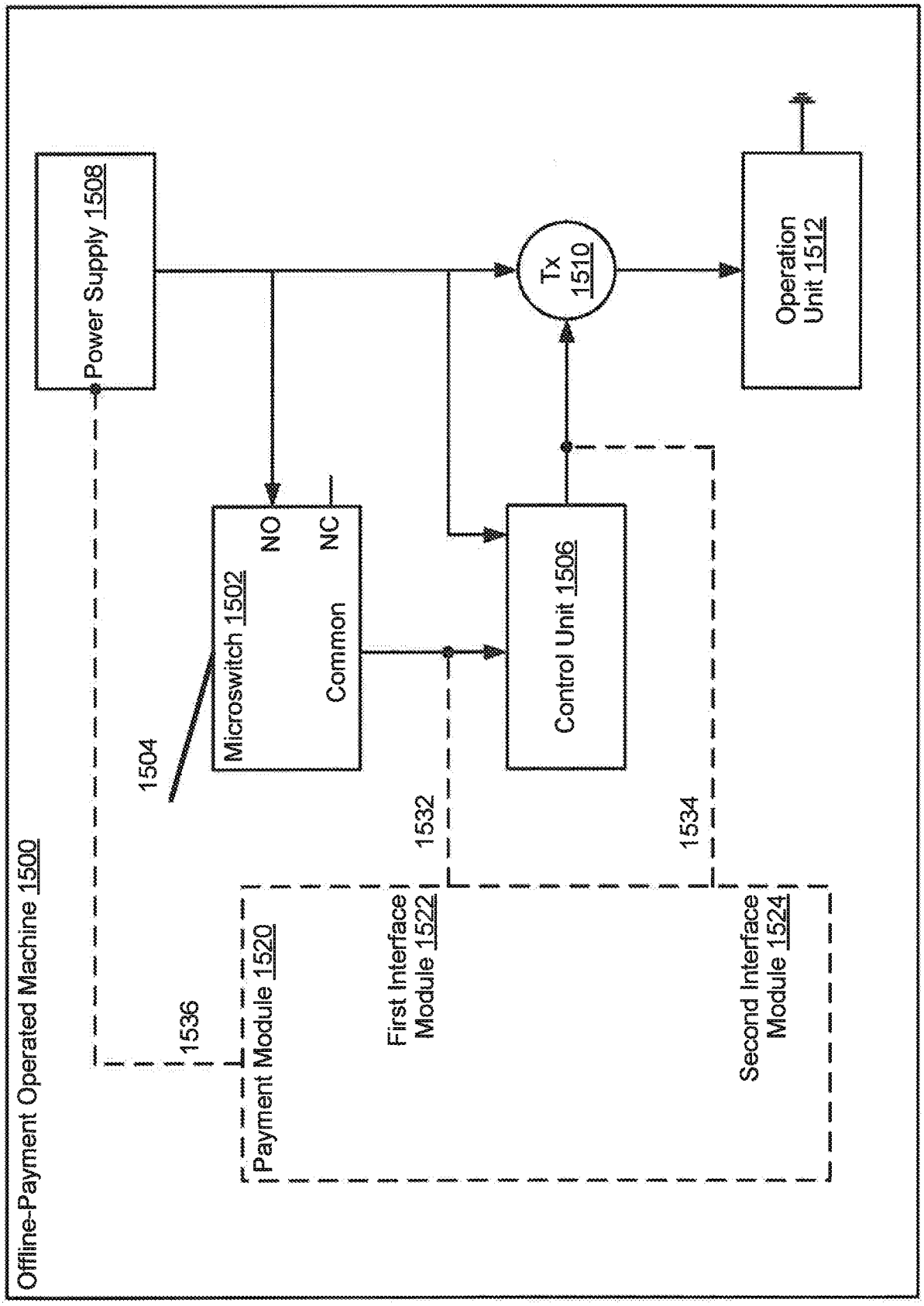

Offline-Payment Operated Machine 1500
Power Supply 1508
Tx 1510
Operation Unit 1512
Microswitch 1502
NO
NC
Common
1504
Control Unit 1506
1536
Payment Module 1520
First Interface Module 1522
1532
1534
Second Interface Module 1524

Figure 28A

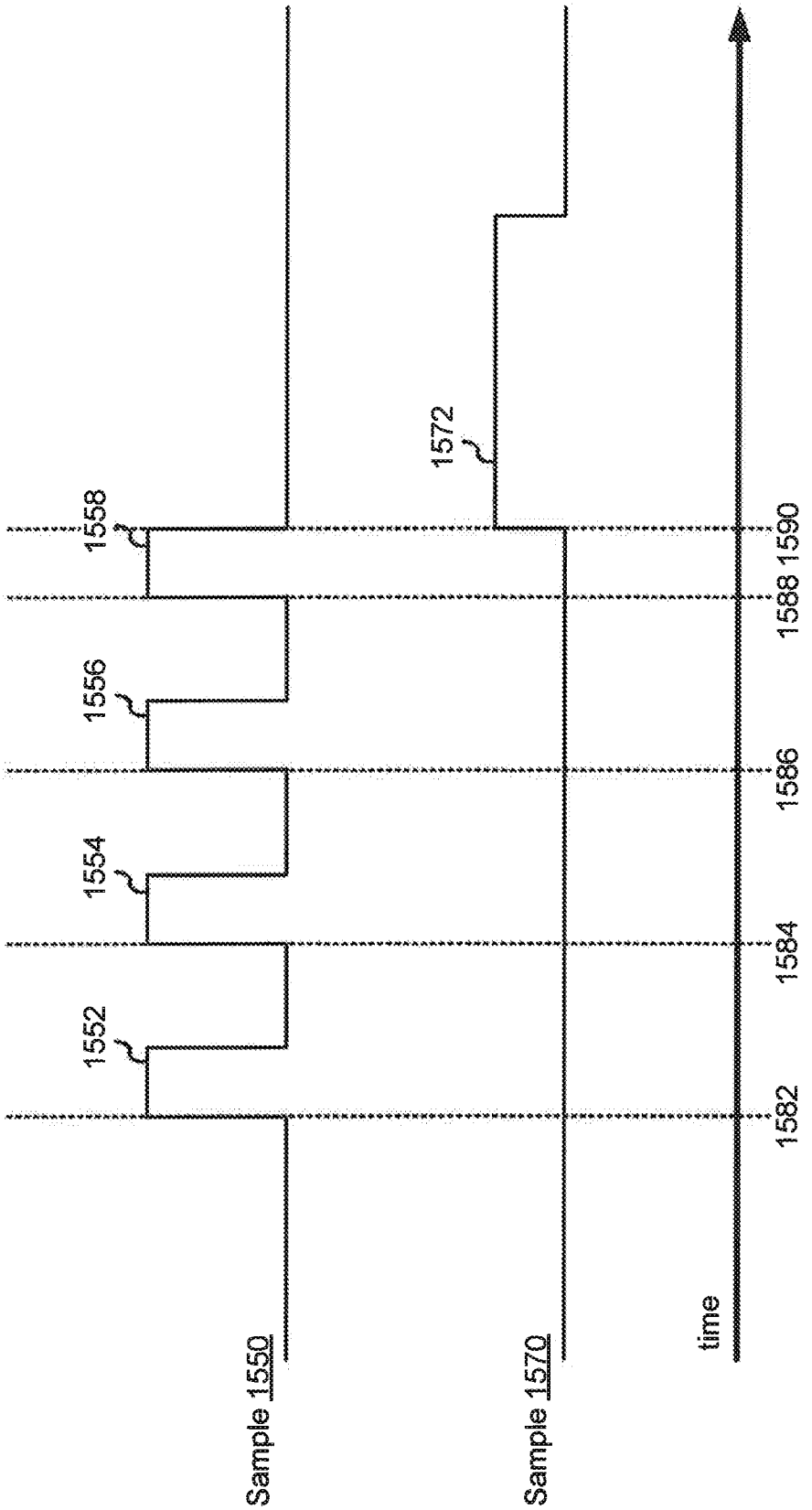

Sample 1550
Sample 1570
time
1552
1554
1556
1558
1572
1582
1584
1586
1588
1590

Figure 28B

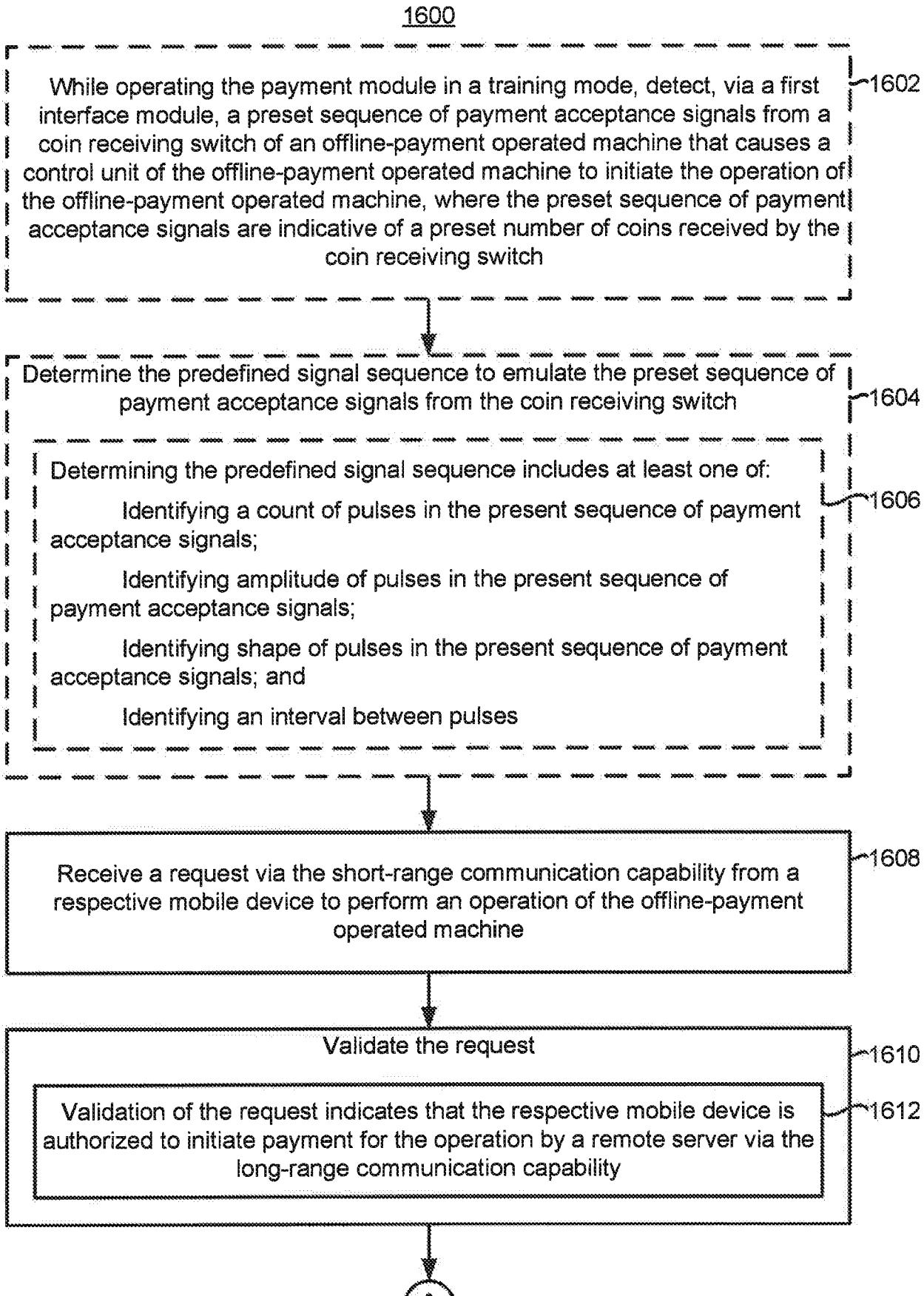


Figure 29A

Petitioner Exhibit 1002-1321

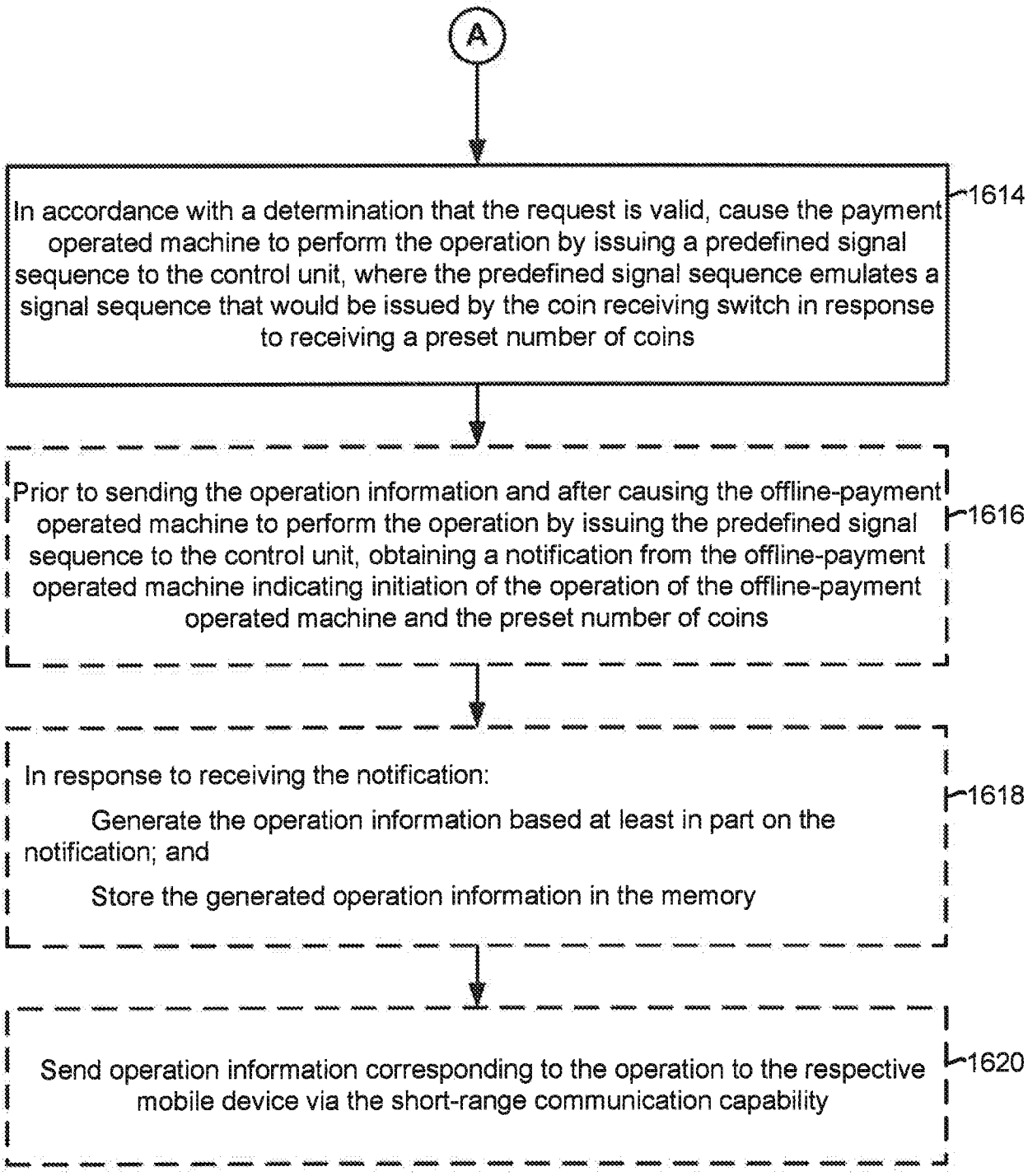

A
In accordance with a determination that the request is valid, cause the payment operated machine to perform the operation by issuing a predefined signal sequence to the control unit, where the predefined signal sequence emulates a signal sequence that would be issued by the coin receiving switch in response to receiving a preset number of coins
1614
Prior to sending the operation information and after causing the offline-payment operated machine to perform the operation by issuing the predefined signal sequence to the control unit, obtaining a notification from the offline-payment operated machine indicating initiation of the operation of the offline-payment operated machine and the preset number of coins
1616
In response to receiving the notification:
Generate the operation information based at least in part on the notification; and
Store the generated operation information in the memory
1618
Send operation information corresponding to the operation to the respective mobile device via the short-range communication capability
1620

Figure 29B

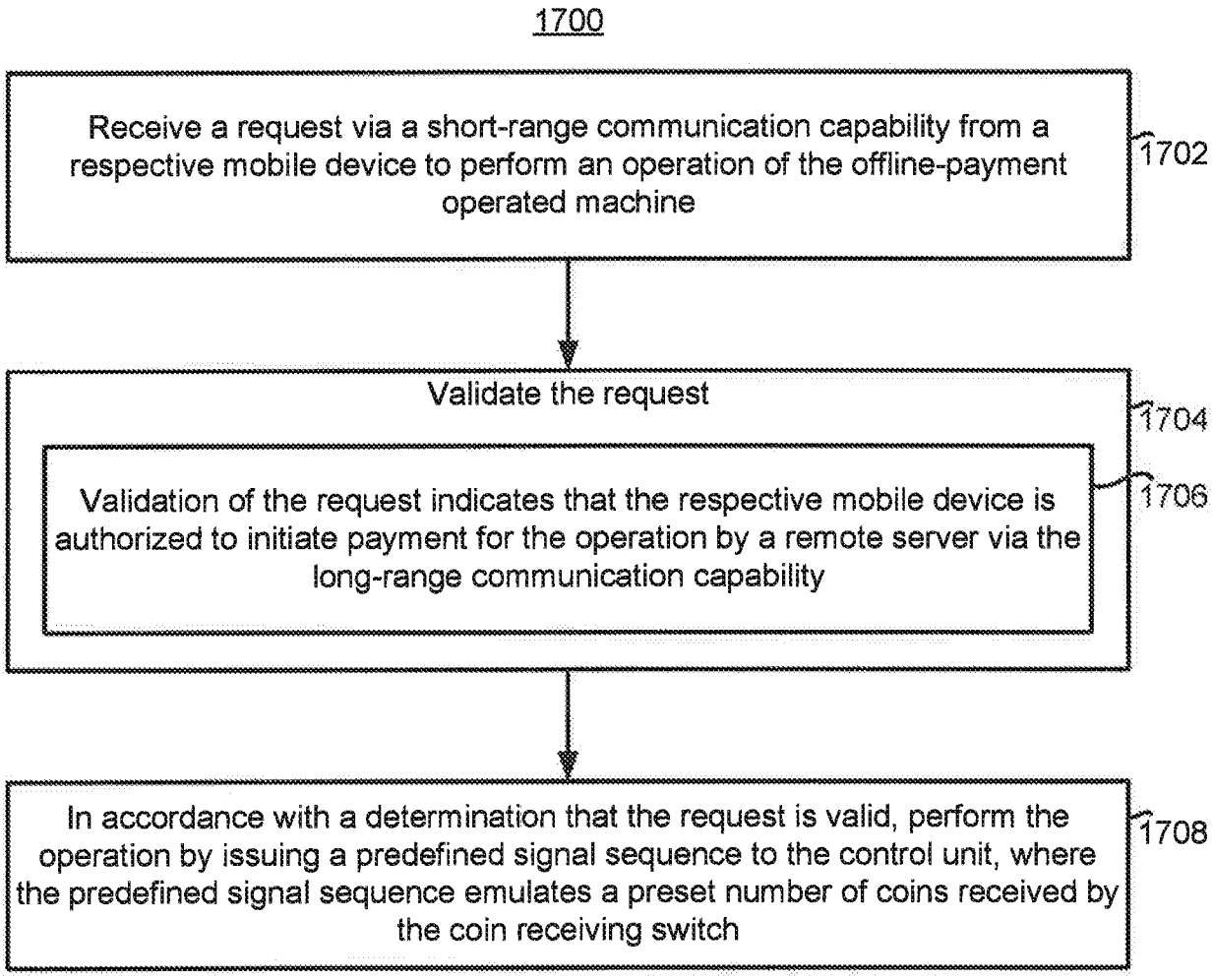

1700
Receive a request via a short-range communication capability from a respective mobile device to perform an operation of the offline-payment operated machine
1702
Validate the request
1704
Validation of the request indicates that the respective mobile device is authorized to initiate payment for the operation by a remote server via the long-range communication capability
1706
In accordance with a determination that the request is valid, perform the operation by issuing a predefined signal sequence to the control unit, where the predefined signal sequence emulates a preset number of coins received by the coin receiving switch
1708

Figure 30

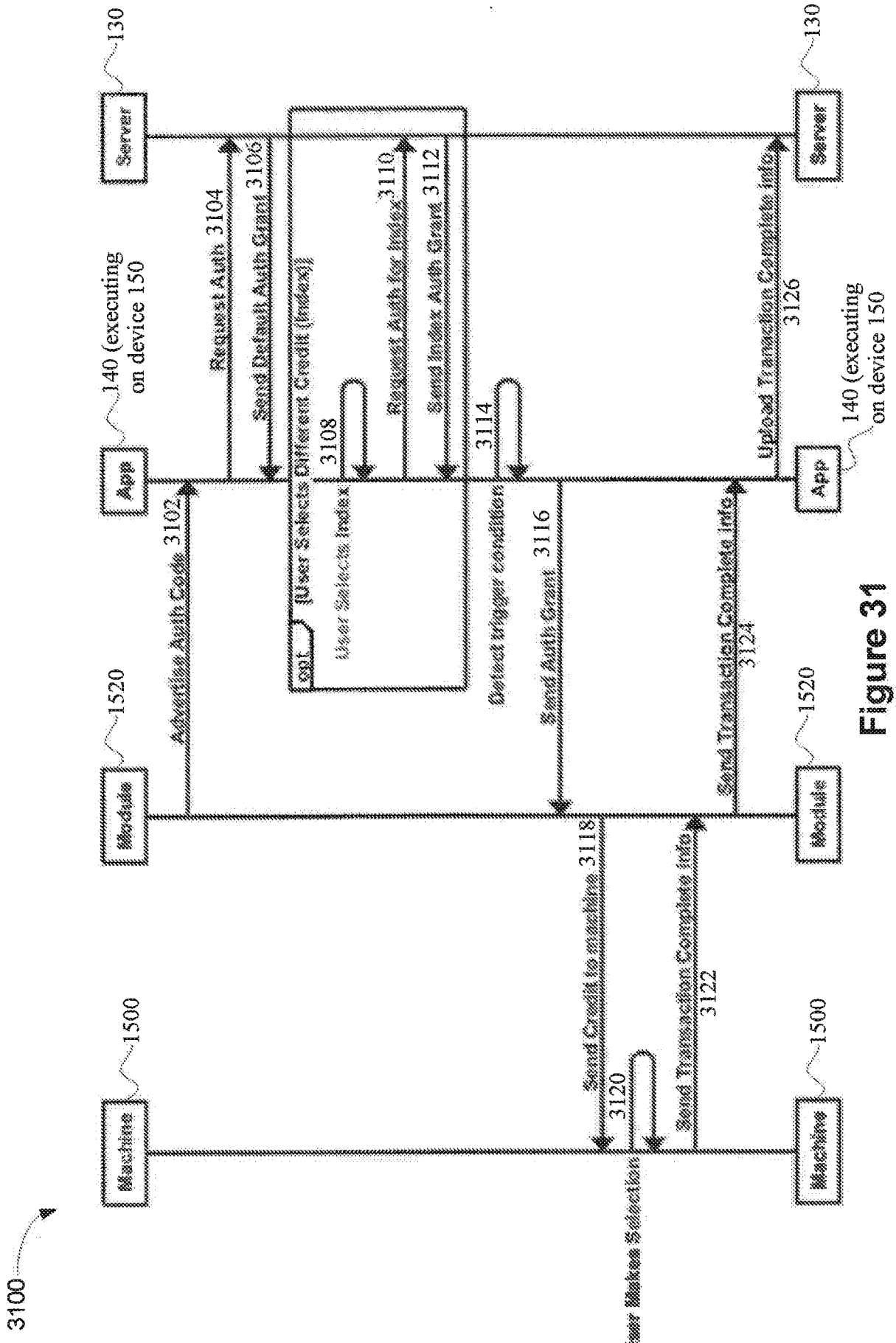

3100
Machine
1500
Module
1520
App
140 (executing on device 150
Server
130
User Makes Selection
Obtain Auth Code 3102
Request Auth 3104
Send Default Auth Grant 3106
loop
[User Selects Different Credit (Index)]
User Selects Index 3108
Request Auth for Index 3110
Send Index Auth Grant 3112
Detect trigger condition 3114
Send Auth Grant 3116
Send Credit to machine 3118
Send Transaction Complete Info 3120
Send Transaction Complete Info 3122
Send Transaction Complete Info 3124
Upload Transaction Complete Info 3126

Figure 31

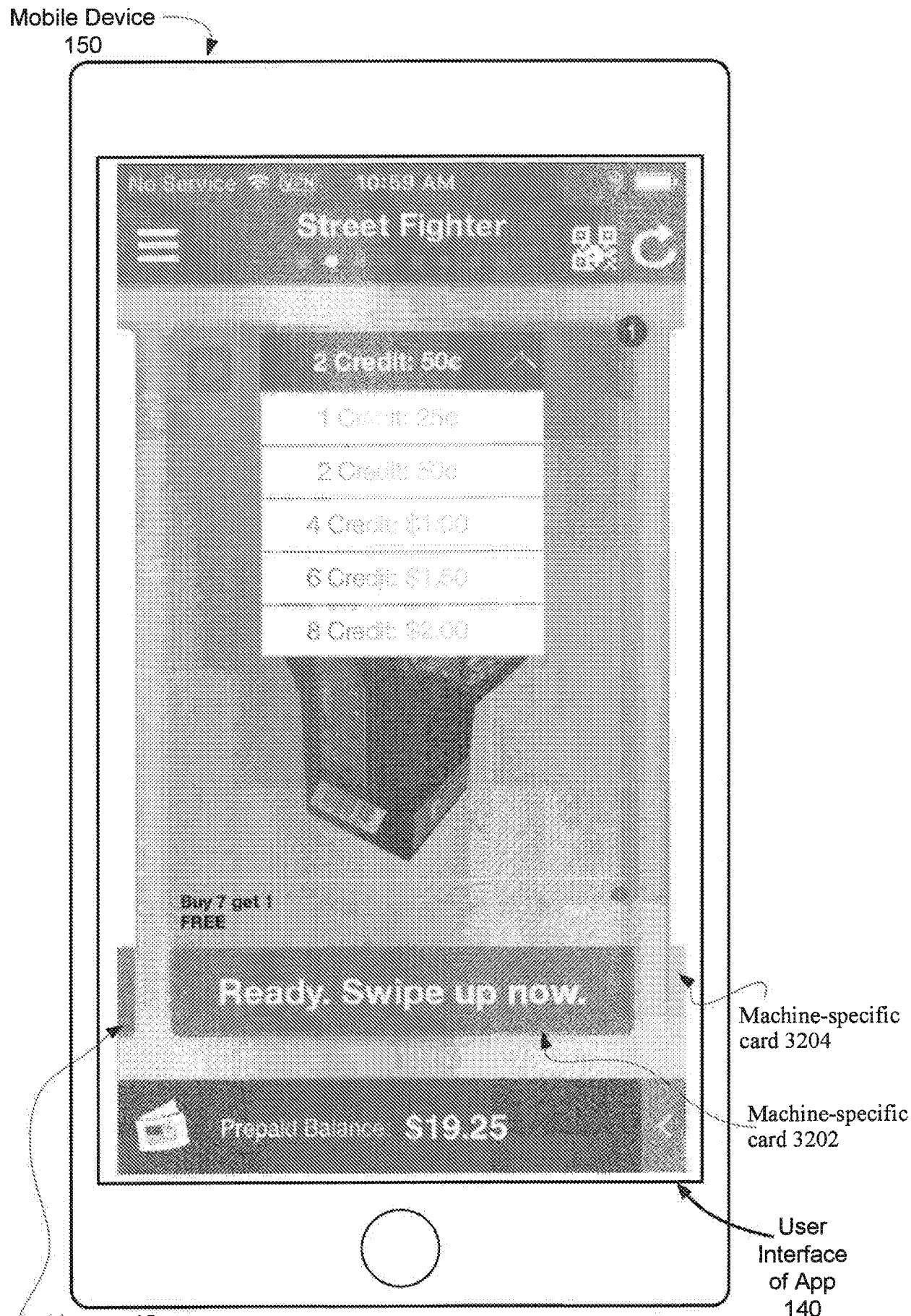

Mobile Device
150
No Service
10:09 AM
Street Fighter
2 Credit: 50c
1 Credit: 25c
2 Credit: 50c
4 Credit: $1.00
6 Credit: $1.50
8 Credit: $2.00
Buy 7 get 1
FREE
Ready. Swipe up now.
Prepaid Balance: $19.25
Machine-specific
card 3204
Machine-specific
card 3202
User
Interface
of App
140
Machine-specific
card 3206

Figure 32

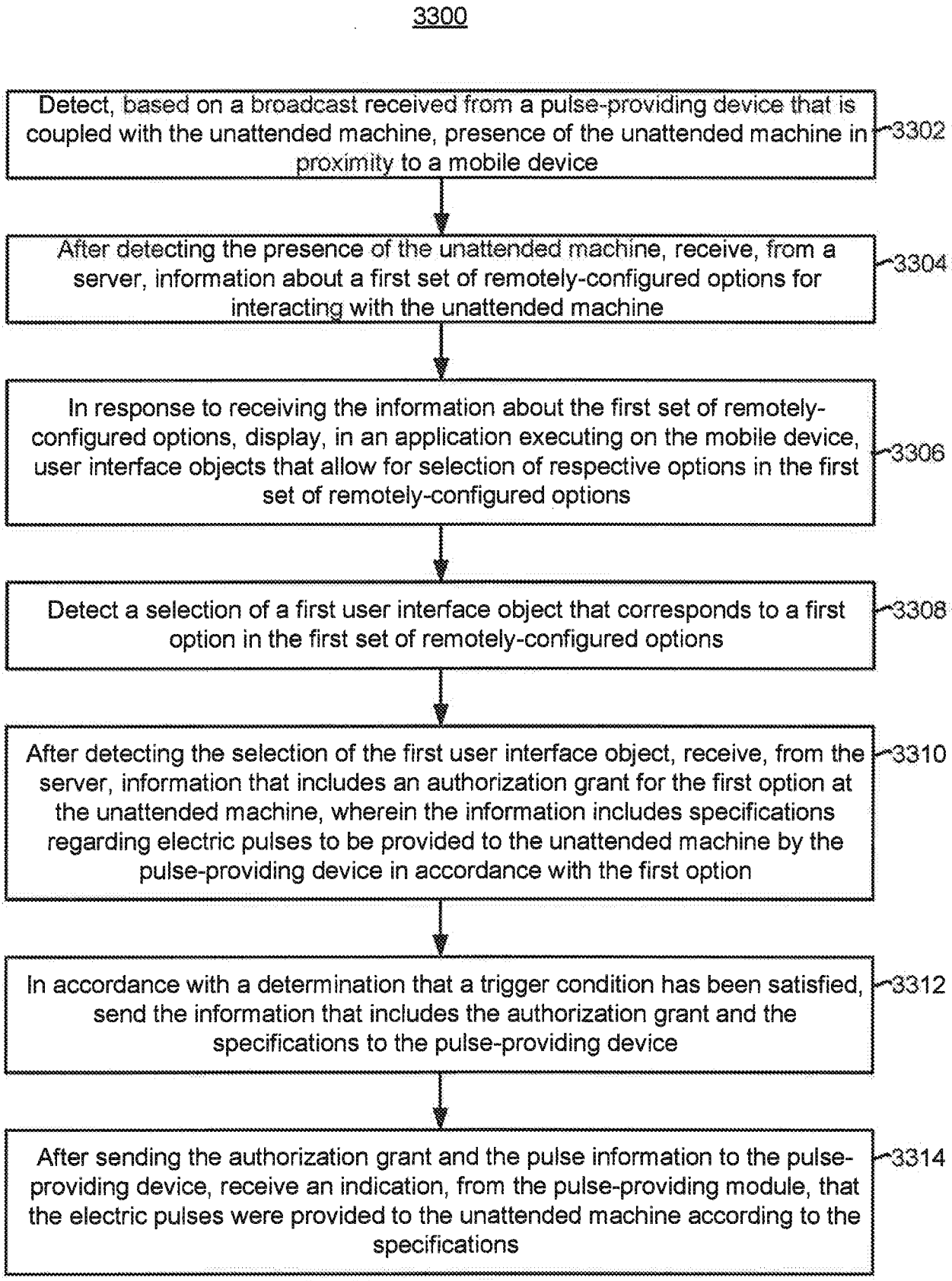

3300
Detect, based on a broadcast received from a pulse-providing device that is coupled with the unattended machine, presence of the unattended machine in proximity to a mobile device
3302
After detecting the presence of the unattended machine, receive, from a server, information about a first set of remotely-configured options for interacting with the unattended machine
3304
In response to receiving the information about the first set of remotely-configured options, display, in an application executing on the mobile device, user interface objects that allow for selection of respective options in the first set of remotely-configured options
3306
Detect a selection of a first user interface object that corresponds to a first option in the first set of remotely-configured options
3308
After detecting the selection of the first user interface object, receive, from the server, information that includes an authorization grant for the first option at the unattended machine, wherein the information includes specifications regarding electric pulses to be provided to the unattended machine by the pulse-providing device in accordance with the first option
3310
In accordance with a determination that a trigger condition has been satisfied, send the information that includes the authorization grant and the specifications to the pulse-providing device
3312
After sending the authorization grant and the pulse information to the pulse-providing device, receive an indication, from the pulse-providing module, that the electric pulses were provided to the unattended machine according to the specifications
3314

Figure 33

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/018194

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q30/06 G07F7/00 G06Q20/16 G06Q20/18 G06Q20/20 G06Q20/32
ADD.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

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

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/170131 A1 (PATEL PARESH K [US]) 18 June 2015 (2015-06-18) paragraphs [0085], [0125] - [0129], [0202] - [0206], [0211], [0215] - [0217], [0221], [0226], [0227]; figures 28A, 28B	1-21
A	US 2015/235202 A1 (ZABALA JOSE RAFAEL [US]) 20 August 2015 (2015-08-20) abstract figures 13,15 paragraphs [0009], [0011], [0071], [0082], [0101], [0102]	1-21
A	US 8 600 899 B1 (DAVIS PAUL R [US]) 3 December 2013 (2013-12-03) abstract; figure 2	1-21

-/--

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 April 2017	12/04/2017

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

Authorized officer
Gabriel, Christian

Petitioner Exhibit 1002-1327

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/018194

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003/158891 A1 (LEI JONATHAN L [US] ET AL) 21 August 2003 (2003-08-21) figure 2 paragraphs [0028], [0029]	1-21

Petitioner Exhibit 1002-1328

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2017/018194

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015170131 A1	18-06-2015	NONE	
US 2015235202 A1	20-08-2015	NONE	
US 8600899 B1	03-12-2013	US 8600899 B1	03-12-2013
		US 2014100977 A1	10-04-2014
US 2003158891 A1	21-08-2003	NONE	

Dialog

STIC
Scientific and Technical Information Center

Report Information from Dialog

December 15 2020 22:35

Petitioner Exhibit 1002-1330
ProQuest

Table of contents

1. How Can Stationary Kiosks Thrive in a Mobile World?..... 1

Bibliography..... 4

ProQuest Petitioner Exhibit 1002-1331

How Can Stationary Kiosks Thrive in a Mobile World?

Author: By John Adams

Publication info: American Banker 177.158: NA. SourceMedia, Inc. (Oct 15, 2012)

ProQuest document link

Abstract (English): Byline: John Adams

Mobile devices and apps pose a threat for traditional banking hardware like ATMs; in theory one day we'll pay for most items with a tap of a phone, eliminating the need for cash. Manufacturers of self-service machines are trying to stay relevant by integrating with mobile channels.

Executives from three self-service firmsA a NCR (NCR), Diebold (DBD) and uGeniusA a discussed their strategies during interviews with American Banker on Thursday in Washington, D.C. NCR is adapting self-service concepts from airlines' mobile ticketing technology to its bank clients' needs. Diebold has developed a software-as-a-service (Saas) delivery model to allow banks to quickly upgrade machines to accept mobile authentication for ATM transactions, and uGenius plans to extend its video teller services to mobile channels.

Links: USPTO Full Text Access

Full text: Byline: John Adams

Mobile devices and apps pose a threat for traditional banking hardware like ATMs; in theory one day we'll pay for most items with a tap of a phone, eliminating the need for cash. Manufacturers of self-service machines are trying to stay relevant by integrating with mobile channels.

Executives from three self-service firmsA a NCR (NCR), Diebold (DBD) and uGeniusA a discussed their strategies during interviews with American Banker on Thursday in Washington, D.C. NCR is adapting self-service concepts from airlines' mobile ticketing technology to its bank clients' needs. Diebold has developed a software-as-a-service (Saas) delivery model to allow banks to quickly upgrade machines to accept mobile authentication for ATM transactions, and uGenius plans to extend its video teller services to mobile channels.

"You have the whole population using mobile. Providing access and a level of service will determine how [consumer] behavior changes for you," says Bob Tramontano, vice president of self-service at NCR.

NCR recently unveiled new software that allows consumers to initiate cash withdrawals from their bank accounts on mobile devices and then finish the transaction at an ATM by scanning a 2D barcode on the ATM's home screen. Consumers authenticate transactions through their mobile banking application, and can use any iOS or Android smartphone. Tramontano, who added that mobile deposit capabilities are being developed, said the strategy borrows in part from NCR's experience in other industries such as airlines. NCR's airline ticketing app optimizes elements from an airline's website for mobile devices, enabling check in, flight status updates, reservation modifications, seat selection, and frequent flier management. Once the passenger checks in via the mobile device, NCR sends an encrypted barcode that's compatible with airport scanners and boarding gate readers.

He also said the ATM software upgrades are designed to reduce disruptions in ATM machine replacement cycles, which can be longer than development cycles for ATM functionality, by allowing features to be turned on or off remotely. "We have found that banks tend to keep ATMs for about seven to ten years," Tramontano said.

Diebold has also introduced new "cardless" ATM transactions. Consumers scan a Quick Response (QR) code on the ATM and enter an authentication code to initiate withdrawals and deposits. The smartphone is used as an authentication device, which Diebold says reduces security risk related to lost cards, stolen cards and skimming. The Saas hosting model is designed for faster upgrades to ATM fleets at a lower upfront deployment cost.

"Banks are struggling with location-based channels," said Jerry Verdi, vice president of market intelligence for

Petitioner Exhibit 1002-1332

Diebold. "How do we [expand] self-service in branches in a world in which the transaction device increasingly sits with the individual?"

Diebold has been upgrading its Opteva line of ATMs with virtualization technology that allows machines to be updated remotely by a centralized data center. Diebold contends its Opteva line of ATMs are configured to quickly add new digital transaction capabilities.

Diebold is also a development partner with FIS, which is piloting "cardless cash access" feature for FIS' mobile wallet. That app also uses a secure QR code that the customer taps at an ATM. Robert Unser, senior director of bank retail enterprise for Diebold, on Friday said the partnership includes Diebold's Agilis software, but the details of how it will be implemented are still in development. That includes the security protocol, though Unser said it will not be a one-time PIN.

As part of its branch automation strategy, Diebold is also encouraging use of two-way video, in which consumers can get service or advice from centralized customer service reps. The company believes this is a way to migrate more people to use complex cross-channel self-service. As people use video, they in become more comfortable with digital channels. "The branch can't be an impediment to self-service," Verdi says.

Video's also a big part of the game at uGenius. The firm has deployed its video teller technology, in which customers engage in web video chats with tellers at centralized locations, at a number of institutions as a way to enable smaller branches, branches in remote locations and to extend hours or existing branches.

The firm is now looking to extend that remote teller technology to mobile devices, and has begun deployment at Defence Bank, a financial institution based in western Australia. Consumers at Defence will be able to similar remote access teller services to what's available at the kiosks, further the remote banking strategy "If you can't get to a branch or if you're shopping and want to reach a bank teller, you'll be able to," said Gene Pranger, CEO of uGenius.

Subject: Banking industry;Banking industry -- Customer relations;Banking industry -- Services;Banking software -- Comparative analysis;Banking/finance/investment software;Communications industry -- Services; Comparative analysis;Computers -- Services;Computers -- Strategic aspects;Customer relations;Financial software -- Comparative analysis;Information technology services -- Strategic aspects;Mobile applications -- Comparative analysis;Services;Strategic aspects;Telecommunications industry -- Services; Telecommunications services industry;Telecommunications services industry -- Services

Location: United States

Identifier (keyword): Trade

Event classification: 360: Services information;240: Marketing procedures

NAICS classification: 513: Broadcasting and Telecommunications

Product classification: 4800000: Communications

SIC classification: 4812: Radiotelephone communications;4813: Telephone communications, exc. radio;6021: National commercial banks;6022: State commercial banks;6029: Commercial banks, not elsewhere classified;7371: Computer programming services;7373: Computer integrated systems design;7374: Data processing and preparation;7376: Computer facilities management;7379: Computer related services, not elsewhere classified

Alternate title: Technology, How Can Stationary Kiosks Thrive in a Mobile World?(Technology)

Publication title: American Banker

Petitioner Exhibit 1002-1333

Volume: 177

Issue: 158

Pagination: NA

Publication date: Oct 15, 2012

Publisher: SourceMedia, Inc.

Journal subject: Banking, finance and accounting industries, Business, Economics

ISSN: 0002-7561

Journal code: 3BKR

Source type: Magazine/Journal

Language of publication: English

Document type: Magazine/Journal

Source attribution: Gale PROMT, © Publisher specific

Accession number: 305195341

Document URL: https://dialog.proquest.com/professional/docview/1114711479?accountid=131444

Copyright: Copyright 2012 Gale, Cengage Learning. All rights reserved.COPYRIGHT 2012 SourceMedia, Inc.

Date created: 2012-10-23

Updates: 2012-10-24

First available: 2012-10-24

Database: Gale Group PROMT® (1972 - current)

Bibliography

Citation style: APA 6th - American Psychological Association, 6th Edition

By, J. A. (2012). How can stationary kiosks thrive in a mobile world? American Banker, 177(158), NA. Retrieved from https://dialog.proquest.com/professional/docview/1114711479?accountid=131444

Contact ProQuest

Copyright © 2020 ProQuest LLC. All rights reserved. - **Terms and Conditions**

Petitioner Exhibit 1002-1335

mFerio: The Design and Evaluation of a Peer-to-Peer Mobile Payment System

Rajesh Krishna Balan†, Narayan Ramasubbu†, Komsit Prakobphol‡, Nicolas Christin‡, Jason Hong‡
†Singapore Management University and ‡Carnegie Mellon University
{rajesh, nramasub}@smu.edu.sg, {kprakobp, nicolasc, jasonhong}@cmu.edu

ABSTRACT

In this paper, we present the design and evaluation of a near-field communication-based mobile p2p payment application, called mFerio, that is designed to replace cash-based transactions. We first identify design criteria that payment systems should satisfy and then explain how mFerio, relative to those criteria, improves on the limitations of cash-based systems. We next describe mFerio's implementation and user interface design, focusing on the balance between usability and security. Finally, we present the results of a two-phase user study, involving a total of 104 people, that shows that mFerio has low cognitive load and is also fast, accurate, and easy to use – even outperforming cash in terms of speed and cognitive load in common payment situations.

Categories and Subject Descriptors

D.4.m [**Operating Systems**]: Misc; H.5.2 [**User Interfaces**]: Mobile Payment Systems

General Terms

Design, Human Factors, Experimentation

Keywords

Mobile Computing, User Study, Mobile Payment, p2p Payment, NFC, Near-Field Communication, Digital Wallet

1. INTRODUCTION

Cell phones have evolved from mere communication devices to becoming calendars, instant messaging devices, address books, cameras, photo browsers, and shopping list organisers. Cell phones have also gained increasing relevance as a payment vehicle. It is already possible, in some places, to use a cell phone to pay for vending machine purchases, groceries, and even airline tickets [32].

This research was supported by the Singapore Management University (Office of Research grant no. 07-C220-SMU-001), the National Science Foundation (NSF) (Grant no. CNS-0627513), and the Hyogo Institute of Information Education Foundation. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Hyogo Institute, NSF, Carnegie Mellon University, or Singapore Management University.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
MobiSys'09, June 22–25, 2009, Kraków, Poland.
Copyright 2009 ACM 978-1-60558-566-6/09/06 ...$5.00.

One problem, however, is that current mobile payment solutions all require infrastructure support. In particular, they cannot work if at least one of the parties involved in the payment is not connected to some back-end payment server, via either SMS or GSM/CDMA-based technology. For example, consider the following scenario.

> *Bob takes a taxi, and tries to pay the taxi driver using his cellphone when he reaches his hotel. However, the unloading lobby is underground and neither Bob nor the taxi driver can get a signal on their wireless equipment. Bob has to dig for cash, and also has to keep track of the receipt so he can be reimbursed later.*

Ideally, there would be ubiquitous wireless networking that is reliable and secure. However, wireless connectivity can be affected by a multitude of factors ranging from bad weather to telecom carrier incompatibilities. For example, it is possible for SMS messages to be delayed by several minutes or even hours, which can lead to a poor user experience for a mobile payment system relying on SMS.

In addition to these connectivity issues, the additional cost of subscribing to a central payment service is a likely adoption barrier for small independent operators ("mom and pop" shops). Furthermore, a mobile payment system has to be usable and secure, both in terms of actual implementation, as well as perception by end-users.

In this paper, we present the design and evaluation of mFerio, a novel peer-to-peer (p2p) mobile payment system. mFerio can be implemented on smartphones, does not require any additional connectivity or infrastructure beyond the cell phones of the participants, and was designed with usability and security in mind. mFerio is comprised of three components: 1) a digital cash system, 2) an authentication system, and 3) an easy-to-use interface coupled with a secure communication protocol for making p2p payments. In this paper, we concentrate on the third aspect and defer to prior work for the first two [6, 7, 17, 22, 39].

We make the following contributions in this paper. First, we describe the challenges involved in designing a mobile p2p payment solution. In particular, we analyse the design space and examine some of the key tradeoffs between usability, utility, and security. Many of these tradeoffs are fundamental ones that any mobile p2p payment system will face. We also identify success criteria that payment systems have to meet. Second, we discuss the design and implementation of mFerio and explain how it satisfies the various success criteria. We focus specifically on the tradeoff between usability and security and explain how mFerio manages to provide a user interaction technique that provides both excellent usability and a reasonable level of security. Third, we present the results of a two-phase user study, involving a total of 104 participants, showing that mFerio is very usable – requiring no training and even outperforming cash in speed and cognitive load under common conditions.

Petitioner Exhibit 1002-1336

2. DESIGN SPACE FOR MFERIO

We start by analysing mFerio's design space; drawing from both prior research [20, 31, 36, 40], and from analysis of the advantages and disadvantages of cash payments. We chose not to compare mobile payments to credit cards as credit cards require infrastructure and thus cannot be used in a peer-to-peer manner. We grouped the design criteria into three main categories: *usability*, *security*, and *auditing*. To be successful, mFerio has to be better than cash in multiple criteria, while not having any significant drawbacks.

2.1 Usability Criteria

A payment system needs to be highly usable by a large cross section of the population to be viable. The following usability criteria provide some guidance towards this goal.

Fast to use. Making a payment should not take too long. Cash is generally a fast payment system, However, as our results show, situations involving even moderate amounts of change can slow down cash transactions significantly.

Easy to use. The payment system should be easy to use by people of different ages and technical competency. Cash satisfies this criterion and is universally used.

Easy to learn. Anyone should be able to quickly learn how to make payments. Cash satisfies that criterion as well, as even young children can be taught to make cash payments.

Predictable performance. Different situations should not affect the performance of the payment system. For example, the time taken to make a payment should not depend on the payment amount. As stated above, cash's speed depends greatly on the situation.

Accurate. Users should be able to transfer exactly the amount of money involved to the intended person, without needing corrections or double checking. Cash is by and large an accurate means of payment. However, its accuracy can be affected by the situation.

Available. The payment system should be usable anywhere and anytime. This is one of the strengths of cash: once created, it essentially requires no infrastructure to be usable. On the other hand, providing high availability for a mobile payment system can be difficult to meet, as it depends on numerous external factors such as digital cash regulatory requirements across the globe, the dynamics between banks, cell-phone manufacturers, telecom service providers and retailers. In this paper, we focus solely on addressing the usability obstacles to availability (i.e., the payment system should not be rejected because it is hard to use).

In summary, a novel payment system, such as mFerio, should achieve the ease of use and (as much as possible) availability of cash, while improving on its accuracy and speed.

2.2 Security Criteria

Payment systems also need to satisfy a number of security criteria. Cash has good security properties, but offers considerable room for improvement as we discuss below.

Preserve transaction semantics integrity. The payment process must ensure that transactions semantics are well defined, and cannot be tampered with. In particular, transactions should be resilient to man-in-the-middle and replay attacks, and guarantee atomicity (i.e., interrupting a transaction will cancel the entire transaction). Usually, transfer of physical currency requires a physical interaction between the parties involved – this provides strong assurance that the transaction semantics will be maintained.

Anonymous. Without external monitoring steps, it should not be possible to identify who made a particular payment. Cash has very strong anonymity properties that make it difficult to trace [21], and a desirable payment choice for privacy-conscious users.

Tamper-proof. It should not be possible to tamper with the payment system and the monetary representation (e.g., digital cash) used. In particular, any attempts to tamper with the system should only result in the system being destroyed and not broken into. Cash, in general, remains usable even if slightly defaced. Alterations resulting in the coin or bill being unusable as legal tender can usually be detected by visual inspection.

Impossible to replicate. The payment system's monetary representation should be impossible to create or duplicate by users. Cash uses numerous physical security measures to prevent counterfeiting without expensive and specialised machinery [1]. In a mobile payment system, this property demands, for instance, that users should not be able to make a backup of their phone, make payments, and then restore their backup and "reclaim" their spent money.

Theft resilience. The system should be resistant to theft. This is one of the main vulnerabilities associated with cash. When a wallet is stolen, the victim has no recovery mechanism available, and ownership of the cash simply transfers to the thief. Mobile payment systems, such as mFerio, can cryptographically store the digital cash on the phone to prevent unauthorised use, thereby ensuring that thieves have no additional incentive to steal phones.

There are already existing solutions for the properties outlined above that can be applied to mobile payment systems. Instead of creating novel low-level security primitives, we chose to integrate existing security technologies [10, 11] into mFerio to achieve a cohesive design, with the goal of yielding a payment system that is both usable and secure.

2.3 Auditing Criteria

It is quite common for users and businesses to regularly perform audits of their spending habits. As such, including auditing criteria in the design of a mobile payment system could improve its mass market appeal. However, satisfying these criteria may require relaxing the anonymity criteria.

Accountable. It should be possible for user to accurately track all payments that they have made.

Dispute resolution. It should be possible to definitively prove that payment has been made to a particular person. This is a stronger form of the accountability criteria.

Cash, by itself, has no provisions for auditing. There are no automatic receipts or mechanisms for dispute resolution. It is possible to layer these features on top of the existing cash system, but they are not available by default. We decided to support both auditing criteria in mFerio; making its anonymity properties weaker than that provided by cash. mFerio uses automatic receipts to provide accounting – allowing the two parties involved in the payment transaction to know more about each other than a corresponding

Petitioner Exhibit 1002-1337

Success Criteria	Implementation Details	Evaluation Results	Satisfied$_{mFerio}$	Satisfied$_{Cash}$	Relative to Cash
Usability Criteria					
Fast to Use	Section 3.3	Section 5.5.1	√	√	Better in Some Situations
Easy to Use	Section 3.3	Section 5.5.2	√	√	Same
Easy to Learn	Section 3.3	Section 5.5.2	√	√	Same
Predictable Performance	Section 3.3	Section 5.5.4	√	×	Much Better
Accurate	Section 3.3	Section 5.5.3	√	√	Same
Available	—	Section 7.1[a]	×	√	Worse
Security Criteria					
Anonymous	Section 3.1	Section 3.2[b]	√	√	Slightly Worse
Transaction Semantics	Section 3.1	[10, 11][c]	√	√	Same
Tamper-Proof	Section 3.1	[5, 7, 26][c]	√	√	Same
Impossible to Replicate	Section 3.1	[6, 26][c]	√	√	Same
Theft Resilience	Section 3.1	[11][c]	√	×	Much Better[d]
Auditing Criteria					
Accountable	Section 3.2	Section 5.5.5	√	×	Much Better[d]
Dispute Resolution	Sections 3.2 and 3.3	Section 5.5.5	√	×	Much Better[d]

[a]We discuss some of the factors affecting mFerio's availability in this section

[b]We get anonymity by design as explained in Section 3.2

[c]We use well-designed protocols that have been rigorously validated by other researchers

[d]Feature is completely unsupported by Cash

This table list the success criteria for mFerio. The "Implementation Details" column lists where the implementation for that criteria is described while the "Evaluation Results" column lists where the evaluation for the criteria is presented. The "Satisfied$_{mFerio}$" and "Satisfied$_{Cash}$" columns graphically summarises how well mFerio and Cash satisfy each of the criteria respectively – ticks (√) are good while crosses (×) are bad. Finally, the "Relative to Cash" column provides a quick comparison between mFerio and Cash (mFerio is the baseline) for that criteria.

Table 1: Success Criteria for mFerio

cash transaction. However, no external party knows anything about the transaction. We believe that this is the right tradeoff between auditing and anonymity. If desired, the auditing features can be turned off to achieve complete anonymity.

2.4 Summary of Criteria

Table 1 summarises the various success criteria, listed above, for mFerio. For each success criteria, it indicates where, in this paper, the implementation details relevant to that criteria are discussed. It then lists where the evaluation results (either in this paper or in related work) for that criteria are presented. It also provides a graphical indication of how well mFerio and cash satisfies each criteria. Finally, it provides a short comparison between mFerio and cash (with mFerio as the baseline) for each criteria. Overall, mFerio is able to satisfy most of the criteria extremely well – the exception being availability which is discussed in Section 7.1.

3. BUILDING MFERIO

We next describe the implementation of mFerio, and relate it to the design considerations presented in Section 2. In particular, we discuss the specific mFerio implementation details that allow it to satisfy each of the three main success criteria groups (shown in Table 1) listed previously.

In the p2p exchanges mFerio aims to support, there are only two parties, the *Initiator* and the *Recipient* – but no central bank. In our design, either party can be *Receiving* or *Sending* payment, resulting in four possible user roles (initiating a payment request, initiating a payment, receiving a payment request, receiving payment)– mFerio supports all four roles. We now discuss how mFerio satisfies each of the three criteria starting with the security criteria, followed by the auditing criteria, and ending with the usability criteria.

3.1 Satisfying the Security Criteria

The security criteria has two main parts; 1) physical security concerning the communications channel and the tokens exchanged between the phones, and 2) user security concerning the sequence of operations that the user must do to complete a transaction. Both are necessary elements for a secure payment system – a highly secure token is useless if the user protocol allows users to pay unintended people while a good user protocol is compromised if the tokens and/or communication channel can be easily tampered with.

3.1.1 Enforcing Physical Security Requirements

A key requirement for a mobile payment solution is a secure monetary token. In this paper, we defer to prior work for an implementation of a secure monetary token – Davies [9] provides an overview of the various digital payment tokens. In a deployed implementation, it is likely that the specific token used will depend greatly on the deployment environment (which country, bank, agency, etc. is deploying the solution). Hence, it seems prudent to concentrate our resources on other aspects of the mobile payment system – that will remain constant across multiple deployments.

Petitioner Exhibit 1002-1338

In addition to the secure monetary token, to achieve its physical security requirements, mFerio extensively relies on hardware support to provide secure wireless communication mechanisms, fast and secure authentication, and secure data storage. Note: we expect mFerio to store about $500 at most – consistent with the limits imposed by complementary stored-value systems [12, 27].

Secure wireless communication mechanism. To promote ease of use, mFerio should use a wireless communication medium for transactions. This medium must be highly secure, both from systems and usability perspectives (i.e., people can easily perform any necessary actions quickly and correctly).

We chose to use near-field communication (NFC) as mFerio's wireless medium. NFC has three primary advantages over other mechanisms; First, NFC has a very short range, on the order of 1-2 inches (2.5-5cm), making it hard for intruders to intercept communications. Users can clearly see anyone trying to intercept a transaction; in contrast to longer range protocols such as WiFi and Bluetooth. Second, it is quick and easy to set up a NFC connection with another nearby NFC device – simply move one device near the other. This is in contrast to Bluetooth peering which is tedious and slow to set up. Third, NFC has a straightforward conceptual model for users – they know exactly what device they are communicating with, as opposed to longer-range wireless protocols.

Fast secure authentication. We designed mFerio to require users to authenticate themselves to the mobile phone before use. Any of the authentication mechanisms such as pincodes [2, 13], graphical passwords and distortion functions [15], or biometric-based mechanisms [34, 35] can be used with the mFerio application. A full comparison of the usability of the different authentication mechanisms is beyond the scope of this paper. For this paper, we used a Wizard of Oz approach [18] (where the system appears to be fully functional but is actually faked under the covers) for biometric fingerprint authentication. It is important to note that mobile authentication mechanisms have their own flaws but they are still better than not having any authentication at all – as is typically the case with cash payments. We designed mFerio to be able to use any authentication mechanism that gains market dominance.

Secure data storage. The last hardware requirement is secure storage (also referred to on cellphones as a secure element), which should only be accessible if authentication credentials have been successfully provided. This storage will contain the cash and the personal details of the user. If this storage is hardware protected, it ensures that thieves will not be able to access the cash and personal details on a stolen cellphone. As such, this eliminates an extra temptation for thieves as users cannot tamper with the electronic cash by hacking the data storage area. These secure hardware protected chips have already been released by several manufacturers such as Gemplus, Sony, and IBM.

The above mentioned hardware enforced security mechanisms coupled with a secure monetary token satisfy the *Tamper-Proof*, *Impossible to Replicate*, and *Theft Resilience* security-related success criteria (Table 1).

3.1.2 *Detailed Payment Protocol*

Hardware-enforced security as discussed above is still only a partial solution and mFerio's payment protocol must still enforce transaction semantics (in the database sense of the term). As such, mFerio mandates authentication before transactions can take place, and uses a protocol that guarantees transaction atomicity (i.e., completed transactions should be correctly registered by both parties involved, with the same being true for incomplete transactions).

Authentication increases the number of user steps, potentially impacting usability negatively. However, in this case, security outweighs usability concerns. We adapted existing atomicity protocols already deployed in NFC payment systems [10] and electronic wallet protocols [11] instead of building one from scratch.

Two-touch payment protocol. We use a two-touch protocol, where both parties must touch phones twice to complete the transaction. The first touch exchanges identifying information, using certificates, ensuring that both parties know who they are transacting with, and also establishes a transient secure shared key, which makes the transaction resilient to replay attacks and tampering by external parties. The second touch finalises the transaction. While it is possible to use a single-touch protocol where the whole transaction completes after just one touch of the phone, it also opens up the possibility of errors where payments could be made to someone other than the intended party. Hence, we chose to err on the side of caution, favouring security over usability in this case.

We chose to use the Even-Goldreich-Yacobi protocol [11] to implement monetary exchanges. An alternative would have been Brands' one-time spending certificate [3] which is more tolerant of compromises of the secure storage element. However, Brands' protocol is primarily designed for asymmetric transactions, e.g., involving a point-of-sale and a payer, and would require considerable modifications to be adapted to a peer-to-peer protocol. Conversely, the Even-Goldreich-Yacobi protocol can be implemented without significant changes, in mFerio. The main extension is an atomicity requirement: if the transfer fails, the balance must revert back to the original state before the transaction.

We chose a counter-based mechanism for mFerio as deployed in the Even-Goldreich-Yacobi protocol, rather than a digital coin-based mechanism because a counter based mechanism provides a constant level of overhead; in contrast, digital coins are indivisible, and therefore may require additional overhead when the payer does not have the exact change. The main drawback of counter-based mechanisms is their dependence on a secure element; but as mentioned before, a secure element (secure data storage) is readily available in modern cellular phones, making the counter-based approach viable for mFerio.

Thus, in the mFerio payment protocol, the payer's wallet and payee's wallet, first (during the first touch), agree on the amount of the transaction and authenticate each others certificates. Then, the payer's secure element makes sure that the amount of the transaction does not exceed the wallet's balance, deducts money, and signs the payment message. When the phones touch again (second touch in the two-touch protocol), the payer's wallet sends the payment message. The payee's observer verifies the payment message and adds the amount to the wallet's balance if the message is valid. The payee's wallet returns an electronic receipt as a proof of a transaction. The transfer of payment message and digital receipt must be atomic. If any of the transfers fail the balance must revert back to the original state before the transaction. This method of ensuring atomicity, typically used in databases and financial transactions, minimises message transfers in the protocol.

To further enhance security, we require users to re-authenticate themselves multiple times, at key points, during the two-touch protocol. In practice, this approach requires the authentication step to be fast and hassle-free. If this assumption proves to be false, alternative strategies, such as single authentication with flexible lock-out timers, are available [15]. We revisit this issue in the user study (asking participants to choose between different types of payment

Petitioner Exhibit 1002-1339

protocols) and the results, shown in Section 5.5.5, reinforce our decision to use a two-touch protocol and multi-point authentication.

Thus the two-touch protocol, coupled with the atomicity considerations discussed above, allows mFerio to satisfy the *Transaction Semantics* criteria.

3.2 Satisfying the Auditing Criteria

A key part of the two-touch protocol discussed previously is the exchange of identifying information between transacting parties after establishing a session key. Identifying information in the two-touch protocols clearly reduces mFerio's anonymity. However, no other party (including banks, certificate authorities, and monitoring agencies) will know anything about the transaction. Thus, mFerio satisfies the *Anonymous* success criteria; but not as much as cash does. Apart from enhanced security, a secondary benefit of compromising anonymity through the use of a two-touch protocol is that it allows us to create automatic signed receipts of each transaction. Availability of signed receipts make accountability and conflict resolution much easier. For true anonymity, mFerio can be easily modified to use pseudonyms instead of actual names – however, that is not in the current implementation. These mechanisms allows mFerio to satisfy the *Auditing Criteria* listed in Section 2.

3.3 Satisfying the Usability Criteria

We implemented several features in mFerio to make it as usable as cash payments while preserving strong security. Firstly, mFerio tells users exactly where they are in the transaction stage (two-touch protocol) and how much more needs to be done – similar to web-based shopping cart checkouts. We display the user's current monetary balance on almost every protocol screen. In addition, mFerio requires users to explicitly confirm the full details of the payment (receiver and amount) involved in a transaction. Once the user has confirmed an action, a transaction summary screen is displayed, where we show both the current, and the expected post-transaction cash balances. This design allows users to a) know exactly how much money they have, and b) completely understand the financial implications of any transaction.

Furthermore, mFerio makes it easy to recover from errors. At any time, the user can click the cancel button and stop the whole process. Before secure keys are exchanged with the other party (first touch in two-touch protocol), the user can also use the back button to go back and change anything they desire. After the first touch in the two-touch protocol, any changes will require cancelling the payment and starting a new one because letting the user go back after exchanging keys would compromise security.

Using User Feedback to Design mFerio. One of our main user study goals was to evaluate the usability of our design decisions. Along with that, we also gathered user feedback to choose among some competing design choices of various mFerio application features. The key design choices we verified in our user studies were

- **One-touch or Two-touch Protocol?**: mFerio uses a two-touch protocol, as described in Section 3.1.2), to ensure that users are confident of who exactly they are paying. However, a two-touch protocol does require a few more steps (and a corresponding increased amount of time) than a one-touch protocol. We verify whether users actually prefer the increased security of a two-touch protocol over the speed of a one-touch protocol in Section 5.5.5.
- **Authentication Mechanism**: mFerio requires users to authenticate themselves before they can perform payment transactions. However, how should this authentication be done? Should the user re-authenticate themselves at every key transaction point? Is a single authentication when starting the mFerio application sufficient? Should there be a timer that triggers re-authentication? If so, what kind of timer (fixed or inactivity-based?) should it be? To gain clarity, we presented users with different possible authentication mechanisms and the results are described in Section 5.5.5.
- **Method for Receiving Transaction Requests**: As stated at the start of Section 3, mFerio can be used in four modes. In all those modes, one party has to receive a request (either for payment or to make payment) from the other party. One key usability decision was deciding how to accept those requests in mFerio. One possibility was for mFerio to always accept requests as long as the user was not performing a transaction at the moment. Another alternative was to require the user to actively state (by entering a special mFerio mode) that they were willing to receive requests. This explicit step increases the burden on the user, but decreases the possibility of the user accidently responding to transient transaction requests. We presented our users with various options for receiving payment requests and present the results in Section 5.5.5.
- **Specifying Reason for Payment**: mFerio automatically creates receipts for each transaction. However, a receipt, by itself, may not be that useful months, weeks, or even days later as many transactions may look similar. Hence, mFerio provides a way for users to annotate their receipts with a reason for the transaction (buying food for example). Section 5.5.5 describes the various options tried and the user response.

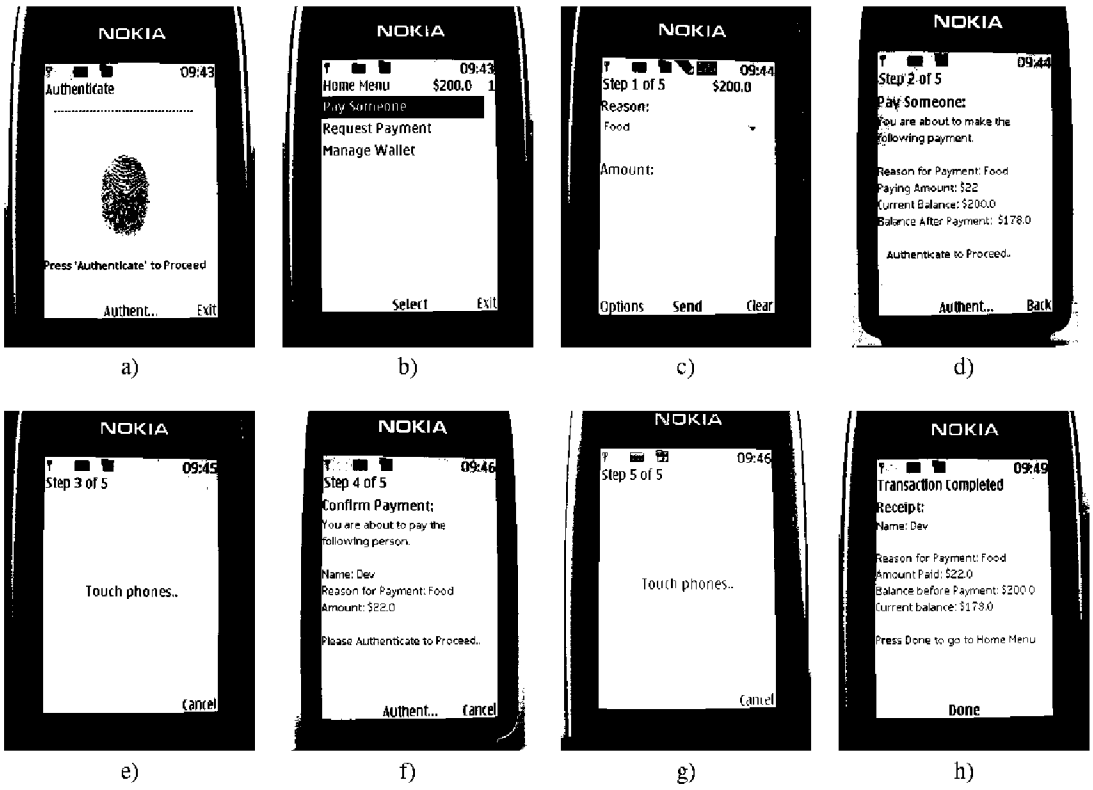
Overall, the various mechanisms implemented into mFerio, coupled with the user-driven selection of various targeted features, allow mFerio to satisfy all but the availability criteria specified in Section 2. This claim is well backed-up by the results of our usability tests (shown in Sections 5 and 6). The availability criteria, unfortunately, depends on more than a good implementation and requires market support. We discuss some factors affecting mFerio's availability in Section 7.1.

3.4 The mFerio p2p Mobile Payment System

In this section, we put everything together and show the end-to-end mFerio application. We developed mFerio as a J2ME application on Nokia 6131 phones with built-in NFC capability. Figure 1 shows the sequence of steps needed to perform a p2p transaction with mFerio. The user clicks on the mFerio application and then performs the following steps:

1. The user first authenticates herself, using, for instance, a fingerprint reader on the mobile phone.
2. The user then selects a task from the main menu. She can either initiate a transaction to pay someone or initiate a transaction to request payment. She can also receive payment requests on this screen. Finally, she can do basic management (a feature not tested in this study) of her transaction preferences. For the rest of the description, we assume that the user has decided to pay someone.
3. The user performs the first transaction step. She enters the payment reason from a pre-defined pull down list, types in the amount to be paid, and clicks okay to proceed. Note that the current step is shown on the top left of the screen.
4. In the transaction's second step, the user confirms the reason for payment and the payment amount. She has to re-authenticate at this screen to confirm the payment.

Petitioner Exhibit 1002-1340



In this example, the user is initiating a payment. The sequence of steps for other three payment modes of mFerio (ask for payment, receive payment, and receive request for payment) are similar. The user (a) first authenticates herself using a biometric fingerprint reader, (b) chooses to pay someone, then (c) selects a reason from a predefined list, and enters an amount to pay. The user (d) sees how much will be paid, (e) touches her phone with the recipient's phone, and then (f) confirms the payment. Once confirmed, the user (g) finalises the payment, and then (h) gets a receipt.

Figure 1: Screenshots of the mFerio Application

5. The user then brings her phone next to the recipient's phone. The recipient must be running mFerio and be in receive mode. During this first connection, a private session key is created for use by both the initiator and the recipient using the Diffie-Hellman protocol. Each party's mFerio application then encrypts basic information such as name and exchanges it with its peer using the adapted Even-Goldreich-Yacobi protocol.

6. Basic information about each party is next displayed along with the transaction details. For example, as shown in Figure 1f), the initiator will see the recipient's name, the payment amount and reason for payment, and the values of her stored cash before and after the transaction. The recipient will see something similar. Both parties must re-authenticate themselves to proceed to the final step.

7. The phones touch again to finalise the payment transaction (using the Even-Goldreich-Yacobi protocol).

8. A "transaction complete" summary page is shown. This page is then stored as an automatically signed receipt.

4. EVALUATION METHODOLOGY

In this section, we explain how we evaluated the performance of mFerio. Our goal was to determine if it satisfied the success criteria described in Section 2 and summarised in Table 1.

We evaluated mFerio in two phases. The goal of the first phase (Phase 1) was to test the effectiveness of the mFerio user interface, and to fix any deficiencies found before investing the effort to build a full system. Thus, we built a complete user interface that followed the exact sequence of steps detailed above, including exchanging information using NFC. However, we did not implement any of the security mechanisms needed for cash exchange as they were unnecessary for validating the user interface – allowing us to focus on key usability criteria without interference from other components. A secondary goal of the phase 1 study was to identify key design decisions that required user input (Section 3.3).

In the second phase (Phase 2), we implemented the complete secure mFerio application, including the key exchange and encryption schemes necessary to guarantee the transaction security.

In both phases, we tested the speed, accuracy, and ease of use of mFerio relative to cash transactions. In phase 1, we also asked users to test specific components of mFerio such as the receipt feature and various authentication methods. In phase 2, we conducted a full cognitive load test, using the NASA TLX method [14], of mFerio and cash transactions to measure exactly what the differences between mFerio and cash are.

In addition, in phase 2, we conducted system performance tests to measure exactly how long the security protocols took to complete a transaction – the performance figures for the rest of mFerio are omitted as it simply involves moving from one screen to another which takes negligible time. The phase 1 study is detailed in Section 5 while the phase 2 study is detailed in Section 6.

5. PHASE 1 STUDY: BASE PROPERTIES

We next describe our phase 1 user study. The primary goal of this first study was to assess how well mFerio met the base criteria laid

Petitioner Exhibit 1002-1341

Expt Code	Amount in Wallet ($)	Payment Amount ($)	Change Received ($)	Objective
CB 1	10 (1 five, 2 twos, 1 one)	2	None	1 bill exchanged with no change.
CB 2	80 (1 fifty, 2 tens, 2 fives)	75.16	4.84	Few bills with change involved
CB 3	85.16 (1 fifty, 2 tens, 3 fives, 1 ten cent, 1 five cent, 1 one cent)	75.16	N/A	Few bills where participant needed to dig for exact change

The participant was the one paying with the experimenter receiving the payment.

Table 2: Core Task Set 1 – Cash

Expt Code	mFerio Starting Value ($)	Payment Amount ($)	Change Received ($)	Objective
mFB 1	80	−75.16	N/A	Using mFerio to pay experimenter
mFB 2	80	+75.16	N/A	Using mFerio to receive payment from experimenter

The participant had to initiate all payments. In one experiment, the participant had to pay the experimenter. In the other, the participant received payment.

Table 3: Core Task Set 2 – mFerio

out earlier. A secondary goal was to gather detailed process data to help identify areas for future improvements and research, and to allow us to refine the design for the subsequent phase 2 user study. We simulated the use of a fingerprint reader for fast authentication by asking the users to press a button on the phone to simulate the fingerprint reader (we added a little delay after the button press).

5.1 Method

We divided the experiments into three sets: tasks involving cash, tasks involving mFerio, and a set of tasks to capture any learning effects. The evaluation was within-subjects, but the task sets were not randomly ordered (cash experiments came first and then the mFerio experiments). Participants performed the cash experiments first and then used mFerio. We chose this approach as we do not believe there are any learning effects going from cash to mFerio since people are already highly familiar with cash payments. Tasks within each core task set were counterbalanced, however.

Each individual task took about 1 minute to complete, and had the same basic structure: participants were asked to either receive payment or pay the experimenter (the amounts involved was provided to them). A task was considered finished when the transaction was completed. To minimise bias, the choice of whether a participant received or sent payment was randomly determined.

After each individual task, participants were provided a simple questionnaire that asked them to rate, on a 5-point Likert scale, a) whether they thought the task was quick to perform, b) how easy they found the task, and c) how confident they were that they completed the task correctly. At the end of each set of tasks, participants were given a longer questionnaire.

Task set 1 – Cash. In these baseline experiments, we measured the time taken by participants to complete three typical cash transactions – using those times to establish a baseline target for mFerio. The cash tasks are described in Table 2. Each individual task started with all money inside the wallets of both the participant and the experimenter, and the wallets kept in their usual place (inside a purse, pocket, etc.). The task was considered finished when the final bills were received, counted, and returned into the appropriate wallet.

Task set 2 – mFerio. In this set of experiments, participants were asked to use mFerio to both pay someone and to send payment to someone. In both cases, the participant was the initiator of the transaction. At the end of the user study, the participant was asked to redo one of the two tasks in this set (chosen randomly) to observe any learning effects. The tasks for this set are described in more detail in Table 3. For each of these tasks, the participant had to click an icon to start the mFerio application. A task was considered complete when the user reached the final confirmation screen and clicked done on that screen (see Fig. 1h).

Task set 3 – mFerio Learning. After completing all the mFerio tasks in Set 2, the participants were asked to repeat the first task they did in Set 2. This was to detect any mFerio learning effects.

5.2 Participants and Setup

We recruited a total of 75 undergraduate students for our phase 1 study. Participation was open to all students at our university, and we solicited participation through flyers, student association emails, and also through specific emails sent to students who had previously registered with the university-wide subject pool list. All 75 students did the same set of cash and mFerio tasks. Each user study took about 30 minutes to complete.

Our participants were a mix of students from technical and non-technical majors. We asked each participant to complete a short (2–3 minutes) demographics survey to determine their familiarity with cell phone technology. The possible answers were, 1) Have you used MMS on your phone? 2) Have you browsed the Internet from your phone? 3) Have you synchronised your phone with any other device or software? 4) Have you installed applications on your phone? Based on the (yes/no) answers given, we categorised users into three buckets – "novice", "intermediate", and "expert".

In addition, we asked each participant to state how important their cell phone was to them by answering the following question: How important is your phone to you? The possible answers were, 1) Not very important. I can go for a day or more without it; 2) Somewhat important. A few hours without it probably will not do any harm; and 3) Very Important, I have to have it with me all the time. Table 4 shows the phase 1 participant demographics.

Participants were compensated at a flat rate of $10 SGD on completion of all tasks. We stressed that they were not under time pressure, and could take as long as they needed to complete the task – a deliberate bias against our goal of fast transaction times.

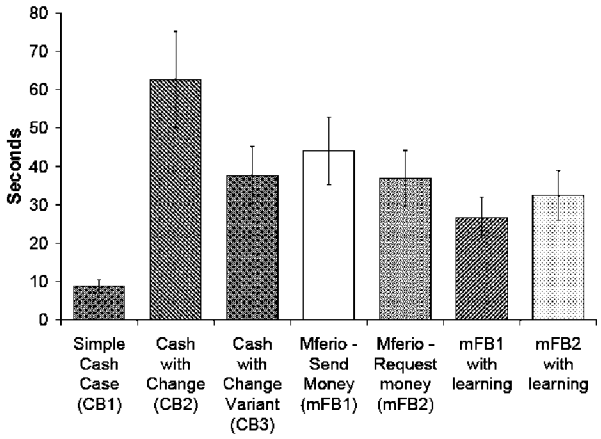
5.3 Experimental Procedure

The participants worked alone in a lab for the duration of the study. For all experiments, a tester played the role of the other person involved in the p2p transaction. Participants were provided phones, basic training in how to use the phone and the NFC capability, and instructions for each task in the study. The training period

Petitioner Exhibit 1002-1342

Total number	75
Gender	Male (35), Female (40)
Proficiency level	Novice (22), Intermed. (30), Expert (23)
Phone importance	Low (8), Medium (36), High (31)

Table 4: Demographic statistics for Phase 1 Study.



The error bars indicate standard deviations. Pair-wise t-tests of the results show significance at 5%.

Figure 2: Measured Speed of mFerio and Cash

lasted less than five minutes, and involved the participant entering alphanumeric input into a text box and then transferring that input to another phone using NFC. This training helped teach the participants how to use the phone's NFC feature, and helped ensure that participants were comfortable with the data entry features of the Nokia 6131 NFC phone (e.g., backspace, decimal point, etc.). We did not train our participants to use mFerio – the first time they saw and used the application was during the real experiment.

5.4 Data Collected

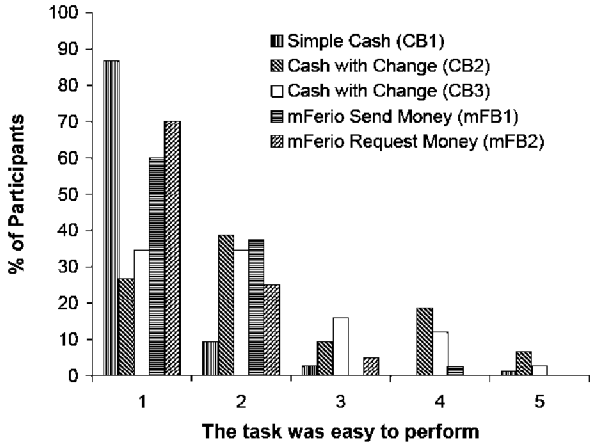
We obtained completion times for each task and subtask (i.e., time to progress from one screen to another) by instrumenting the phones. We also observed the participants during the study and noted where they had trouble, were confused, or made mistakes. Finally, we measured our participants perceptions, through an exit survey, on quality of training, ease of use of mFerio, and user reported performance for each subtask.

5.5 Results of Phase 1 User Study

5.5.1 mFerio is Fast

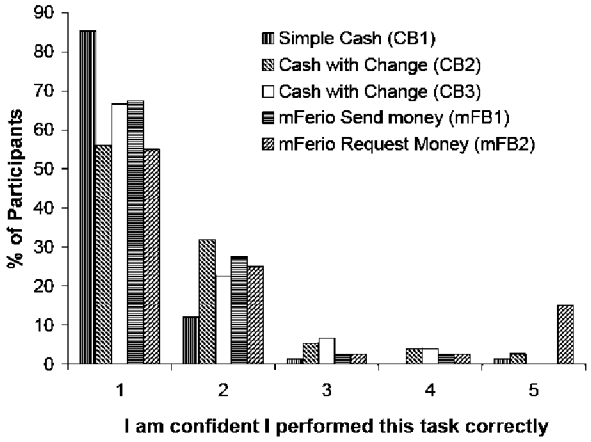
Figure 2 shows the time taken by the 75 participants to complete the 3 cash experiments (Table 2) and the 2 mFerio base case experiments (Table 3). In addition, participants were asked to repeat the mFerio base case experiments at the end of the user study to observe the effect of learning on speed of use. We also show the results for these repeated experiments.

As expected, the simplest cash experiment (CB1) was the fastest to complete. However, more complex tasks, where change was involved, was slower to complete with cash than mFerio (comparing CB2 and CB3 with mFB1 and mFB2). For task CB3, we did not tell the participants a-priori that the cashier did not have change. If the participants provided a larger amount, they were told to provide exact change. As such, we expected task CB2 (paying and getting change in return – a fairly straightforward task) to be the same or faster than task CB3 (paying exact change), but our results show



The x-axis is a 5-pt Likert scale. Scores to the left are better.

Figure 3: Perceived ease-of-use of mFerio



The x-axis is a 5-pt Likert scale. Scores to the left are better.

Figure 4: Perceived Accuracy of mFerio

the opposite. We observed that our participants were more careful about checking the amount of change they received, thus leading to slower task completion in CB2.

In addition, mFerio showed a strong learning effect (comparing mFB1 and mFB2 with the corresponding "With Learning" bars) and after just 15 minutes of use, participants showed improvements of up to 40% in performance. Hence, we conclude that the speed of using mFerio is comparable to or even faster than a large number of common cash use cases.

Participants also rated, on a 5-point Likert scale, how fast they thought mFerio was to use. mFerio scored a 1.7 (1 is best, 5 is worst) with a standard deviation of 0.75 – indicating that users were happy with mFerio's speed.

5.5.2 mFerio is Easy to Use with Minimal Training

Figure 3 shows how participants rated mFerio's ease of use on a 5-point Likert scale (lower is better). Results are promising – 60 to 70% strongly agree that mFerio is easy to use while less than 5% were either neutral or somewhat disagree. No participant strongly disagreed that mFerio is easy to use.

5.5.3 mFerio Payments are Perceived as Accurate

Figure 4 shows the perceived accuracy of mFerio (same 5-point Likert scale, lower scores better). Overall, participants were positive, with 68% strongly agreeing that it is accurate. We had a few

Petitioner Exhibit 1002-1343

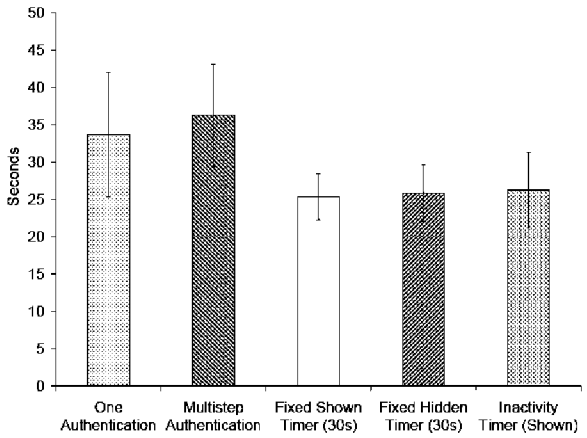


Figure 5: Task Speed in different Authentication Modes

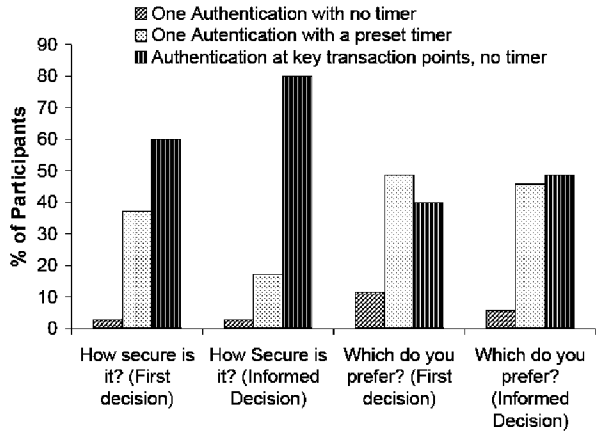


Figure 6: User Perception of Authentication Modes

outliers, that strongly disagreed that mFerio is accurate. The outlier observations were all for the "Request Money" task (the accuracy question for this task was reverse coded); 66% of the outliers were female students; and 33% of them were expert users. We did not find any other abnormal behaviour, with respect to these outlier participants, across the other tasks that would suggest a design flaw in mFerio. Hence we do not see this as a cause for concern.

Even with these outliers, a large majority of the participants still perceived mFerio as being very accurate. Given that the participants had never used mFerio previously, these results are very encouraging. Our future work involves developing techniques to further improve mFerio's perceived accuracy.

We assessed the actual task accuracy only at the end of each task; by checking if the correct sum of money had been transferred (either physically or digitally). We did not capture any errors that took place during the task and were subsequently corrected. We found that in all cases, the amount of money transferred was correct.

5.5.4 *mFerio has Predictable Performance*

We estimated task performance differences for the cash experiments by calculating the difference in time and perceived ease-of-use between the cash experiments. The difference in times between CB1 and CB2 (Fig. 2) is significant at 1% (CB2 is on average 53 seconds or more than 6x slower to complete than CB1), while the difference in perceived ease-of-use between CB1 and CB2 is also significant at 1% (1.35 points, or 27%, on the 5 point scale).

However, we found no significant difference in time, perceived accuracy, or perceived ease-of-use between different mFerio experiments. This suggests that mFerio does not suffer from unpredictable performance problems even when the payment amount changes. This was not unexpected, as paying someone $75.16 with cash requires more operations and counting than $2, whereas with mFerio, the difference is primarily a few extra text entry steps.

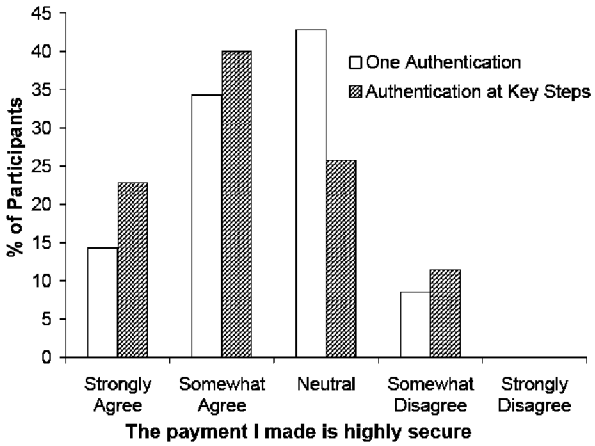


Figure 7: Perceived Security of Different Authentication Modes

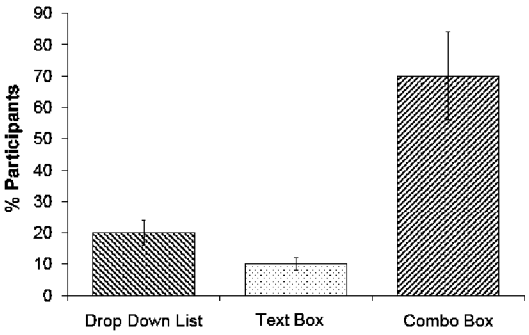


Figure 8: User Preference for Receipt Modes

5.5.5 *mFerio User Design Choices*

In this section, we present the results of the user-verified usability choices described in Section 3.3

One-touch or Two-touch Protocol? : After completing all experiments, users were both interviewed and presented with an end of experiment survey to obtain feedback on their preferred design choices. A significant majority (90%) indicated that they preferred a two-touch protocol even though it enforces several additional steps (an extra touch, two additional confirmations) in a transaction. Users felt that the additional steps in the two-touch protocol gave them more control and better overall security.

Method for Receiving Transaction Requests : After demonstrating the automatic (mFerio automatically accepts requests when not performing transactions), and manual (an explicit receive request mode must be selected) transaction receiving modes, we asked each user which method they preferred. Our results from this survey indicate no significant difference in user preferences. 52% of the users preferred the automatic mode of receiving transaction requests, and 48% preferred having manual control over the ability to receive requests. We thus retained the automatic mode as the default mFerio mode – with a view to change it later if necessary.

Petitioner Exhibit 1002-1344

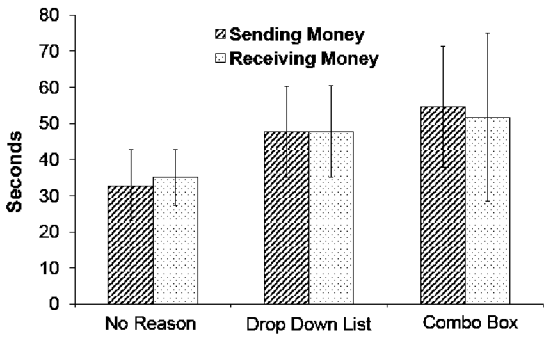


Figure 9: Task Speed in Different Receipt Modes

Authentication Mechanism : During our experiments, we asked users to execute payments using five different authentication mechanisms: One authentication step only (when starting mFerio), multi-point authentication (where authentication is needed at key points during the two-touch protocol), one authentication step at the start of the mFerio application combined with a fixed timer shown to the user, one authentication step at the start of the mFerio application combined with a fixed timer hidden to the user, and one authentication step at the start of the mFerio application combined with an inactivity timer (timer decreases only when the user stops using the cellphone) shown to the user. In the authentication modes with timers, the application would close automatically, cancelling any pending transactions, once the timers reached zero.

We decided to use, guided by our base-case time results (Section 5.5.1), a forty-five second limit for all the timers in our authentication experiments. The time taken to complete transaction when using different authentication mechanisms is shown in Figure 5, while the user preference for various authentication mechanisms is shown in Figure 6. From these results, we can conclude that the timers (both shown and hidden) enhance task speeds. Also, users perceive the multi-point authentication mechanisms as being more secure than the one-step authentication (with or without timers).

We asked users to state their preferred authentication mechanism without explaining to them the security differences between the different mechanisms. At the end of the user study, we explained these differences to the users and asked them to re-state their preferred authentication mechanism (at this point, most users had forgotten their previous answers). The "Informed Decision" bars in Figure 6 show the answers given by users after they were given an explanation of each mechanism. It is interesting to note that, while more users initially prefer to choose one-step authentication with a preset-time, several of them convert to choose the multi-step authentication mechanism after the debrief session.

We also captured user perceptions of payment security when they experimented with the various authentication mechanisms. These results are show in Figure 7. We see somewhat polarised results here. Among users who agreed that the mFerio payment was secure, there were more who perceived multi-step authentications as more secure than the one-step authentication with preset timers. On the other hand, among users who remained neutral or disagreed that mFerio payment was secure, there were more users who perceived one-step authentication with preset timers are more secure than a multi-step authentication mechanism. Overall, both one-step authentication with a preset timer shown to the user, and a multi-step authentication choice seem to be viable for mFerio – the one-step authentication with preset timer enhances task speed, while the multi-step authentication gives users a better sense of control in their payments. For the next phase of mFerio testing (testing a complete system), we used one-step authentication as we did not have any reasonably quick method to perform multi-step authentication. Again, we plan to revisit this design decision, as users seem to prefer multi-step authentication, if fast, reliable authentication mechanisms become commonly deployed.

Specifying Reason for Payment : mFerio provides various ways for users to annotate their receipts with a reason for the transaction (buying food for example). We compared user preference and performance when they used a simple textbox, a drop-down list, and a combobox (editable drop-down list) for annotating their receipts during a mFerio payment transaction. These results are presented in Figures 8 and 9 respectively. Although, the combobox method of receipt annotation increases time taken to complete a transaction (15 seconds more than the base case), there is an overwhelming preference for that. Hence we chose to adopt a combobox style of receipt annotation for the final mFerio prototype build.

6. PHASE 2 USER STUDY: FULL SYSTEM

In phase 2, we tested a complete mFerio implementation, with all security protocols fully implemented. This complements the phase 1 study, by 1) assessing the exact cognitive load of mFerio relative to cash, 2) testing mFerio with a more diverse population, and 3) comparing cash and mFerio in more diverse treatments. The overall experimental setup, procedure, and data collected was similar to that used in phase 1, but the experimental treatments were different.

6.1 Method

This study used three scenarios: base, time pressure, and low light. In the base scenario, participants performed eight tasks – four cash and four mFerio tasks. We used the same four tasks, as stated in Figure 5, for both the cash and mFerio experiments. We only used tasks 1B and 2B (for both cash and mFerio) for the time pressure and low light scenarios as we were primarily interested in user performance with more difficult tasks under adverse conditions.

The evaluation was within-subjects, but the task sets were not randomly ordered. In each scenario, all the cash tasks were performed in sequence first followed by the mFerio tasks (also in sequence). Each task took a minute or less to complete.

After each individual task, participants were provided a simple questionnaire that asked them to rate, on a 5-point Likert scale, a) whether they thought the task was quick to perform, b) how easy they found the task, and c) how confident they were that they completed the task correctly. They were also asked to complete the NASA-TLX survey [14] after each experiment. At the end of all the experiments, the participants received a longer questionnaire.

Scenario 1 – Baseline. The base scenario was used to obtain baseline cognitive load values for cash and mFerio.

Scenario 2 – Time Pressure. In this scenario, we told each participant that they only had 30 seconds to finish each task – simulating real-world situations where payments have to be made quickly.

Scenario 3 – Low Light. In this scenario, we lowered the lighting in the experiment room to simulate low light conditions – such as street light conditions. This simulates common situations where cash payments are made in locations without perfect lighting.

6.2 Participants and Setup

We recruited a total of 29 participants for our phase 2 study. All 29 users did the same set of cash and mFerio tasks. Each phase 2 user study took about 30 minutes to complete.

Petitioner Exhibit 1002-1345

Expt Code	Payment Amount ($)	Cash Received ($)	Objective
1A	Pay $5	N/A	Simple Cash Exchange
1B	Pay $8.65	N/A	Pay non-trivial Amount
2A	Ask for $1.30	Receive $2 and return $0.70	Collect small payment
2B	Ask for $36.40	Receive $50 and return $13.60	Collect large payment

These four experiments are used for both the cash and mFerio experiments in phase 2 (for all three scenarios). For cash experiments 2A and 2B, the participant received more than the requested amount and had to provide change (amount stated in the "Cash Received" column).

Table 5: Core Task Set – Phase 2

Total Number	29
Gender	Male (19), Female (10)
Age	20 and below (12), 20 to 30 (13) Above 30 (4)
Proficiency Level	Novice (10), Intermediate (7), Expert (12)
Importance of Phone	Low (12), Medium (14), High (3)

Table 6: Demographic Statistics for Phase 2 Study.

Our participants were a mix of undergraduate students (12), graduate students (2), and teaching and support staff (15). The participants had a mix of technical and non-technical backgrounds. We used the same demographics survey as in phase 1 to identify their cell phone proficiency levels and their perceived importance of their cell phone. Table 6 details the phase 2 participant demographics.

6.3 Results of Phase 2 User Study

We observed that the speed, ease-of-use, and accuracy results from phase 2 were similar to those obtained in phase 1 – validating our phase 1 results. Due to space constraints, we only present the new security protocol performance, and cognitive score results.

6.3.1 Measured mFerio Runtime Performance

During these experiments we logged the time taken by the mFerio application to execute the two-touch protocol, using the adapted Even-Goldreich-Yacobi security protocols, described in Section 3.1.2 separately from the user transaction time. As expected, the first touch (exchanging credentials) protocol times (average: 1.069 seconds, minimum: 0.995 seconds, maximum: 1.295 seconds, standard deviation: 0.0732), were significantly lower than the second touch (making payment and signed receipt transfer) protocol times (average: 4.850 seconds, minimum: 4.697 seconds, maximum: 5.242 seconds, standard deviation: 0.150).

Overall, the results are on the high side and indicate that public-key cryptography may not be the most suitable security primitives to use on some cellphones – an area for future mFerio research and implementation. Nonetheless, even with these high protocol times, users still found mFerio faster, with significantly less cognitive load (as shown in the next section), than cash in some scenarios.

6.3.2 mFerio has low cognitive load

Table 7 shows the cognitive load scores for the three scenarios in the phase 2 user study. We computed the cognitive load scores using the method proposed by Hart [14] (ask the user to provide ratings for six dimensions of load and combine those ratings using the user-provided importance rankings). The values in the table are average scores with the standard deviation provided in brackets. The "% Diff." column is the percentage difference between Cash and mFerio for that scenario (i.e. $\frac{Cash-mFerio}{Cash} * 100$)). Positive values indicates that mFerio has lower cognitive scores than cash.

There are no scores for experiments 1A and 2A for the Time Pressure and Low Light scenarios as we did not run these experiments in those scenarios. The "% Change" columns indicate how much the value has changed from the corresponding base scenario value – a positive number indicates that the cognitive load has increased by that percentage compared to the base scenario value.

From the table, we observe that cash has lower cognitive load than mFerio only for experiment 1A in the base scenario (cash has 48.2% less cognitive load). In every other case, mFerio has lower cognitive loads – reaching a high of 68.1% lower load for experiment 2B in the time pressure scenario. Figure 10 shows the breakdown of the cognitive load components for all the base experiments – for both cash and mFerio. The figure clearly shows that, except for experiment 1A, cash has a much higher cognitive load than mFerio – for almost every load component.

We also observe, from the table, that the cognitive load for cash significantly increased in the time pressure and low light scenarios. For example, participants performing experiment 1B reported, on average, 60.8% higher cognitive load values when doing the experiment under time pressure compared to the base scenario.

The cognitive load scores for mFerio also increased in three of the four non-base scenarios (time pressure and low light). However, these increases were not significant. In the last experiment (Low Light scenario, experiment 1B), mFerio's cognitive load actually significantly decreased relative to the base load (by 22.1%). We are investigating the cause of this decrease – we suspect that it might be due to various learning effects (mFerio is not really affected by low light conditions as the phone has a built-in light source).

Overall, mFerio significantly outperformed cash, in terms of cognitive load, in a number of common scenarios. This validates our goal of building an easy intuitive system for mobile p2p payments.

7. DISCUSSION

7.1 Additional Requirements for Deployment

In this paper, we presented part of the overall solution needed for a practical p2p payment system – we focused on the design and evaluation of the user interface. Before such a system can be deployed, several additional challenges need to be addressed:

Stake Holder Dynamics: A successful mFerio deployment will require cooperation from multiple stake holders, such as banks (to support the digital cash used), cellphone manufacturers and telecom service providers (to promote mFerio to their customers), retailers, regulatory bodies (to legalise p2p payments), and consumers. Unfortunately, satisfying the business and strategic goals of multiple stake holders is very difficult and achieving sufficient buy-in may require governmental and regulatory body support. A more detailed discussion of the policy changes and strategies necessary for industry adoption of mFerio is beyond the scope of this paper.

Mass Market Appeal: Ensuring mass market appeal for mFerio is important to leverage scale economies and the network externality effect where mFerio's utility is influenced by one's social network.

Petitioner Exhibit 1002-1346

Expt Code	Base			Time Pressure					Low Light				
	Cash	mFerio	% Diff.	Cash		mFerio		% Diff.	Cash		mFerio		% Diff.
				Actual	% Change	Actual	% Change		Actual	% Change	Actual	% Change	
1A	8.2 (2.4)	12.1 (3.2)	-48.2 *	N/A									
1B	15.3 (3.3)	10.6 (3.2)	30.9 *	24.7 (9.2)	60.8 *	11.5 (4.1)	8.4	53.4 *	20.1 (6.2)	31.4 *	8.3 (1.2)	-22.1 *	59.0 *
2A	11.6 (3.5)	6.6 (2.2)	43.1 *	N/A									
2B	18.8 (4.3)	6.5 (1.8)	65.4 *	23.7 (9.0)	25.6 *	7.5 (2.4)	15.6	68.1 *	21.5 (5.5)	13.9 *	7.7 (2.2)	17.6	64.3 *

results significant at 5% (using two-tailed tests) are indicated by *; lightly shaded results are not significant.

Table 7: Cognitive Load Scores

If the entities in a person's network are not mFerio ready, then one has to still use cash for payments. One way to increase mFerio's mass market appeal is to make it highly usable and an easy replacement for all cash transactions. This, unlike the various other challenges, is something that we can impact. Hence, we concentrated on making mFerio as usable as possible.

Phased Deployment: mFerio is more likely to succeed if it can be introduced gradually. In Singapore, one possible path is to initially introduce mFerio as a replacement for existing mobile payment systems, such as CashCard [27] or EZ-Link [12], that use NFC-enabled cards to make payments; users top up their cards, via NFC, at special machines. mFerio can easily be modified to support these systems initially. As the mFerio user base grows (people might prefer paying with their phones instead of carrying a separate card), the p2p aspects of mFerio can be enabled. We are currently investigating this phased deployment strategy in more detail.

7.2 Comparing mFerio With Other Systems

In this paper, we chose to compare mFerio solely with traditional cash payments. However, there are other mobile payment systems; for example, token-based NFC-enabled payment systems (CashCard, EZ-Link, etc.), SMS-based payment systems (Gpay [33], Obopay [28] etc.), and custom-application or browser-based online payment systems (Paypal Mobile [29] etc.).

These systems are fundamentally different from mFerio as they either use physical secure tokens (Cashcard etc.), or infrastructure support (SMS and online methods). Their protocols can thus be greatly simplified (to one-touch/one-step systems even) as a) the burden of authentication is moved to the infrastructure and/or tokens, and b) the usage scenarios limit the amount of user interaction needed. For example, the amount to pay is automatically computed by the token-based systems (based on length of travel etc.), the cell phone provider has verified details for all participants in an SMS-based payment systems, and Paypal authenticates all participants a-priori. In a true p2p payment system, the onus of authentication mostly falls on the participants of the system. The mFerio protocol is thus quite different and, generally, longer (to provide user input and user-visible authentication) compared to other payment systems; making direct comparisons misleading in our opinion.

7.3 User Study Limitations

Our two user studies are an important first step in identifying the usability of mFerio. However, they do have limitations. First, our participants were mostly 18 – 25 year old undergraduate students – a general population might show different results. Second, both studies were conducted in a controlled test environment – real world situations could affect mFerio's usability differently.

7.4 Effect of Demographics on Usability

We also noticed that the mFerio task completion times did not significantly vary across the experts and novices. Further, we noticed that there was no significant learning differences between the expert and novice population as well. Also, the only significant difference in the mFerio task completion time across the male and female participants was in the mFerio sending money task in phase 1(mFB1). The male participants were faster than the female participants by about 3 seconds on the average in this case. However this difference in performance across the genders disappears when learning effects are accounted for. Hence we infer that there is no significant difference in the necessary design requirements of mFerio across the expertise or gender spread.

8. RELATED WORK

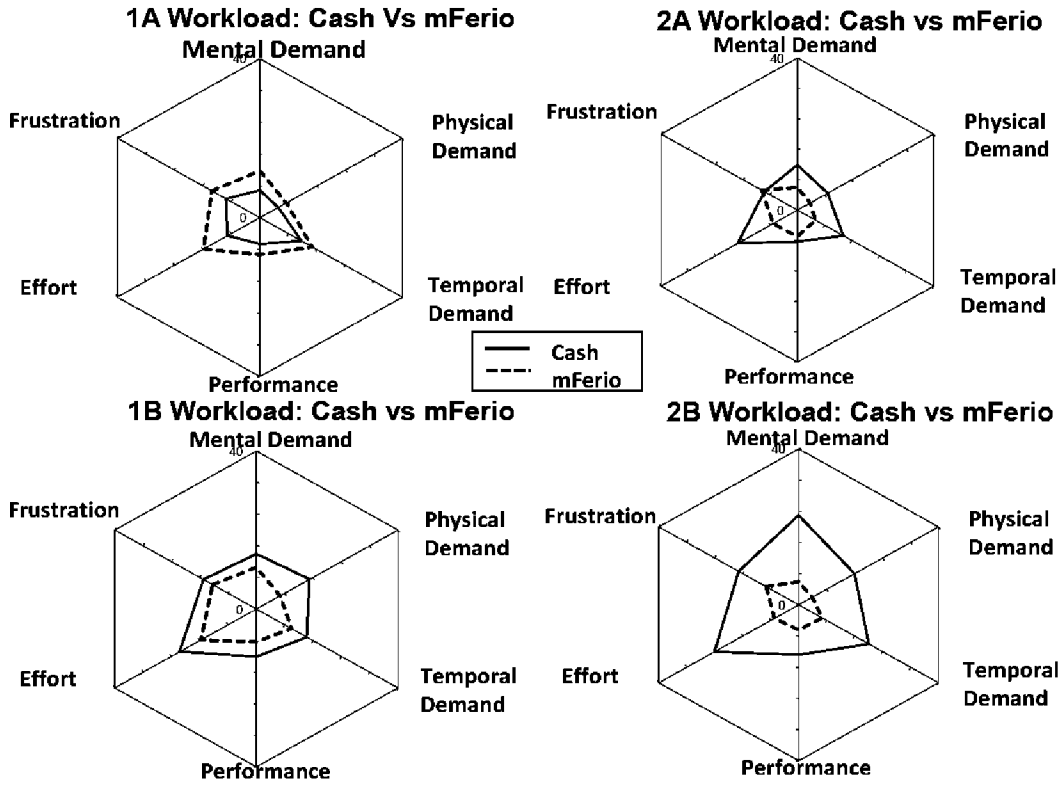
Davies [9] summarises various technological innovations with monetary payment systems including traditional cash and digital cash. There has also been a fair amount of past work looking at mobile payment in general. Kreyer et. al offer a typology of different mobile payment systems [19] – mFerio falls under the macropayments to stationary merchants and customer-to-customer transaction categories. They also spell out three criteria for general acceptance of mobile payment systems: cost, security, and convenience. In this paper, we focused primarily on convenience though mFerio was also designed with the first two criteria in mind.

Zmijewska [41] provides a summary of various wireless technologies for mobile payment, describing the pros and cons of 2G, 2.5G, 3G, infrared, NFC, and Bluetooth. Zmijewska also describes results from field trials showing that NFC is perceived to be more trusted due to required proximity. Near-field communication is already in wide use for contactless payments, for example, with smart cards and fixed readers. Our work here leverages the growing trend of NFC being installed on mobile phones, and focuses on making payments using phones rather than fixed readers.

Past UI research has looked at using NFC for novel interaction techniques. For example, Pering et. al [30] look at how a gesture to connect two devices together can be implemented using NFC and accelerometers and Want et. al [38] looked at how RFIDs could be used to bridge the gap between the physical and virtual worlds. Chen and Adams [8] provide a survey of different kinds of NFC technologies that could be used for mobile payments. Our work focuses less on developing novel interaction techniques, and more on using NFC to facilitate the sending or receiving of payments.

In addition to commercial smartcard payment systems [12, 25, 27, 37], many other types of mobile payment systems have been developed. For example, SmartRestaurant [24] allows customers to order and pay for meals at university campus restaurants. U-Payment [23] describes techniques for secure and private financial

Petitioner Exhibit 1002-1347



Each kiviat graph represents a different experiment. Each of the six axis ranges from 0 to 40 – smaller values are better.

Figure 10: Base Scenario: Cognitive Load Breakdown

transactions using mobile devices. Herzberg [16] describes many of the security issues involved in mobile payment systems. Our work differs as we are investigating the design and usability evaluation of a distributed peer-to-peer payment system, that uses mobile phones and NFC, rather than a centralised one.

Finally, there are a number of commercial companies that either have or are planning to release mobile payment solutions. For example, in addition to offerings in Japan and South Korea [32] (by service providers), Obopay Inc. [28] and Paypal [29] have already deployed mobile payment solutions with Google about to offer an additional solution (Gpay [33]). Kreyer et al [19] list several other commercial ventures. However, all these competing solutions use SMS or GPRS (requiring infrastructure) as their message protocol and do not support p2p communications. The work closest to mFerio is the mNETS [4] mobile payment system. However, even this NFC-based system does not support p2p transfers.

9. CONCLUSION AND FUTURE WORK

In this paper, we presented the design and evaluation of mFerio, a NFC-enabled mobile p2p payment system. mFerio's design was informed by analysing the key tradeoffs between usability, utility, and security – fundamental to any mobile p2p payment system.

Our analysis led us to a set of requirements for usability, security, and auditing. We then iterated our design several times to minimise the number of steps involved, while providing a strong level of security from the end-user's perspective. Finally, the results of a two-phase user study conducted with a total of 104 participants showed that mFerio is highly usable and is even faster than cash under various common scenarios. mFerio also showed lower cognitive loads than cash in a majority of cases.

The current mFerio prototype is part of a longer term project that aims to create a digital wallet-type architecture for cellphones. This digital wallet will allow users to store everything currently in their physical wallets (cash, identification, credit cards, receipts, etc.) inside their cellphones. We are already developing different aspects of a digital wallet, in parallel, and plan to work with various vendors to overcome some of the real-world challenges of deploying a digital wallet solution, such as getting mass market appeal.

In the near future, we plan to deploy a full version of mFerio in a real environment using a larger and more varied population pool. We also plan to test a variety of usable authentication schemes that can be employed on mFerio.

10. ACKNOWLEDGEMENTS

The authors would like to thank Bhatt Dev S/O Digantrai, Vidit Drolia, Anand Sujith Henry, Xiao Sa, Sridhar Venkataraman, and Dexter Huang Yaolin for their help in building the initial mFerio prototypes and for their help in conducting the phase 1 user studies.

11. REFERENCES

[1] Acquisti, A., Christin, N., Parno, B., and Perrig, A. Countermeasures against government-scale monetary forgery. *Proceedings of the Twelfth International Conference on Financial Cryptography and Data Security (FC'08)*, pages 262–266, Cozumel, Mexico, Jan. 2008.

[2] Adams, A. and Sasse, M. A. Users are not the enemy. *Commun. ACM*, 42(12):40–46, 1999.

[3] Brands, S. A. An efficient off-line electronic cash system based on the representation problem. Technical Report CS-R9323, CWI (Centre for Mathematics and Computer Science), Amsterdam, Netherlands, 1993.

Petitioner Exhibit 1002-1348

[4] Chan, J. *Wallet Replacing Phones – Eventually*. CNET Asia. http://asia.cnet.com/crave/2007/09/04/wallet-replacing-phones-eventually/, Sept. 2007.

[5] Chaum, D. Blind signatures for untraceable payments. *Proceedings of the International Crytology Conference (CRYPTO)*, Santa Barbara, CA, Aug. 1982.

[6] Chaum, D. and Brands, S. Minting electronic cash. *IEEE Spectrum*, 34(2):30–34, Feb 1997.

[7] Chaum, D., Fiat, A., and Naor, M. Untraceable electronic cash. *Proceedings of 8th Annual International Cryptology Conference (CRYPTO)*, Santa Barbara, CA, Aug. 1989.

[8] Chen, J. J. and Adams, C. Short-range wireless technologies with mobile payments systems. *ICEC '04: Proceedings of the 6th international conference on Electronic commerce*, pages 649–656, New York, NY, USA, 2004. ACM Press.

[9] Davies, G. *A History of money from ancient times to the present day*. University of Wales Press, Cardiff, UK, 2002. 3rd Edition.

[10] Ecma International. *Standard ECMA-340: Near Field Communication Interface and Protocol (NFCIP-1)*. http://www.ecma-international.org/publications/standards/Ecma-340.htm, Dec. 2004. 2nd Edition.

[11] Even, S., Goldreich, O., and Yacobi, Y. Electronic wallet. *Proceedings of CRYPTO'83*, pages 383–386, Santa Barbara, CA, Aug. 1983.

[12] EZ-Link Pte. Ltd. *EZ-Link Contactless Payment Card*, Mar. 2009. http://www.ezlink.com.sg.

[13] Gheringer, E. F. Choosing passwords: security and human factors. *ISTAS'02: Proceedings of International Symposium on Technology and Society*, pages 369–373, June 2002.

[14] Hart, S. G. NASA-task load index (NASA-TLX); 20 years later. *Proceedings of the 50th Annual Meeting of the Human Factors and Ergonomics Society (HFES)*, San Francisco, CA, Oct. 2006.

[15] Hayashi, E., Christin, N., Dhamija, R., and Perrig, A. Use your illusion: Secure authentication usable anywhere. *Proceedings of the Fourth Symposium on Usable Privacy and Security (SOUPS'08)*, Pittsburgh, PA, July 2008.

[16] Herzberg, A. Payments and banking with mobile personal devices. *Commun. ACM*, 46(5):53–58, 2003.

[17] Horn, G. and Preneel, B. Authentication and payment in future mobile systems. *Journal of Computer Security*, 8(2–3):183–207, Aug 2000.

[18] Kelly, J.F. An iterative design methodology for user-friendly natural language office information applications. *ACM Transactions on Office Information Systems*, 2(1), March 1984.

[19] Kreyer, N., Pousttchi, K., and Turowski, K. Characteristics of mobile payment procedures. *Proceedings of the International Syposium on Methodologies for Intelligent Systems (ISMIS)*, Lyon, France, June 2002.

[20] Kreyer, N., Pousttchi, K., and Turowski, K. Standardized payment procedures as key enabling factor for mobile commerce. *Proceedings of the Third International Conference on E-Commerce and Web Technologies (EC-Web)*, Prague, Czech Republic, Sept. 2002.

[21] Kügler, D. On the anonymity of banknotes. *Proceedings of the 4th International Workshop on Privacy Enhancing Technologies (PET'04)*, pages 108–120, Toronto, Canada, May 2004.

[22] Kungpisdan, S., Srinivasan, S., and Le, B. P. D. A secure account-based mobile payment protocol. *Proceedings of International Conference on Information Technology: Coding and Computing*, Las Vegas, NV, Apr. 2004.

[23] Lee, K. J., Ju, J.-I., and Jeong, J. M. A payment & receipt business model in u-commerce environment. *ICEC '06: Proceedings of the 8th international conference on Electronic commerce*, pages 319–324, New York, NY, USA, 2006. ACM Press.

[24] Lukkari, J., Korhonen, J., and Ojala, T. Smartrestaurant: mobile payments in context-aware environment. *ICEC '04: Proceedings of the 6th international conference on Electronic commerce*, pages 575–582, New York, NY, USA, 2004. ACM Press.

[25] MasterCard Worldwide Suite. *Mondex*. http://www.mondex.com, Apr. 2008.

[26] Micali, S. and Rivest, R. L. Micropayments revisited. *Proceedings of the The Cryptographer's Track at the RSA Conference on Topics in Cryptology*, San Jose, CA, Feb. 2002.

[27] Network For Electronic Transfers (Singapore) Pte Ltd. *NETS CashCard Contactless Payment Card*, Mar. 2009. http://www.nets.com.sg/consumers/netscashcard/index.php.

[28] Obopay Incoporated. http://www.obopay.com, Sept. 2007.

[29] Paypal Incorporated. *Paypal Mobile Services Overview*, Sept. 2007. https://www.paypal.com/?cmd=xpt/cps/mobile/MobileOverview-outside.

[30] Pering, T., Anokwa, Y., and Want, R. Gesture connect: facilitating tangible interaction with a flick of the wrist. *TEI '07: Proceedings of the 1st international conference on Tangible and embedded interaction*, pages 259–262, New York, NY, USA, 2007. ACM Press.

[31] Pousttchi, K. Conditions for acceptance and usage of mobile payment procedures. *Proceedings of the Second International Conference on Mobile Business*, Vienna, Austria, June 2003.

[32] Rebbeck, T. *South Korea and Japan show the way on mobile payments and banking*. Analysys Research, Apr. 2006. http://research.analysys.com/articles/standardarticle.asp?iLeftArticle=2100.

[33] Riley, D. *Could Gpay be Google's Killer App?* TechCrunch. http://www.techcrunch.com/2007/09/02/could-gpay-be-googles-killer-phone-app/, Sept. 2007.

[34] Toledano, D. T., Pozo, R. F., Álvaro Hernández Trapote, and Gómez, L. H. Usability evaluation of multi-modal biometric verification systems. *Interacting with Computers*, 18(5):1101–1122, Sept. 2006.

[35] Václav Matyás, J. and Ríha, Z. Biometric authentication - security and usability. *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, Portoroz, Slovenia, Sept. 2002.

[36] Varshney, U. Mobile payments. *IEEE Computer*, 35(12):120–121, Dec 2002.

[37] VISA. *payWave*. http://www.visapaywave.co.uk, Apr. 2008.

[38] Want, R., Fishkin, K. P., Gujar, A., and Harrison, B. L. Bridging physical and virtual worlds with electronic tags. *CHI '99: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 370–377, New York, NY, USA, 1999. ACM Press.

[39] Wayner, P. *Digital Cash: Commerce on the Net*. Academic Press, San Diego, CA, Mar 1997. 2 Sub Edition.

[40] Wrona, K., Schuba, M., and Zavagli, G. Mobile payments - state of the art and open problems. *Proceedings of the Second International Workshop on Electronic Commerce*, Heidelberg, Germany, Nov. 2001.

[41] Zmijewska, A. Evaluating wireless technologies in mobile payments " a customer centric approach. *ICMB '05: Proceedings of the International Conference on Mobile Business (ICMB'05)*, pages 354–362, Washington, DC, USA, 2005. IEEE Computer Society.

Petitioner Exhibit 1002-1349

e-EMV: Emulating EMV for Internet Payments with Trusted Computing Technologies

Shane Balfe
Royal Holloway,
University of London
s.balfe@rhul.ac.uk

Kenneth G. Paterson
Royal Holloway,
University of London
kenny.paterson@rhul.ac.uk

ABSTRACT

This paper shows how the functionality associated with EMV-compliant payment cards can be securely emulated in software on platforms supporting Trusted Computing technology. We describe a detailed system architecture encompassing user enrolment, card deployment (in the form of software), card activation, and subsequent transaction processing. Our proposal is compatible with the existing EMV transaction processing architecture, and thus integrates fully and naturally with already deployed EMV infrastructure. We show that our proposal, which effectively makes available the full security of PoS transactions for Internet-based CNP transactions, has the potential to significantly reduce the opportunity for fraudulent CNP transactions.

Categories and Subject Descriptors

K.4.4 [**Electronic Commerce**]: Payment Schemes

General Terms

Security

Keywords

Trusted Computing, EMV, Card Not Present

1. INTRODUCTION

The use of magnetic stripe cards for Point Of Sale (PoS) transactions is slowly being phased out in favour of Integrated Circuit Cards (ICCs) compliant with the Europay-Visa-Mastercard (EMV) specifications [15]. This process is essentially complete in Europe, well underway in the Far East, and under active consideration for North America. This major technology change is motivated by the susceptibility of magnetic stripe cards to cloning, and the projected fraud losses associated with the continued use of such cards. ICC cards, having chips that are actively engaged in the transaction authorisation process, are much less easily cloned. The U.K., which began the transition process in 2004, has seen a 47% post-migration reduction in PoS fraud [5]. However, with this reduction in PoS fraud has come an accompanying increase in Internet-based Card Not Present[1] (CNP) fraud. For example, CNP transaction fraud is now the predominant means through which payment card fraud is committed in the U.K. [6]. Specific figures are harder to come by for other countries, but we believe the U.K. experience to be illustrative of the global trend.

The level of fraud seen with CNP transactions has raised significant concern amongst the card processing community. Over the years a number of proposals have been put forward to address this problem. The most noteworthy of these are SET [35] and 3-D Secure [43]. However, neither of these proposals have gained widespread adoption. Indeed, the vast majority of CNP payments are protected today just using SSL/TLS to secure data in transit and to provide a limited form of merchant authentication. Customer authentication is provided through the customer's ability to provide relevant card details such as the Personal Account Number (PAN) and the corresponding Card Security Code (CSC) over the established SSL/TLS session.

Thus, from the merchant's perspective, there is no guarantee that the customer is actually in possession of the card corresponding to the details being proffered in a payment transaction. This problem is exacerbated by the perpetual increase in "phishing" attacks [22]: through a combination of social engineering and technical subterfuge, customers may be tricked into revealing their card account details to an attacker. In the past, these attacks have required some active participation from the user. However, as attacks become more sophisticated, the human element is becoming removed, with malicious software (malware) residing on a customer's platform being used to capture customer account details and manipulate customer transactions (including possibly instigating new transactions). We use the term Transaction Generator (TG), introduced in [24], to describe such malware in the remainder of this paper.

On the other hand, from the customer's perspective, there is little, if any, assurance that a merchant will endeavour to protect sensitive cardholder data stored on the merchant's servers. In a PoS environment, a customer's suspicion may be aroused by environmental cues, such as damage to the housing of the payment terminal or the demeanour of the sales assistant. Based on this physical evidence, a customer may decide not to engage in a transaction. However, in

[1]For the remainder of this paper all references to CNP transactions refer to Internet-based CNP transactions.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
STC'08, October 31, 2008, Fairfax, Virginia, USA.
Copyright 2008 ACM 978-1-60558-295-5/08/10 ...$5.00.

Petitioner Exhibit 1002-1350

an on-line setting, the environmental (browser-based) cues that are available are often either poorly interpreted, or not heeded [13]. In an attempt to instill greater confidence in customers, the Payment Card Industry Data Security Standard (PCI-DSS) [12] has been proposed. This standard details 12 mandatory requirements that merchants and third party processors must satisfy. A customer then trusts that a (legitimate) merchant is in compliance with this standard and has adopted best practice procedures to protect their credit card details. However, PCI-DSS-compliance levels are still low, and there have been instances of companies passing a PCI-DSS conformance audit, only to be later shown to be non-compliant with the standard at the time of a breach [33]. Recently, concerns over merchants running vulnerable payment applications have become so great that beginning in January 2008, Visa began implementing a series of mandates to eliminate the use of non-secure payment applications from the Visa payment system [45]. Visa will only accept payments from merchants using payment applications that adhere to, and have been validated against, Visa's Payment Application Best Practices (PABP) [44].

In summary, current CNP transaction processing cannot make use of the robust security features available from EMV-compliant ICC cards, and simply reverts to pre-EMV card authentication procedures. This weakness is now being ruthlessly and increasingly exploited by fraudsters, and closing this attack vector represents a significant challenge to the payment card industry.

1.1 Our Work

To combat the threats posed by malware TGs (and by merchants that are non-conformant with the PABP), we propose e-EMV, a system that makes use of Trusted Computing technology to securely emulate EMV for CNP transactions. We describe a system architecture encompassing user enrolment, deployment of software cards to customer platforms, card activation, and subsequent transaction processing. Our e-EMV proposal uses a combination of application software, a Trusted Platform Module (TPM) [41], a processor (with chipset extensions) [23] and Operating System (OS) support [32, 1] to securely emulate the functionality of a standard EMV-compliant card in software. We provide a detailed description, at the level of individual TPM commands, showing how this emulation is achieved. We also explain how the security features provided by Trusted Computing are used to obtain an appropriate level of security for our system.

Our approach of emulating EMV on Trusted Platforms for CNP transactions provides the following benefits:

1. It is possible to demonstrate e-EMV card ownership and authentication for CNP transactions as in standard EMV card authentication procedures. Thus a merchant can ensure that a customer claiming to possess a particular e-EMV card is the legitimate owner of that card.

2. A merchant can obtain a payment guarantee through being able to demonstrate customer authorisation of a transaction.

3. A customer can gain an assurance prior to transaction initiation that a merchant will endeavour to protect sensitive cardholder information. Such a feature is is absent from EMV's use at PoS terminals, a fact which is now allegedly being exploited by criminal gangs [42].

4. An executing e-EMV application can avoid the threat posed by malware TGs, by hosting e-EMV cards in their own isolated memory partition, free from observation and interference.

5. Our proposal supports EMV cards that are more cryptographically capable and offers enhanced authentication and transaction authorisation procedures, relative to cards used in current EMV deployments for PoS transactions. While these enhanced security features (Dynamic Data Authentication (DDA) and Combined DDA and application cryptogram generation (CDA)) are specified in the EMV standards [15], they are not ubiquitous on today's EMV ICCs because of their cost implications; instead, some banks find it more economical to work with cheaper cards and accept the higher level of risk implied by the use of Static Data Authentication (SDA) [15]. However, our proposal, involving only software running on mass-market consumer computing platforms, is not restricted in this way.

6. In e-EMV, modifications and enhancements (resulting from, for example, changes to the EMV specifications) can be realised through relatively straightforward software update processes. In contrast, traditional EMV requires complicated and expensive card upgrades to achieve the same thing. This lends our e-EMV approach an inherent degree of "future proofing".

The motivation for emulating EMV, rather than designing a new protocol from scratch, comes from real-world, practical constraints. By creating an environment where EMV transaction flows can be mapped directly to e-EMV transactions we can avoid any expensive re-engineering of the back-end financial network. Indeed, our proposal is compatible with the existing EMV transaction processing architecture, and thus integrates fully and naturally with already deployed EMV infrastructure. Additionally, as a consequence of EMV having been developed and deployed over many years, many of the protocol bugs should already have been ironed out.

The relative applicability of our approach is obviously dependent on the ubiquity of Trusted Computing on commodity computing platforms. This is, however, not an unreasonable assumption, and once made, allows a number of interesting solutions to a whole host of security problems plaguing CNP transactions. Currently available sales figures for 2005 [37] showed estimates of 32% of all notebook systems shipped that year being TPM-enabled. This figure is expected to nearly triple by the end of 2008, with processor and OS support to follow soon after [1, 23, 32]. In addition to this, the recently released Trusted Mobile specifications [40] holds particular promise for our architecture, as market penetration of mobile devices typically occurs at an expedited rate compared to that of Personal Computer (PC) clients.

Our e-EMV proposal could result in a mutually beneficial arrangement for TPM manufacturers and card issuers. Indeed, our e-EMV proposal could be a "killer application" for Trusted Computing in the consumer space, something that seems to be currently lacking.

Organisation: In Section 2, we present an overview of related work. In Section 3, we provide a brief introduction to EMV and Trusted Computing. In Section, 4 we describe the payment model used for CNP payments. Section 5 provides a high-level overview of our e-EMV architecture. Section 6 explains in detail the procedures and processes involved in establishing an e-EMV card within a Trusted Computing enhanced platform. Following on from this, Section 7 high-

Petitioner Exhibit 1002-1351

lights how a normal EMV transaction flow can be mapped to an e-EMV transaction. Section 8 examines how the threats posed to CNP transactions are mitigated by e-EMV. We conclude with Section 9.

2. RELATED WORK

Herreweghen and Wille [21] present a detailed evaluation of the security requirements for card-based Internet payments. These include: payment guarantee for merchant, mutual authentication between customer and merchant, customer privacy and anonymity, and transaction authorisation.

The real world roll-out of EMV and the accompanying desire to replicate the fraud reduction seen with PoS transactions has resulted in a number of proposals that utilise EMV's functionality for Internet-based payments [2, 14, 21, 25, 29]. However, these approaches have not seen any real traction in the market place. A possible explanation for this is these proposals' underlying assumption that customers would make use of card readers connected to their PC platforms. This assumption engenders an additional cost in the form of distributing card readers to end-users. Even if the cost issue could be surmounted, these approaches alone offer only limited security gains. This is due to the lack of a trusted path between the card-reader and host, as well as a lack of OS support for application isolation. Without these, a Transaction Generator (TG) could passively observe Personal Identification Number (PIN) entries, actively modify transaction data and possibly generate new transactions, enabling criminals to remotely take control of users' payment cards. There has, however, been a recent development in integrating EMV with CNP transactions that aims (albeit indirectly) to address the TG issue. This is the proposed use of "unconnected" card readers [27] which have been rolled out by a number of prominent UK banks. Unfortunately, this approach also suffers with respect to the additional costs associated with distributing card readers to end-users and, once deployed, cannot be updated to address new threats as they emerge.

The use of Trusted Computing to combat phishing has been proposed in [3] and [16]. The primary threat considered in [3] is external attack, whereby a credential needs to be extracted from the client's platform in order for it to have any value to an attacker. No consideration is given to the ever-increasing threat posed by malware TGs. The threat from malware is examined in greater detail in [16, 24]. Here, much like in our approach, Virtual Machines (VMs) are used to constrain the use of malware to an individual VM "compartment". These authors also suggest using visual cues as to the trustworthiness of the VM with which an end-user interacts, an idea originating in [7]. Such work is complementary, but orthogonal, to our own: these cues could be adopted in e-EMV and might help enhance customer protection from TGs.

3. EMV AND TRUSTED COMPUTING

In this section, we provide a high-level overview of the main features of EMV and of Trusted Computing, providing references for readers who require more detail. This section introduces many acronyms on which we will later rely. We include a table of acronyms to assist the reader in Table 1.

3.1 EMV

EMV, as described in the current iteration of the specifications defines the full spectrum of interactions, from the physical to the logical, between an ICC and an ICC-enabled PoS terminal [15]. A readable introduction to the technical content of the EMV specifications can be found in [29]. EMV supports both cardholder authentication, through new Cardholder Verification Methods (CVMs), and ICC authentication through either SDA, DDA or CDA. SDA cards allow the terminal to determine if the data on the card has been modified since card personalisation. DDA cards are more complex in that they allow for the same checks as SDA but also enable the terminal to determine if the card is genuine or not through a challenge-response mechanism. This involves the ICC generating a signature (using a card-specific private key, with the card storing a certificate issued by the card's issuer for the corresponding public key) over the terminal-supplied challenge. CDA cards are similar to DDA cards except the message signed by the ICC includes an additional Application Cryptogram (AC). ACs are used to protect transaction messages generated by the ICC using AC Session Keys (derived from a long-term master key, the ICC AC Master Key, that is shared between the ICC its card issuer). This ICC AC Master Key is unique per card and is derived from a customer's PAN, PAN sequence number and an issuer Master Key. Here the PAN sequence number helps to identify a card amongst several cards belonging to the same customer with the same PAN.

EMV defines a number of different types of transaction messages. Depending on the reconciliation of card and terminal risk management routines one of the following will be generated by the card: an Application Authentication Cryptogram (AAC), an Authorisation Request Cryptogram (ARQC), an Authorisation Response Cryptogram (ARPC) or a Transaction Certificate (TC). If the transaction is approved, the ICC will generate a TC which will be passed to the terminal and can be used to claim payment during the clearing process. If a transaction is declined, the ICC will generate an AAC. In the event that the transaction needs to be approved on-line the ICC generates either an AAC or an ARQC. which will be forwarded to the issuer. The issuer will then reply with an ARPC indicating whether the transaction should be approved or declined, in which case a TC or an AAC will be generated by the ICC.

3.2 Trusted Computing

Trusted Computing is based on the inclusion a hardware "root of trust", the Trusted Platform Module (TPM), within a platform, that aims to allow users (and third parties) to assess the "trustworthiness" of the devices with which they interact. To achieve this, a Trusted Platform will be able to attest to its current operating environment, or any subcomponent thereof. Interested second parties can make requests for this information, and any divergence from an intended operating state can be detected by the second party, allowing them to make informed decisions as to whether to continue to interact with the current system. We assume the reader is familiar with Trusted Computing and the TPM command set, literature for which can be found in [28, 41]. We now briefly outline some of the Trusted Computing functionally which we use in the remainder of this paper.

Measuring events on a platform is a two-stage process that begins with an *extend* command. This command appends a

Petitioner Exhibit 1002-1352

AAC	Application Authentication Cryptogram	OIAP	Object Independent Authorisation Protocol
AC	Application Cryptogram	TG	Transaction Generator
AIK	Attestation Identity Key	TC	Transaction Cryptogram
ARPC	Authorisation Response Cryptogram	TCG	Trusted Computing Group
ARQC	Authorisation Request Cryptogram	TLV	Tag Length Value
CDA	Combinded DDA and AC Generation	PABP	Payment Application Best Practices
CMK	Certified Migratable Key	PCI-DSS	Payment Card Industry Data Security Standard
CSC	Card Security Code	PoS	Point of Sale
DAA	Direct Anonymous Attestation	PCR	Platform Configuration Register
DDA	Dynamic Data Authentication	PIN	Personal Identification Number
DRTM	Dynamic Root of Trust for Measurement	SDA	Static Data Authentication
EMV	Europay Mastercard Visa	SML	Stored Measurement Log
ICC	Integrated Circuit Card	SVM	Secure Virtual Machine
MOG	Merchant Operator Guidelines	TXT	Trusted Execution Technology
MVMM	Measured VM Monitor	VM	Virtual Machine

Table 1: Table of Acronyms

hash of the event being measured (typically an application's instruction sequence, its initial state and its input) to one of a number of Platform Configuration Registers (PCRs) located internally to the TPM. These PCRs store a representative hash of all the events generated so far to form a picture of the current platform state. The second stage in this process is the writing of events, reflected in a PCR, to permanent storage. This logging of integrity-altering events within a platform occurs in the Stored Measurement Log (SML).

When a verifier wishes to inspect a host platform's configuration, it requests (a portion) of the challenger platform's SML and asks the challenger's TPM to produce a signature over a specific set of PCR values describing a portion of the platform's operating state. The TPM uses the private component of a key pair called an Attestation Identity Key (AIK) to perform the signing operation over the requested PCR values. However, in order for the values being attested by a platform to have meaning outside of the confines of a challenger's platform, it is necessary for the challenger's platform to first obtain a credential for the signing AIK from a trusted third party recognised by the verifier. How this credential is obtained differs between version 1.1b and version 1.2 of the TPM specifications. Version 1.1b uses what is referred to as the "Privacy CA" model (see [39]) whilst version 1.2 introduced a new (optional) model in the form of Direct Anonymous Attestation (DAA) [11, 41].

A TPM can manage an unlimited number of cryptographic keys. Every TPM_Key [41] has an assigned attribute designation (migratable, Certified Migratable or non-migratable) for defining key mobility as well as a defined key type (signing, storage or legacy) for defining what particular operations a TPM_Key is capable of performing. In addition, individual private keys may require explicit authorisation data to be entered by a user before the key can be used, or require a specific set of platform metrics to be present before the key can be loaded and used.

In addition to the features provided by the TPM, both Operating System (OS) and processor support represent integral components in the realisation of Trusted Platforms. As well as providing access to TPM functionality, a Trusted OS will be capable of launching sandboxed Virtual Machines in which applications can run. A Dynamic Root of Trust for Measurement (DRTM), as defined by Intel in their Trusted Execution Technology (TXT) and AMD in their Secure Virtual Machine (SVM) system architectures [23, 4], refers to the instantiation of one or more protected Virtual Machines (VMs) running on-top of a Measured Virtual Machine Monitor (MVMM) [1]. These VMs run in parallel to the standard OS partition without requiring a system reboot. The following are generic security services for a protected VM based on an MVMM; we assume the presence of such functionality in our later discussions.

No interference: Ensures that a program is free from interference from entities outside its execution space.

Trusted path: Assumes a trusted path between a program and an input device, similar in function to Intel's trusted mobile keyboard controller [19].

Secure inter-process communication: Enables one program to communicate with another, without compromising the confidentiality and integrity of its own memory locations.

Non-observation: Ensures an executing process and the memory locations it is working upon are free from observation.

4. PAYMENT MODEL

The processing model used for most card payment systems (including EMV) is typically referred to as the four-corner-model. Within this model, a number of steps are necessary to complete a given transaction (see Figure 1). Prior to a customer being able to interact with a merchant, it is necessary that they follow some issuer-specific enrolment procedure in order to obtain a physical payment card. A merchant, likewise, can only accept payments from a customer if they have preregistered to accept payments for that customer's particular card type with their acquirer. The dashed line in Figure 1 represents the boundary of the financial network domain. Payment processing occurs as follows:

Step 1: The process begins with a customer signalling their intent to purchase goods by forwarding a payment record to a merchant. In this instance, the actual characteristics of a payment record differ depending on the environment in which it was created. For an on-line purchase, a payment record typically includes the information embossed on the customer's physical payment card in conjunction with certain merchant supplied information (such as the invoiced amount).

Steps 2-5: These steps occur immediately after receiving the customer's payment record. They consist of a merchant submitting the transaction details to their acquirer which will either authorise or reject the transaction based on their interactions with the customer's card issuer. Then the merchant will either confirm payment or reject the transaction.

Petitioner Exhibit 1002-1353

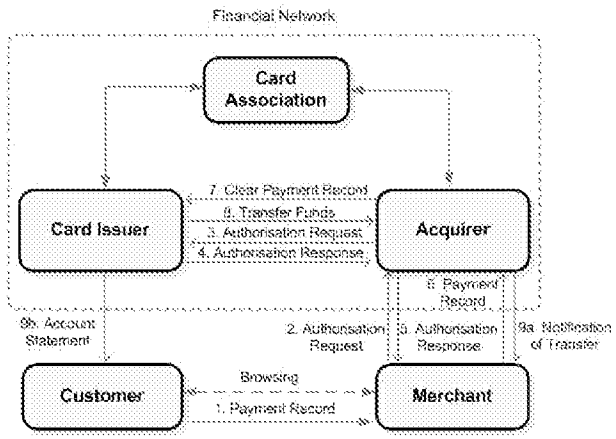


Figure 1: Generic model for card processing.

Steps 6-9: Based upon the transaction being approved, either as a result of a successful outcome from steps 2-5 or merchant risk management routines, steps 6-9 represent the account settlement process through which funds are debited from a customer's account and credited to the merchant's.

Perhaps the most surprising feature of this model is that a positive transaction authorisation does not guarantee payment for a merchant. It is merely an indication that the card account details being proffered have not been reported stolen and that the customer has sufficient funds to cover the transacted amount. Indeed, unless the card has been reported stolen, it is difficult for a card issuer, and by extension a merchant, to ascertain whether a particular transaction is fraudulent or not.

Our e-EMV architecture closely follows the generic four corner model presented above. The only differences in our approach are that the communication channel between the customer and the merchant is now Internet-based (instead of being based on physical proximity of card and terminal), and that both card issuers and acquirers must provide enrolment facilities for their e-EMV clients, separate to the facilities provided for the physical issuance of an EMV card. In doing so, we assume the presence of a Public Key Infrastructure (PKI), which can be an extension of the one that currently exists for EMV. In this regard, enrolment facilities should be able to be authenticated by customers and merchants via public key certificates issued by a particular card association.

5. AN OVERVIEW OF E-EMV

This section aims to present a high-level overview of our e-EMV proposal. Our overall aim is to provide functionality akin to that of a standard EMV card by replicating that functionality through procedures and capabilities natively supported by a host that is augmented with Trusted Computing. This allows us to provide a secure and extensible architecture for CNP transactions.

The procedure for establishing an e-EMV card on a Trusted Computing platform is a two-stage process consisting of an account activation stage and an application delivery stage. In describing this architecture we are making the following important assumptions, reiterated from Section 4: we assume the presence of a PKI extending the one currently in existence for EMV, we assume that Trusted Computing Platforms are ubiquitous within the merchant/customer domain, and additionally, that strong process isolation is available on all platforms within this domain [1, 4, 23]. We also assume a trusted path exists between the customer's keyboard and TPM. Methods for achieving this are discussed in [19]. Furthermore, we have the underlying assumption that a card issuer has already made the decision to extend credit or debit facilities to a particular customer.

5.1 Enrolment

Enrolment in our e-EMV architecture involves a customer formally registering as a legitimate cardholder, allowing him to obtain an e-EMV card. Much like enrolment in the traditional EMV architecture, a card issuer within our system is responsible for enrolling cardholders as well as later authenticating their transactions (and possibly the cardholders themselves). Acquirers can be seen as providing similar functionality to their merchant customers. The stages for establishing an e-EMV card on a TPM-enabled platform are as follows.

Account Activation: Account activation is the process through which a customer becomes a member of a card-issuer-controlled group. In this case, membership is indicative of a customer activating their account within the system. In the context of Trusted Computing, this means enrolling with a Privacy CA (see [39]) or optionally becoming a member of a card-issuer-controlled DAA group (see [11, 41]). This is achieved by the customer demonstrating the presence of a non-migratable TPM-controlled secret over which certification is requested, this private key being either an AIK in the case of the Privacy CA or a secret value f for DAA. Note, in discussing the use of a Privacy CA and DAA here, we are not suggesting that our approach should actually benefit from the privacy-enhancing features available from either of these choices. Rather, we see the card-issuer playing the role of either a Privacy CA or DAA issuer as providing a convenient mechanism for achieving client-side authentication within the limitations of the TPM specifications.

At this point, the actual binding between the customer and his platform can be established through a mechanism of the issuer's choosing. For example, the customer might provide information such as a passcode supplied to them in the pre-enrolment stage (in which the card issuer agreed to extend debit/credit facilities), communicated using an out-of-band mechanism. In addition to this authentication information, a platform will send various platform credentials (describing the binding of the TPM to the platform) as well as evidence of the existence of a non-migratable TPM-controlled secret. After receiving this information, the card issuer performs due diligence to satisfy itself as to the relationship between a customer and his platform. This is achieved through a reconciliation of the provided authentication information with an examination of evidence supporting the existence of a TPM-controlled secret. If the card issuer is satisfied by this evidence, the customer's platform will receive certification on their TPM-controlled secret. This certification will later be used to demonstrate the customer's membership of a particular card scheme.

Enrolment for the merchant, by contrast, involves satisfying the requirements for payment processing as laid down by the relevant acquirer's Merchant Operator Guidelines

Petitioner Exhibit 1002-1354

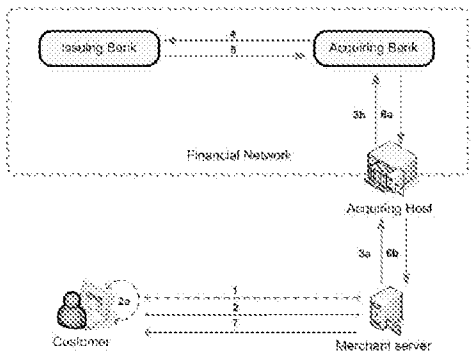


Figure 2: Transaction architecture for e-EMV.

(MOGs). During the merchant enrolment procedure, the merchant's acquirer also becomes a certificate issuer, again in the context of the Privacy CA or DAA models.

Secure Application Delivery: The customer downloads a small secure application bundle that fulfils the role of an e-EMV card as well as acting as a guide through the process of creating/installing the requisite TPM managed keys [15]. This bundle, once installed will enable a platform to perform electronic transactions analogous to those carried out by an EMV card at a PoS terminal. Our e-EMV application contains all the keys required to perform CDA authentication. However, unlike an EMV card, our e-EMV application will need to provide some of the functionality typically seen in PoS terminals, particularly when it comes to cardholder verification (see Section 7).

The merchant will need to download and install a terminal plug-in application, similar in function to a 3-D Secure merchant plug-in [43], but capable of emulating certain EMV terminal functionalities. The most important of these will be the authentication of customer-supplied credentials. Much like terminals in the physical setting, merchants will require card issuer's public key certificates in order to verify customer transactions. This plug-in must be compliant with Visa's PABP and the PCI-DSS standards. We do not discuss the operation of the merchant terminal plug-in in any greater detail in this paper as this information is outside the scope of the EMV specifications and is largely proprietary to individual acquirers.

5.2 Transaction Architecture

In order for an e-EMV application (card) to be launched, a Trusted Platform's OS sends an instruction sequence to the DRTM to create a new isolated memory partition. The DRTM launches a VM into this newly created memory area, which in turn executes our e-EMV application, free from observation and influence of TGs. For the details of launching a secure VM, we refer readers to [23]. With the exception of Step 1 (see Figure 2), the basic flow for e-EMV transaction processing follows EMV's transaction processing at a PoS. The steps are as follows:

Step 1 represents the browsing phase in which a customer peruses a particular merchant site. During this step, the customer verifies that the merchant is a member of a valid group of merchants, corresponding to a particular Privacy CA/DAA issuer (acquirer). Additionally, the customer's e-EMV application, acting on the customer's behalf, may verify that the merchant is in a state that exemplifies an adequate policy for addressing privacy and confidentially concerns (for example, conformance with the PCI-DSS or Visa's PABP) via Trusted Computing's attestation procedures.

Step 2 represents the typical EMV ICC and terminal interaction, except that the communication channel between the two is now exclusively Internet-based.

Step 2a represents the creation of an AC. As part of this step the customer's platform generates a signature over its AC (using the certified non-migratable TPM-controlled secret established during the account activation phase) as well as the Platform Configuration Register (PCR) values that provide evidence as to the platform's current state at the time of transaction authorisation. These data items are communicated over a secure and authenticated channel to the merchant server.

Steps 3 to 7 are executed if the optional decision to go "on-line" has been exercised. As a result of either terminal or card risk management procedures, the AC (possibly in conjunction with the information adducing the current platform state) is forwarded to the customer's card issuer (Steps 3a–4). After examining the received data, the card issuer returns an AC of its own (Steps 5–7). This AC informs both the card and the merchant as to whether the request is to be approved or declined, in which case the card application will either proceed with the transaction or reject it. It is important to note that all e-EMV messages exchanged in Steps 2–7 are standard EMV message flows.

Where additional Trusted Computing platform state information has been added to EMV's AC messages in our architecture, it is optional for an card issuer to examine this state information as part of its decision making process. The Tag Length Value (TLV) encoding mechanism used in EMV makes it easy for an card issuer to ignore any extraneous information from a transaction referral request. Significantly, if the card issuer does decide to take a customer's platform state into consideration, the customer's card issuer would not need any Trusted Computing hardware to examine these characteristics. It would only need to be capable of hashing some supplied records, comparing them against known good metrics for a particular card application and verifying a signature (as we shall see in Section 6). Indeed, such functionality could be provided by a third party facility or performed by the merchant plug-in.

6. INSTANTIATING AN E-EMV CARD

This section explains in greater detail the process involved in establishing an e-EMV card within a Trusted Platform.

6.1 Account Activation

In order for a customer's e-EMV account to be activated, the customer's Trusted Platform must become a member of a card issuer controlled group. This process is mirrored for the merchant server account activation procedure with respect to a merchant's acquirer. In both cases, account activation is achieved by successfully obtaining/generating a credential issued for an AIK public key. This credential could be in the form of X.509 certificate issued by a Privacy CA or a credential issued by a DAA Issuer [41].

In either case, the choice of a Privacy CA or DAA Issuer will end with a similar result: the customer will have their account activated, later allowing them to demonstrate physical/logical possession of an active card within the system.

Petitioner Exhibit 1002-1355

Through the establishment of a customer-centric credential embedded within a platform, the customer will be able to attest to the existence of a key capable of replicating EMV's SDA/DDA/CDA functionality.

In obtaining this credential, the credential issuer needs to ensure that a request is coming from a particular customer. This can be achieved, for example, through a customer demonstrating knowledge of a shared secret created in the pre-enrolment stage over a secure channel. However, the actual mechanism used is orthogonal to our discussion.

6.1.1 Privacy CA Approach

Here the process involves a customer's TPM generating an attestation key pair (S_{AIK} and P_{AIK} for the private/public portions respectively) and having P_{AIK} incorporated into an ICC Public Key Certificate (AIK credential). When creating this key, the customer specifies a password for S_{AIK}, which will be required every time the key is loaded for use. The process involved in the generation of a new attestation key within a platform maps to the generation of an AIK key within a TPM, that is, as a result of performing the TPM_MakeIdentity command [41]. The P_{AIK} portion of this AIK, along with various platform credentials and customer authentication data, are encrypted with the Privacy CA's public key and sent to the card-issuer-controlled Privacy CA. After authenticating a particular customer and satisfying itself that the request is coming from a genuine TPM, the Privacy CA will issue an AIK certificate (ICC Public Key Certificate) to the customer's TPM-enabled platform. This credential can then be used to provide evidence of card activation within the system. The AIK certificate could be further enhanced through X.509v3 extensions. For example, it is possible to add key and policy information to the credential, such as setting a private key usage period during which the AIK signing key will be valid.

6.1.2 DAA Approach

The DAA enrolment procedure occurs exactly as laid out in [11]. However, here the role of the DAA Issuer is provided by the card-issuer-controlled issuing host. After a successful completion of the DAA_Join command [41], the customer will instruct his TPM to create a new AIK pair (S_{AIK} and P_{AIK} for the private/public portions respectively). As part of this key generation process, the customer specifies a password for S_{AIK}, which will be required every time the key is loaded for use. The customer then instructs his TPM to sign the P_{AIK} component using their newly enrolled DAA key to create the ICC Public Key Certificate. This will later allow the customer to be able to demonstrate that his account has been activated with respect to a particular card issuer.

Subsequent to a successful completion of either the DAA join procedure or upon receipt of an AIK certificate from a Privacy CA, the card issuer activates the customer's account within its systems. This enables the soon-to-be-downloaded e-EMV application to be used in ensuing financial transactions.

6.2 Secure Application Delivery

The delivery of the e-EMV application to a customer's platform involves an interactive process between a customer and his card issuer. The delivery of the software itself necessitates a number of checks to ensure the binding between a customer and his platform. The software set-up utility requires the inclusion of a unique EMV ICC AC Master Key per card issuance, and this key cannot be generated by the platform itself as it is derived from a card issuer Master Key. Instead the ICC AC Master Key needs to be injected into the platform as part of the application delivery process. In addition to the secure delivery of the application, there is an underlying customer-driven requirement to ensure the authenticity and the "behaviour" of the application once delivered. The dual concerns of authenticity and behaviour can typically be addressed using what is termed a validation credential in the Trusted Computing literature [39]. In this way, load-time metrics can be compared against known good values to assure customers (and merchants) that their applications will perform as intended.

The issue of secure delivery of an application using Trusted Computing has previously been examined in the context of conditional access in mobile systems [17]. Much like the approach adopted in [17] in which a third party specifies the state to which an broadcast application must be bound, we require the card issuer to be able to specify the state on the customer's platform to which the e-EMV application will be "sealed". Sealed messages in the context of Trusted Computing are messages that are bound to a set of platform metrics (specified by one or more PCR values) and that can only be opened when the platform is in a certain state. This is normally achieved with the TPM_Seal [41] or the TPM_Sealx command [41]. However, the TPM_Seal and TPM_Sealx commands only allow messages to be sealed locally to a customer's platform. To overcome this problem, a card issuer can specify a state to which a private key must be sealed on the customer's platform. The corresponding public key can be sent to the card issuer, who can satisfy themselves that the private component of this key is indeed sealed to a specified platform state (by examining the TPM_PCR_INFO structure associated with the signed public key). The card issuer may then encrypt the e-EMV application with this public key and send it to the customer.

In our proposal, the delivery of an application to a customer's platform, as well as the corresponding requirement of securely storing the application upon receipt, is handled in three stages. In the first stage, the customer generates an asymmetric key pair, specifying security constraints for the private key. In the second stage, the customer sends the public key of this key pair to the card issuer. The card issuer will then encrypt the customer's e-EMV application with the customer's public key. In the third stage, the customer decrypts his e-EMV application (provided the security constraints specified for the private key are satisfied by the platform). The details of these stages are as follows.

Stage 1: In the first stage, the customer's TPM generates either a CMK or a non-migratable key pair. The set-up phase of this is illustrated in Algorithm 1.

Algorithm 1 Set-up Phase

1: Issuer → Cust: Sealed State || Issuer_{Cert1} || Guide || $Sign_{Issuer}$(Sealed State || Guide)
2: IC_Key := TPM_CreateWrapKey(TPM_Auth_Priv_Use_Only, digestAtCreation, digestAtRelease)
3: TPM_Certify_Info := TPM_CertifyKey(IC_Key)

Petitioner Exhibit 1002-1356

Notation: Here Issuer is the card issuer and Cust is the customer. $Sign_X(Y)$ denotes a signature with the private key of entity X over data item Y and X_{cert1} is the public key certificate for entity X for which the corresponding private key is used for signing only. Finally, Guide is a small software applet that guides the customer through the creation of the necessary TPM keys for secure application delivery.

In **step 1**, the customer's card issuer specifies a state to which it would like the customer to "seal" a private key. This state will typically be a representation of the MVMM and the minimal VM software components necessary for e-EMV application virtualisation. In this step the customer also receives the card issuer public key certificate (from the EMV PKI [15]) and a small signed application that will guide the user through the creation of the requisite TPM keys.
In **step 2**, after having verified the signatures received in step 1, the guide application, acting on the customer's behalf, creates a new asymmetric key pair, IC_Key. The application calls the TPM_CreateWrapKey command to generate a new asymmetric key pair, and asks the customer to enter a password ($usageAuth$) which will be required every time the private component of this key pair is loaded (TPM_Auth_Priv_Use_Only). The application captures the current platform state at the time the key pair is created (digestAtCreation) as well as the future platform state required for private key usage (digestAtRelease). Here digestAtRelease is specified to be the *SealedState* provided by the card issuer.
In **step 3**, the newly generated IC_Key is certified by S_{AIK} using the TPM_CertifyKey command [41]. Here the customer's TPM is effectively producing a signature over the public component of IC_Key using a signature key that the card issuer knows to be bound to a particular customer. The ability to demonstrate use of the private component of IC_Key can provide the same level of assurance as results from the TPM_Seal command. This is because the "digestAtRelease" parameter is specified during the generation of the private component of the IC_Key. In this case specifying digestAtRelease is semantically equivalent to sealing. The output of the TPM_CertifyKey command produces a signed TPM_Certify_Info structure which includes a TPM_PCR_INFO structure describing the state to which the private component of the IC_Key key pair is sealed.

Stage 2: Once the set-up stage is complete, the download of a customer's e-EMV card application can proceed:

Algorithm 2 Downloading the e-EMV Application

1: Issuer → Cust: R_{Issuer} ‖ $Issuer_{cert2}$ ‖ [Optional Platform Attestation]
2: Cust → Issuer: E_{Issuer}(TPM_Certify_Info ‖ P_{IC_Key} ‖ Platform Attestation ‖ R_{Issuer} ‖ R_{Cust} ‖ $Sign_{S_{IC\_Key}}$(Cust ‖ Issuer ‖ R_{Cust} ‖ R_{Issuer}))
3: Issuer → Cust: R_{Cust} ‖ $E_{P_{IC\_Key}}$(e-EMV application)

Notation: Here R_x is a random number, P_{IC_Key} is the public key of the IC_key key pair generated in the set-up stage and S_{IC_Key} is the private key of the IC_key key pair generated in the set-up stage. $Sign_{S_{IC\_Key}}(Y)$ denotes a signature with the IC_Key private key over data item Y, $E_X(Z)$ denotes encryption with the public key of entity X over data item Z, and X_{cert2} is a public key certificate issued by entity X for which the corresponding private key is used for decryption only.

In **step 1**, the card issuer sends a challenge, its public key certificate and optionally its own platform state.
In **step 2**, the customer verifies this platform state (if present) as well as his card issuer's public key certificate. The customer returns the TPM_Certify_Info structure (generated in the set-up phase) which contains a hash of the public component of IC_Key and a description of the security constraints (of the private component) of IC_Key. In addition to this, it sends the public component of IC_Key and signed platform metrics, responds to the challenge of the card issuer, and sends a challenge of its own, all encrypted with the public key of the Issuer.
In **step 3**, the card issuer examines the received data. Provided the storage semantics for the private key (IC_Key) match the card issuer's security policy and the customer correctly responded to the earlier challenge, then the card issuer sends a reply to the customer's challenge and the customer's e-EMV application encrypted with the public key of the customer's IC_Key pair.
Stage 3: The final stage of the protocol for secure application delivery is application retrieval and launch. Providing that the current platform state matches the requirements for the sealed data (as specified by the card issuer) and the incoming authorisation data matches the authorisation data set for the private key during the set-up phase, then the application is unsealed by the TPM. If one or both of these two conditions is not met then the application will remain sealed until both conditions can be fulfilled. Following a successful delivery of the e-EMV application, the customer is now able to utilise their card on their TPM-enabled platform.

7. E-EMV IN OPERATION

Once our e-EMV application (card) is launched into its own isolated VM by the platform's MVMM, transaction processing proceeds as follows.

7.1 Customer to Merchant Interaction

Customer-to-merchant interaction in our e-EMV system uses the same transaction processing used for EMV at PoS terminals. EMV transaction flows can be mapped directly to e-EMV transactions flows as follows:

Application Selection: Typically, application selection occurs in response to a terminal-initiated command to select the appropriate EMV application from a multi-application card. In this case we assume a single application instance in which customer/merchant application matching is dependent on finding a suitable set of validation credentials supported by the platform or a reported set of one or more PCR values in the form of a platform attestation, representing a valid application execution.

Initiate Application Processing: The customer's application next commences application processing. In the physical world this would yield a response in which the card returns its application interchange profile and its application file locator. However, in the e-EMV setting as the cards are virtualised and free from the constraints of typical ICC cards, all e-EMV cards would have CDA capabilities. Additionally, as part of this step the merchant terminal plug-in provides to the e-EMV application any terminal-related information pertaining to the business environment at the

Petitioner Exhibit 1002-1357

point of sale. An example of such information would be terminal capabilities or the country in which the terminal is operating.

Read Application Data: The steps involved in issuing one or more READ RECORD commands [15] in our setting is redundant as we assume the application is executing solely in main memory on a customer's platform.

Processing Restrictions: This mandatory step is performed by the merchant and doesn't require any direct interaction with the customer's execution environment. This step is primarily concerned with judging the compatibility of the e-EMV application with that of the terminal application. This process can be handled in an e-EMV environment through a process of reconciliation between terminal-supported applications and customer-supplied validation credentials/platform attestation.

Off-line Data Authentication: The three options for off-line data authentication available in EMV-compliant cards are SDA, DDA and CDA. These all involve a PoS terminal issuance of an INTERNAL AUTHENTICATE command [15]. We achieve this functionality in our e-EMV application through the platform's attestation mechanism. We now discuss how this is achieved for each of the three options.

SDA: SDA is relatively simple process whereby a validation credential (generated by a card issuer) providing metrics for a correctly functioning e-EMV card application is compared against load-time PCR metrics reported in an attestation challenge to a merchant. An outline of this process is as follows (here M is the merchant and Req is a request for one or more PCR registers):

1: $M \rightarrow Cust : \mathrm{M}_{Cert} \parallel \mathrm{Req} \parallel \mathrm{S}_M(\mathrm{Req}) \parallel$ Platform Attestation
2: $Cust \rightarrow M : \mathrm{E}_M(\mathrm{Cust}_{Cert} \parallel \mathrm{P}_{AIK} \parallel$ Platform Attestation)

In step 1, the merchant server requests one or more PCR values corresponding to the PCRs to which the e-EMV application is bound. In addition to this request the merchant attests its own platform metrics for examination by the customer's platform. The customer's platform then examines the attested merchant metrics and determines the suitability of the merchant for adherence to certain desirable policies, such as the PCI-DSS standards for card processing or Visa's PABP. If satisfied, a customer's platform agent culls its SML for the events responsible for generating the requested PCR values. The TPM then loads the AIK signing key using customer-provided authorisation data. The e-EMV application, using the now loaded AIK key, calls the TPM_Quote command [41] to sign the requested PCR registers. This will either be the AIK for which a certificate was obtained during the e-EMV account activation stage (as per the Privacy CA model) or an AIK over which a DAA signature has been generated (as per the DAA model). This information is returned to the merchant server for verification, as the platform attestation part of message 2. The merchant then examines the AIK credential, checks signatures[2] and compares a hash of the SML entries to the attested PCR values. If they match, then the merchant can be sure as to the current state of the VM in which the e-EMV application is executing.

[2]There may be a situation in which a merchant is unfamiliar with certificate authority referred to in an ICC public key certificate. However, provided each card issuer is itself a link in a chain traversing back to globally recognised root CA, for example Visa or Mastercard, then this verification can be as a result of certificate chain traversal.

In effect, this procedure achieves the same function as SDA does in standard EMV.

DDA: DDA requires a slight modification to the SDA mechanism as outlined above. During the operation of SDA's TPM_Quote in which the PCR registers are signed, the customer incorporates a merchant-supplied 160-bit random challenge to the attestation. This challenge takes the place of the operand *externalData* which is of type TPM_NONCE [41] in the PCR attestation process.

CDA: In the EMV PoS environment, CDA involves an ICC private key signature over the dynamic application data of which an AC (specifically a TC or an ARQC) and a random challenge (as per DDA) are integral parts. Replicating this in e-EMV environment is not substantially more complicated than either the SDA or DDA approaches. The e-EMV application carries out the AC generation process. The AC, along with its data output (TC/ARQC) can be integrated into a PCR register. The actual examinable output, that is the TC or ARCQ, is then correspondingly appended to the SML and a signature is generated over the representative PCR values using S_{AIK}. In this way the merchant, upon receipt of the attestation bundle can examine the SML for the inclusion of an AC and verify its veracity through a signature verification.

Card-holder Verification: In the typical PoS EMV operation, this step allows the terminal to verify the authenticity of a cardholder. This authentication is based on the card and terminal both supporting a particular Card-holder Verification Method (CVM). In addition to the CVM being used to verify a customer, some CVMs, particularly PIN authentications, are used as a means of authorising transactions.

Through the use of Trusted Computing functionality we can make PIN authentication and authorisation intrinsic to transactions. This is achieved through the TPM key authorisation mechanism, whereby certain keys require 20 bytes of authorisation data to be supplied prior to being loaded. The AIK usage requires authorisation data to be securely communicated to a TPM. In our architecture, this authentication data is communicated over a secure Object-Independent Authorisation Protocol (OIAP) session [41]. The use of an OIAP session allows authorisation information to be sent to a TPM without revealing the data on the channel over which it is sent. The necessary authorisation data is itself specified during the account activation process.

The ability to actually use a key as part of a transaction demonstrates to a merchant that a CVM has occurred successfully. By verifying the state of the platform, a merchant can be assured that only a valid customer would be capable of using the AIK private key generated in the account activation stage.

To prevent malware from launching a dictionary attack against key authorisation data, it is important that the TPM provide some form of resiliency to such an attack. The current iteration of the TPM specifications [41] details an example mechanism where a count of failed authorisation attempts is recorded. If this count exceeds a threshold, the TPM is locked and remains non-responsive to further requests for a predetermined time-out period. However, at present, the implementation of a dictionary attack resistant authorisation mechanism is vendor-specific and not always implemented securely [30].

Petitioner Exhibit 1002-1358

Terminal Risk Management and Action Analysis: The purpose of terminal risk management and terminal action analysis is to protect the issuer, acquirer and payment system from fraud. The existing variety of measures used by EMV in terminal risk management, such as floor limits, random transaction selection and velocity checking can all be replicated in the merchant terminal plug-in in our e-EMV architecture.

Card Risk Management and Action Analysis: Details of card risk management are proprietary to card issuers and are outside the scope of the EMV specification and as such would remain proprietary to individual card issuers within our e-EMV system.

On-line Authorisation: During EMV transaction processing the merchant terminal may decide to proceed with an on-line check; this again can be replicated in our e-EMV environment via standard EMV message exchanges.

Issuer Script Processing: To allow updates to EMV cards in the field, the card issuer can return scripts via the terminal to the ICC for processing. These scripts are not necessarily relevant to the current transaction and may be used to update applications during the utilisation phase of the ICC's lifecycle, or to transition the card into a blocked or unblocked state. Updates to e-EMV cards can be performed in a similar manner. An issuer can send update scripts via the merchant plug-in to the customer's e-EMV card. The issuer can then distribute new state measurements for updated e-EMV cards to merchants via new validation credentials. Merchants should only allow e-EMV cards whose attestation matches the values contained in the latest validation credential to perform e-EMV transactions. Card blocking scripts are a more difficult EMV feature to replicate in an e-EMV setting. It may be illegal in certain jurisdictions for a card issuer to force an update on a customer's platform without gaining customer consent.

7.2 Payment

As we saw in Section 3.1, in EMV, an ICC uses session keys derived from the ICC Master Key to protect the transaction messages. In our e-EMV architecture, in conjunction with the information typically sent in the AC message, the e-EMV application sends the current platform state as signed by its issuer-validated signing key (S_{AIK}). After examining the AC message as well as the supplied state, the verifier (a merchant or a card issuer) can make a decision as to whether or not to proceed with a transaction. In the instance where an AC is an ARQC, as mentioned in Section 5.2, the TLV encoding scheme used in EMV allows the issuer to ignore extraneous information if they so choose. The card issuer can then respond with an ARPC indicating whether the transaction should be approved or declined, in which case a TC (which can be signed, see CDA in Offline Data Authentication) or an AAC will be generated by the customer's platform. The transition to Internet-based communications in e-EMV requires that ACs be protected in transit between the customer and merchant. Such protection can be achieved by establishing a TPM-centric SSL tunnel between customer and merchant, as per [8, 18].

7.3 Migration

Enabling the migration of an e-EMV card from one Trusted Platform to another would be useful in our architecture. We could achieve such a feature by using the TPM's certifiable migration functionality. If the customer creates a CMK during the application delivery process (see Section 6.2), a customer may later migrate his application bundle to another TPM-enabled platform. However, as neither DAA secrets nor AIK private keys obtained in the enrolment phase are migratable from a TPM, the customer would need to rerun the account activation phase (see Section 6.1) in order for their card to be usable on the new platform. In this instance, the cost of providing additional infrastructural elements to support a trusted migration service [38] may be somewhat prohibitive for issuers, and it may just be simpler in practice for the customer to enrol his new platform with his card issuer from scratch.

8. ANALYSIS

The semantics of trust enforced by Trusted Computing functionality enables both parties, the merchant and the customer, to obtain certain guarantees that were hitherto unrealisable in past proposals [35, 43]. Both merchant and server can be sure as to the integrity of their communicating peer's platform, i.e. that each peer will behave in the expected manner (in this case, adhere to, and faithfully adduce state characteristics corresponding to legitimate transaction states). It is important to point out that we do not expect the customer to be able to recognise or validate software states within our system. This function can be fulfilled by the application software itself and should be reported to the customer in a way that is understandable.

We now analyze the effectiveness of our e-EMV architecture as a means of securing electronic payments. This is achieved by examining how well it satisfies the security requirements of Herreweghen and Wille [21] described in Section 2.

Mutual authentication of customer and merchant: In our architecture both customers and merchants are authenticated via their card issuer/acquirer supplied credentials, providing a much stronger form of authentication than that currently employed for CNP payments. Balfe *et al.* [8] have shown how such credentials can be used to authenticate the establishment of SSL/TLS sessions, thus providing an additional layer of protection for the transport of e-EMV transaction messages over the Internet. Their proposal can also be adopted here.

An added benefit of our approach is that it allows the customer to examine a merchant's platform state prior to transaction authorisation. This enables the customer to satisfy himself that the merchant will behave in a manner that will protect his sensitive card data. Such a feature is lacking with current PoS transactions, a fact which is now allegedly being exploited by criminal gangs [42].

Transaction authorisation & payment guarantee for merchant: In our architecture, the use of the private transaction authorising key is contingent on a particular platform state being present on the customer's platform. Much like PIN entry at a PoS, the completion of a transaction is conditioned on the input of correct authorisation data, ensuring the physical presence of the cardholder in the remote transaction. Additionally, as part of the transaction authorisation process, a customer's platform must attest to the VM in which the e-EMV application is executing. Any divergence from intended operating state (due to unwanted memory resident applications) will be picked up in during the attestation procedure, allowing merchant risk manage-

Petitioner Exhibit 1002-1359

ment routines to terminate the transaction. Assuming a transaction goes ahead, payment guarantee for the merchant is provided by CDA. CDA provides a signature over an e-EMV card's Transaction Certificate, providing the merchant with non-repudiable evidence of payment. Cardholder non-repudiation is dependent on the degree to which the cardholder's private signing key is securely generated and stored in the cardholder's Trusted Platform.

Customer privacy and anonymity: Customer privacy is somewhat problematic in any CNP transaction as the customer will typically provide copious amounts of personally identifiable information, such as name and billing address. It is not provided by EMV, and therefore not provided by e-EMV.

9. CONCLUSIONS

The use of the Internet as an avenue for electronic commerce, in the form of CNP transactions, has seen something of an explosion in recent years. However, CNP transactions are currently far from secure. This paper proposed a new security architecture for securing CNP transactions. By creating software-based EMV cards running on Trusted Platforms, our e-EMV proposal replicates many of the features of standard EMV-compliant cards for use in CNP transactions. Through our account activation and secure application delivery procedures, we established how cards can be remotely provisioned within our system. We showed how card ownership can be demonstrated by the customer through the use of an OIAP session enabling secure PIN entry. We also showed how EMV transaction messages can be mapped to e-EMV transaction messages. We demonstrated how EMV keys can be generated and bound to a particular TPM-enabled platform. Through these various measures, we can achieve a significant improvement in the level of security afforded to CNP transactions.

Our work raises a number of areas for further research. In this paper, we have focused on describing architectural and technical aspects of our e-EMV proposal. Our future work will examine security and system management issues. A prototyping activity based on the OpenTC framework[3] with SVM [4], L4 μ-Kernel[4] and Xen [10] support is also likely to be useful in terms of revealing unforeseen practical issues, operational problems, and the like. Additionally, as part of future work we also look to examine the role of physical presence in providing enhanced transaction authorisation [9] within our e-EMV framework. At present, our approach is reliant on MVMMs and Trusted Computing augmented processors being present in commodity platforms. Unfortunately, such support is not widely available today. A more immediate avenue for adoption would be Trusted Computing enhanced mobile phones [40] which do not require MVMM support. However, at present only preliminary details of the TCG's trusted mobile architecture are available [40]. We believe that Trusted Computing can provide an enhanced level of security compared to EMV's deployment at PoS. However, given the perpetual increase in attacks (both in terms of number and sophistication) targeting end-user systems, we see an increased role for both terminal and card risk management routines to control transaction risk in our e-EMV architecture.

[3]http://www.opentc.net/

[4]http://os.inf.tu-dresden.de/L4/

Whilst outside of the immediate scope of this paper, in developing our architecture we note two weaknesses in the current attestation mechanisms adopted by the TCG. Firstly, as noted in [20], the current TCG attestation is static, inexpressive and has poor handling of patches and upgrades to system software. Secondly, the TCG attestation mechanism only concerns itself with load-time measurements of applications. Recent approaches that attempt to address these issues have been proposed in [20, 31, 36] and [26, 34, 36] respectively. Investigating these proposals in the context of e-EMV will be of interest. In the absence of more expressive attestations we must rely on the properties of the MVMM to ensure that our executing e-EMV application cannot be interfered with by outside applications.

10. REFERENCES

[1] M. Abadi and T. Wobber. A Logical Account of NGSCB. In *Proceedings of the 24th International Conference on Formal Techniques for Networked and Distributed Systems*, volume 3235 of *LNCS*, pages 1–12. Springer Verlag, 2004.

[2] M. Al-Meaither and C. J. Mitchell. Extending EMV to Support Murabaha Transactions. In *Proceedings of the 7th Nordic Workshop on Secure IT Systems*, pages 95–108. NTNU, 2003.

[3] A. Alsaid and C. J. Mitchell. Preventing Phishing Attacks Using Trusted Computing Technology. In *Proceedings of the 6th International Network Conference*, pages 221–228, 2006.

[4] AMD. *AMD64 architecture programmer's manual: Volume 2: System programming*, AMD Publication no. 24594 rev. 3.11 edition, 2006.

[5] APACS. Card Fraud Losses Continue to Fall. `http://www.apacs.org.uk/`, March 2007.

[6] APACS. Card Fraud The Facts 2007. `http://www.apacs.org.uk/`, April 2007.

[7] B. Balacheff, D. Chan, L. Chen, S. Pearson, and G. Proudler. Securing Intelligent Adjuncts Using Trusted Computing Platform Technology. In *Proceedings of the 4th working Smart Card Research and Advanced Applications*, pages 177–195. Kluwer Academic, 2001.

[8] S. Balfe, A.D. Lakhani, and K.G. Paterson. Securing Peer-to-Peer networks using Trusted Computing. In C.J. Mitchell, editor, *Trusted Computing*, pages 271–298. IEE Press, 2005.

[9] S. Balfe and K.G. Paterson. Augmenting Internet-based Card Not Present Transactions with Trusted Computing: An Analysis. Technical report, Technical report RHUL-MA-2006-9-v2, (Department of Mathematics, Royal Holloway, University of London). `http://www.rhul.ac.uk/mathematics/techreports`.

[10] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauery, I. Pratt, and A. Warfield. XEN and the Art of Virtualization. In *Proceedings of the 19th ACM Symposium on Operating Systems Principles*, pages 164–177. ACM Press, 2003.

[11] E. Brickell, J. Camenisch, and L. Chen. Direct Anonymous Attestation. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, pages 132–145. ACM Press, 2004.

Petitioner Exhibit 1002-1360

[12] PCI Security Standards Council. Payment Card Industry Data Security Standard – Version 1.1. https://www.pcisecuritystandards.org/, 2006.

[13] R. Dhamija, J. D. Tygar, and M. Hearst. Why Phishing Works. In *Proceedings of the 2006 Conference on Human Factors in Computing Systems*, pages 581–590. ACM Press, 2006.

[14] EMVCo. *Book 3 - Application Specification*, 4.0 edition, December 2000.

[15] EMVCo. EMV Specifications Version 4.1. http://www.emvco.com, June 2004.

[16] S. Gajek, A-R. Sadeghi, C. Stüble, and M. Winandy. Compartmented Security for Browsers–Or How to Thwart a Phisher with Trusted Computing. In *Proceedings of the 2nd International Conference on Availability, Reliability and Security*, pages 120–127. IEEE Computer Society, 2007.

[17] E. Gallery and A. Tomlinson. Conditional Access in Mobile Systems: Securing the Application. In *Proceedings of the 1st International Conference on Distributed Frameworks for Multimedia Applications*, pages 190–197. IEEE, 2005.

[18] Y. Gasmi, A-R. Sadeghi, P. Stewin, M. Unger, and N. Asokan. Beyond Secure Channels. In *Proceedings of the 2007 ACM Workshop on Scalable Trusted Computing*, pages 30–40. ACM Press, 2007.

[19] D. Grawrock. *The Intel Safer Computer Initiative: Building Blocks for Trusted Computing*, chapter Protected Input and Output, pages 143–164. Intel Press, 2006.

[20] V. Haldar, D. Chandra, and M. Franz. Semantic Remote Attestation: A Virtual Machine Directed Approach to Trusted Computing. In *USENIX Virtual Machine Research and Technology Symposium*, pages 19–41. USENIX, 2004.

[21] E.V. Herreweghen and U. Wille. Risks and Potentials of Using EMV for Internet Payments. In *Proceedings of the 1st USENIX Workshop on Smartcard Technology*, pages 163–174. USENIX, 1999.

[22] IBM-Global-Services. IBM Global Business Security Index Report, February 2005.

[23] Intel-Corporation. *LaGrande Technology Preliminary Architecture Specification*, Intel Publication no. D52212 edition, May 2006.

[24] C. Jackson, D. Boneh, and J. Mitchell. Attack of the transaction generators. http://crypto.stanford.edu/SpyBlock/spyblock.pdf.

[25] V. Khu-Smith and C.J. Mitchell. Using EMV Cards to Protect E-commerce Transactions. In *Proceedings of the 3rd International Conference on E-Commerce and Web Technologies*, volume 2455, pages 388–399. Springer-Verlag, 2002.

[26] J.M. McCune, B. Parno, A. Perrig, M.K. Reiter, and A. Seshadri. Minimal TCB Code Execution. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pages 267–272. IEEE Computer Society, 2007.

[27] P. Meadowcroft. Combating card fraud. http://www.scmagazine.com/uk/news/article/459478/combating+card+fraud/, January 2005.

[28] C.J. Mitchell, editor. *Trusted Computing*. IEE Professional Applications of Computing Series 6. The Institute of Electrical Engineers (IEE), London, UK, April 2005.

[29] C. Radu. *Implementing Electronic Card Payment Systems*. Artech House, Inc., 2002.

[30] A-R. Sadeghi, M. Selhorst, C. Stüble, C. Wachsmann, and M. Winandy. TCG inside?: A Note on TPM Specification Compliance. In *Proceedings of the 1st ACM workshop on Scalable Trusted Computing*, pages 47–56. ACM Press, 2006.

[31] A-R. Sadeghi and C. Stüble. Property-Based Attestation for Computing Platforms: Caring About Properties, Not Mechanisms. In *Proceedings of the 2004 Workshop on New Security Paradigms*, pages 67–77. ACM Press, 2004.

[32] A-R. Sadeghi, C. Stüble, and N. Pohlmann. European Multilateral Secure Computing Base: Open Trusted Computing for You and Me. http://www.prosec.rub.de/, 2004.

[33] U.S. Securities and Exchange Commission. Form 10-K – The TJX Companies, INC. http://www.sec.gov/, 2007.

[34] A. Seshadri, M. Luk, N. Qu, and A. Perrig. SecVisor: A Tiny Hypervisor to Provide Lifetime Kernel Code Integrity for Commodity OSes. In *Proceedings of 21st ACM SIGOPS Symposium on Operating Systems Principles*, pages 335–350. ACM Press, 2007.

[35] SETCo. SET Secure Electronic Transaction 1.0 Specification — The Formal Protocol Definition, May 1997.

[36] E. Shi, A. Perrig, and L.V. Doorn. BIND: A Fine-Grained Attestation Service for Secure Distributed Systems. In *Proceedings of the 2005 IEEE Symposium on Security and Privacy*, pages 154–168. IEEE Computer Society, 2005.

[37] TCG. Trusted computing: Opportunities and challenges. https://www.trustedcomputinggroup.org/downloads/tcgpresentations/, 2004.

[38] TCG. *Interoperability Specification for Backup and Migration Services*, 1.0 revision 1.0 edition, 2005.

[39] TCG. *TCG Specification Architecture Overview Revision 1.2*, 1.2 revision 93 edition, 2006.

[40] TCG. *TCG Mobile Trusted Module Specification*, 1.0 revision 1 edition, 2007.

[41] TCG. *TPM Main: Parts 1–3: Design Principles, Structures and Commands*, 1.2 revision 103 edition, 2007.

[42] The Sunday Times. Don't Use Cards at Petrol Stations. http://business.timesonline.co.uk/, Febuary 18 2007.

[43] Visa. 3-D Secure Protocol Specification: System Overview. http://international.visa.com/fb/paytech/secure/main.jsp, May 2003.

[44] Visa. CISP – List of Validated Payment Applications. http://usa.visa.com/merchants/, October 2007.

[45] Visa. CISP Bulletin 102307– Visa Announces New Payment Application Security Mandates. http://usa.visa.com/merchants/, October 2007.

Petitioner Exhibit 1002-1361

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	DRAWINGS	TOT CLAIMS	IND CLAIMS
60/871,898	12/26/2006		450	16222U-028500US	9		

CONFIRMATION NO. 2152

66945
TOWNSEND AND TOWNSEND CREW LLP
TWO EMBARCADERO CENTER, 8TH FLOOR
SAN FRANCISCO, CA94111

FILING RECEIPT

Date Mailed: 01/25/2007

Receipt is acknowledged of this provisional Patent Application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please mail to the Commissioner for Patents P.O. Box 1450 Alexandria Va 22313-1450. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

Applicant(s)

Mark Carlson, Half Moon Bay, CA;

Power of Attorney: The patent practitioners associated with Customer Number 66945

If Required, Foreign Filing License Granted: 01/19/2007

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US60/871,898**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

Title

VALUE BASED OFFERS

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant

to 37 CFR 5.15(b).

Application Data Sheet

Application Information

Application number::	
Filing Date::	
Application Type::	Provisional
Subject Matter::	Utility
Suggested classification::	
Suggested Group Art Unit::	
CD-ROM or CD-R??::	
Number of CD disks::	
Number of copies of CDs::	
Sequence Submission::	
Computer Readable Form (CRF)?::	
Number of copies of CRF::	
Title::	VALUE BASED OFFERS
Attorney Docket Number::	16222U-028500US
Request for Early Publication::	No
Request for Non-Publication::	No
Suggested Drawing Figure::	
Total Drawing Sheets::	9
Small Entity?::	No
Latin name::	
Variety denomination name::	
Petition included?::	No
Petition Type::	
Licensed US Govt. Agency::	
Contract or Grant Numbers One::	
Secrecy Order in Parent Appl.::	No

Applicant Information

Applicant Authority Type::	Inventor

Petitioner Exhibit 1002-1365

Primary Citizenship Country::	US
Status::	Full Capacity
Given Name::	Mark
Middle Name::	
Family Name::	Carlson
Name Suffix::	
City of Residence::	Half Moon Bay
State or Province of Residence::	CA
Country of Residence::	US
Street of Mailing Address::	153 Miramontes Avenue
City of Mailing Address::	Half Moon Bay
State or Province of mailing address::	CA
Country of mailing address::	US
Postal or Zip Code of mailing address::	94019

Correspondence Information

Correspondence Customer Number:: 66945

Representative Information

Representative Customer Number:: 66945

Domestic Priority Information

Application:: Continuity Type:: Parent Application:: Parent Filing Date::

Foreign Priority Information

Country:: Application number:: Filing Date::

Assignee Information

Assignee Name::

Street of mailing address::

City of mailing address::

State or Province of mailing address::

Country of mailing address::

Postal or Zip Code of mailing address::

VALUE BASED OFFERS

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] Not applicable.

BRIEF SUMMARY

[0002] Embodiments of the invention are directed to systems and methods using portable consumer devices that can be used payments and the like.

[0003] One embodiment of the invention is directed to a method comprising: receiving a payment request message from a mobile phone operated by a payer, wherein the payment request message includes a request to pay a payee a predetermined amount of money, and wherein the payment request message comprises a personal alias associated with the payee and a transaction amount; analyzing the payment request message to determine if the payer is authorized to pay the payee; and sending a payment notification message to the payee indicating that a payment from the payer to the payee has been made.

[0004] Another embodiment of the invention is directed to a method comprising: receiving a payment request message from a mobile phone operated by a consumer, wherein the payment request message includes a request to pay for a product from a vending machine; analyzing the payment request message to determine if the consumer is authorized to pay for the product; sending a payment response message back to the vending machine; and receiving an acknowledgement message from the vending machine that the product was purchased.

[0005] Another embodiment of the invention is directed to a method comprising: reviewing contact information associated with a vending machine; sending a payment request message using the contact information and a mobile phone; selecting a product in the vending machine; and receiving the product from the vending machine.

[0006] Another embodiment of the invention is directed to a method comprising: receiving information from a consumer regarding how the consumer wants to be notified if potentially fraudulent activity is occurring with respect to a portable consumer device being

Petitioner Exhibit 1002-1368

used by the consumer; and alerting the consumer in a manner consistent with the received information if potential fraudulent activity is occurring.

[0007] Another embodiment of the invention is directed to a method comprising: receiving a coupon comprising a code at a mobile phone operated by a consumer; and manually providing the code to a merchant, wherein the merchant thereafter provides a discount to the consumer.

[0008] Another embodiment of the invention is directed to a method comprising: receiving a coupon comprising a code at a portable consumer device comprising an antenna operated by a consumer; and providing the code to a merchant using an antenna.

[0009] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 shows a block diagram of a payment processing system.

[0011] FIG. 2 shows a schematic illustration of a method for using an alias when paying a consumer.

[0012] FIG. 3 shows a block diagram of a pre-enrollment model according to an embodiment of the invention.

[0013] FIG. 4 shows a screen from a POS terminal.

[0014] FIGS. 5(a)-5(c) show different screenshots on a phone. The screenshots include coupons.

[0015] FIGS. 6(a)-6(c) show various mobile vending schemes.

[0016] FIG. 7 shows a diagram of a single POS setup.

DETAILED DESCRIPTION

[0017] I. Payment Processing Systems

[0018] Embodiments of the invention are directed to the use of portable consumer devices, and methods and systems that use them. Preferred portable consumer devices are

Petitioner Exhibit 1002-1369

mobile phones. The mobile phones can be used in payment processing systems like those shown in FIG. 1.

[0019] FIG. 1 shows a system **20** that can be used in an embodiment of the invention. The system **20** includes a merchant **22** and an acquirer **24** associated with the merchant **22**. In a typical payment transaction, a consumer **30** may purchase goods or services at the merchant **22** using a portable consumer device **32**. The acquirer **24** can communicate with an issuer **28** via a payment processing system **26**.

[0020] The acquirer **24** is typically a bank that has a merchant account. The issuer **28** may also be a bank, but could also be business entity such as a retail store. Some entities are both acquirers and issuers, and embodiments of the invention include such entities. The issuer **28** may operate a server computer **21**, which may have a computer readable medium comprising code for performing the functions that the issuer **28** performs. A database **23** comprising account number information and other information may be operatively coupled to the server computer **21**.

[0021] The consumer **30** may be an individual, or an organization such as a business that is capable of purchasing goods or services.

[0022] The portable consumer device **32** may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit devices (*e.g.*, a debit card), credit devices (*e.g.*, a credit card), or stored value devices (*e.g.*, a stored value card).

[0023] The portable consumer device **32** may comprise a computer readable medium **32(a)** and a body **32(b)**. The computer readable medium **32(a)** may be on the body **32(b)**. The body **32(b)** may in the form a plastic substrate, housing, or other structure. The computer readable medium **32(a)** may be a memory that stores data and may be in any suitable form. Exemplary computer readable media **32(a)** may be in any suitable form including a magnetic stripe, a memory chip, etc. If the portable consumer device **32** is in the

Petitioner Exhibit 1002-1370

form of a card, it may have an embossed region **32(a)** which is embossed with a PAN (primary account number).

[0024] The payment processing network **26** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0025] The payment processing network **26** may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The payment processing network **26** may use any suitable wired or wireless network, including the Internet.

[0026] The merchant **22** may also have, or may receive communications from, an access device **34** that can interact with the portable consumer device **32**. In FIG. 4, the access device **34** is located at the merchant **22**. However, it could be located at any other suitable location in other embodiments of the invention.

[0027] The access devices according to embodiments of the invention can be in any suitable form. Examples of access devices include point of sale (POS) devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like.

[0028] If the access device **34** is a point of sale terminal, any suitable point of sale terminal may include a reader **34(a)**, a processor **34(b)** and a computer readable medium **34(c)**. The reader **34(b)** may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer device **32**.

Petitioner Exhibit 1002-1371

[0029] In a typical purchase transaction, the consumer **30** purchases a good or service at the merchant **22** using a portable consumer device **32** such as a credit card. The consumer's portable consumer device **32** can interact with an access device **34** such as a POS (point of sale) terminal at the merchant **22**. For example, the consumer **30** may take a credit card and may swipe it through an appropriate slot in the POS terminal. Alternatively, the POS terminal may be a contactless reader, and the portable consumer device **32** may be a contactless device such as a contactless card.

[0030] An authorization request message is then forwarded to the acquirer **24**. After receiving the authorization request message, the authorization request message is then sent to the payment processing network **26**. The payment processing network **26** then forwards the authorization request message to the issuer **28** of the portable consumer device **32**.

[0031] After the issuer **28** receives the authorization request message, the issuer **28** sends an authorization response message back to the payment processing network **26** to indicate whether or not the current transaction is authorized (or not authorized). The transaction processing network **26** then forwards the authorization response message back to the acquirer **24**. The acquirer **24** then sends the response message back to the merchant **22**.

[0032] After the merchant **22** receives the authorization response message, the access device **34** at the merchant **22** may then provide the authorization response message for the consumer **30**. The response message may be displayed by the access device **34**, or may be printed out on a receipt.

[0033] At the end of the day, a normal clearing and settlement process can be conducted by the transaction processing network **26**. A clearing process is a process of exchanging financial details between and acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position.

[0034] Some of the embodiments described below may use a payment processing system like the one described above, or any suitable combination of components in the payment processing system.

[0035] II. Mobile Payment System and Method Using Alias

[0036] Some embodiments of the invention can be directed to person to person (P2P) and person to business (P2B) payments, using a portable consumer device such as a mobile

Petitioner Exhibit 1002-1372

phone. Mobile phones can be used to transfer money from one person to another person or a person to a business. The mobile phone can be used to initiate such activity.

[0037] There are three ways to push money from one entity to another entity. First, one can push money from one entity to another entity through the Web. Second, one can push money from one entity to another entity using an SMS message (i.e., a text message). Third, one can push money from one entity to another entity using an application on the phone.

[0038] In an exemplary embodiment of the invention, a first person such as Jane and a second person such as John register on a Web site run by a remote server computer. As shown in FIG. 2, when registering, Jane may register her name, mobile telephone number, first credit card account number, second credit card account number, and a personal alias. John may similarly register the same type of information. In this example, Jane may create the personal alias "worldtraveler" while John may create the personal alias "beachbum."

[0039] After registering, a service entity provides both John and Jane with a phone number for the service that will facilitate further payment processing. The service entity may instead provide John and Jane with service alias instead of or in addition to the service phone number. For example, instead of providing John and Jane with the service phone number 555-555-5555, the service entity may provide the service alias "myvisa" to John and Jane. The service alias may be referred to as a "short-code" in some cases, and may include 4, 5, or 6 digits. Each time that John and Jane want to pay some other entity using their mobile phones, they can enter either the service phone number or the service alias into their phones.

[0040] At some point in time, Jane wants to pay John $15.00. Jane may have Jane initiate an SMS payment to John by keying in "myvisa pay beachbum $15.00" in her phone. The alias "beachbum" is used instead of John's phone number. The service alias "myvisa" is used instead of the phone number of the service. As shown in FIG. 2, Jane may also use a portable consumer device alias such as "CC2" to indicate the particular credit card that Jane wants to use to pay John. Jane may designate a default credit card account number if she wants to do so.

[0041] After entering the payment request message "myvisa pay beachbum $15.00 CC2" into her mobile phone, the appropriate message gets routed to a payment processing network (e.g., as described above), and then to an issuer of the portable consumer device. In embodiments of the invention, a payment request message may include money transfers that

Petitioner Exhibit 1002-1373

may be may not be performed in exchange for some sort of return consideration (e.g., a good or service purchased). For example, a payment request message may be a request to pay another person for a debt owed to that person.

[0042] At some point in the process, an interactive voice response unit (IVR) at a telecom server or the like can then call Jane back asking her to enter her mobile PIN (personal identification number). After Jane enters the correct PIN, the issuer (or a server computer operated by the issuer) can then analyze the payment request message and can approve or decline the transaction as described above. If approved, John can be notified that a payment request has been initiated. In some embodiments, a payment notification message in the form of an SMS, e-mail, or some other type of message may be sent to John. John's portable consumer device account (e.g., credit card account) at John's bank could then be credited with the appropriate amount.

[0043] The consumer aliases such as "worldtraveler" and "beachbum", and the service aliases such as "myvisa," can be stored in one or more databases that are accessible to the issuer. These various aliases can be registered for a fee, and consumers may be charged a registration and renewal fee for using certain aliases in some embodiments. This can allow for cross institution payments, by uniquely identifying an individual, business, etc. The aliases may be associated with many accounts or services, if desired.

[0044] The use of payment aliases in a mobile phone payment environment is particularly useful, since one consumer may not want to disclose his or her phone number to the other consumer. A database comprising a lookup table correlating various aliases and phone numbers may be situated between the portable consumer devices that are operated by the payer and the payee.

[0045] Another feature of embodiments of the invention is to have a bank push pre-enrollment data to an enrollment database. The bank validates the user ahead of time, since the bank already knows the users. The users then come in and set customized parameters if appropriate. This is different than a credit pre-approval process in that cash would be available, instead of credit. An exemplary system and flow are shown in FIG. 3. This may be referred to as a trust transfer concept, as trust and history associated with an established source are built up over time.

[0046] Another feature of embodiments of the invention is to provide each portable consumer device with an applet that will provide for a secure communication channel

Petitioner Exhibit 1002-1374

between the portable consumer device of the payer and the portable consumer device of the payee.

[0047] Embodiments of the invention can be used for person to person payments, money transfers, person to business payments, etc.

[0048] **III. Mobile Vending Purchasing**

[0049] Other embodiments of the invention are directed to mobile vending purchasing processes and systems using portable consumer devices such as mobile phones.

[0050] Referring to FIG. 6(a), in one embodiment, a consumer dials the number seen on a vending machine to make a purchase, and then follow directions. A payment processing organization such as Visa authorizes the transaction, and tells the vending machine that payment has been accepted. Then, the vending machine displays a message that says "Please choose your product." After the message is displayed, the customer makes a selection or the credit will time out after 20 seconds. The vending machine then returns a vend acknowledgement to Visa, and the purchased item will appear on the next statement.

[0051] Referring to FIG. 6(b), in another embodiment of the invention, a consumer may send an SMS message to a number on a vending machine to make a purchase. The consumer may get an automated call back asking for a PIN. The payment processing system then authorizes the transaction and tells the vending machine that payment has been accepted. The vending machine then shows the message "please choose your product." The customer makes a selection or the credit will timeout after 20 seconds. The vending machine returns a vend acknowledgement to the payment processing organization and the purchased item will appear on the consumer's next statement.

[0052] Referring to FIG. 6(c), in yet another embodiment of the invention, a user may use a "machine alias" seen on a vending machine. A consumer may then use a mobile wallet to make a vending purchase. The payment processing organization authorizes the transaction, and tells the vending machine that payment has been accepted. The vending machine display shows the message "please choose your product." The customer makes a selection or the credit will time out after 20 seconds. The vending machine returns a vend acknowledgement to the payment processing organization and documentation of the purchased item will appear on the next statement.

Petitioner Exhibit 1002-1375

[0053] In order to facilitate such processes, the vending machine may have a contactless reader and the mobile phone of the consumer may have a contactless transmitter.

[0054] **IV. Multiple Party Incentive System and Method**

[0055] Many different parties may have different incentive systems. A first party may include the issuing bank who may only care if the card being used is issued from it. A second party my include Visa who may only care if a Visa card is used. A third party may be a merchant who may only care if purchases are made at that merchant. A point of service terminal could have sufficient intelligence that would allow it to appropriately route the reward request to the appropriate party that can provide the appropriate reward. The "terminal driver" in FIG. 7 may have the intelligence to route the appropriate reward request to the appropriate party.

[0056] Embodiments of the invention can be used to introduce new type of coupons. Such coupons may be issuer coupons, payment processing organization coupons (e.g., Visa coupons), merchant coupons, combo affinity coupons, etc. The terminal may have logic to provide or redeem coupons only if the appropriate rules are satisfied. For example, a payment processing organization coupon may be redeemable by a consumer or provided to a consumer only if a payment processing organization branded credit card is used. In another example, an issuer (e.g., Citibank) may provide or act on a coupon if the consumer uses an issuer specific portable consumer device.

[0057] Some specific examples of coupons from different entities are provided below. These different types of coupons can be processed by a single terminal in some embodiments of the invention.

- Partner merchant issued coupons. Here, a merchant is setting the goals of the coupon. The prompt probably would be "USE CARD". The merchant probably doesn't care about payment type. The merchant's goal is to get people in a store to buy products, or to target sales of specific items.

- Payment processing organization (e.g., Visa) issued coupons: The organization's goal may be to crease brand usage. The organization may only pay for a coupon if the customer is going to pay with an organization branded card.

Petitioner Exhibit 1002-1376

- Coupon issued by a card issuer: The prompt could be "use [issuer] card." The issuer is not concerned with the particular payment processing organization that a card is affiliated with. It only cares if its card is used..
- Any combination of payment processing organization, merchant, and issuer

[0058] V. Mobile Device Value Loading System and Method

[0059] There are many consumers who can be referred to as "unbanked" consumers, in that they do not have bank accounts. Such consumers may use prepaid cards to pay for such purchases. Some embodiments of the invention can use a portable consumer device such as a mobile phone to reload a prepaid card. SMS messages or the like can be used to do this.

[0060] In embodiments of the invention, a message may be sent to a server computer at an issuer with an instruction to reload a prepaid card using a mobile phone. Account balances associated with such prepaid cards can also be checked using the mobile phone.

[0061] VI. Customized Payment Transaction Notification System and Method

[0062] Other embodiments of the invention are directed to customized alerts and notifications for payment transactions. Such embodiments of the invention can be used with or without mobile phones. In these embodiments of the invention, a consumer would be able to customize the way (e.g., only notify the consumer if the transaction that is occurring is greater than $5000 in value), the time (e.g., at work, at home, from 2 am to 6 am), and/or mode (e.g., e-mail, telephone, SMS, etc.) of notification when potential fraudulent activity is occurring. For example, if a $5000 credit card transaction is occurring at 2 a.m. in the morning, the cardholder may want to receive a phone call on his home phone. If a $5000 transaction is occurring at 10 am in the morning, then the user may want to be notified using his wireless e-mail device.

[0063] VII. Mobile Coupon Method and System

[0064] In an exemplary embodiment, a coupon is sent to a user's phone. The coupon may be sent via an SMS message, SMS link, or e-mail.

Petitioner Exhibit 1002-1377

[0065] FIG. 4 shows a screen from a POS terminal. The screen shows buttons that a cashier might select to initiate a pre-arranged discount.

[0066] FIGS. 5(a)-5(c) show examples of three screenshots showing graphical coupons in different forms. The screenshots can be displayed on a mobile phone display. FIG. 5(a) shows a screenshot including a bar code (which is an example of a machine readable code). The bar code can be scanned with a scanner. FIG. 5(b) shows a screenshot showing a mobile coupon, without a barcode. Instead of a barcode, a six digit number "024248" is shown. This number can be entered into a POS terminal to give the consumer a discount on a purchase. Lastly, FIG. 5(c) shows a screenshot showing a "30% off" coupon. To use this coupon, the user shows the display to the cashier and the cashier selects a button on a POS terminal display (see FIG. 4) to provide the discount to the consumer.

[0067] Another variation may be a near field communication of the coupon. In this variation, the six digit code can be transmitted to the POS terminal via a reader using a contactless device such as an antenna. In this embodiment, the six digit code may or may not be displayed on the display of the phone. The consumer may receive a text message, a phone call, or e-mail indicating that the consumer has received a coupon. The consumer may then receive use his phone to transmit a code corresponding to the coupon a contactless reader coupled to a POS terminal. The system shown in FIG. 1 can be used in conjunction with this embodiment.

[0068] Other details of embodiments of the invention are described in the attached APPENDIX.

[0069] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0070] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical

Petitioner Exhibit 1002-1378

medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0071] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0072] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0073] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

Petitioner Exhibit 1002-1379

WHAT IS CLAIMED IS:

1. A method comprising:

receiving a payment request message from a mobile phone operated by a payer, wherein the payment request message includes a request to pay a payee a predetermined amount of money, and wherein the payment request message comprises a personal alias associated with the payee and a transaction amount;

analyzing the payment request message to determine if the payer is authorized to pay the payee; and

sending a payment notification message to the payee indicating that a payment from the payer to the payee has been made.

2. The method of claim 1 further comprising:

sending an identification request message to the payer, wherein the identification request message includes a message asking the user to enter a PIN; and then

receiving a payee identification message.

3. A computer readable medium comprising:

code for receiving a payment request message from a mobile phone operated by a payer, wherein the payment request message includes a request to pay a payee a predetermined amount of money, and wherein the payment request message comprises a personal alias associated with the payee and a transaction amount;

code for analyzing the payment request message to determine if the payer is authorized to pay the payee; and

code for sending a payment notification message to the payee indicating that a payment from the payer to the payee has been made.

4. A server computer comprising the computer readable medium of claim 3.

5. A system comprising the server computer of claim 4 and the mobile phone.

Petitioner Exhibit 1002-1380

6. A method comprising:

receiving a payment request message from a mobile phone operated by a consumer, wherein the payment request message includes a request to pay for a product from a vending machine;

analyzing the payment request message to determine if the consumer is authorized to pay for the product;

sending a payment response message back to the vending machine; and

receiving an acknowledgement message from the vending machine that the product was purchased.

7. The method of claim 6 further comprising automatically calling the mobile phone and requesting that the consumer enter a PIN into the phone.

8. A computer readable medium comprising:

code for receiving a payment request message from a mobile phone operated by a consumer, wherein the payment request message includes a request to pay for a product from a vending machine;

code for analyzing the payment request message to determine if the consumer is authorized to pay for the product;

code for sending a payment response message back to the vending machine; and

code for receiving an acknowledgement message from the vending machine that the product was purchased.

9. A server comprising the computer readable medium of claim 8.

10. A method comprising:

reviewing contact information associated with a vending machine;

sending a payment request message using the contact information and a mobile phone;

selecting a product in the vending machine; and

receiving the product from the vending machine.

Petitioner Exhibit 1002-1381

11. A terminal comprising:

a processor; and

a computer readable medium comprising code for processing or providing a first coupon associated with a first entity and code for processing or providing a second coupon associated with a second entity.

12. The terminal of claim 11 wherein the first entity is an issuer and the second entity is a merchant.

13. The terminal of claim 11 wherein the terminal comprises a reader coupled to the processor.

14. The terminal of claim 11 wherein code for processing or providing the first coupon comprises code for providing the first coupon.

15. The terminal of claim 11 wherein the terminal is adapted to process credit cards.

16. A method comprising:

receiving a reload request message from a mobile phone; and

reloading a portable consumer device with value, in response to receiving the reload request message.

17. The method of claim 16 wherein the portable consumer device is a prepaid card.

18. The method of claim 16 wherein the reload request message is an SMS message.

19. A computer readable medium comprising:

code for receiving a reload request message from a mobile phone; and

code for reloading a portable consumer device with value, in response to receiving the reload request message.

20. A server computer comprising the computer readable medium of claim 19.

Petitioner Exhibit 1002-1382

21. A method comprising:

receiving information from a consumer regarding how the consumer wants to be notified if potentially fraudulent activity is occurring with respect to a portable consumer device being used by the consumer; and

alerting the consumer in a manner consistent with the received information if potential fraudulent activity is occurring.

22. The method of claim 21 wherein the received information includes the time when the consumer wants to be notified.

23. The method of claim 21 wherein the received information includes the date when the consumer wants to be notified.

24. A computer readable medium comprising:

code for receiving information from a consumer regarding how the consumer wants to be notified if potentially fraudulent activity is occurring with respect to a portable consumer device being used by the consumer; and

code for alerting the consumer in a manner consistent with the received information if potential fraudulent activity is occurring.

25. A server computer comprising the computer readable medium of claim 24.

26. A method comprising:

receiving a coupon comprising a code at a mobile phone operated by a consumer; and

manually providing the code to a merchant, wherein the merchant thereafter provides a discount to the consumer.

27. The method of claim 26 wherein the code is a numeric code.

28. The method of claim 26 wherein the coupon includes a machine readable code.

Petitioner Exhibit 1002-1383

29. A method comprising:

receiving a coupon comprising a code at a portable consumer device comprising an antenna operated by a consumer; and

providing the code to a merchant using an antenna.

30. The method of claim 29 wherein the antenna is an RF antenna and the portable consumer device is a mobile phone.

Petitioner Exhibit 1002-1384

VALUE BASED OFFERS

ABSTRACT OF THE DISCLOSURE

A system and a method for using a portable consumer device such as a mobile phone are disclosed.

60945584 v1

Petitioner Exhibit 1002-1385

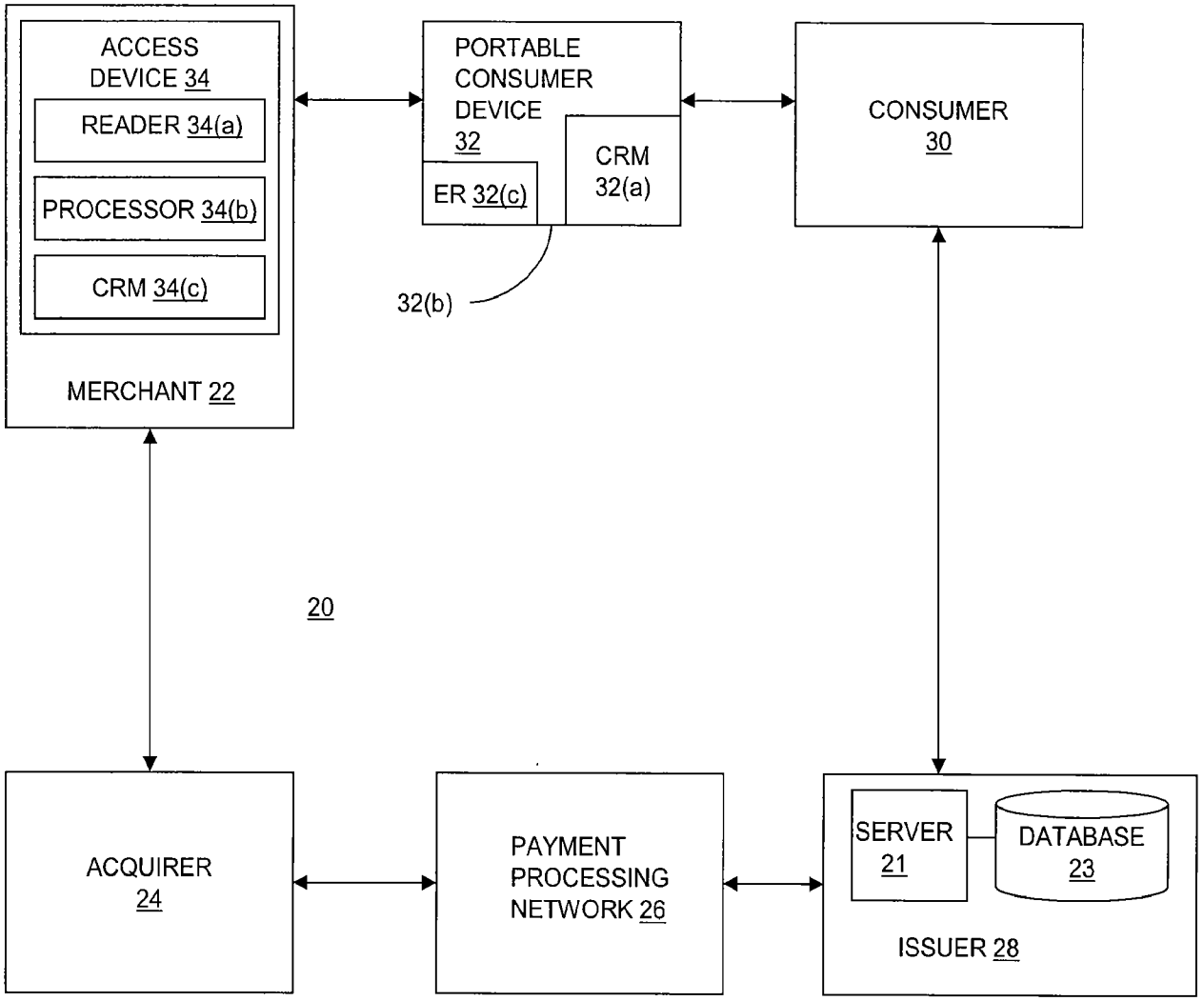
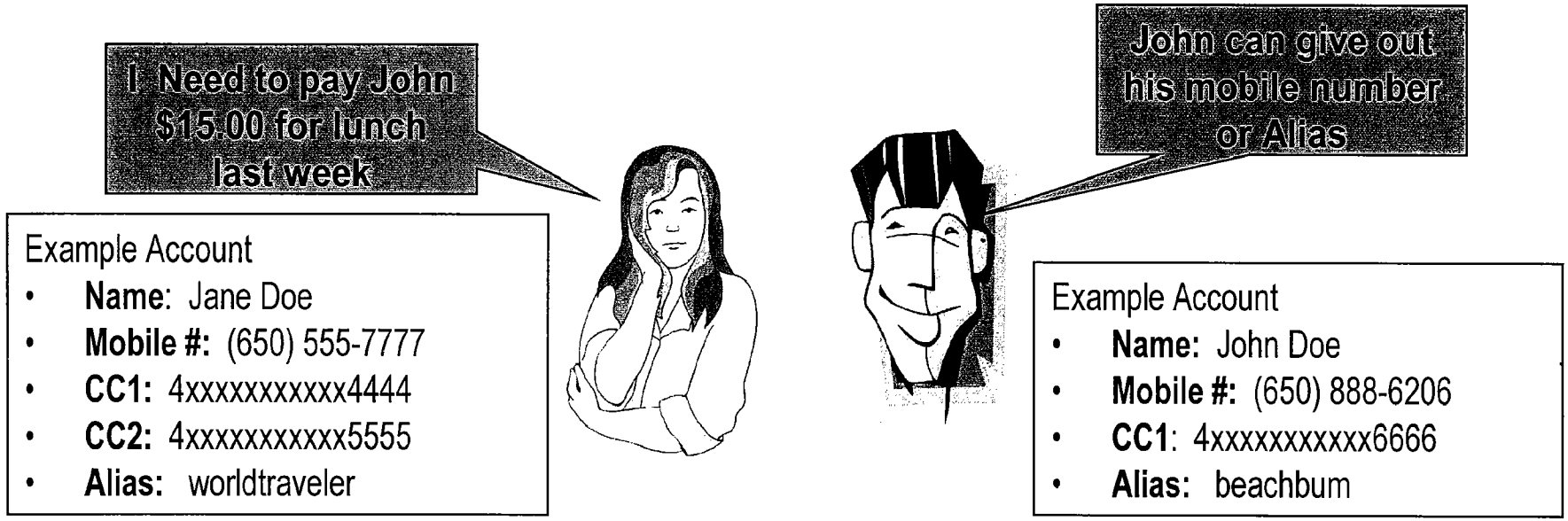


FIG. 1

Petitioner Exhibit 1002-1386



1) Jane initiates an SMS payment:

- visa1 pay 6508886206 $15.00

or

- myvisa pay beachbum $15.00 CC2

FIG. 2

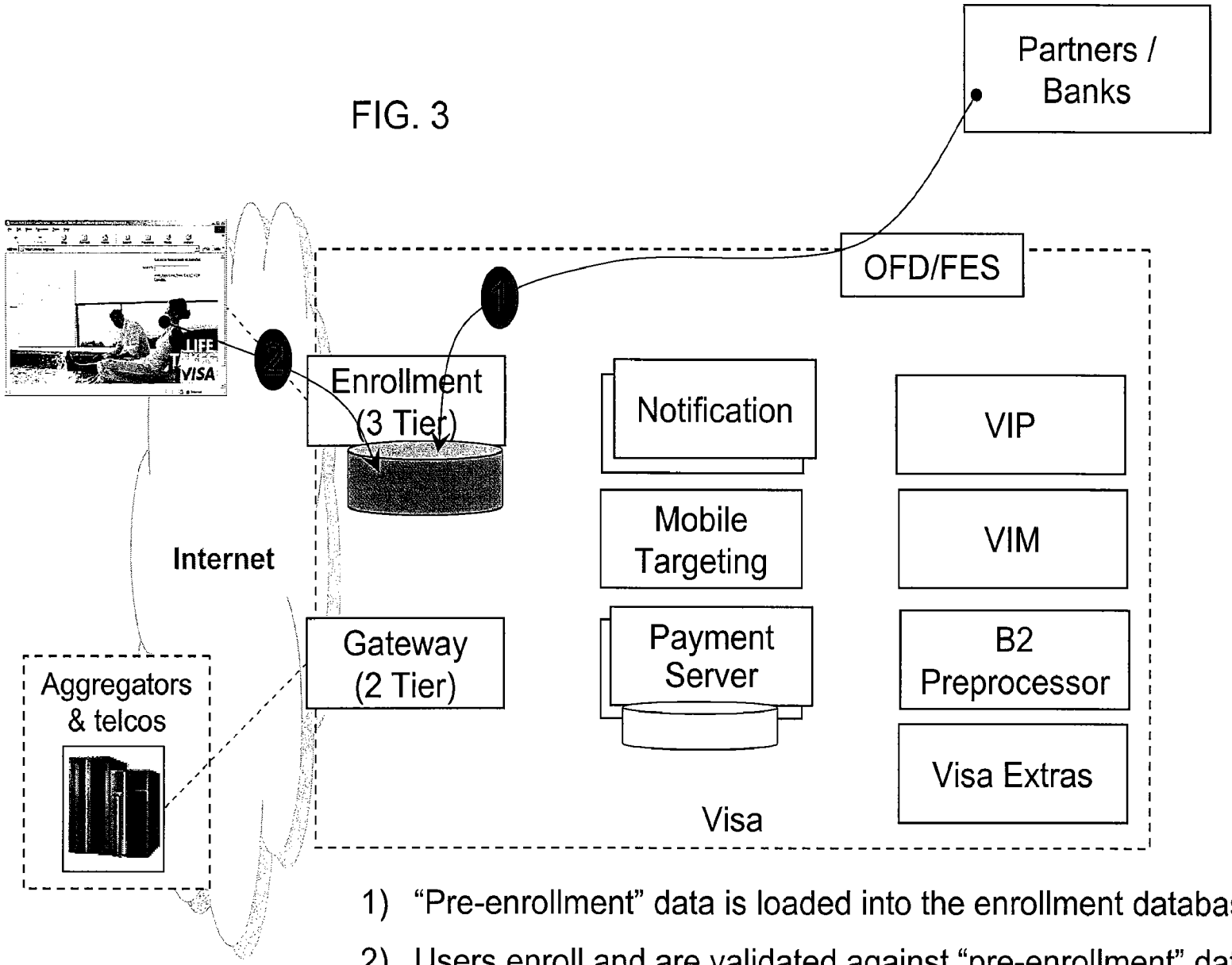
2) Receives a IVR call back asking her to enter her mobile pin

3) John is notified that a payment request has been initiated (SMS and/or e-mail)

- World traveler requested $15.00 be paid to your mobile account

Petitioner Exhibit 1002-1387

FIG. 3



1) "Pre-enrollment" data is loaded into the enrollment database

2) Users enroll and are validated against "pre-enrollment" data

Petitioner Exhibit 1002-1388

Discount / coupon Key

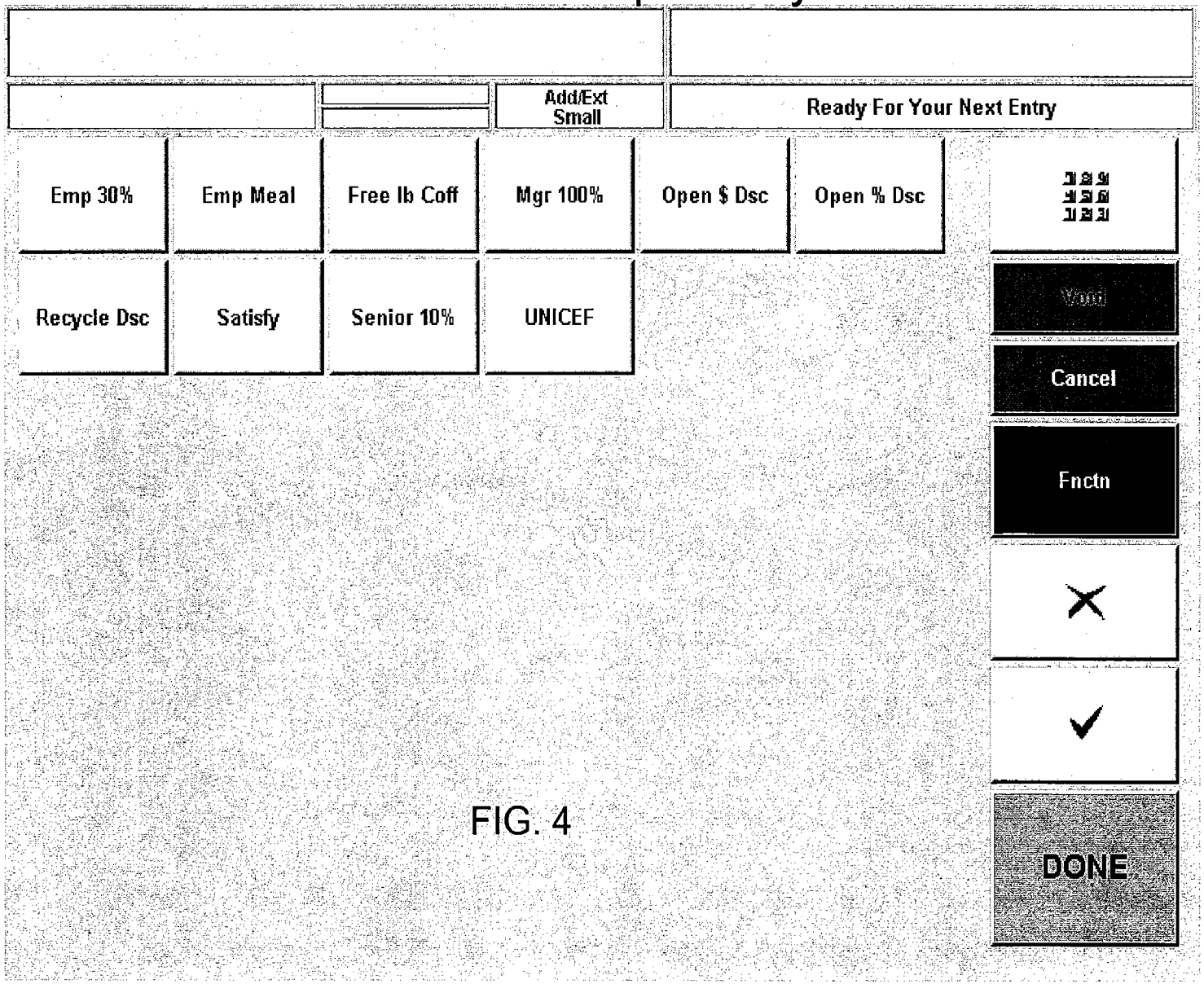


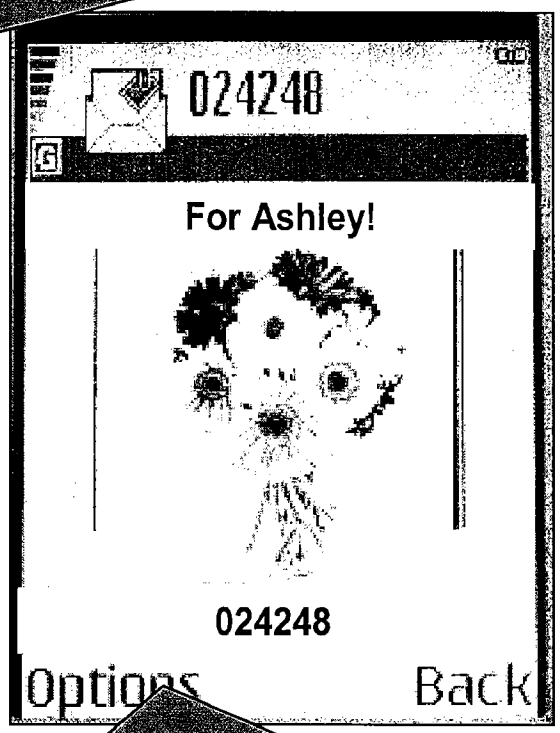
FIG. 4

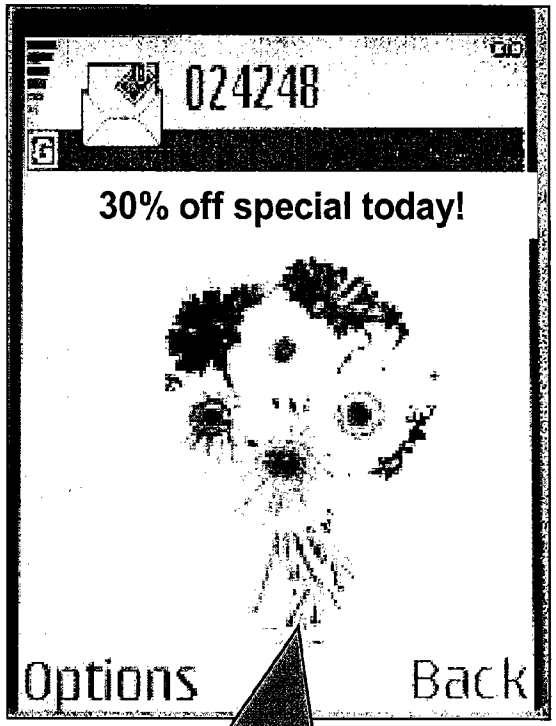
Petitioner Exhibit 1002-1389

M-Coupon type: Barcode
Input method supported: Scan or keyed
POS programming options: NLU only (for micros)

FIG. 5(a)







M-Coupon type: Visual w/ NLU #
Input method supported: keyed
POS programming options: Discount key or NLU

FIG. 5(b)

FIG. 5(c)

M-Coupon type: Visual only
Input method supported: Keyed (discount key)
POS programming options: Discount Key for 30% off

Petitioner Exhibit 1002-1390

Consumer vending purchase using Dial/IVR

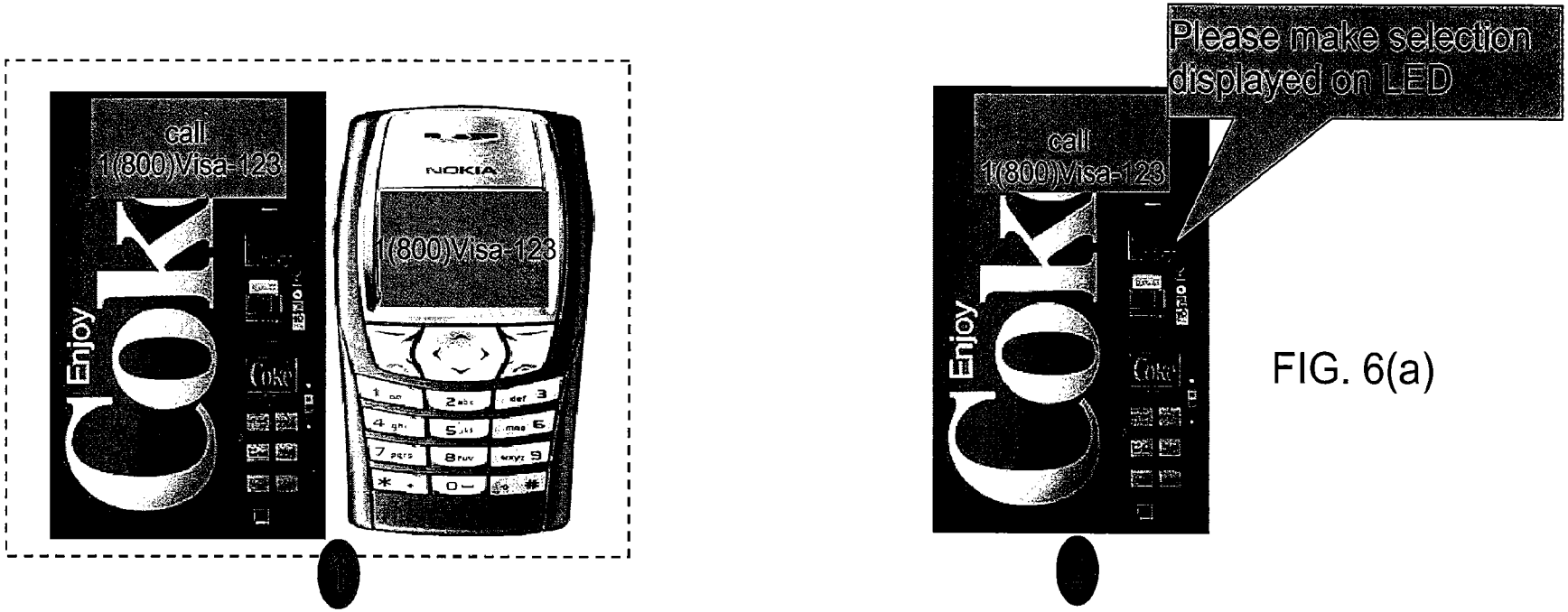


FIG. 6(a)

1. The consumer dials the number seen on the vending machine to make a purchase, then follows directions.
2. *A payment processing organization such as Visa authorizes the transaction, and tells the vending machine that payment has been accepted.*
3. *The vending machine display shows the message 'Please choose your product'.*
4. *The customer makes a selection or the credit will timeout after 20 seconds.*
5. *The vending machine returns a vend acknowledge to Visa*
6. *The purchased item will appear on their next statement.*

Petitioner Exhibit 1002-1391

Consumer vending purchase using SMS

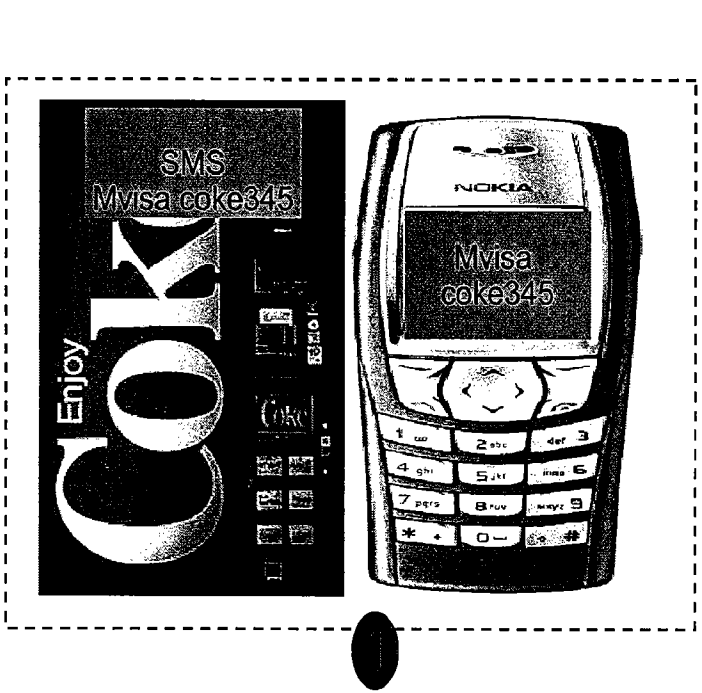




FIG. 6(b)

1. The consumer sends an SMS message to the number seen on the vending machine to make a purchase. The consumer gets a automated call back asking for PIN.
2. *Visa authorizes the transaction, and tells the vending machine that payment has been accepted*
3. *The vending machine display shows the message 'Please choose your product'.*
4. *The customer makes a selection or the credit will timeout after 20 seconds.*
5. *The vending machine returns a vend acknowledge to Visa*
6. *The purchased item will appear on their next statement.*

Petitioner Exhibit 1002-1392

Mobile App
Visa Vending Concepts

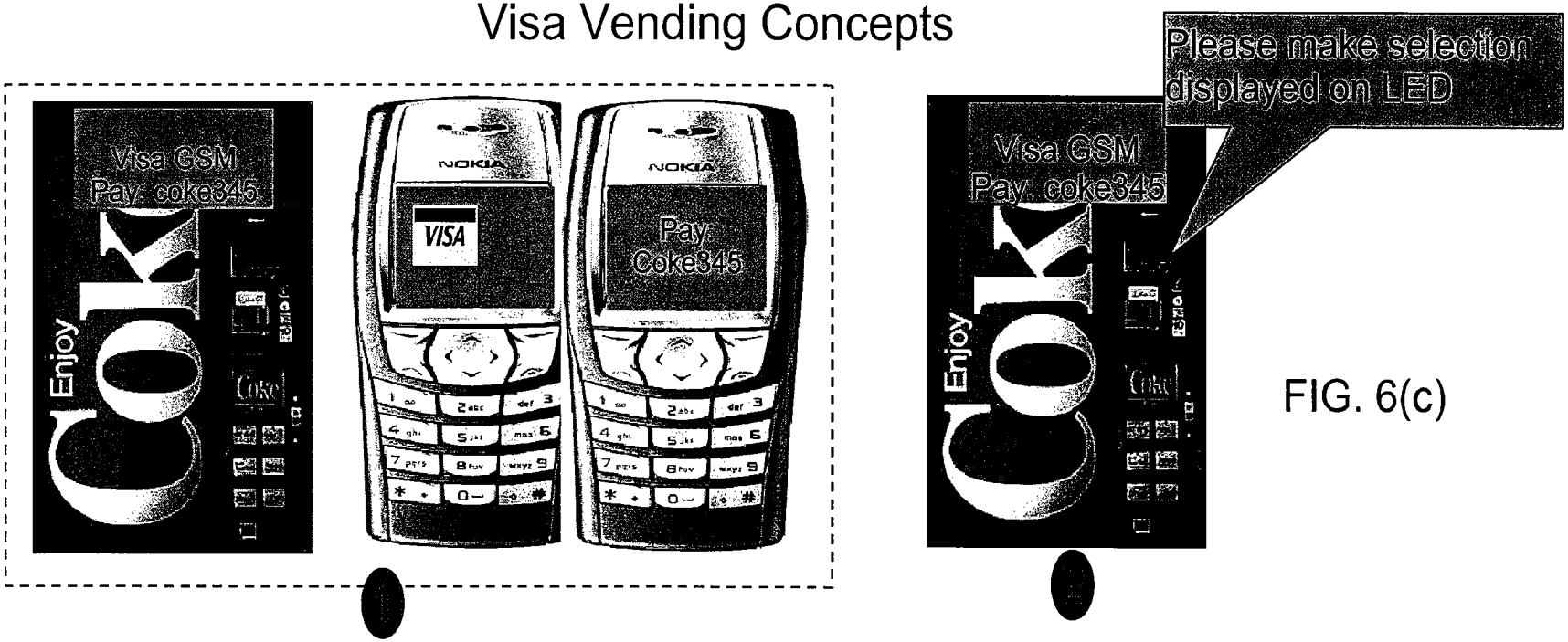


FIG. 6(c)

1. Using the "machine alias" seen on the vending machine, a consumer uses his mobile wallet to make a vending purchase.
2. *Visa authorizes the transaction, and tells the vending machine that payment has been accepted*
3. *The vending machine display shows the message 'Please choose your product'.*
4. *The customer makes a selection or the credit will timeout after 20 seconds.*
5. *The vending machine returns a vend acknowledge to Visa*
6. *The purchased item will appear on their next statement.*

Petitioner Exhibit 1002-1393

Single POS set up

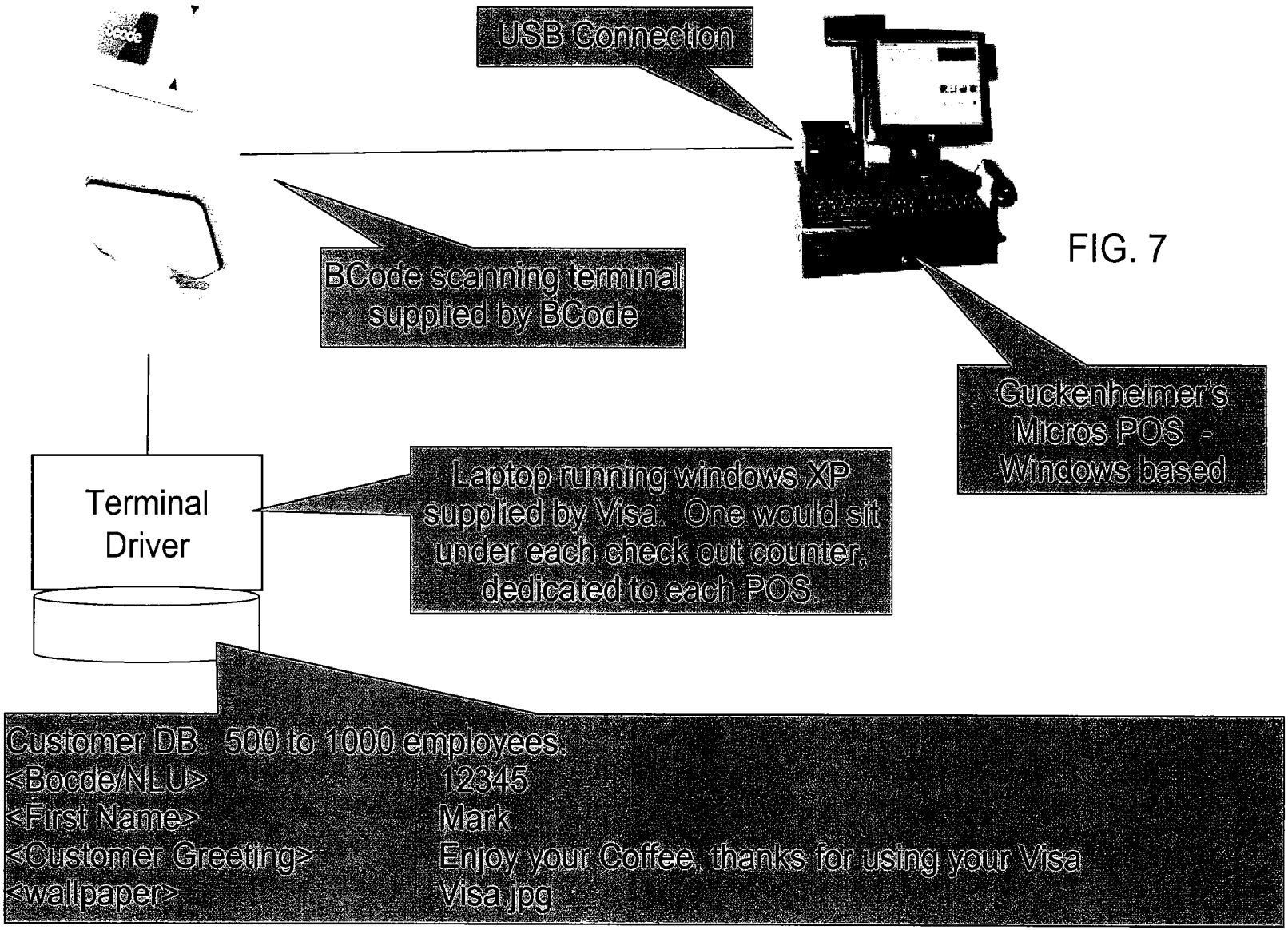


FIG. 7

Petitioner Exhibit 1002-1394

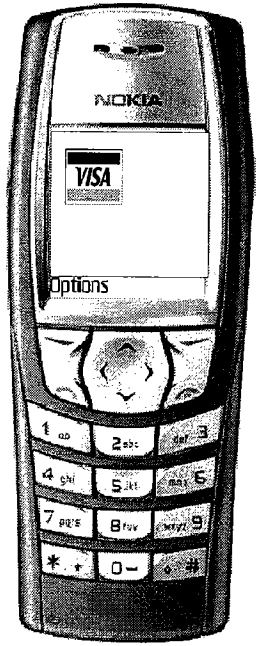
APPENDIX

P2P & P2B

/ Petitioner Exhibit 1002-1396

P2P Options





Option 1: SMS Based

- On nearly every phone already
- PayPal or unpaid model
- SMS charge

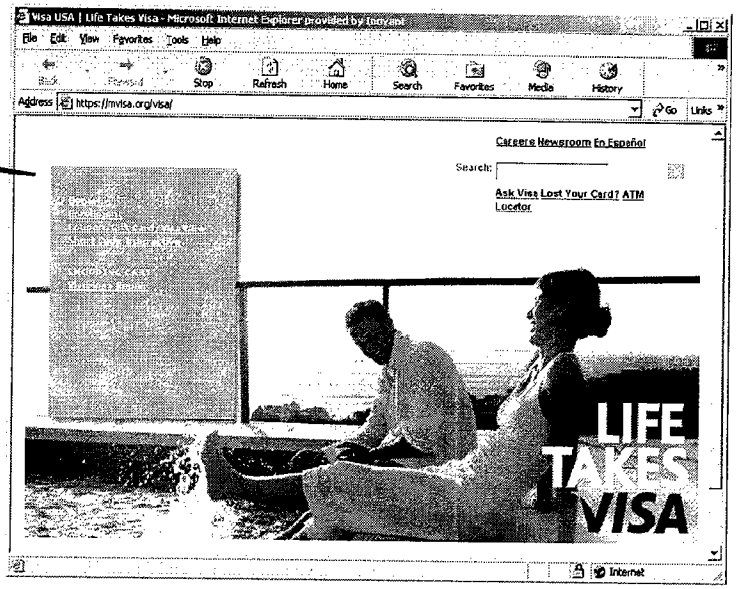
Option 2: Application on the phone

- More control over transaction and user experience
- Requires provisioning
- Requires user to have GPRS/GSM service
- Much more secure
- No SMS charges
- Faster

Petitioner Exhibit 1002-1397

How does the consumer: Enroll?

- Consumer goes to the Visa Enrollment Server
- Enrollment server can be skinned to be Visa or for a partner



- Consumer Creates a "Mobile Pay" account
  - Name
  - Mobile Number
  - Account Number (s)
  - Optional Alias
  - And additional Validation Info
- Consumer verifies they have read appropriate disclaimers (Opt in)
- Entered Information is verified.

Verifications:

- Consumer has physically has phone
- Phone belongs to consumer
- Account belongs to consumer

- An online tutorial is available to help consumer use SMS pay if needed.

3 Petitioner Exhibit 1002-1398

How does the consumer: Make a P2P Mobile Payment?

I Need to pay John $15.00 for lunch last week



Example Account
- **Name**: Jane Doe
- **Mobile #:** (650) 555-7777
- **CC1:** 4xxxxxxxxxx4444
- **CC2:** 4xxxxxxxxxx5555
- **Alias:** worldtraveler

John can give out his mobile number or Alias



Example Account
- **Name:** John Doe
- **Mobile #:** (650) 888-6206
- **CC1**: 4xxxxxxxxxx6666
- **Alias:** beachbum

1) Jane initiates an SMS payment:
- visa1 pay 6508886206 $15.00

or
- myvisa pay beachbum $15.00 CC2

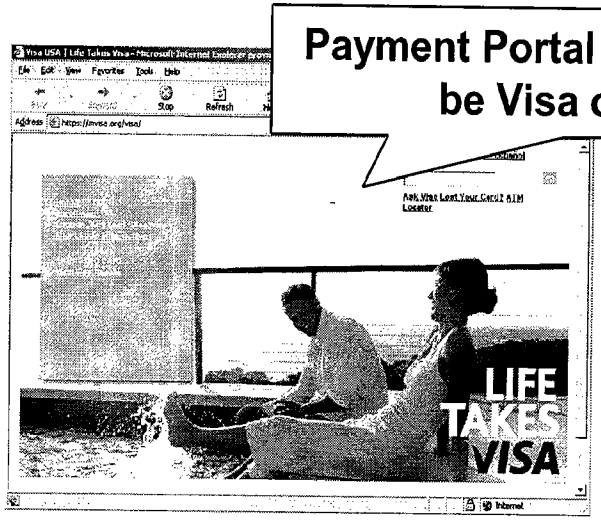
2) Receives a IVR call back asking her to enter her mobile pin

3) John is notified that a payment request has been initiated (SMS and/or e-mail)
- World traveler requested $15.00 be paid to your mobile account

Petitioner Exhibit 1002-1399

How does the consumer: Make a P2P Payment with out a phone?





1) Jane logs into her account:

- Makes a transfer of $15.00 to 6508886206 $15.00

or

- Makes a transfer of $15.00 to beachbum $15.00

2) John is notified that a payment request has been initiated (SMS and/or e-mail)

- World traveler requested $15.00 be paid to your mobile account

Petitioner Exhibit 1002-1400

Good For:

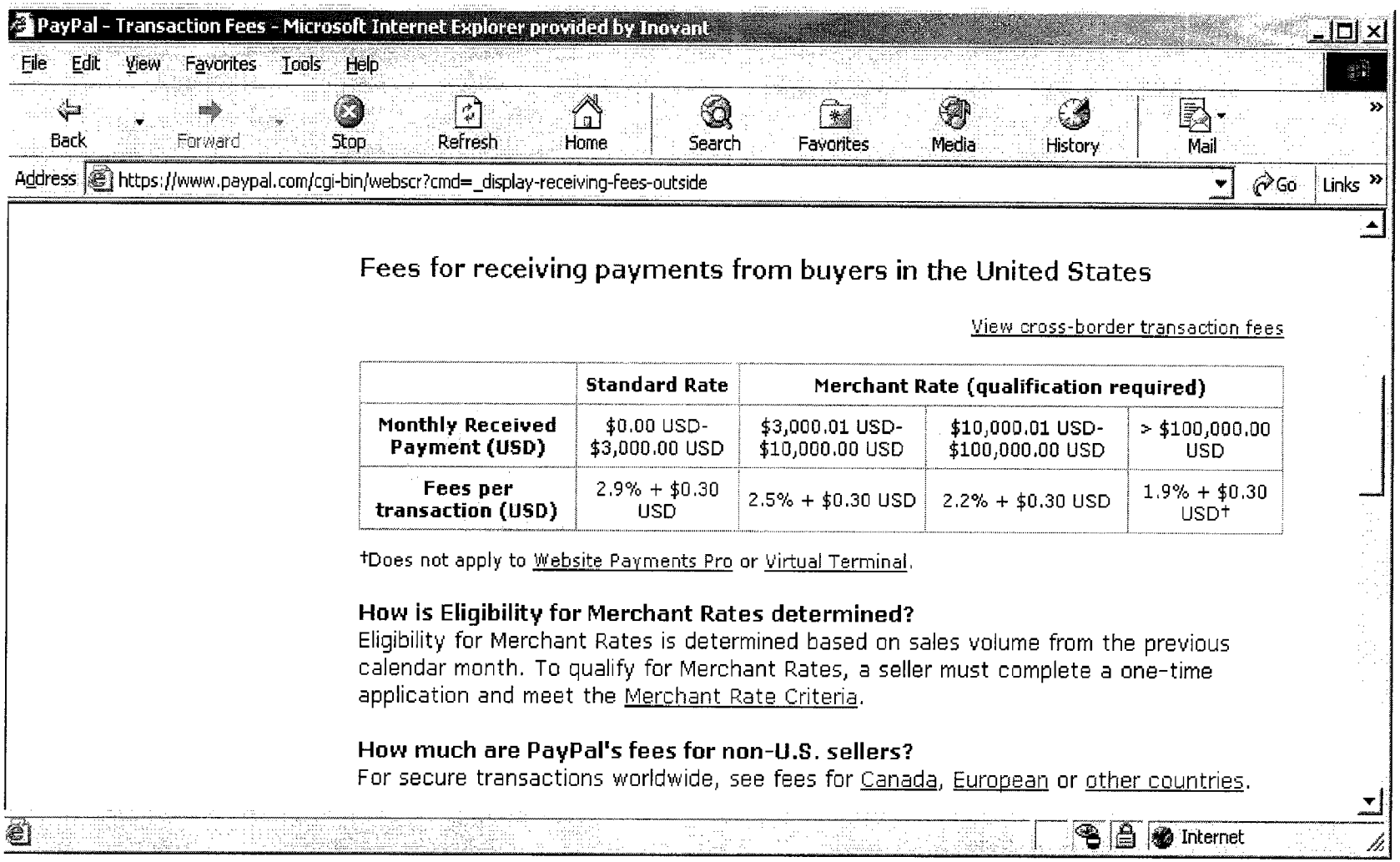
Payment between any two enrolled people (with a Visa Account).
The person being paid never sees the transaction.

- Pay a Friend
- Sending money to kids at school
- Sending money to family
- E-bay transactions
- Cross border transactions
- Money transfer / Western Union transactions

- *Person to Business (Alias or phone number can be for a business)*

Petitioner Exhibit 1002-1401

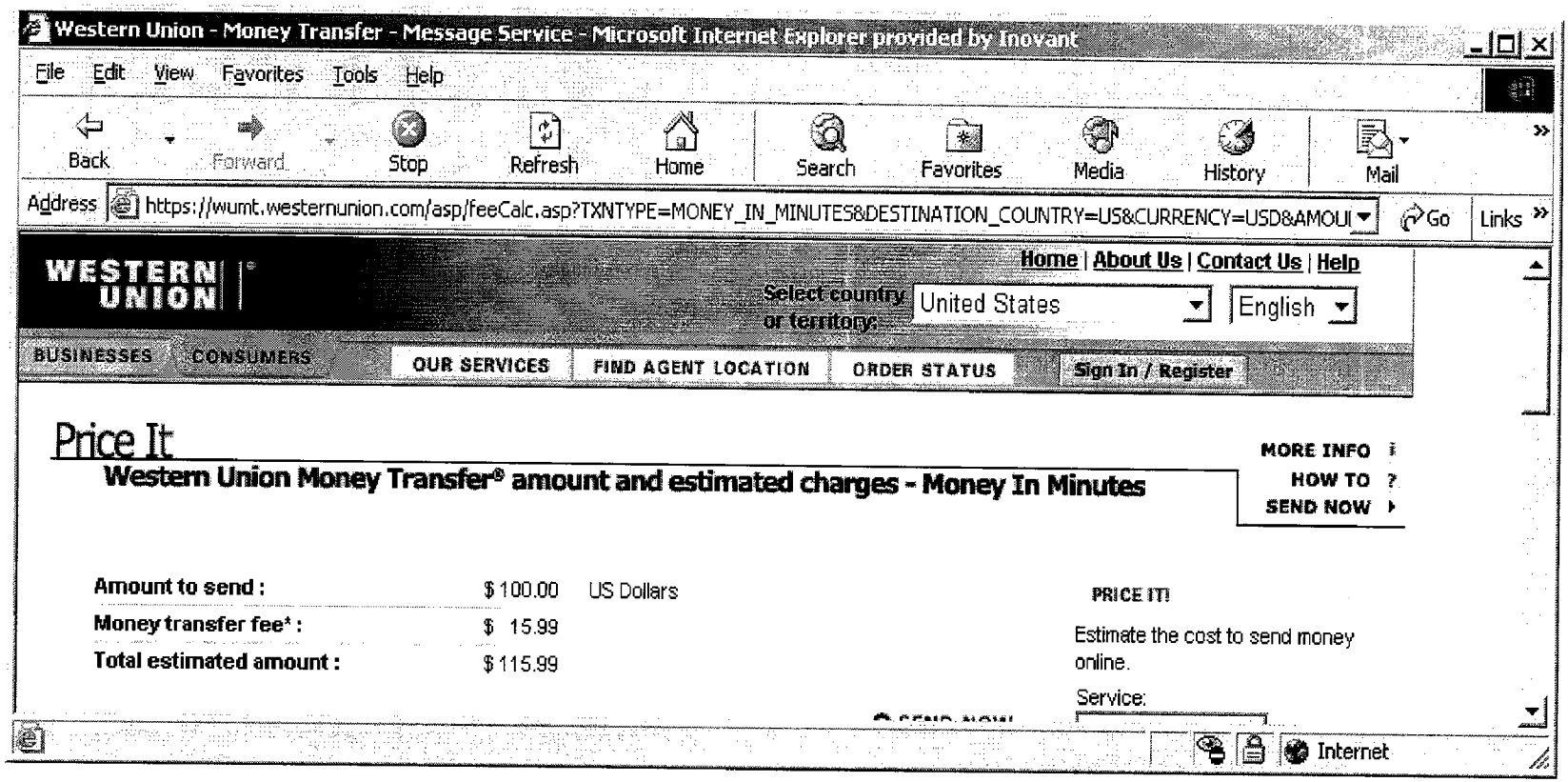
Payment Cost Model?



Would require a new cost model to make cost effective
However, there seems to be ample room for a new cost model!

Petitioner Exhibit 1002-1402

Payment Cost Model?



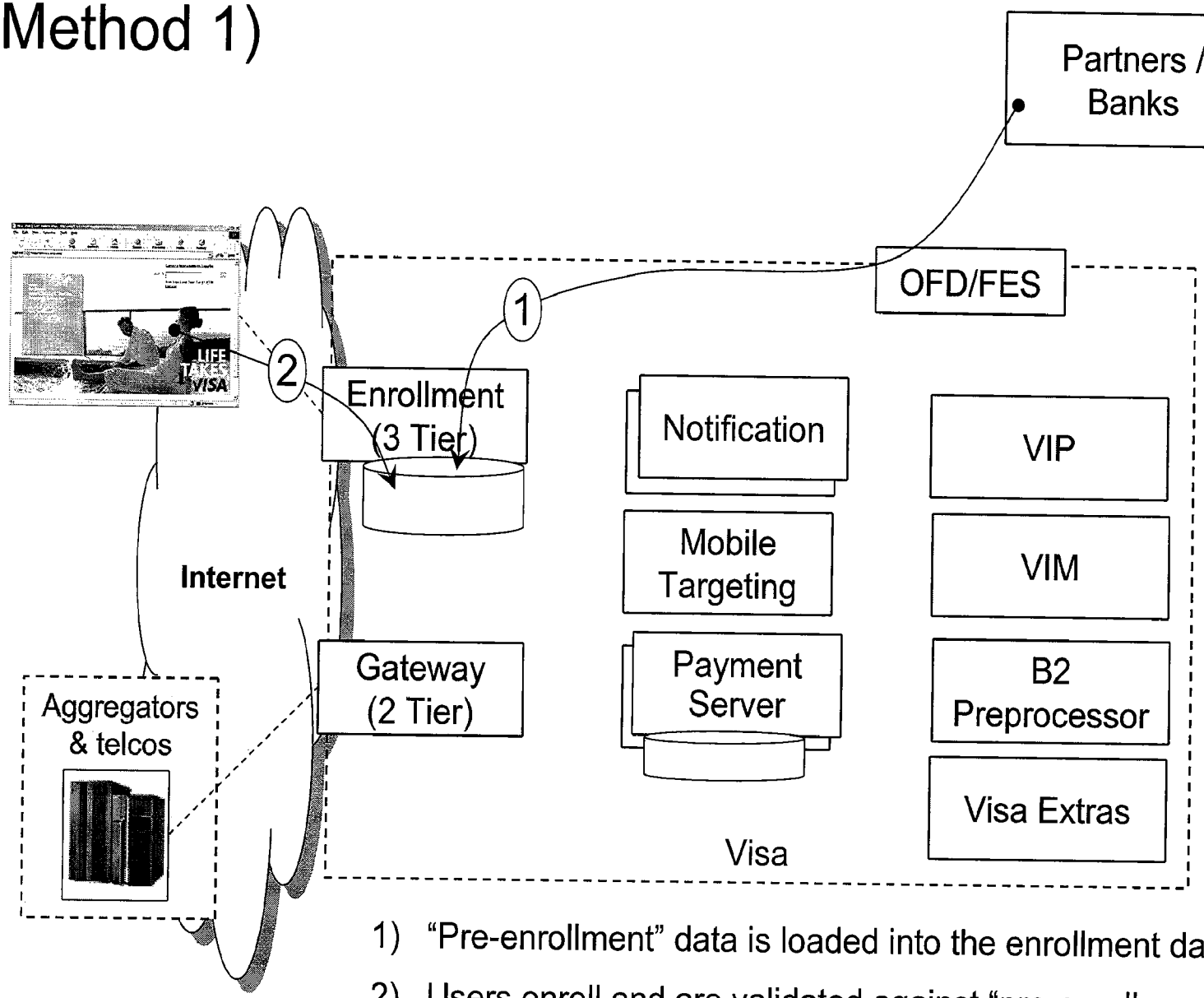
For two destinations in California!

Petitioner Exhibit 1002-1403

Enrollment Methods

Petitioner Exhibit 1002-1404

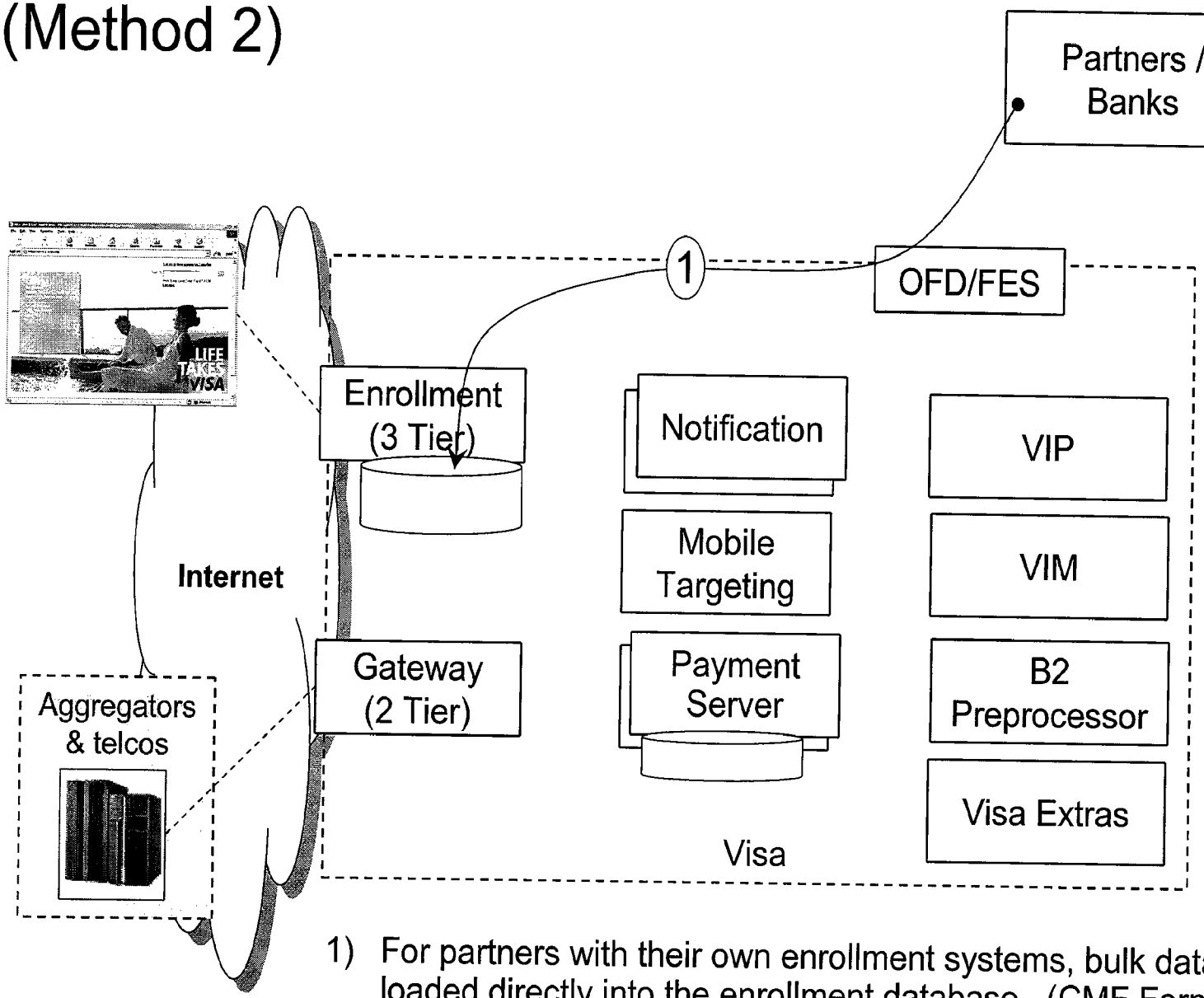
User Enrollment (Method 1)



1) "Pre-enrollment" data is loaded into the enrollment database
2) Users enroll and are validated against "pre-enrollment" data

Petitioner Exhibit 1002-1405

Batch Enrollment (Method 2)



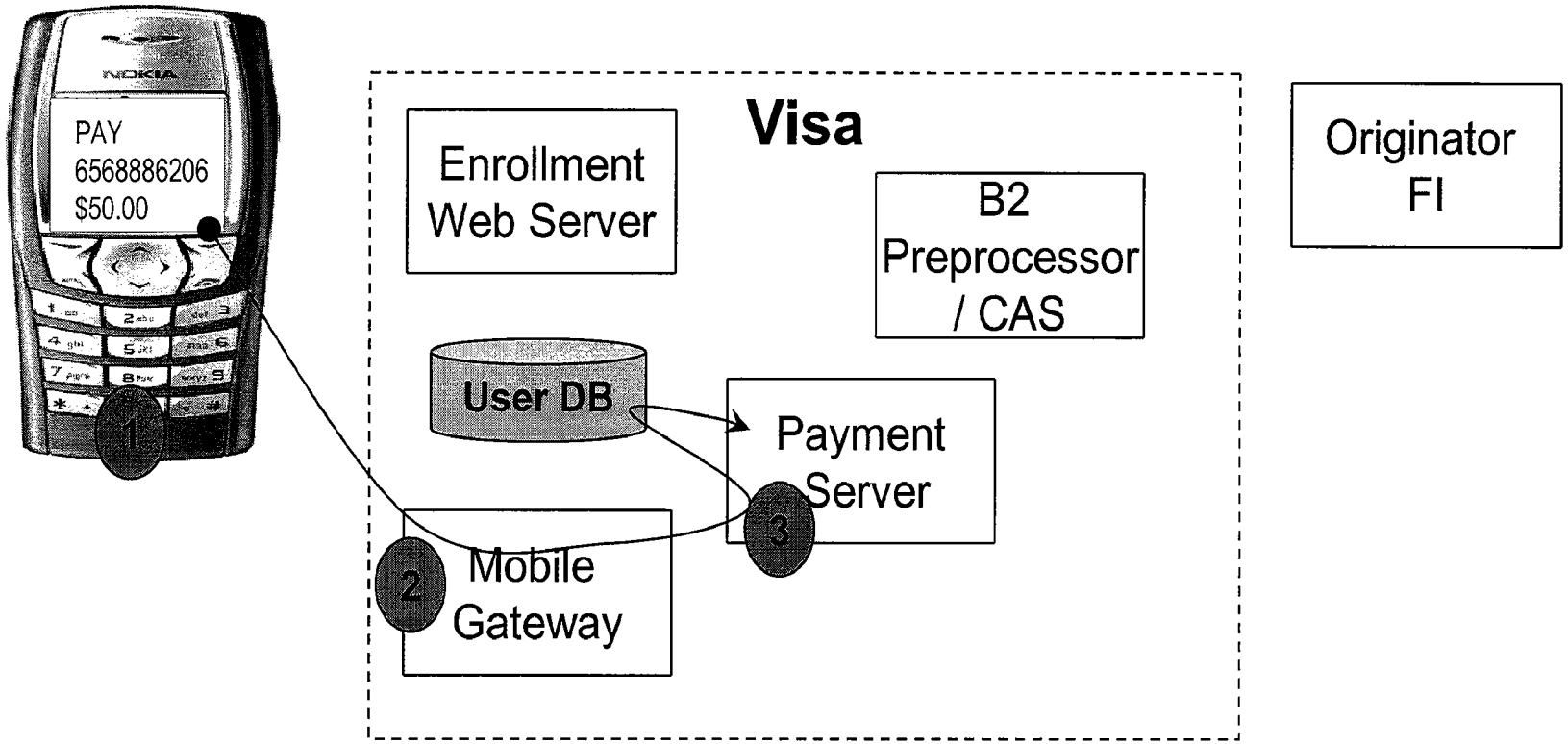
1) For partners with their own enrollment systems, bulk data can be loaded directly into the enrollment database. (CMF Format?)

Petitioner Exhibit 1002-1406

Payment Request Initiated by an SMS message

Petitioner Exhibit 1002-1407

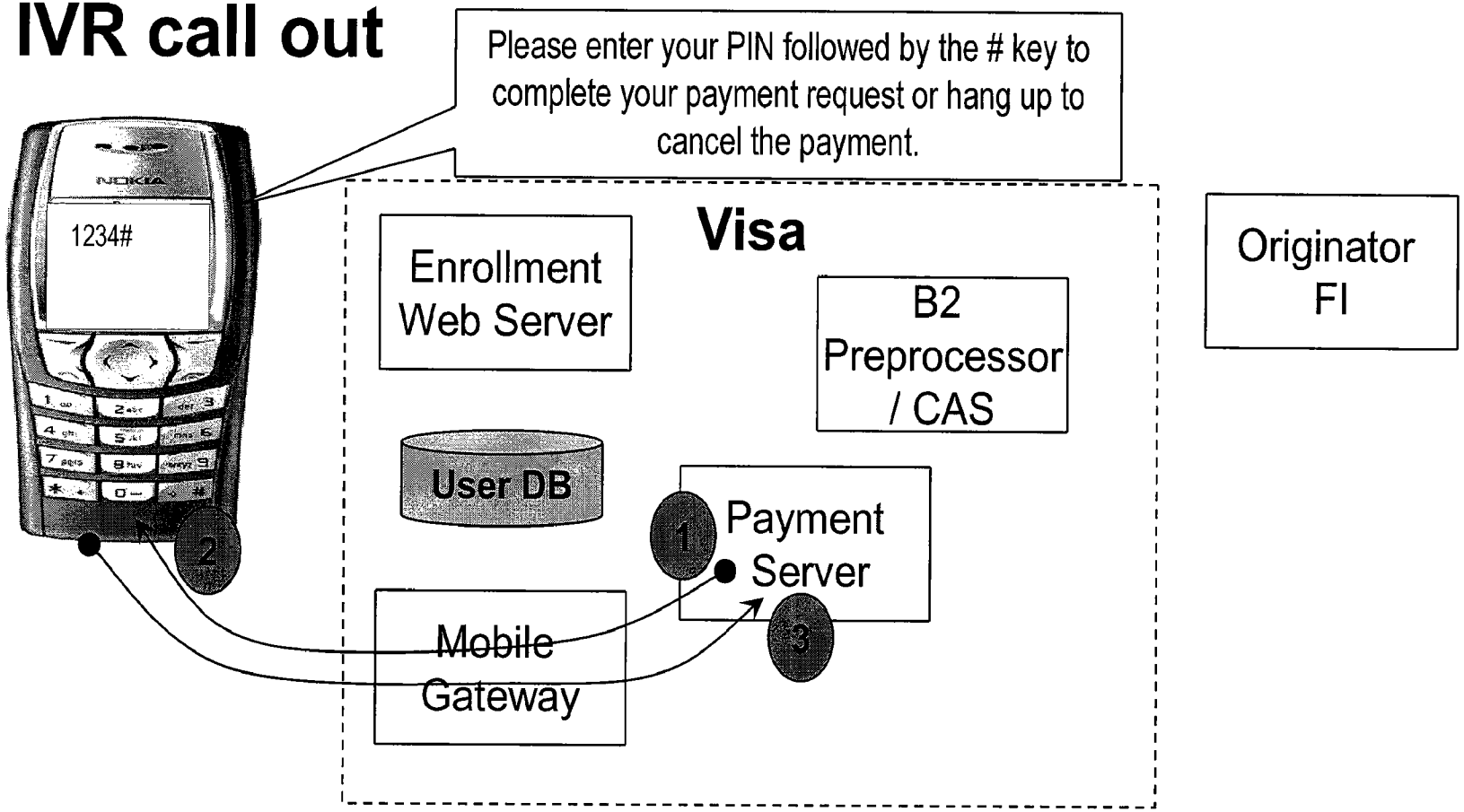
P2P Pilot – SMS initiated



1) **Enrolled user initiates a payment by sending a SMS message to MYVISA (or partner short code)**
2) **The message reaches the mobile gateway through an aggregator**
3) **The payment server validates the message against the enrolled user database, augments the message with recipient information, and logs the transaction**

/ 3 Petitioner Exhibit 1002-1408

P2P Pilot – SMS Initiated IVR call out



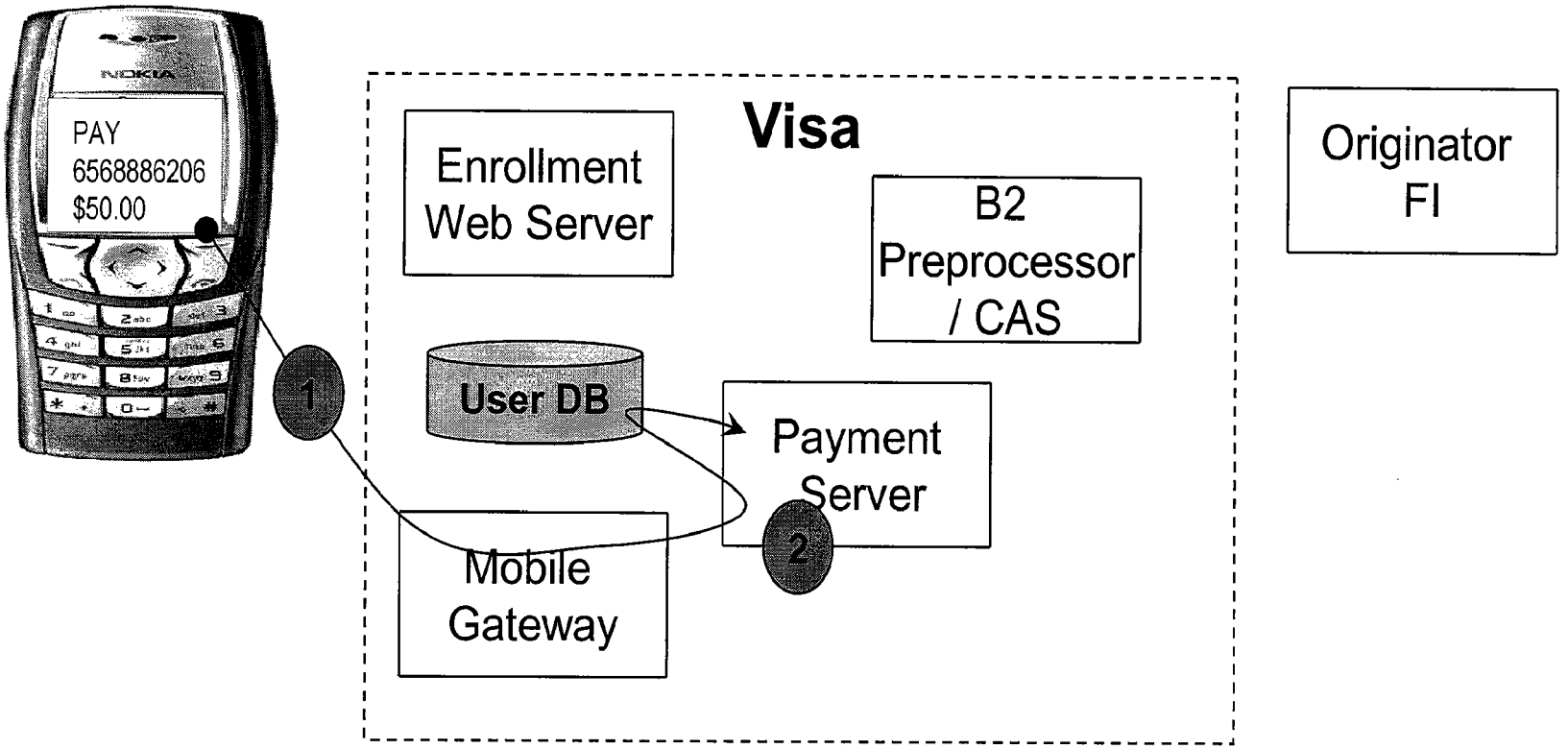
1) **The Payment server initiates an IVR call out request to validate the transaction (IVR call out will be handled either through the Visa call center or through a partner)**
2) **The requestor receives a phone call, asking them to enter their mobile PIN number to complete the transaction**
3) **The response is returned to the payment server**

14 Petitioner Exhibit 1002-1409

Payment Request Initiated by a mobile application

Petitioner Exhibit 1002-1410

P2P Pilot – payment initiated



1) **Enrolled user initiates a payment through a mobile application which connects directly to the mobile gateway. (Payment details & Pin are passed securely to Visa)**
2) **The payment server validates the message against the enrolled user database, augments the message with recipient information, and logs the transaction**

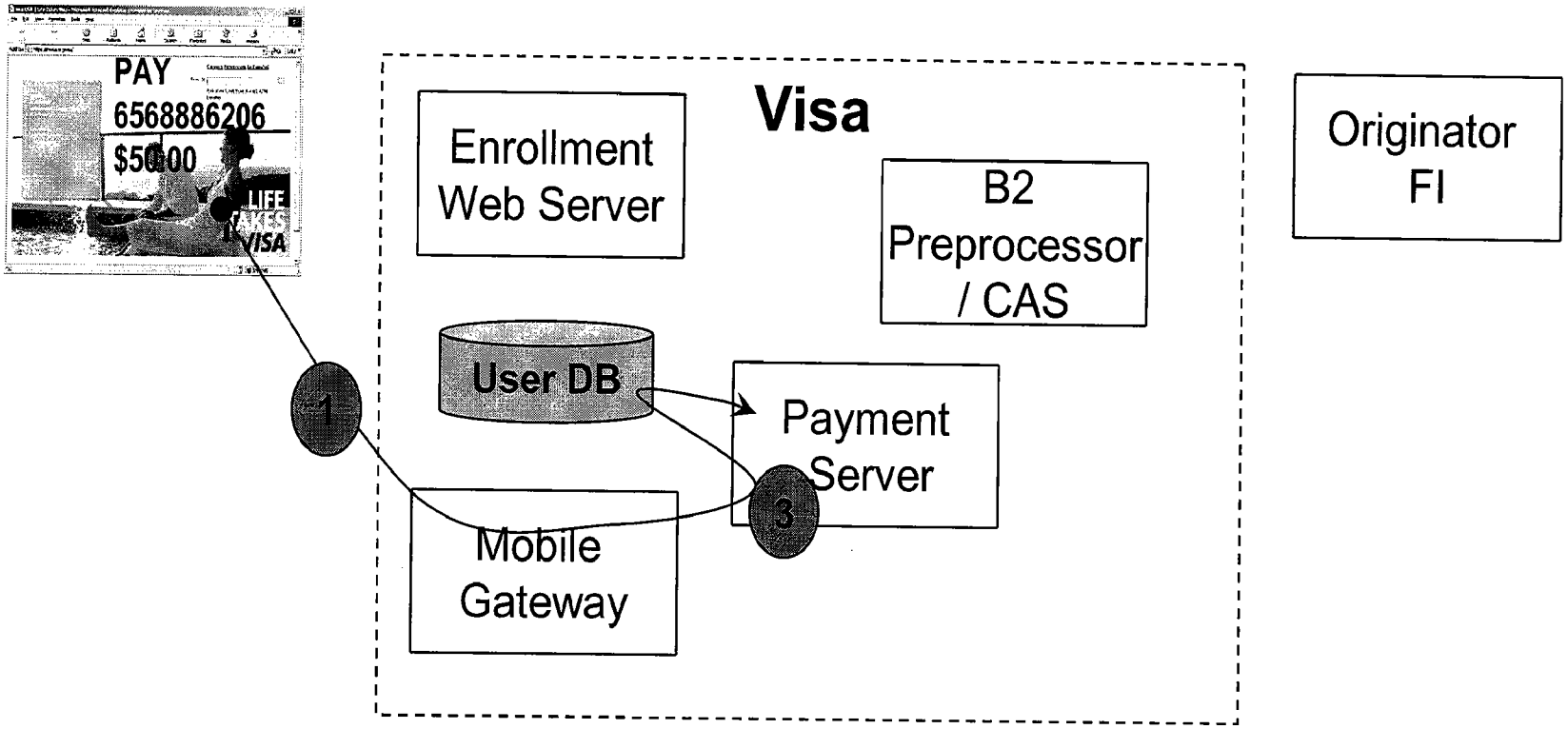
No need for an IVR call back. User PIN was transmitted securely directly to the mobile gateway

Petitioner Exhibit 1002-1411

Payment Request From Web Browser

Petitioner Exhibit 1002-1412

P2P Pilot – payment initiated



1) **Enrolled user initiates a payment via browser**
2) **The payment server validates the message against the enrolled user database, augments the message with recipient information, and logs the transaction**

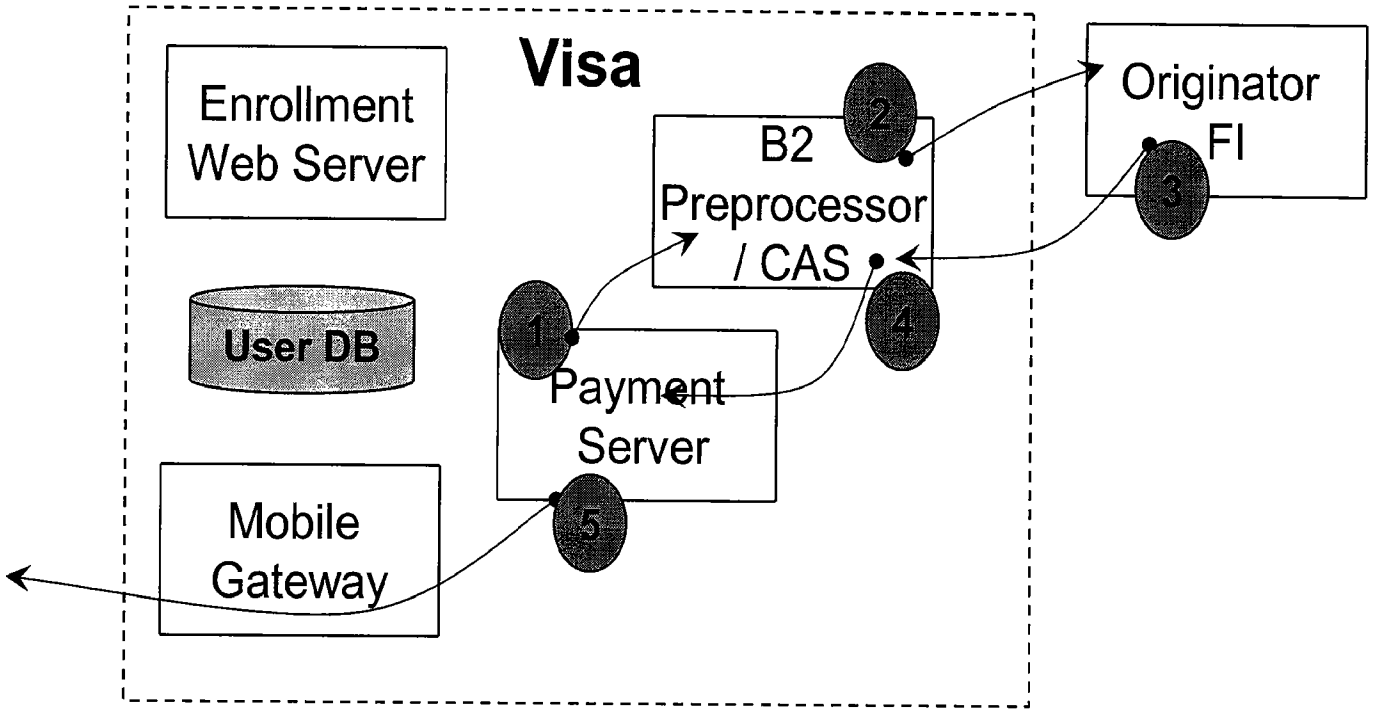
No need for an IVR call back. **User PIN was transmitted securely directly to the mobile gateway**

Petitioner Exhibit 1002-1413

Acquired Payment processed

Petitioner Exhibit 1002-1414

P2P Pilot – Process Payment



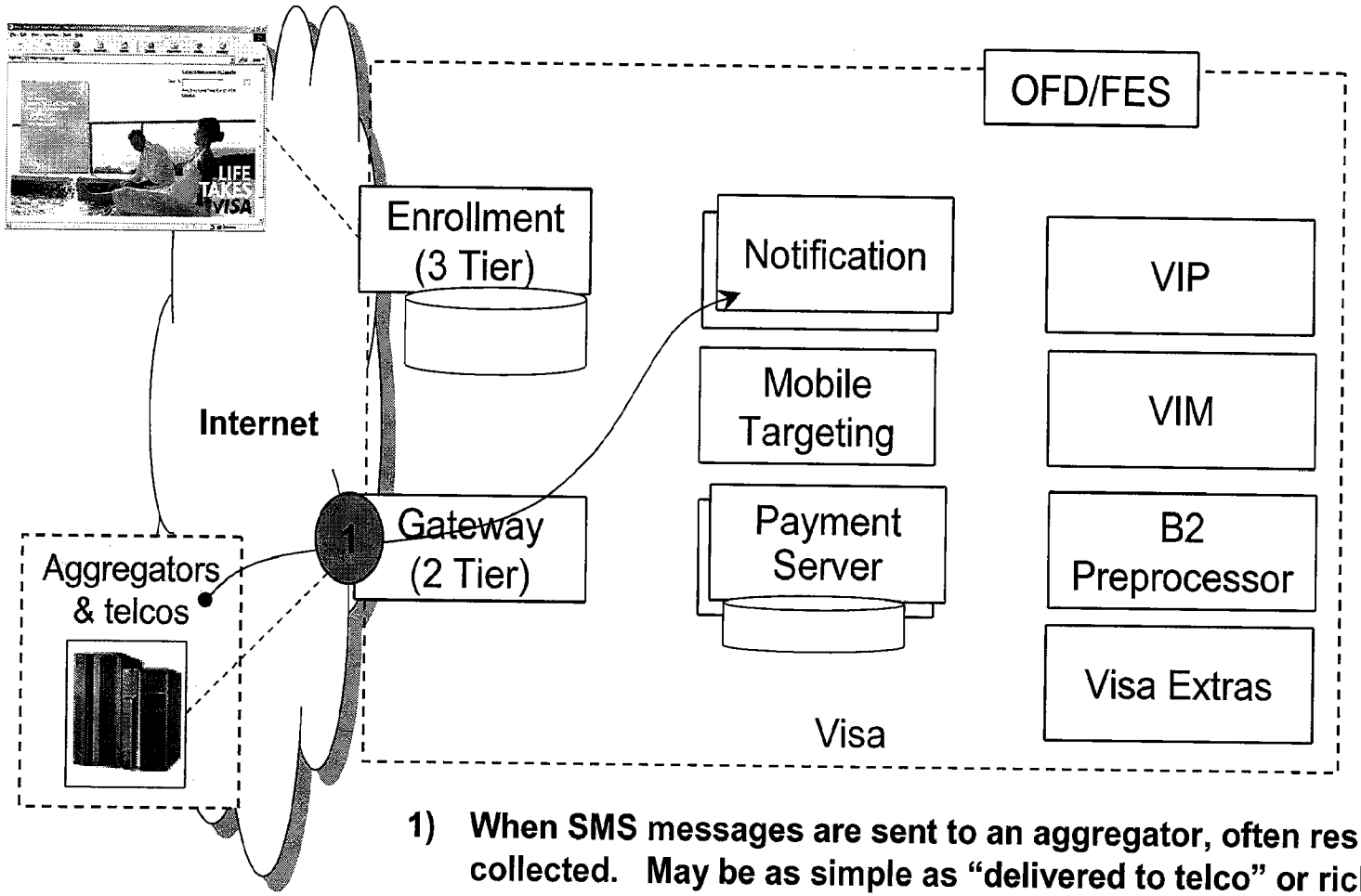
1) Periodically the payment server hands groups of records to the B2 preprocessor (With Tran ID)
2) The B2 preprocessor creates TC57's (Data Capture Advice) which is passed to CAS, which in turn passes the TC57's to the Originator FI (Via OFD) as part of the normal clearing process
3) The originator FI authorizes the transaction, and passes a TC06 (collection), a TC05 (Distribution), and a TC50 (Free Text advice with tran ID & status) back to CAS for processing
4) The TC05 & TC06 are part of the normal settlement flow. The TC50 is passed back to the payment server
5) The person receiving money, is optionally notified

Petitioner Exhibit 1002-1415

Collect SMS results from Aggregator

21 Petitioner Exhibit 1002-1416

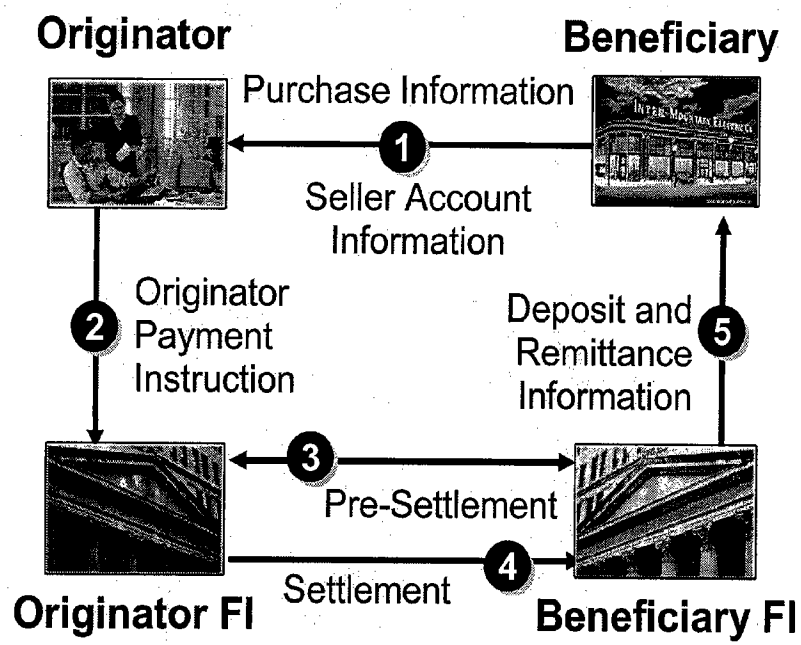
P2P Pilot
Collect SMS results



1) **When SMS messages are sent to an aggregator, often results can be collected. May be as simple as "delivered to telco" or rich with additional details about the mobile device and carrier.**

22 Petitioner Exhibit 1002-1417

Push Settlement Model



Originator controls payment request information
Originator initiates payment before/after delivery
Originator FI can ensure good payment data
Expands number of beneficiaries
"Good funds" validated before transaction
Low beneficiary overhead
Focused on "giving" funds to beneficiary

Present—Original Credit

Definition

A push transaction defined as a transaction initiated by a Member or on behalf of its merchant that results in a credit to a Visa account for a purpose other than refunding a Visa purchase.

Systematically defined as:

- A modified TC06, with transaction code qualifier = 2

Details

A basic push transaction

Use for applications with minimal data requirements

Or with a sophisticated "on-behalf-of" (OBO) service

- Limitations on how large it can scale
- Limitations on how far it can extend

2.3 Petitioner Exhibit 1002-1418

Mobile Vending

24 Petitioner Exhibit 1002-1419

Mobile Vending Concepts

There are several possible approaches to mobile vending.

Vending Purchase triggered by a Dial (IVR), SMS or a mobile based application

- A payment processing organization can be directly involved in driving the POS devices

Vending Purchase triggered by an NFC enabled mobile device

- The payment processing organization's involvement is indirect.
- Uses established acquiring model to process transactions.

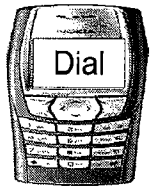
25 Petitioner Exhibit 1002-1420

Visa Confidential

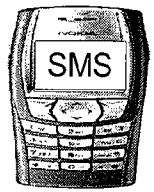
Pro's & Con's with each approach



- Transactions are cheap and secure
- Requires a mobile app to be provisioned on phone
- Requires a data service
- Only available on "smart phones"
- High degree of involvement / control by payment processing organization
- Application could support for electronic receipts



- Dial is available on every phone
- Transaction cost depends on cost of phone call.
- High degree of involvement / control by payment processing organization
- Weak receipt mechanism



- SMS is on almost every phone
- Transaction cost is high . . . Each SMS costs $
- Requires an IVR call back for PIN to be secure. (Additional cost)
- High degree of involvement / control by payment processing organization
- Weak receipt mechanism



- Requires mobile device to be provisioned with NFC chip and app
- Solution is less likely to be driven directly by payment processing organization, but is a standard POS / acquirer model.
- Application could support electronic receipts

Visa Confidential

2-6 Petitioner Exhibit 1002-1421

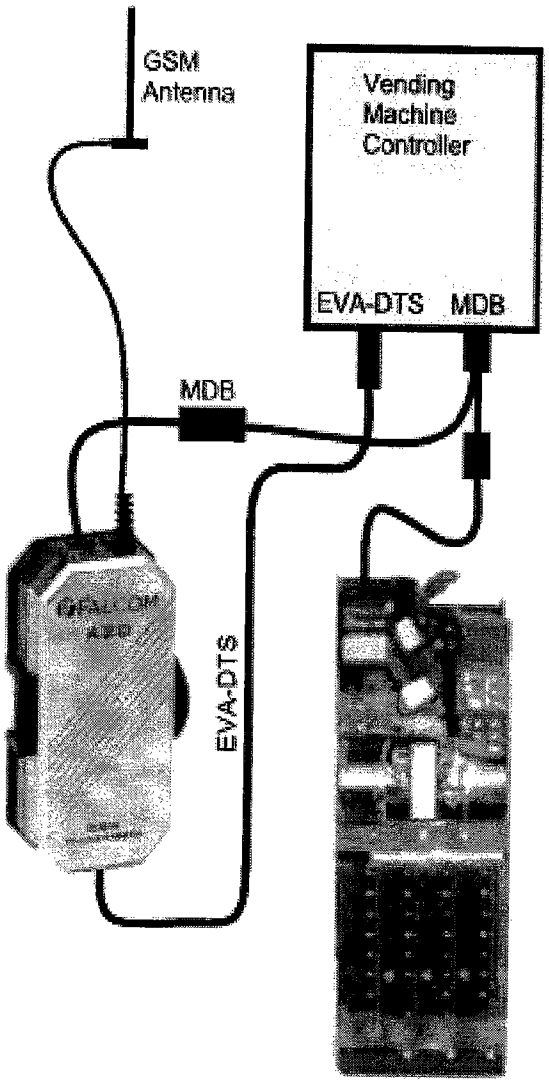
Solutions where a payment processing oragnization could be directly involved

Vending purchases triggered by dial (IVR), SMS or a mobile based application

Visa Confidential

27 Petitioner Exhibit 1002-1422

Setting up the Vending Machine



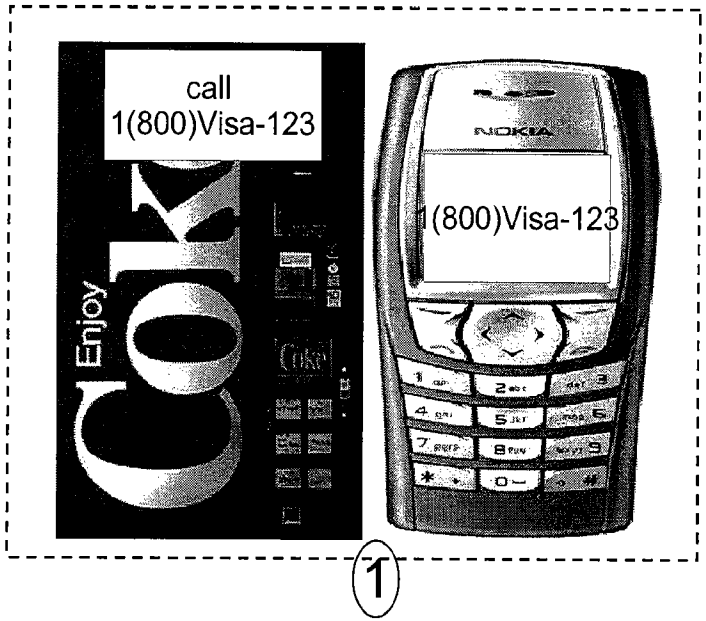
This set up, allows the payment processing organization to remotely tell a vending machine that "payment has been accepted, let consumer make a selection".

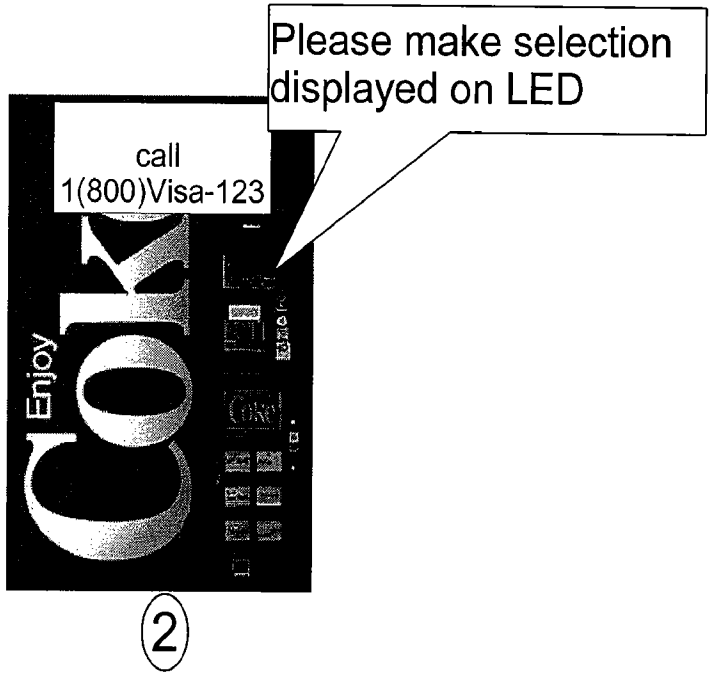
- Equipment needed to do this can be found at http://www.bonusdata.net/IntusJunior/GSMVend/gsmvend.htm
- Once the vending machine has been set up, a consumer can make a vending purchase by contacting the payment processing organization through a variety of channels (Dial/IVR, SMS or GSM)

Visa Confidential

28 Petitioner Exhibit 1002-1423

Consumer vending purchase using Dial/IVR



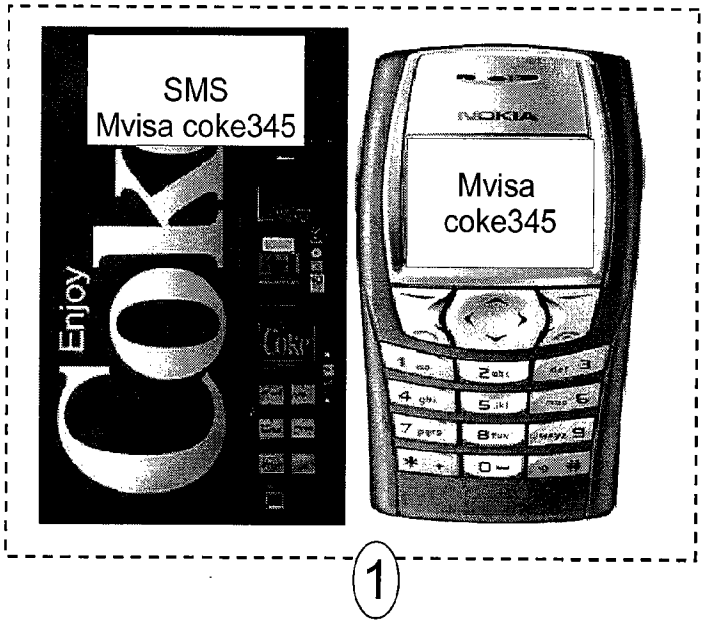


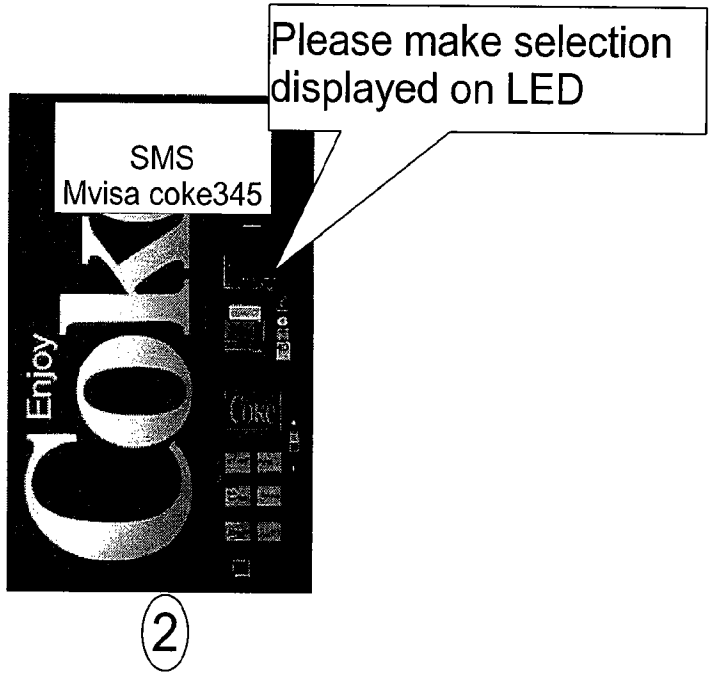
1. The consumer dials the number seen on the vending machine to make a purchase, then follows directions.
2. *A payment processing organization such as Visa authorizes the transaction, and tells the vending machine that payment has been accepted.*
3. *The vending machine display shows the message 'Please choose your product'.*
4. *The customer makes a selection or the credit will timeout after 20 seconds.*
5. *The vending machine returns a vend acknowledge to Visa*
6. *The purchased item will appear on their next statement.*

Visa Confidential

29 Petitioner Exhibit 1002-1424

Consumer vending purchase using SMS



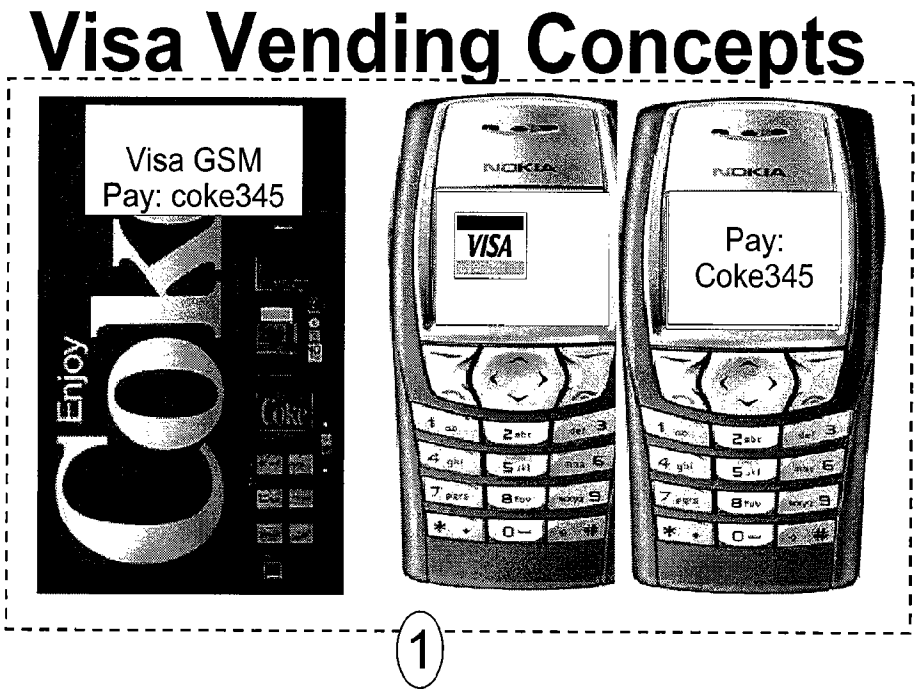


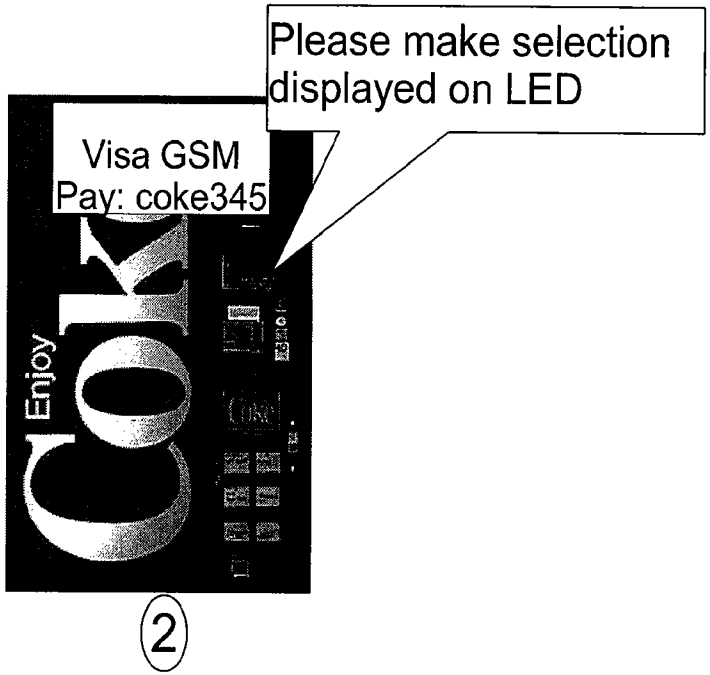
1. The consumer sends an SMS message to the number seen on the vending machine to make a purchase. The consumer gets a automated call back asking for PIN.
2. *Visa authorizes the transaction, and tells the vending machine that payment has been accepted*
3. *The vending machine display shows the message 'Please choose your product'.*
4. *The customer makes a selection or the credit will timeout after 20 seconds.*
5. *The vending machine returns a vend acknowledge to Visa*
6. *The purchased item will appear on their next statement.*

Visa Confidential

30 Petitioner Exhibit 1002-1425

Mobile App
Visa Vending Concepts





1. Using the "machine alias" seen on the vending machine, a consumer uses his mobile wallet to make a vending purchase.
2. *Visa authorizes the transaction, and tells the vending machine that payment has been accepted*
3. *The vending machine display shows the message 'Please choose your product'.*
4. *The customer makes a selection or the credit will timeout after 20 seconds.*
5. *The vending machine returns a vend acknowledge to Visa*
6. *The purchased item will appear on their next statement.*

Visa Confidential

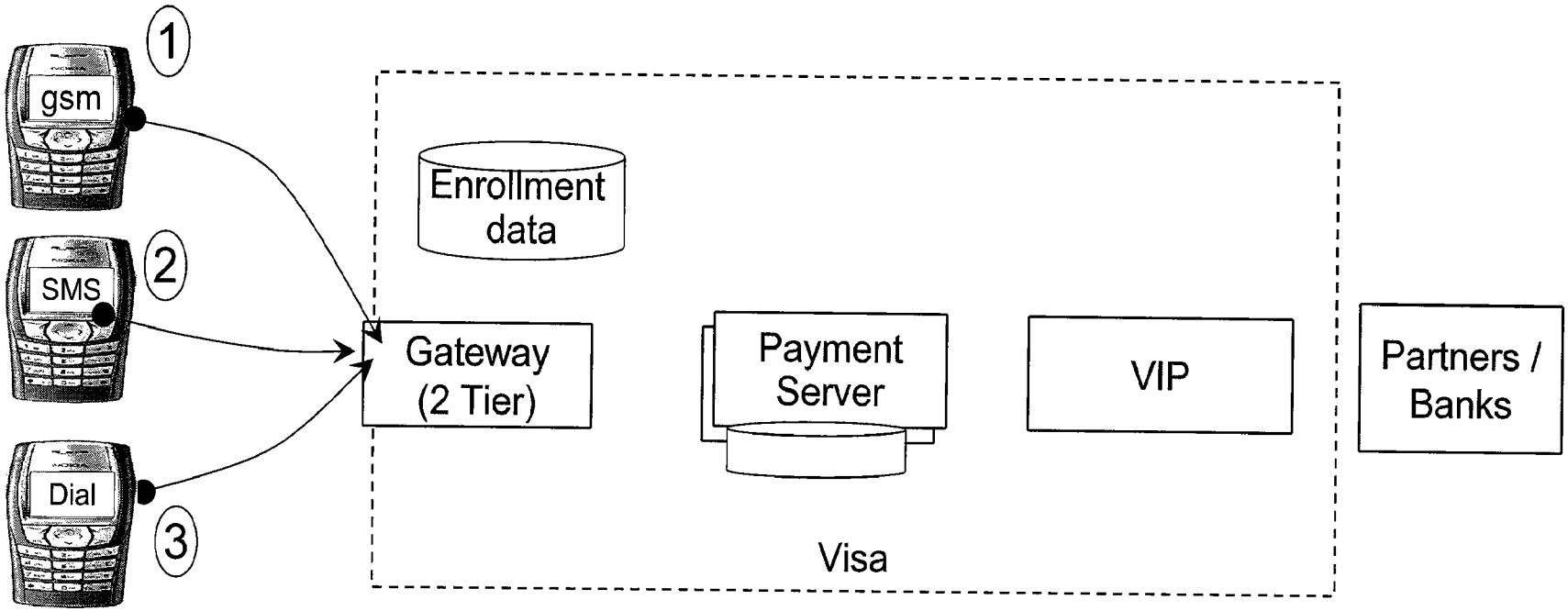
31 Petitioner Exhibit 1002-1426

Payment Flow for Dial, SMS, & Mobile App vending solutions

Visa Confidential

32 Petitioner Exhibit 1002-1427

Request Initiated

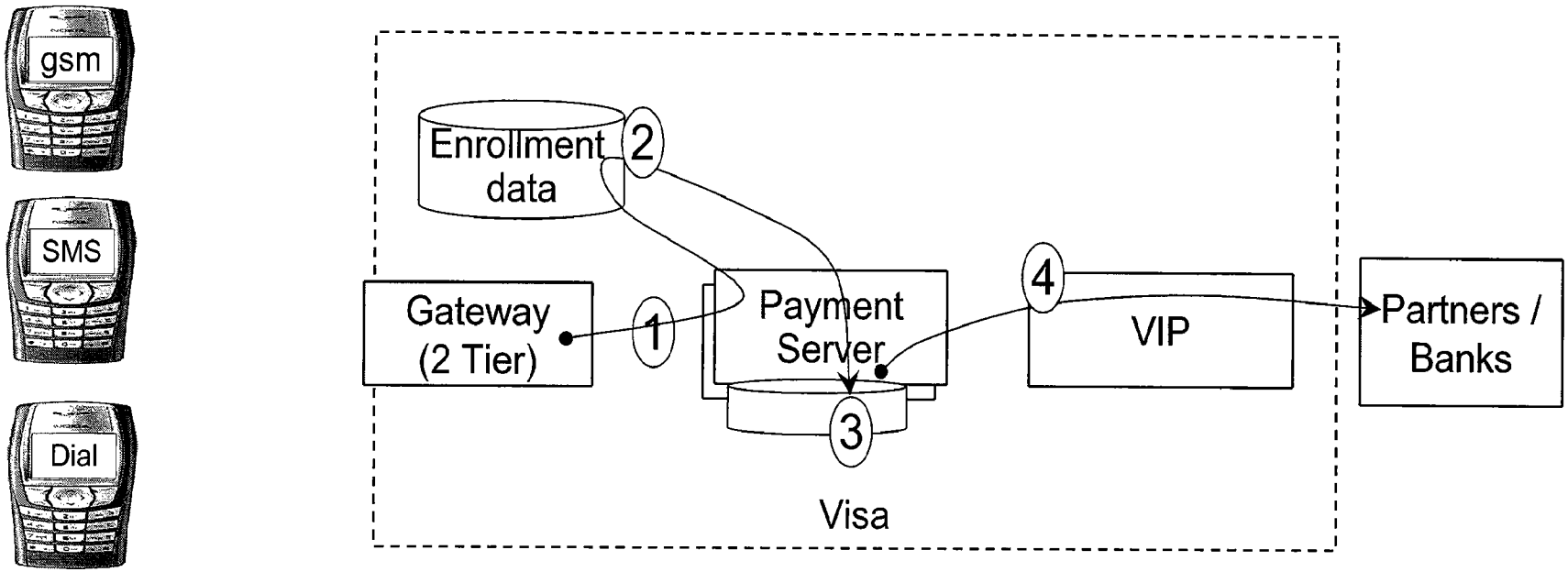


1) Mobile Application. Mobile application connects directly to Visa's mobile gateway
2) SMS. An SMS is passed to the mobile gateway (from an aggregator)
3) Dial. A dial request is passed to the mobile gateway (from IVR system)

Visa Confidential

33 Petitioner Exhibit 1002-1428

Process request

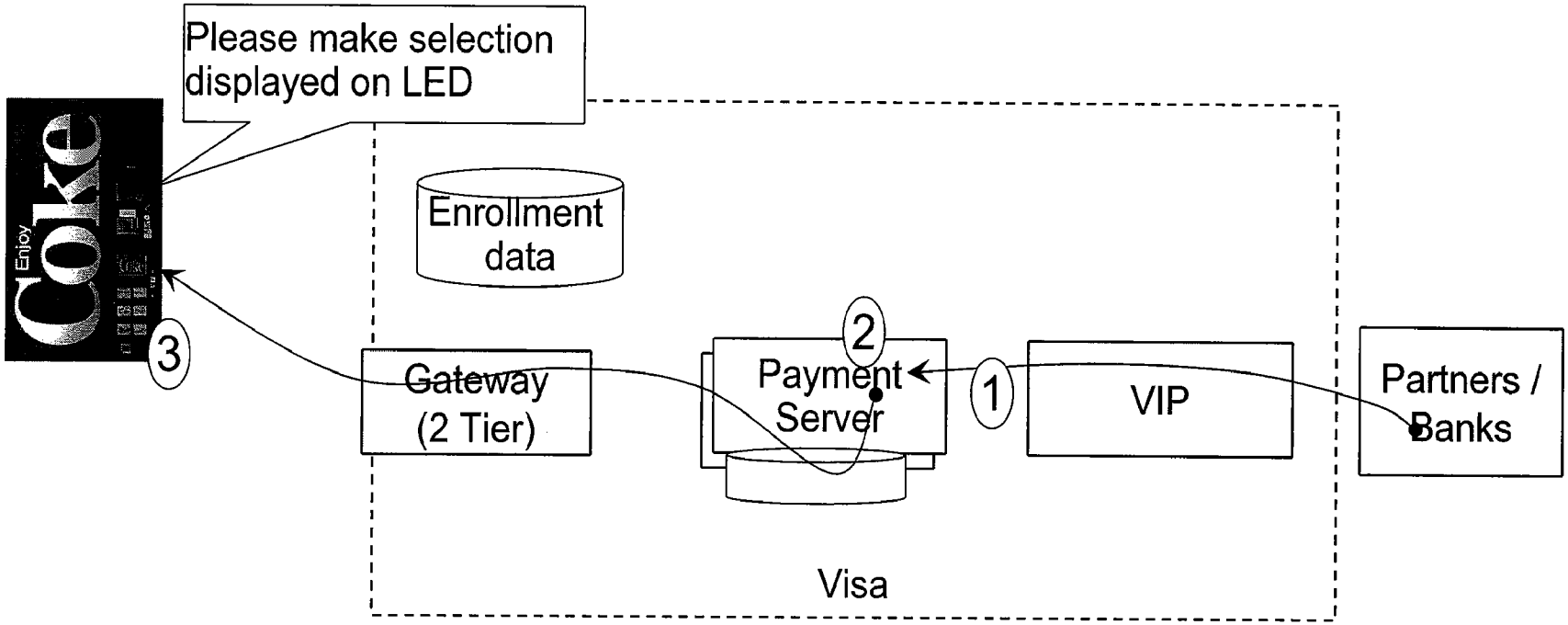


1) The mobile gateway passes the message to the payment server.
2) The payment server validates & augments the message
3) The payment server logs the request
4) The payment server hands the message to VIP where it is formatted and passed to the cardholders issuer.

Visa Confidential

34 Petitioner Exhibit 1002-1429

Process response
Complete vending purchase



1) The Issuer (or VIP/STIP) approves the purchase, and hands the response back to the payment server
2) The payment server logs the response, and sends a message to the vending machine that payment has been accepted.
3) The consumer makes a purchase with in 20 seconds, and the purchase is complete

Visa Confidential

35 Petitioner Exhibit 1002-1430

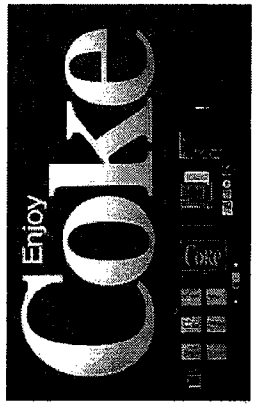
Solution where a payment processing organization such as Visa would probably be indirectly involved

Vending purchases triggered by NFC enable mobile device



36 Petitioner Exhibit 1002-1431

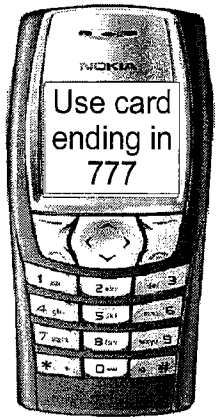
NFC
Vending Concepts



1



2



3



4

1. Provision a vending machine with an NFC reader (http://www.hypercom.com/ has vending smart card solutions)
2. Provision a mobile device with a NFC chip & wallet application
3. Consumer uses application wallet to select which card to purchase drink with
4. Consumer waves the phone in front of the NFC reader in the vending machine.

Visa Confidential

Petitioner Exhibit 1002-1432

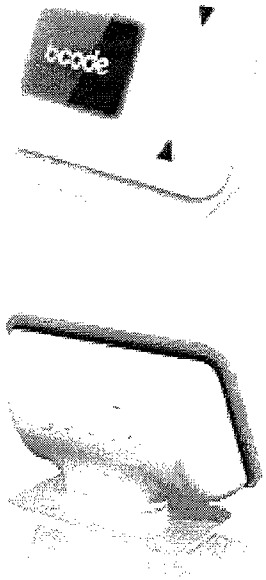
NFC
Details & Notes

- There is a contactless reader in the vending machine
- The contactless reader can be managed by an acquirer like any other POS device
- The transaction flow to Visa is like any transaction on plastic
- The US issue with vending is the need to provide a "paper" receipt.

38

Petitioner Exhibit 1002-1433

Visa Confidential



BCODE

Petitioner Exhibit 1002-1434

Lessons learned

✓2d barcodes are difficult to scan directly off a mobile phone in real world applications due to human factors, lighting, condition of phone, display characteristics of phone.

✓Phone is personal. Customers don't want to hand over their phone to be scanned

✓Some phones won't scan at all.

Look for a scanner that:
✓Can scan coupons that can be passed through SMS messages with no graphics

✓Doesn't require a consumer to hand over their phone

4/6 Petitioner Exhibit 1002-1435

Visa Confidential

What is the difference in coupons?

2D barcode:

✓Graphic. Must be sent by MMS, SMS link or pulled up by an onboard application.

✓Issues Scanning

✓Format is Universal, but issues scanning.

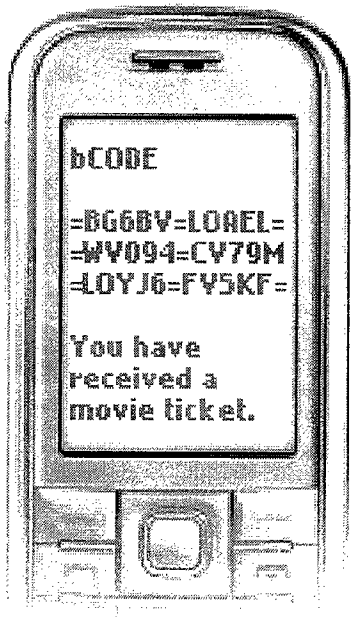


BOCDE barcode:

✓Can be distributed via SMS

✓Claim it can be scanned in 1 second from any orientation

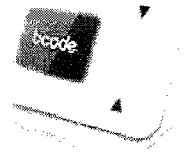
✓Format is proprietary, but requires special terminal



Visa Confidential

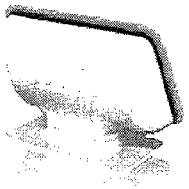
41 Petitioner Exhibit 1002-1436

Single POS set up



USB Connection





BCode scanning terminal supplied by BCode

Guckenheimer's Micros POS - Windows based

Terminal Driver

Laptop running windows XP supplied by Visa. One would sit under each check out counter, dedicated to each POS.

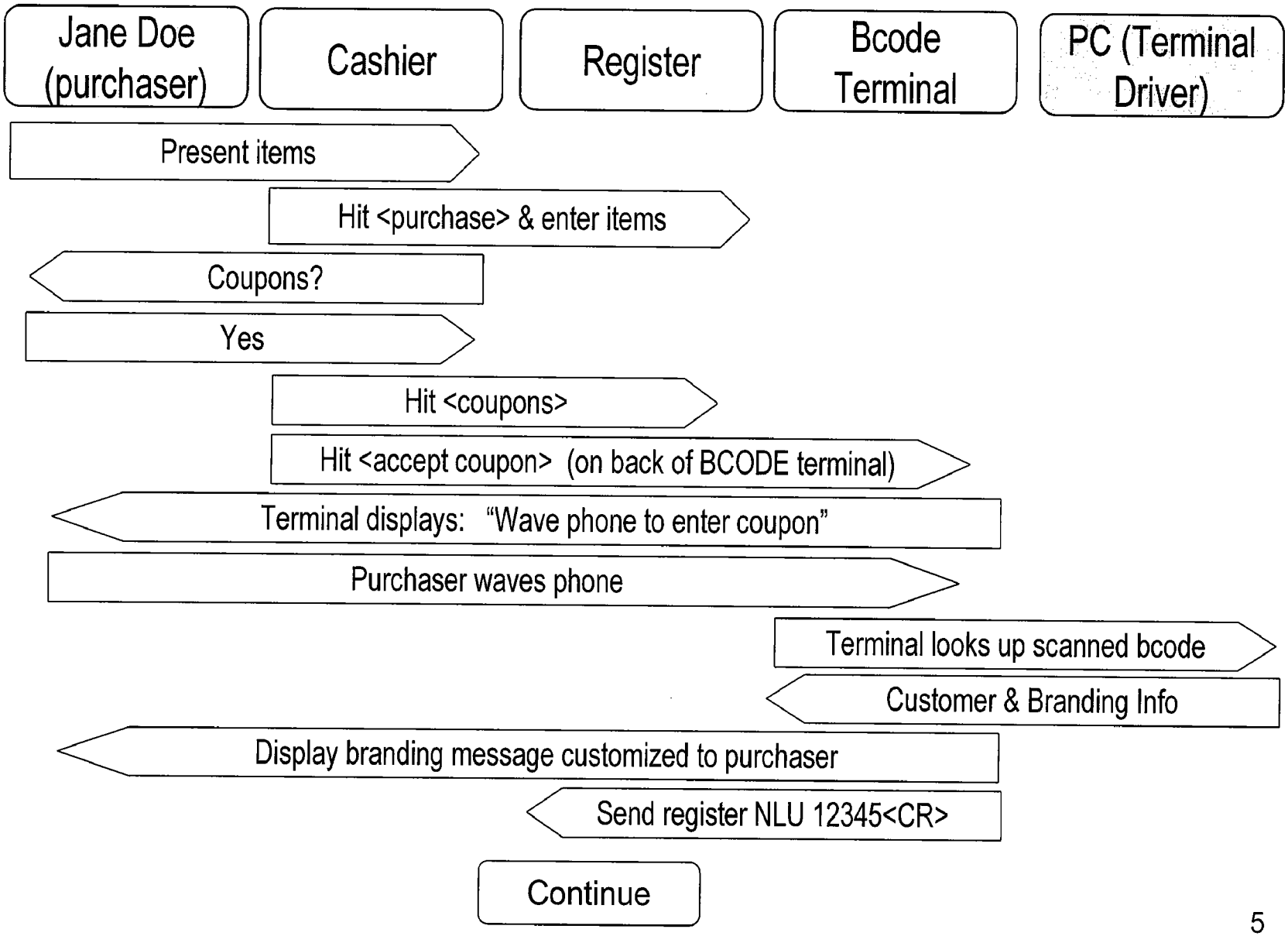
Customer DB. 500 to 1000 employees.

<Bocde/NLU>	12345
<First Name>	Mark
<Customer Greeting>	Enjoy your Coffee, thanks for using your Visa
<wallpaper>	Visa.jpg

Visa Confidential

42 Petitioner Exhibit 1002-1437

Proposed Path



Visa Confidential

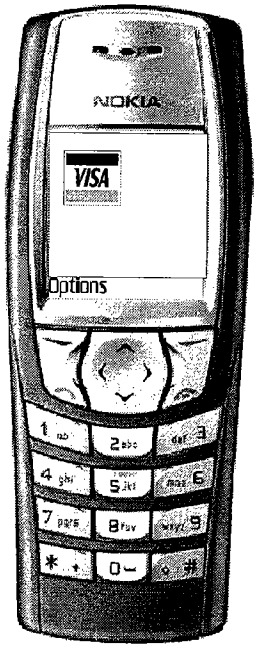
43 Petitioner Exhibit 1002-1438

Account Balance Inquiry
Rewards Balance Inquiry

44 Petitioner Exhibit 1002-1439

Channel Options





Option 1: SMS Based

- On nearly every phone already
- Fast to Pilot
- SMS charge for every msg

Option 2: Application on the phone

- More control over transaction and user experience
- Requires provisioning
- Requires user to have GPRS/GSM service
- Secure
- No SMS charges
- Faster Response

45
Petitioner Exhibit 1002-1440

Good For:

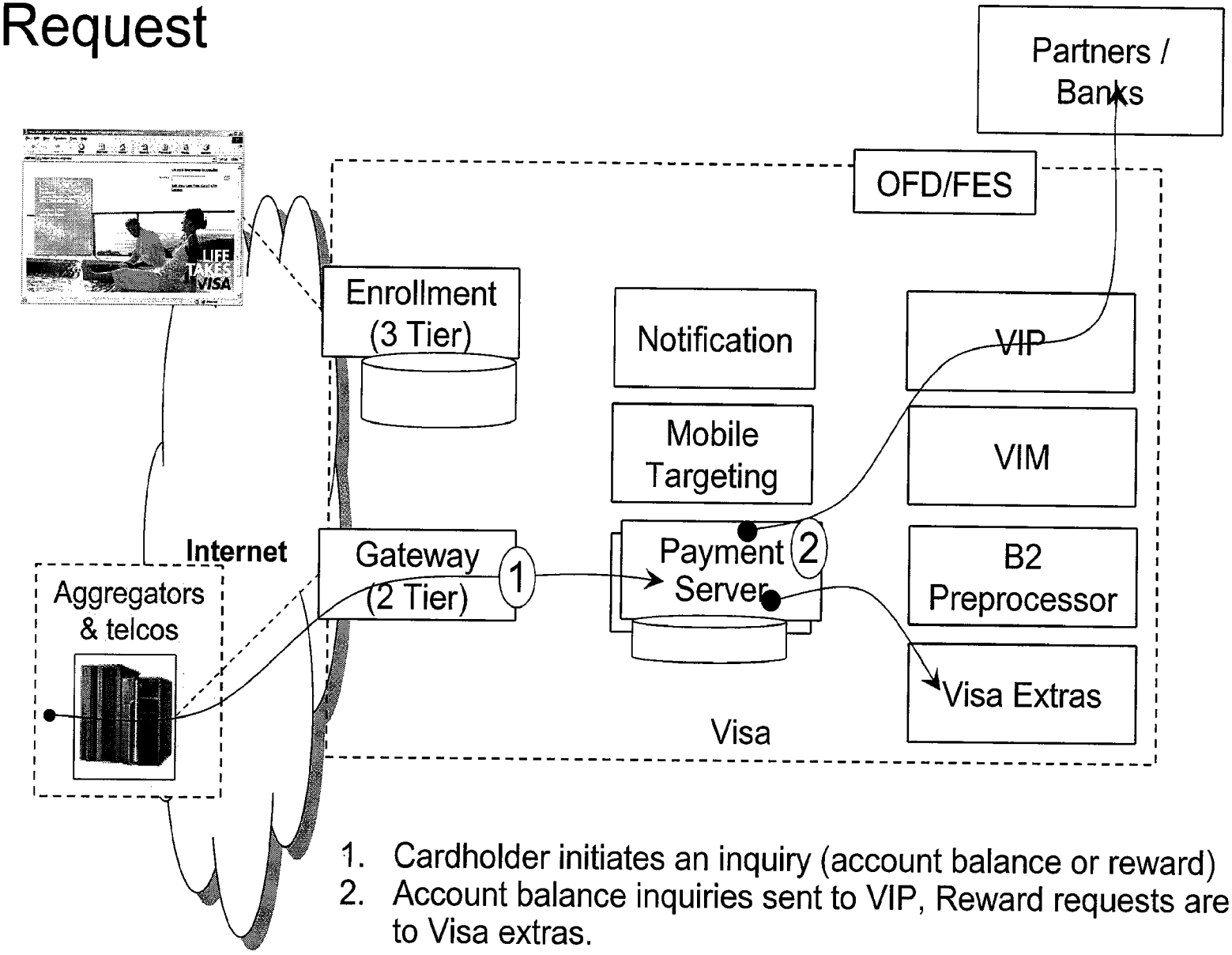
A quick way for a cardholder to check:

- Account Balance & Credit Remaining
- Rewards balance

- *Post pilot, this channel can be "plumbed" to any rewards system to provide reward balance*

46 Petitioner Exhibit 1002-1441

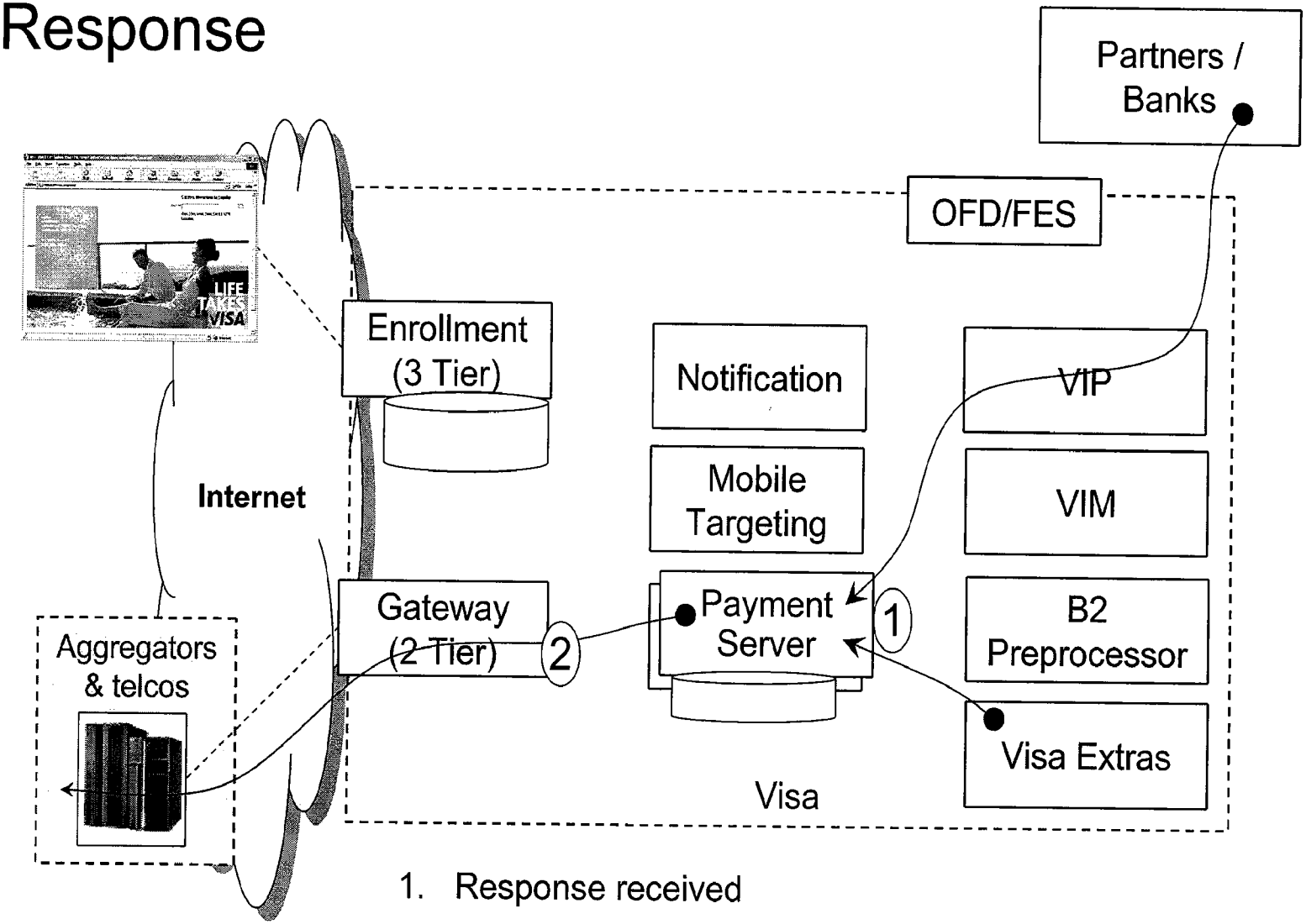
Inquiry Pilot Request



1. Cardholder initiates an inquiry (account balance or reward)
2. Account balance inquiries sent to VIP, Reward requests are sent to Visa extras.

47 Petitioner Exhibit 1002-1442

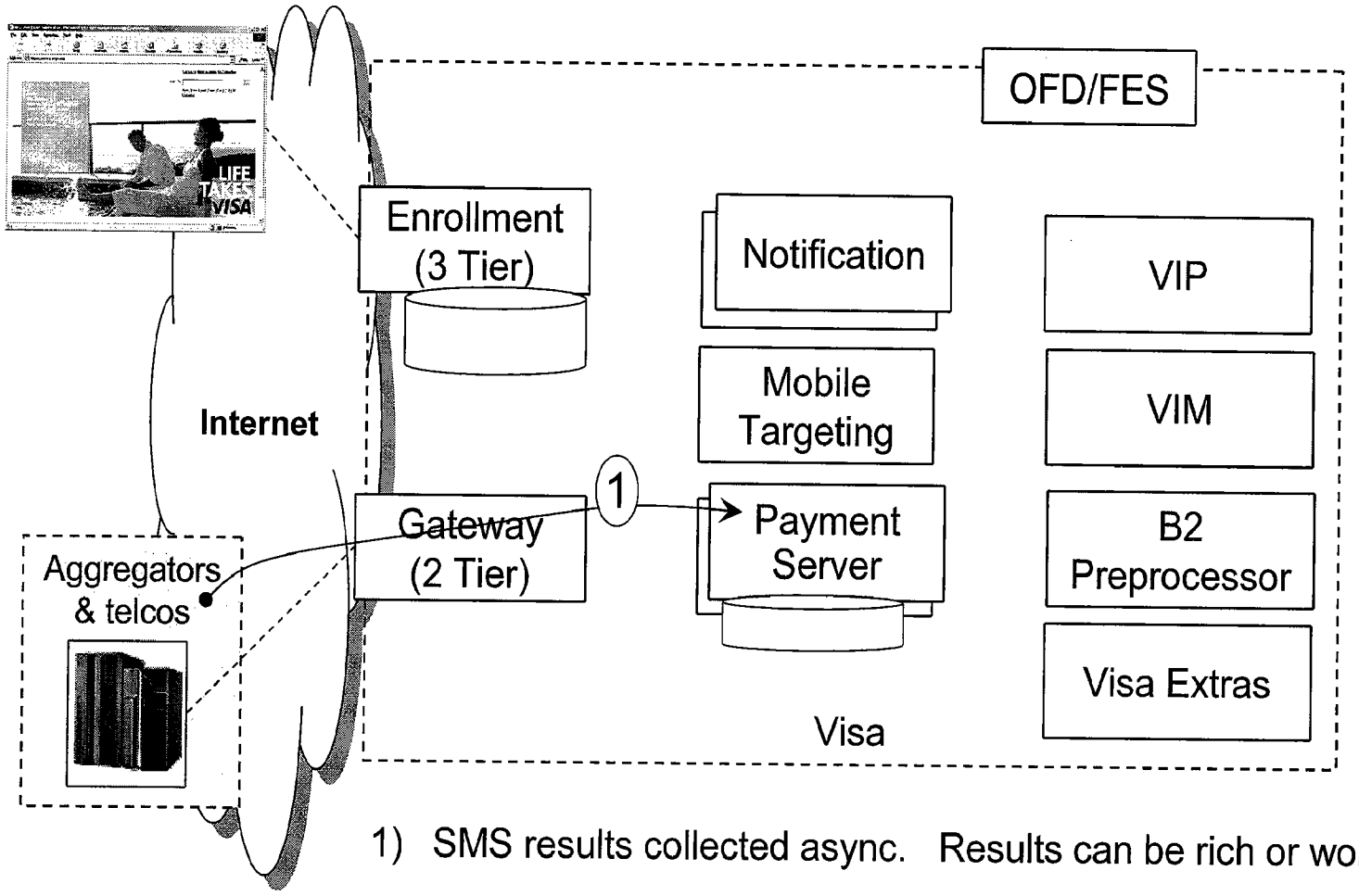
Inquiry Pilot Response



1. Response received
2. Passed back to cardholder

4 8 Petitioner Exhibit 1002-1443

Inquiry Pilot
Collect results



1) SMS results collected async. Results can be rich or worthless.

49 Petitioner Exhibit 1002-1444

Identity Fraud Notification

Petitioner Exhibit 1002-1445

How can the consumer notified?
Notification Channels





Notification Channel available with in seconds of transaction

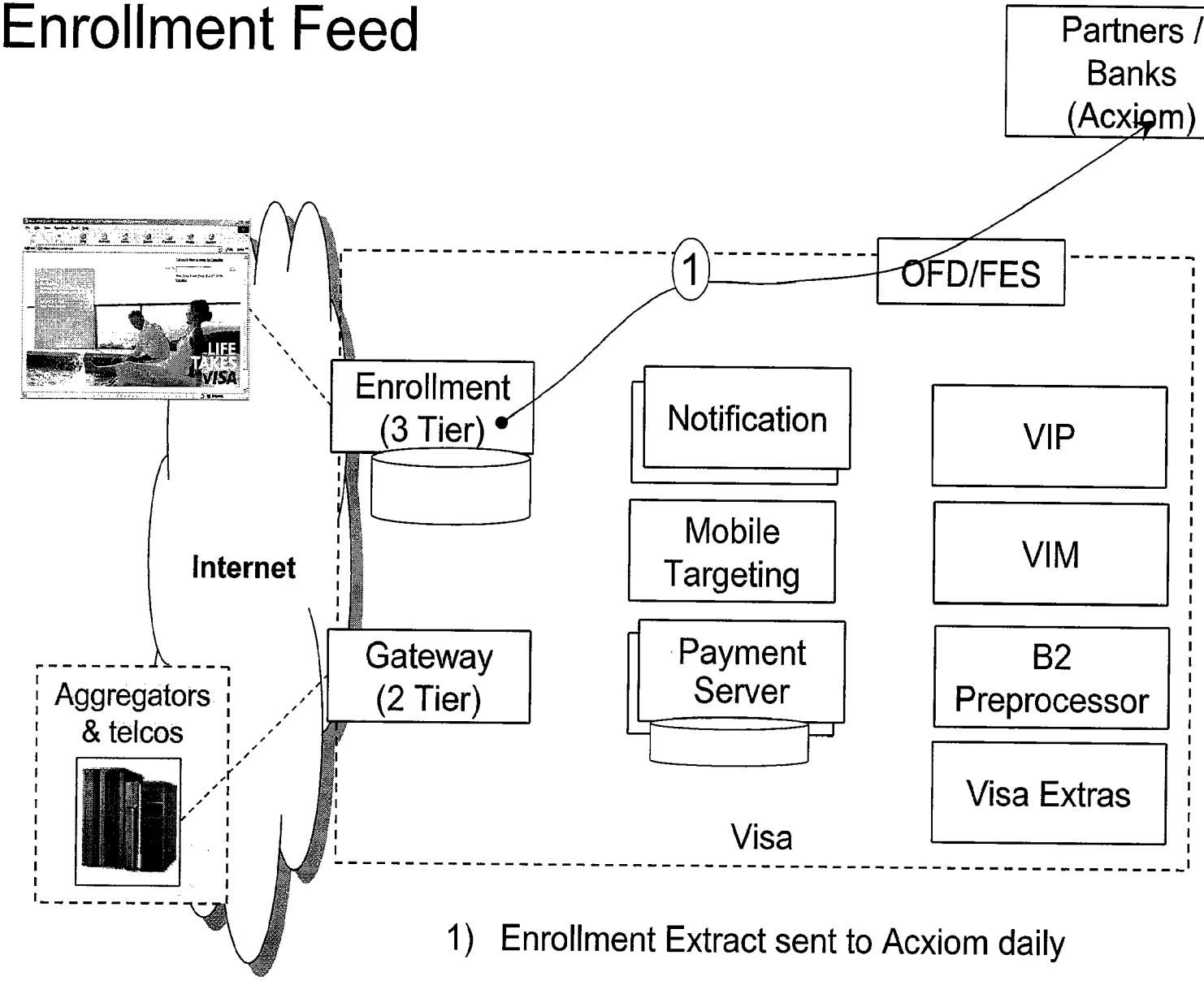
- **SMS (Mobile)**
- **Instant Message**
- **Voice**

Slower notifications:

- **E-mail**
- **Fax**

Petitioner Exhibit 1002-1446

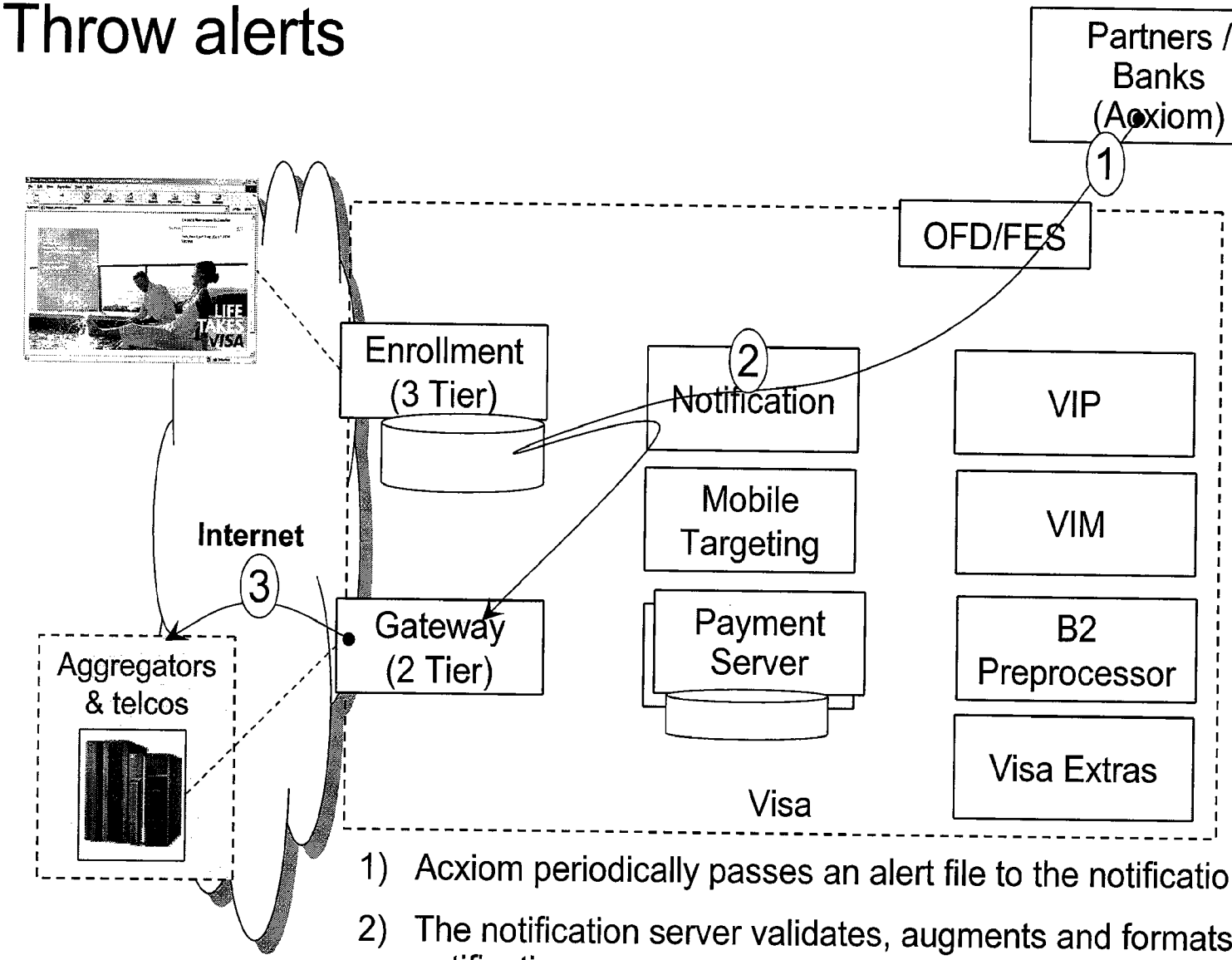
Identity Fraud Notification Pilot Enrollment Feed



1) Enrollment Extract sent to Acxiom daily

52 Petitioner Exhibit 1002-1447

Identity Fraud Notification Pilot
Throw alerts

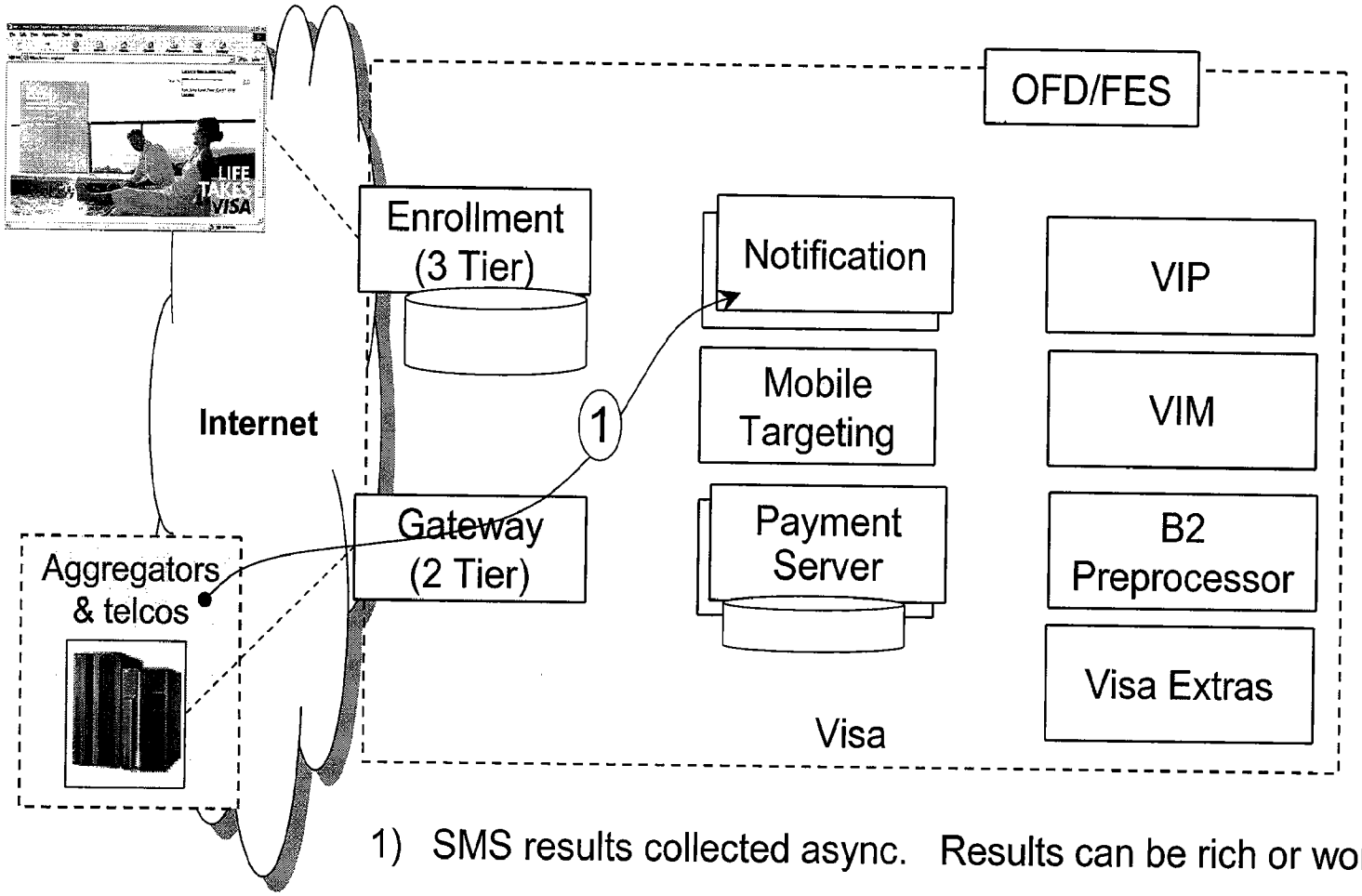


1) Acxiom periodically passes an alert file to the notification server
2) The notification server validates, augments and formats notification messages.
3) Notification alerts sent (SMS, IM, e-mail, Voice, etc.)

53 Petitioner Exhibit 1002-1448

Identity Fraud Notification Pilot
Collect results

Partners / Banks (Acxiom)



1) SMS results collected async. Results can be rich or worthless.

54 Petitioner Exhibit 1002-1449

3rd Party - Batch Notification

Acxiom

OFD

Mobile Gateway

Aggregator

Channel Providers

John doe

3rd party sends a properly formatted batch of alerts to OFD

OFD passes alert file to the mobile gateway (Batch Interface)

Mobile gateway hands individual messages to Aggregator. John Doe is notified via SMS, e-mail, voice, etc.



Delivery Results (Asynchronous)

Delivery results are collected, bundled and passed back to OFD

3rd Party receives Notification results

Petitioner Exhibit 1002-1450

Mobile Notification

Background
What can trigger a notification?

Anything, is up to the business

- A qualifying visa transaction has been made
- A spending threshold has been reached
- An online account has been accessed
- John Doe has badged into a server room
- Your online banking account has just been accessed
- Consumer elected Reminder:
  - ✓ a payment is due with in x days
  - ✓ a payment is overdue
- Employee has made a corporate card or p-card
- Child or spouse has made a transaction
- An issuer, or merchant system

For 811616, VIP will be the triggering system.

57 Petitioner Exhibit 1002-1452

Assumptions

- ***This is a starting point . . .***

  - ✓ **Enrollment file may come from a member**
  - ✓ **Enrollment file may come from our own enrollment server as part of a different project.**

  - ✓ **Cardholders may have multiple notification channels**

Petitioner Exhibit 1002-1453

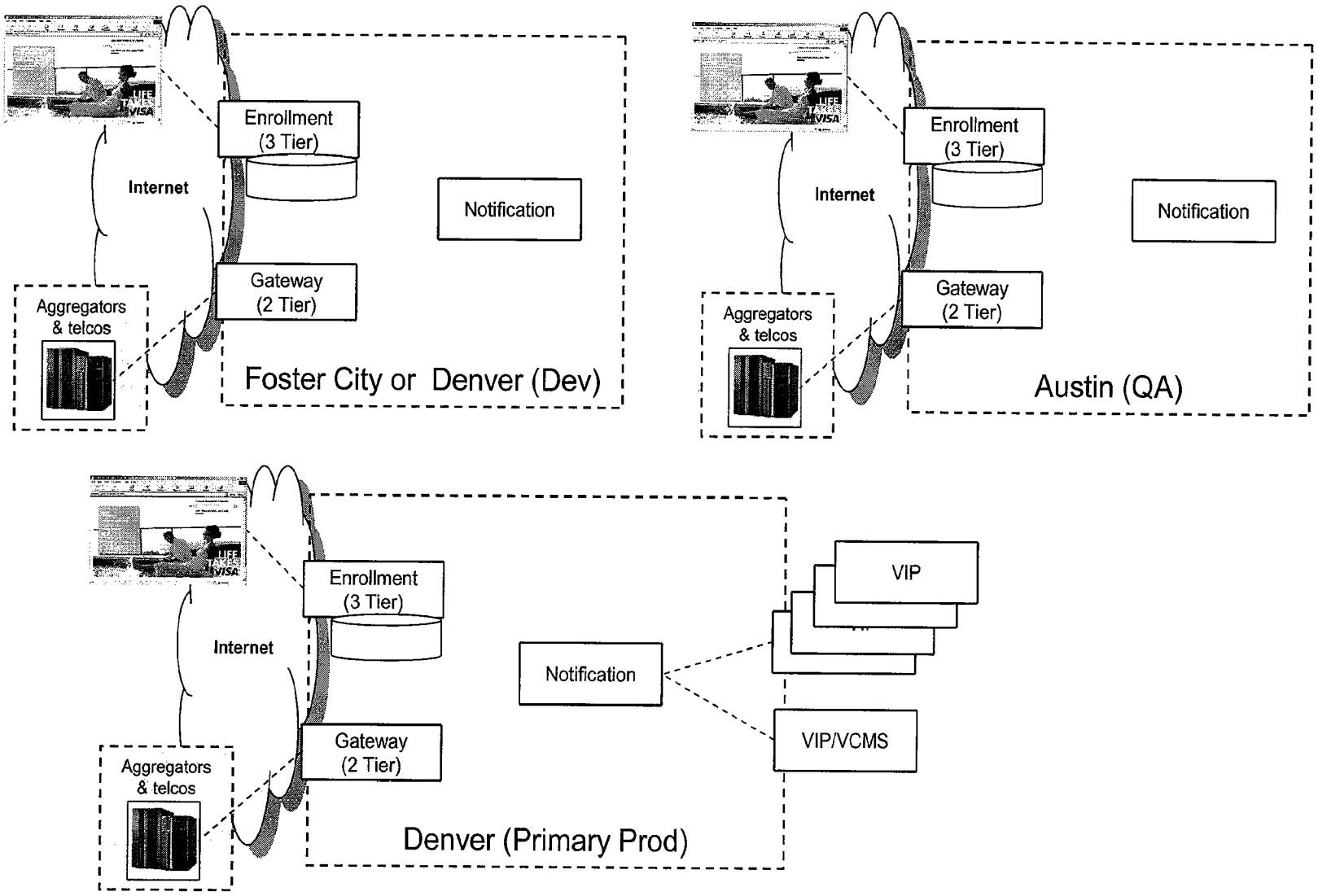
Vision

Vision:

- **Get alerts to a cardholder as quickly as possible.**
- **Try to get alerts fast enough to stop a second back to back fraudulent purchase.**
- **In the future, make this a robust service, and add in issuer banks as triggering systems.**
- **Alerts for pilot are SMS and e-mail**

Petitioner Exhibit 1002-1454

Notification Environment



Petitioner Exhibit 1002-1455

Current Triggers

1. Ticket size
2. ATM Cash MCC equal to 6011 and a cash withdrawal message
3. Other Cash = MCC not equal to 6011 and a cash withdrawal message
4. Other Purchase = used as default if no other MCG group is applicable
5. Risky Purchase - An internal table maintained by Visa of risky merchant MCCs is used to determine this grouping
6. Airlines
7. Lodging
8. Auto Rental
9. Restaurants
10. Mail/phone order - If when F25 = 08 and or F60.8 = 01 --- regardless of the actual MCC value
11. Medical

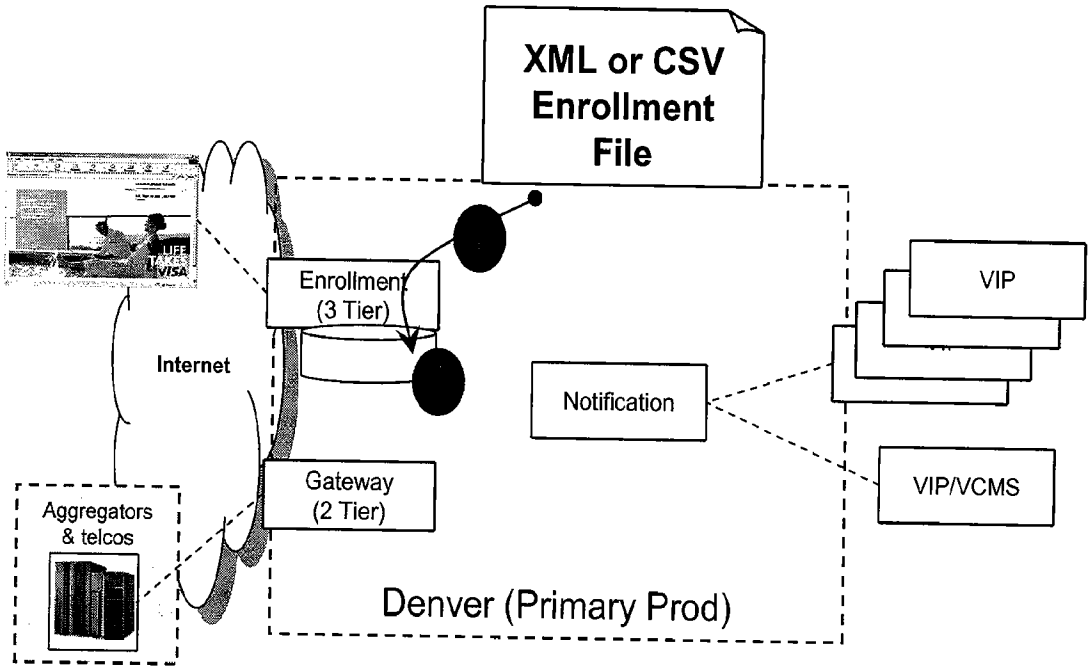
61 Petitioner Exhibit 1002-1456

Enrollment Data

<Name>Mark Carlson
<CC>xxxx xxxx xxxx 6666
<Sub CC>3234890147534545
<Mobile 1>650-888-xxxx
<Mobile 2>650-888-yyyy
<email 1> carlson@visa.com
<email 2> carlson@inovant.com
<Trigger 1 (Amt)>
<Alert channel>Mobile 1, Mobile 1, e-mail 1, email 2
<$>10
<Notification msg>Mark, **<$amt>** was charged to your account ending 6666. Please contact 800-888-Visa if this is incorrect.
<Trigger 2 (ATM)>
<Alert channel>Mobile 1
<Notification msg>Mark, a ATM cash transaction for **<$amt>** was charged to your account ending 6666. Please contact 800-888-Visa if this is incorrect.
<Trigger 5 (Risky)>
<Alert channel>Mobile 1, Mobile 1, e-mail 1, email 2
<Notification msg>Mark, a Risky transaction for **<$amt>** was charged to your account ending 6666. Please contact 800-888-Visa if this is incorrect.
<Trigger 10 (MOTO)>
<Alert channel>Mobile 1
<Notification msg>Mark, a mail order / telephone order transaction for **<$amt>** was charged to your account ending 6666. Please contact 800-888-Visa if this is incorrect.

62 Petitioner Exhibit 1002-1457

Use Case 1
Enrollment Data

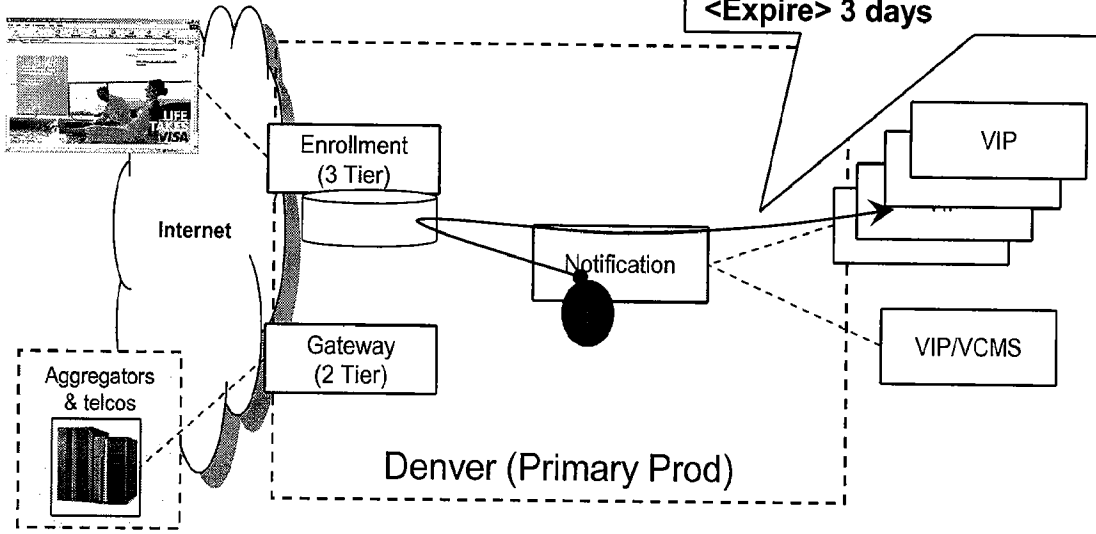


1. **Enrollment file (from Kris/Pat) will be manually staged to the enrollment server (**
2. **Data will be inserted into the enrollment DB (encrypted)**

63 Petitioner Exhibit 1002-1458

Use Case 2
Distribute Trigger Records

FTP to local VIP
<CC>Add/Replace
<CC>xxxx xxxx xxxx 6666
<Sub CC>3234890147534545
<Trigger 1 (Amt)>
<$>10
<Trigger 2 (ATM)>
<Trigger 5 (Risky)>
<Trigger 10 (MOTO)>
<Expire> 3 days



For Pilot

- **Each evening, the enrollment DB will be scanned.**
- **A full replacement will be handed to the local VIP (FTP)**

Post Pilot

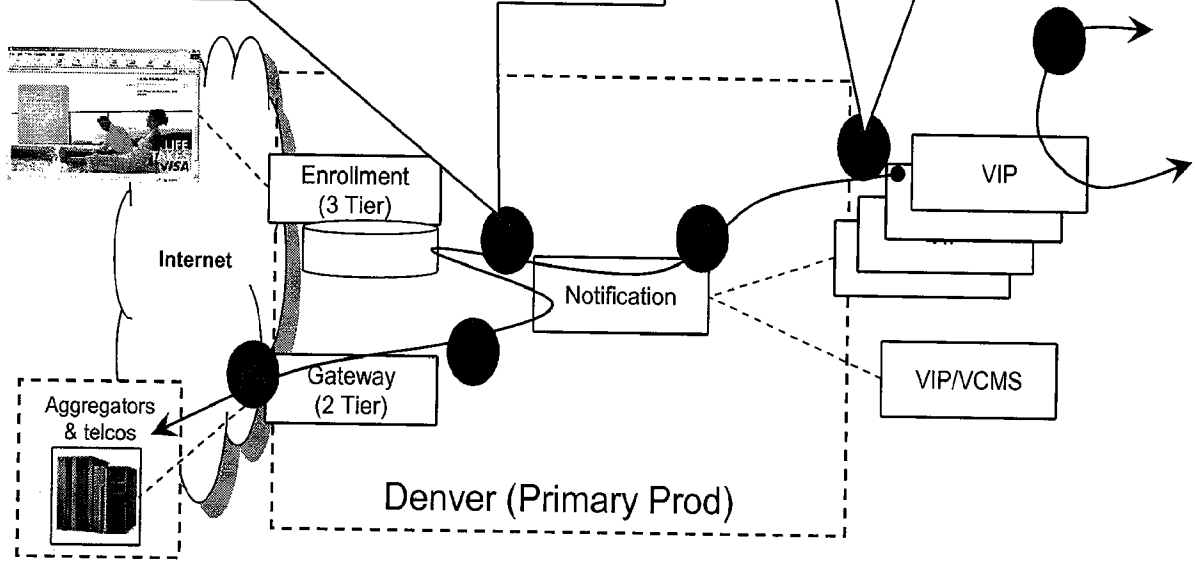
Instead of daily, updates can be on demand, and done on a record by record basis

64 Petitioner Exhibit 1002-1459

Use Case 3
VIP Alert

<Mobile 1>650-888-xxxx
<Mobile 2>650-888-yyyy
<email 1> carlson@visa.com
<email 2> carlson@inovant.com
<Notification msg>Mark, **<$99.00>** was just charged to your account ending 6666. Please contact 800-888-Visa if this is incorrect.

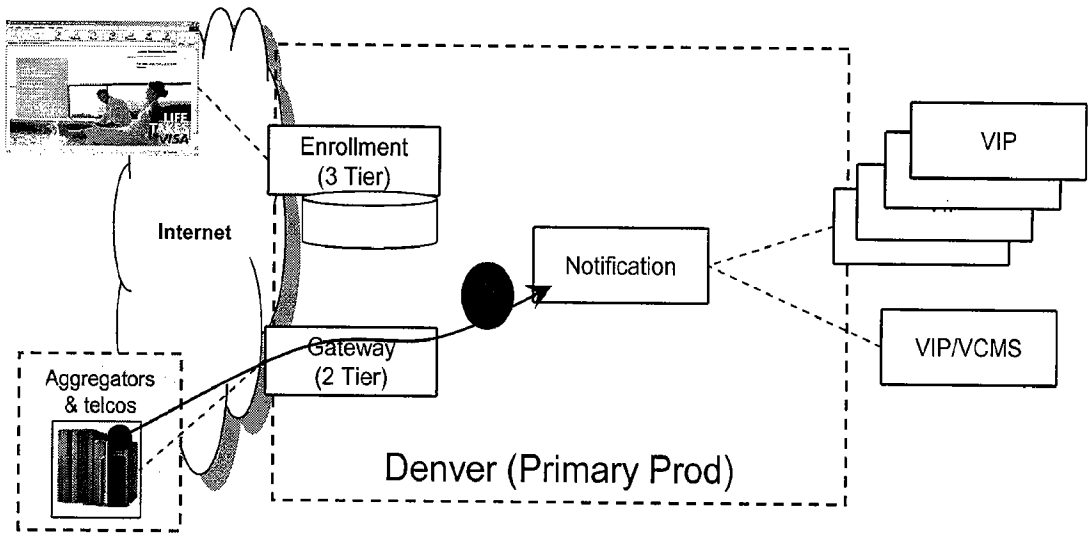
MQ to notification server
<Sub CC>3234890147534545
<Trigger 1 (Amt)>
<$>99.00



1. Any VIP detects a transaction over threshold.
2. VIP creates a notification record, and puts it on a MQ channel to the notification server
3. The notification server reads the notification record
4. The notification server verifies the consumer is still receiving alerts, formats a message and then passes it to the
5. Notification server hand passes the message to the mobile gateway
6. Gateway sends the appropriate alert

65 Petitioner Exhibit 1002-1460

Use Case 4
Collect Results



1. Results are sent async to the notification server.

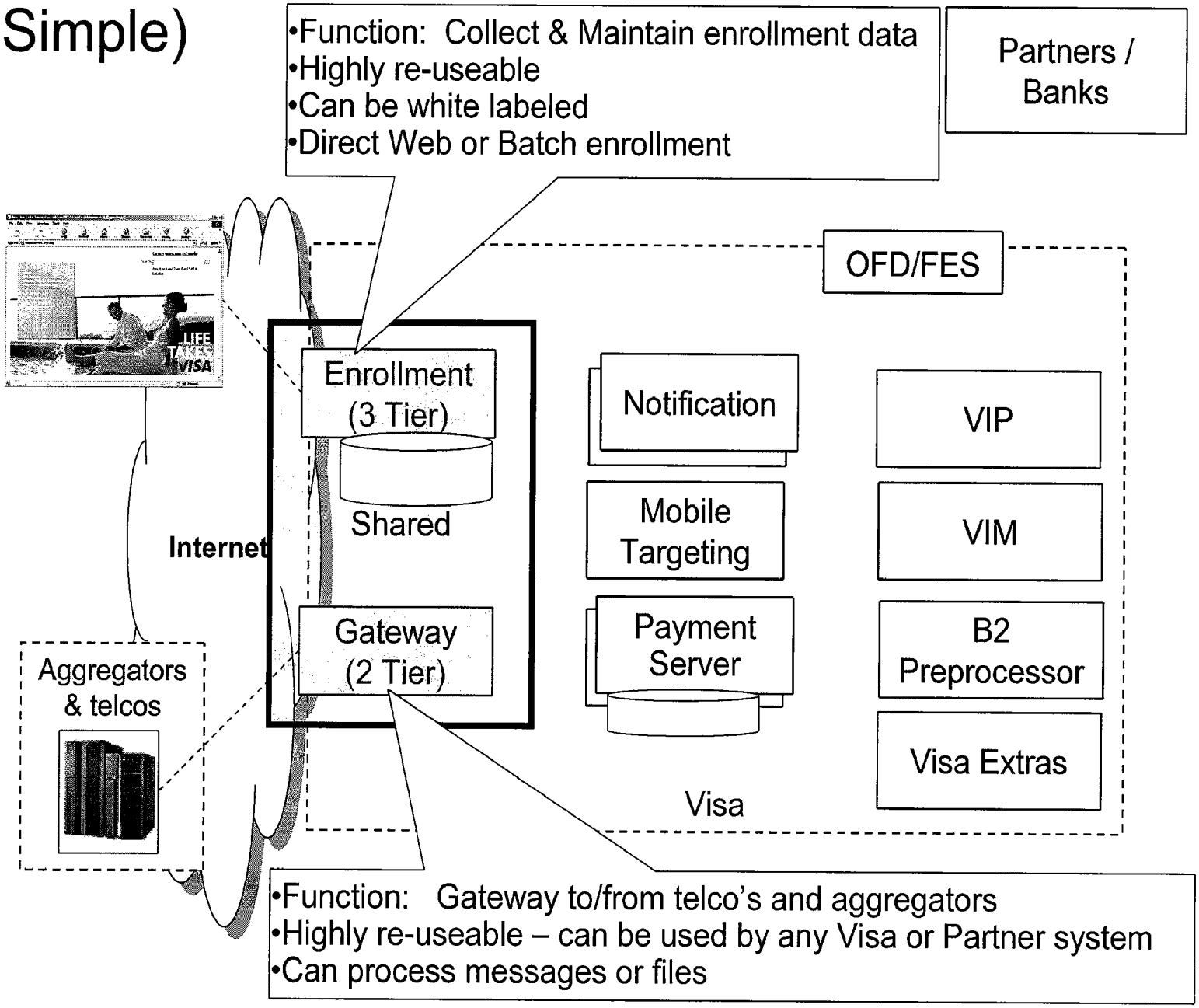
Future: If not delivered, can retry, or try a different channel.
Results can be used for reporting, billing, augmenting enrollment DB, etc.

Petitioner Exhibit 1002-1461

Mobile Parts

Petitioner Exhibit 1002-1462

Topology (Simple)

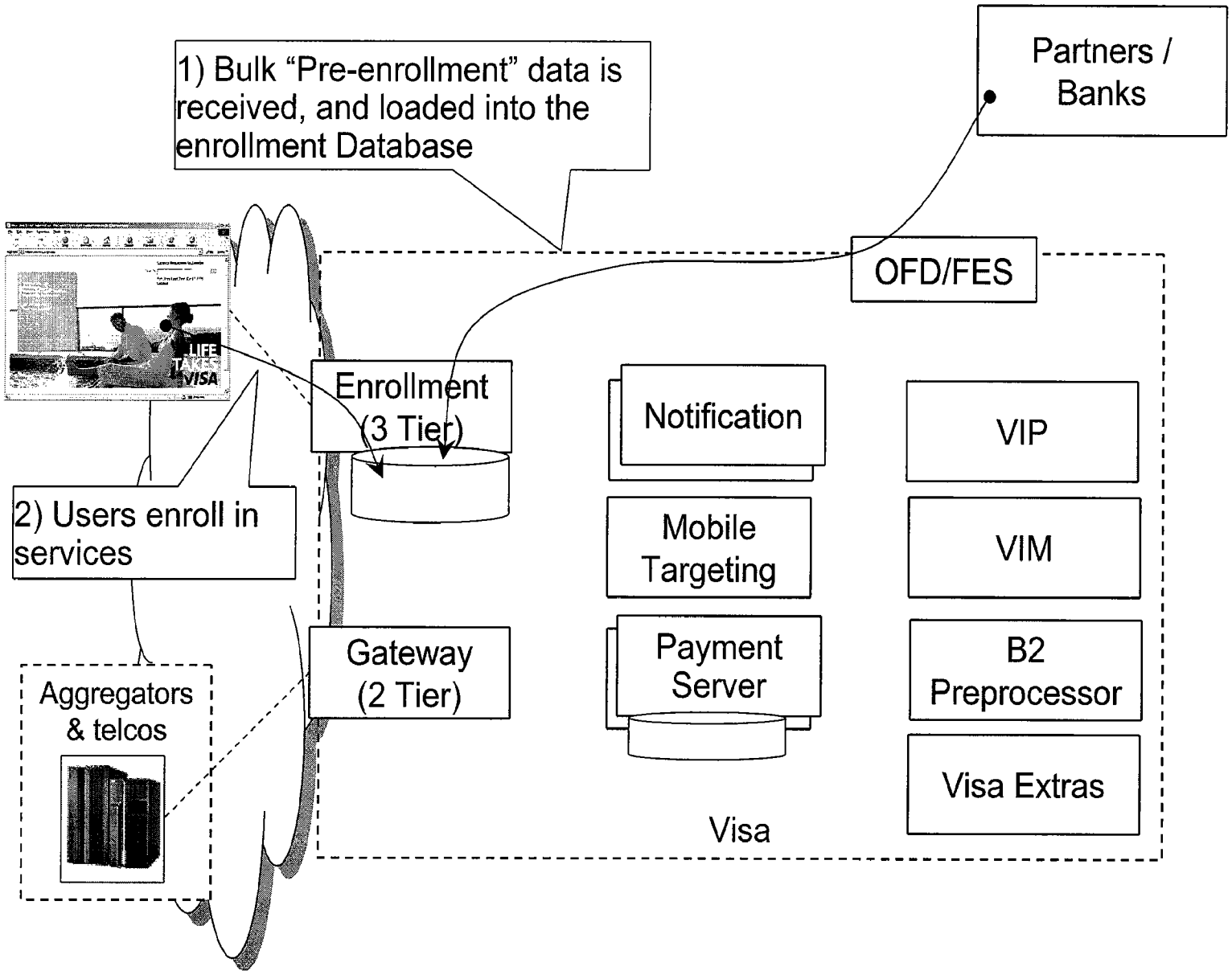


68 Petitioner Exhibit 1002-1463

Enrollment

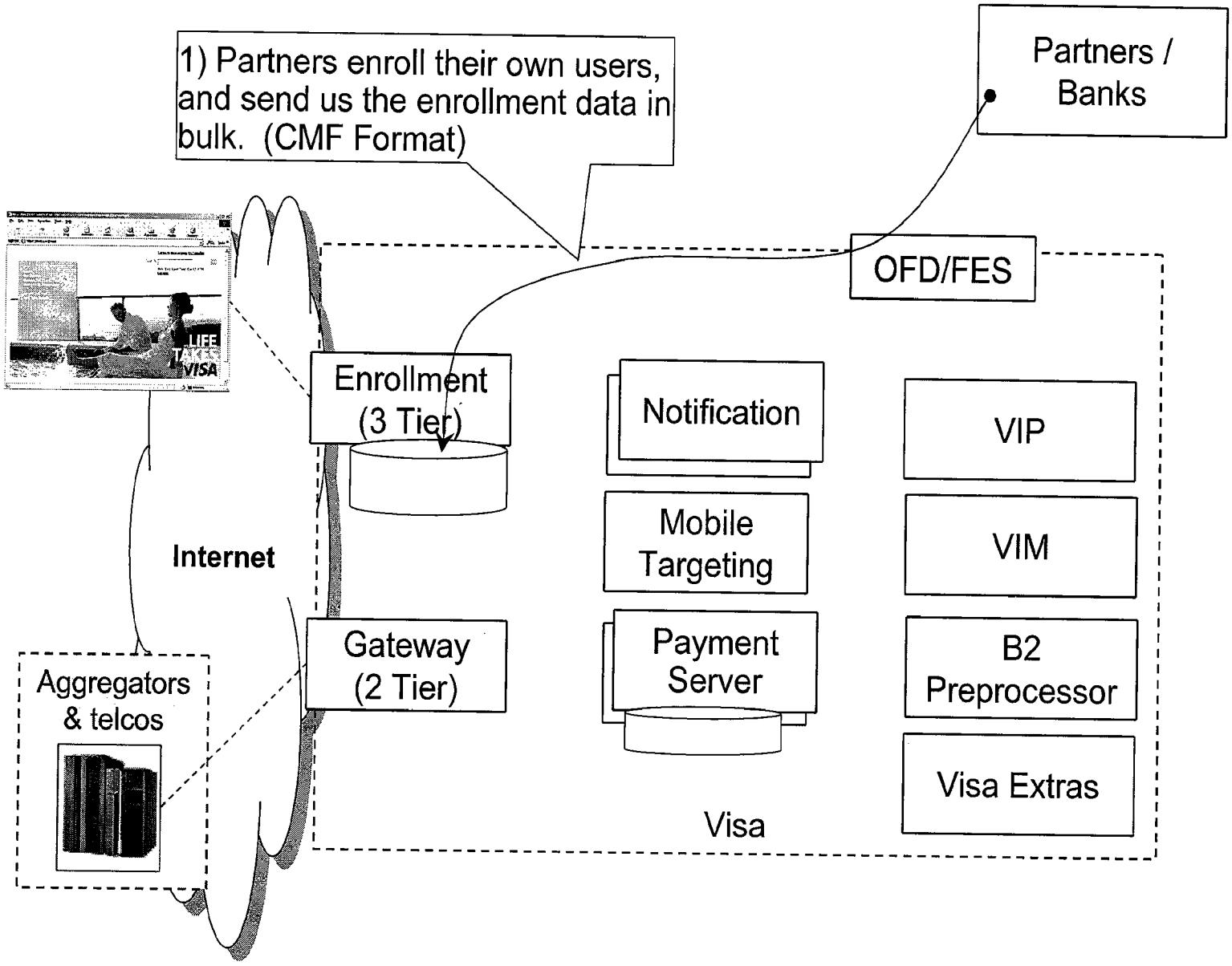
69 Petitioner Exhibit 1002-1464

User Enrollment



Petitioner Exhibit 1002-1465

Batch Enrollment

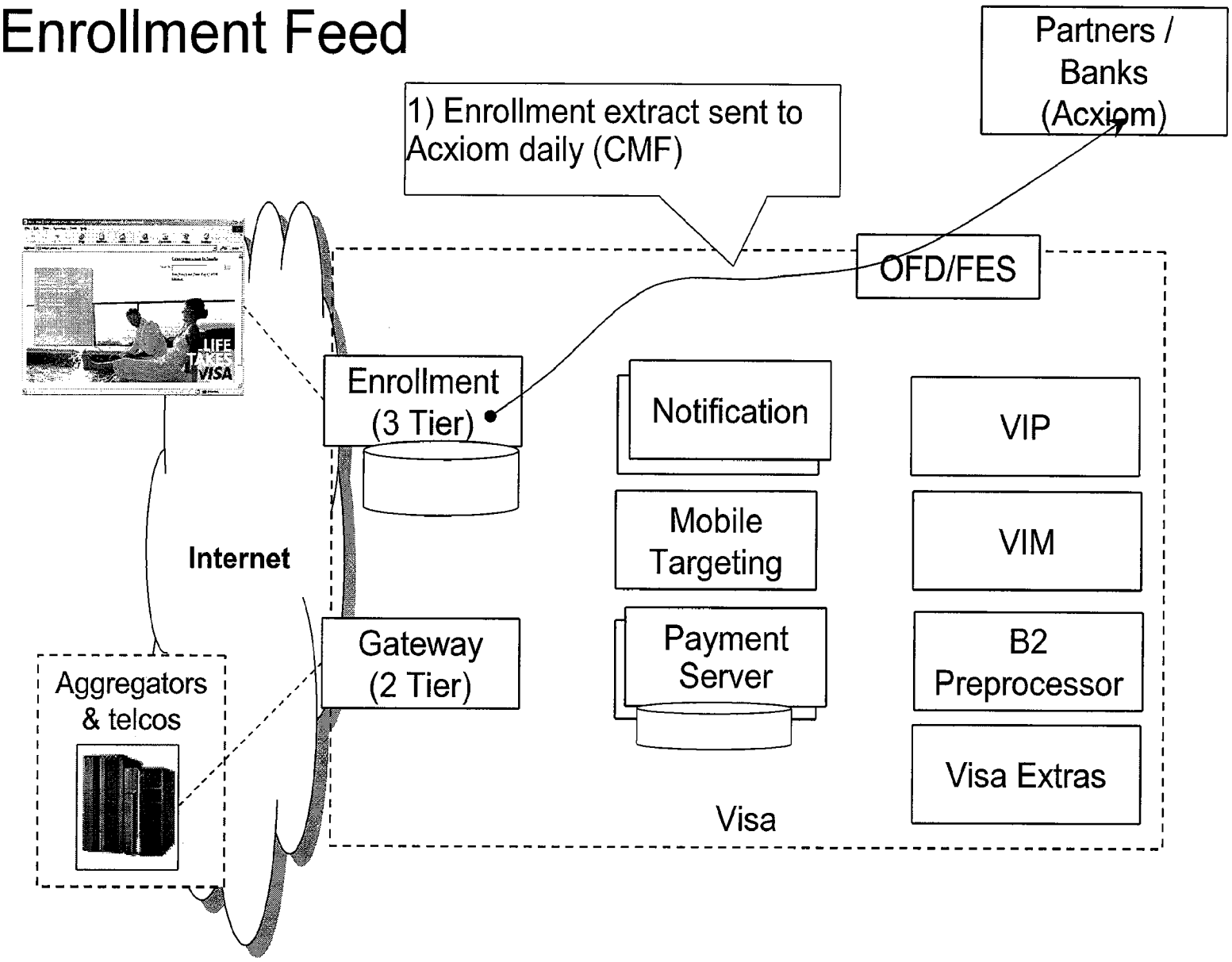


74 Petitioner Exhibit 1002-1466

Acxiom Notification (Pilot)

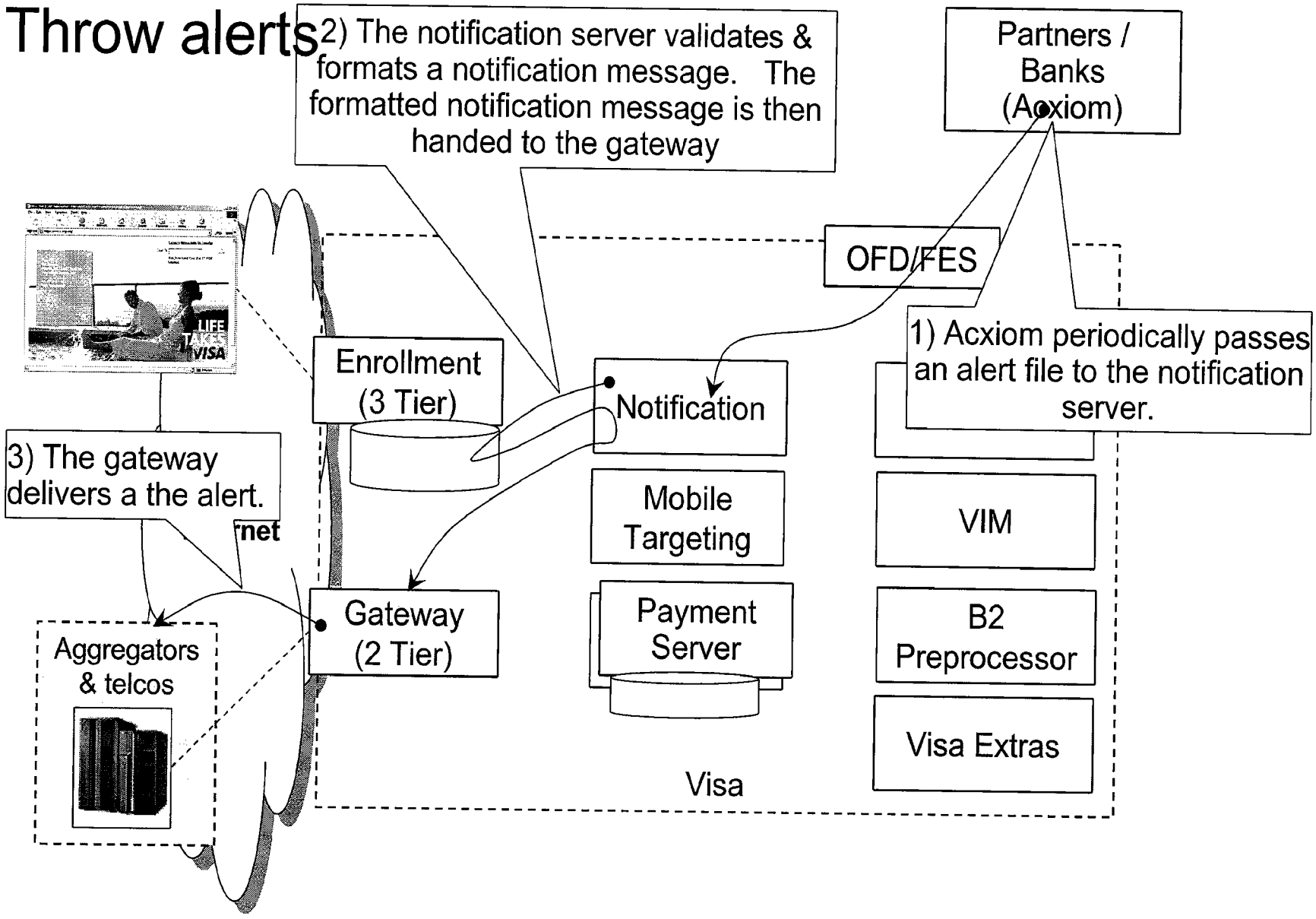
72 Petitioner Exhibit 1002-1467

Acxiom Notification Pilot Enrollment Feed



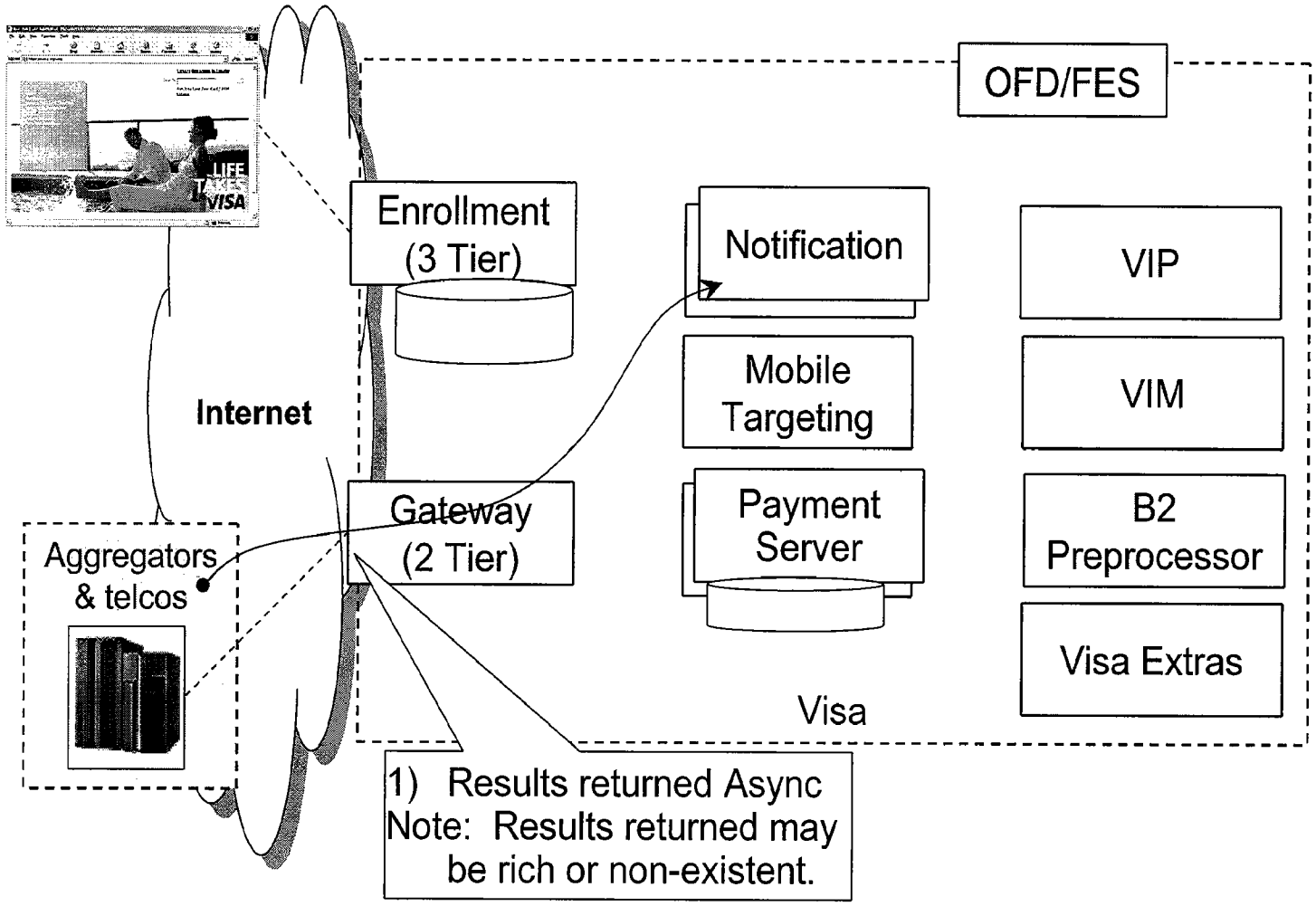
73 Petitioner Exhibit 1002-1468

Acxiom Notification Pilot
Throw alerts



74 Petitioner Exhibit 1002-1469

Acxiom Notification Pilot
Collect results

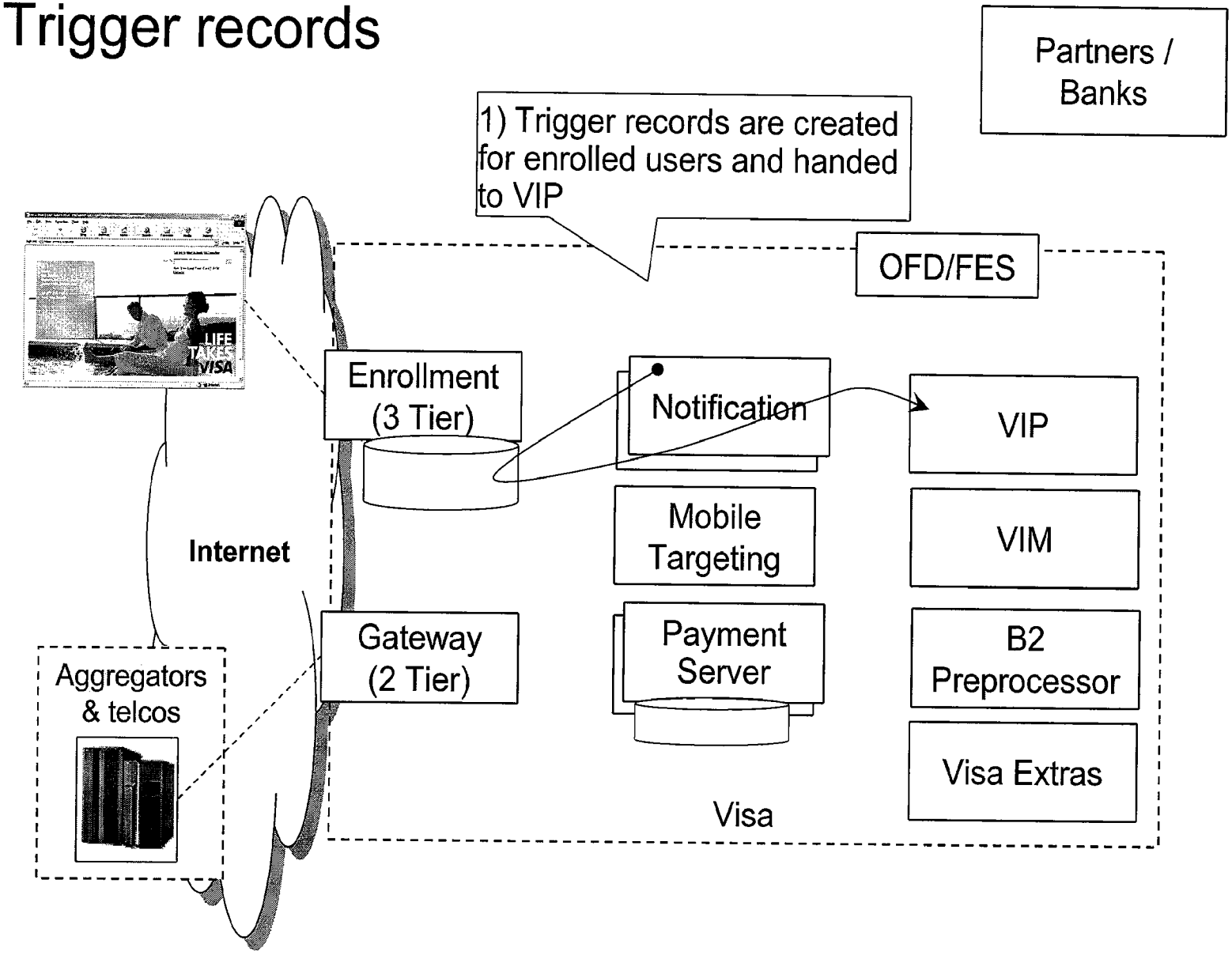


Petitioner Exhibit 1002-1470

VIP Notification (Pilot)

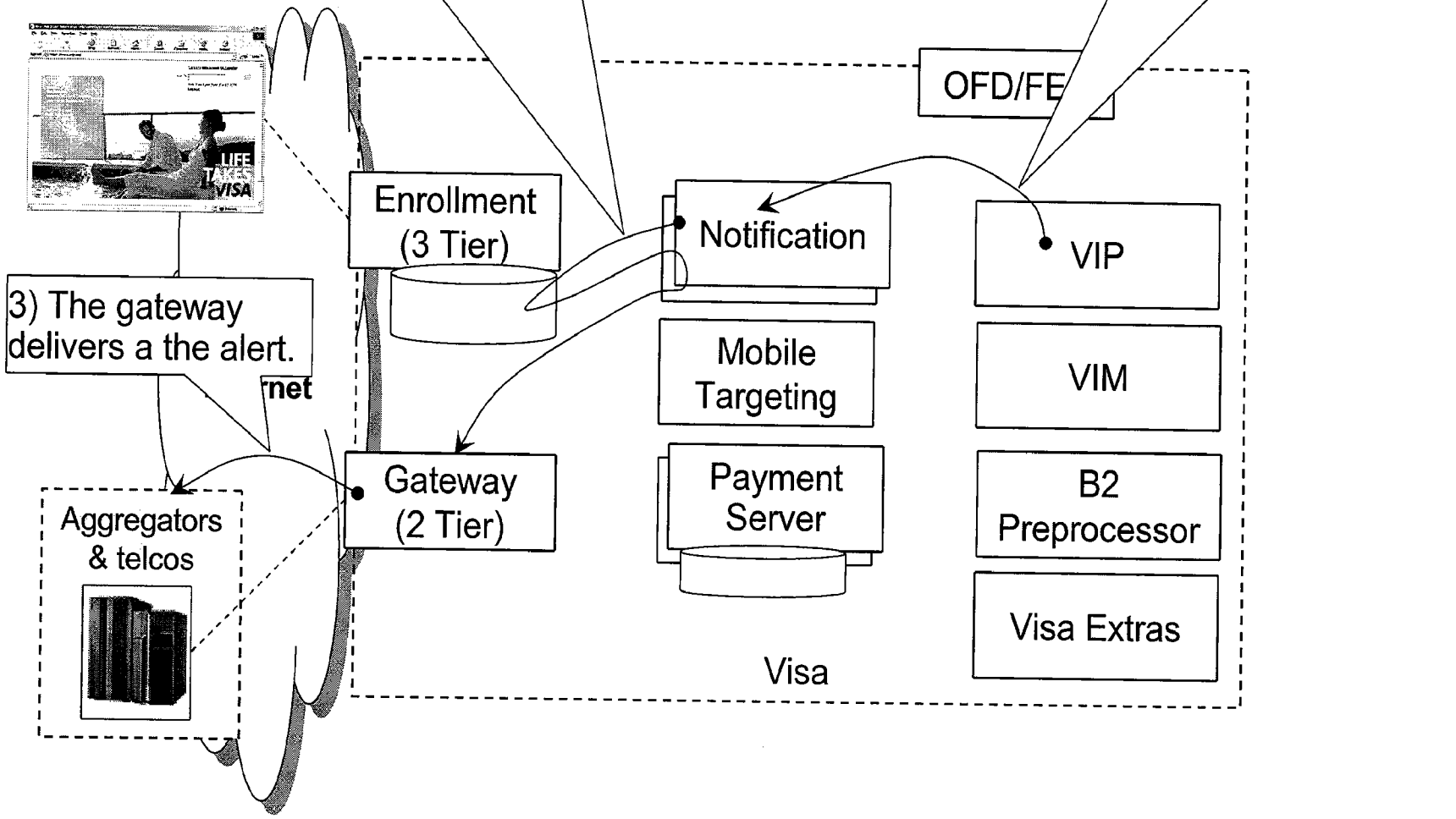
76 Petitioner Exhibit 1002-1471

VIP Notification Pilot
Trigger records



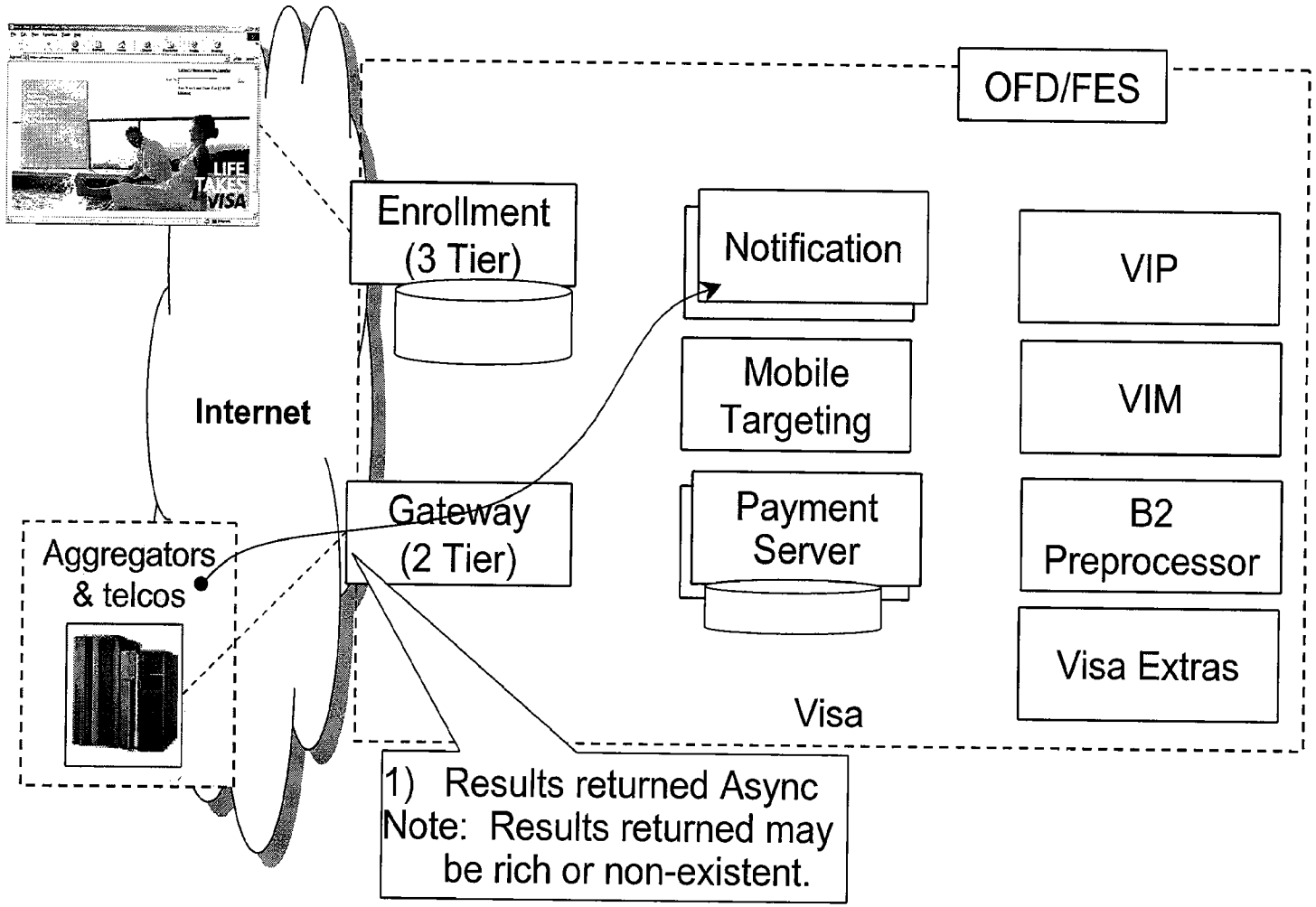
7-7 Petitioner Exhibit 1002-1472

VIP Notification Pilot Throw Alerts



Petitioner Exhibit 1002-1473

VIP Notification Pilot
Collect results

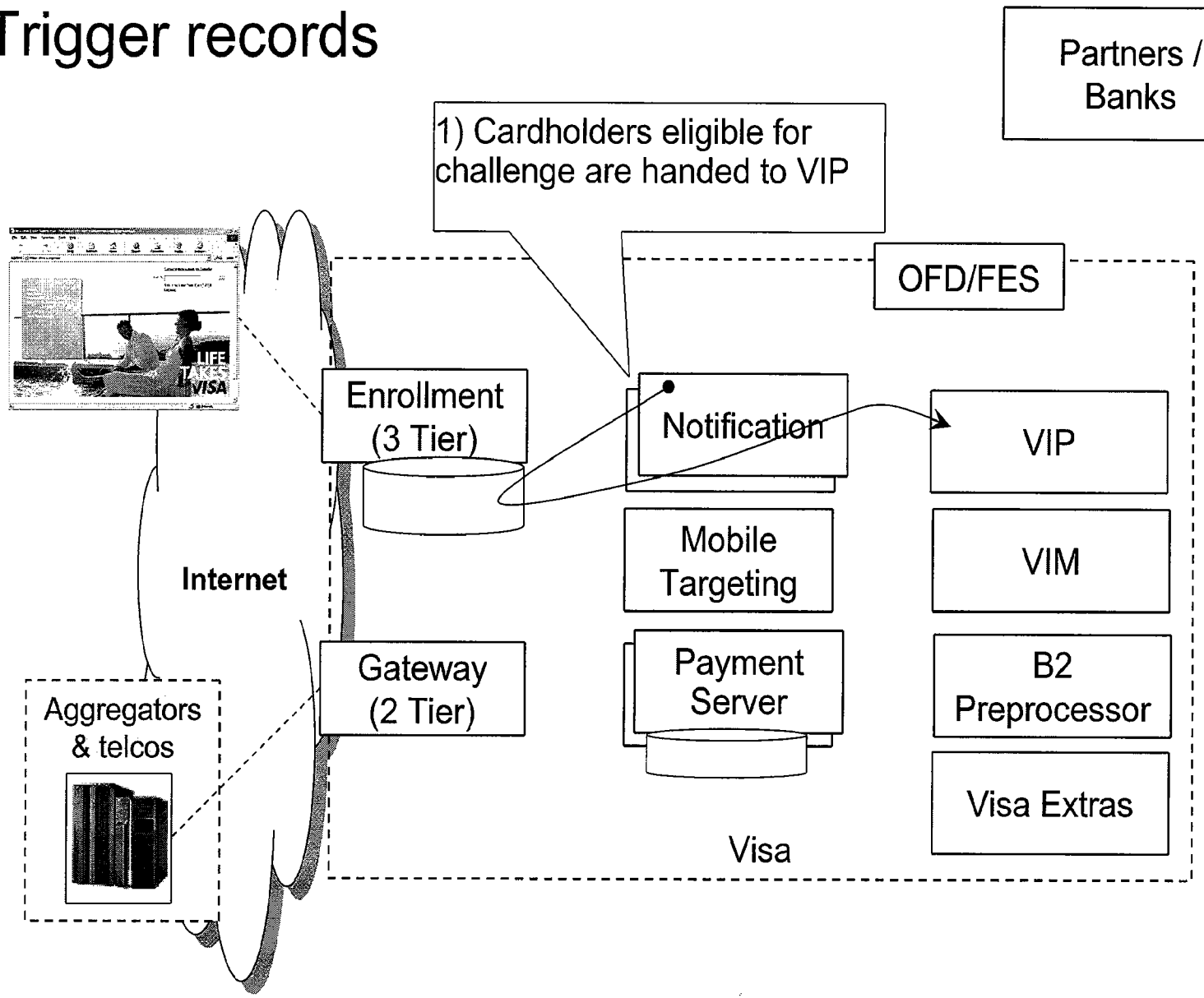


Petitioner Exhibit 1002-1474

2nd factor Authentication Pilot

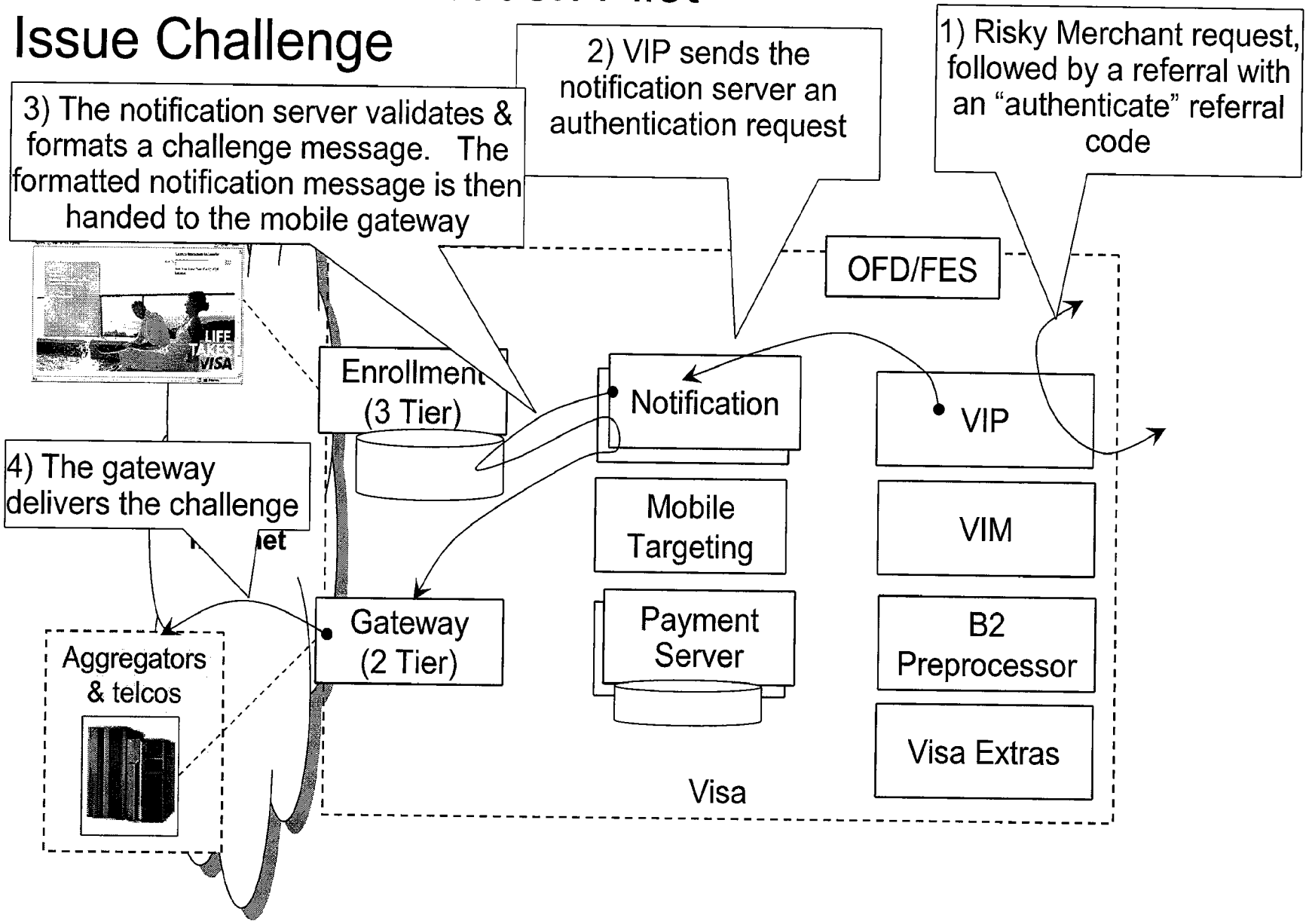
80 Petitioner Exhibit 1002-1475

2nd factor Authentication Pilot Trigger records



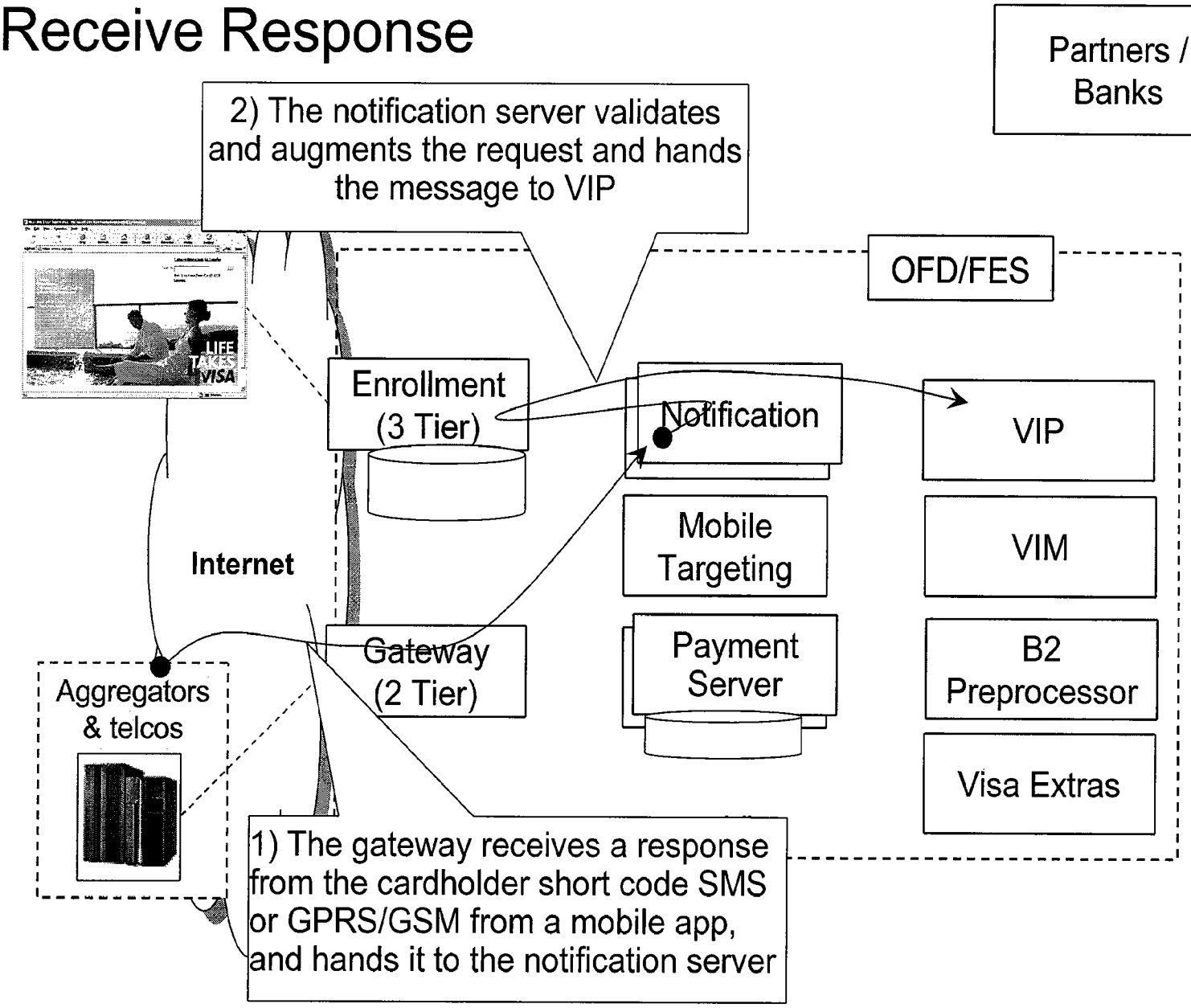
Petitioner Exhibit 1002-1476

2nd factor Authentication Pilot Issue Challenge



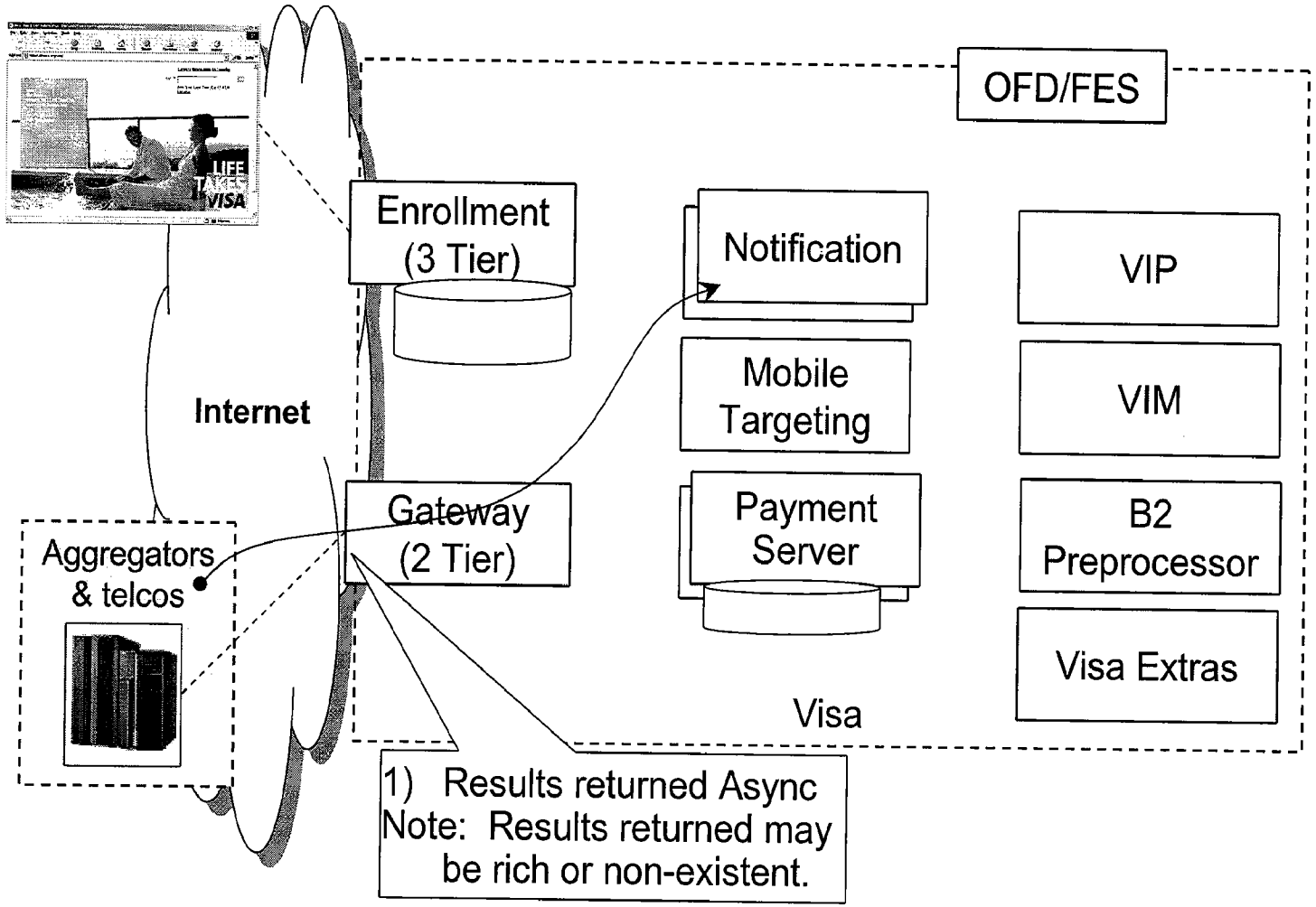
Petitioner Exhibit 1002-1477

2nd factor Authentication Pilot Receive Response



83 Petitioner Exhibit 1002-1478

2nd factor Authentication Pilot
Collect results

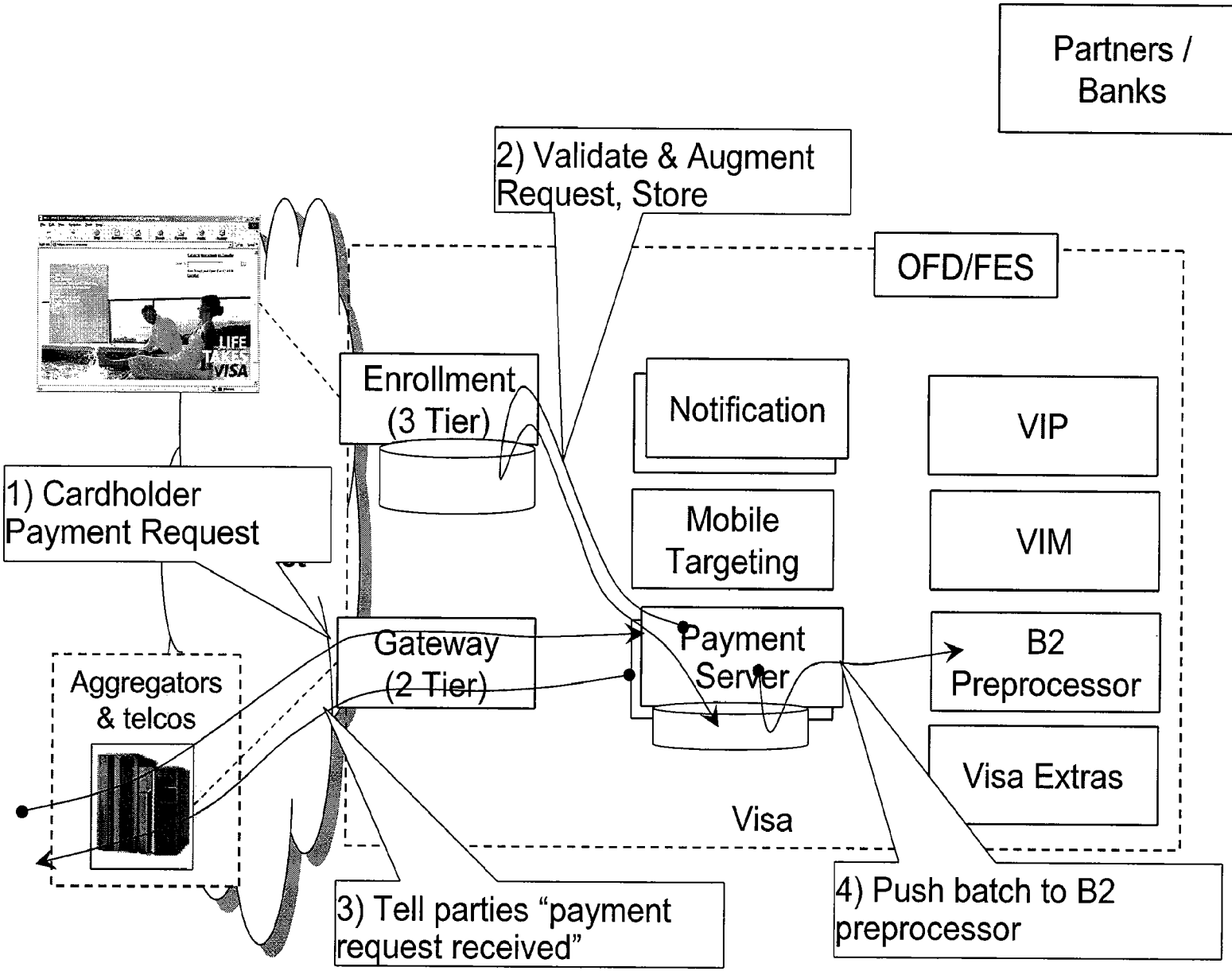


Petitioner Exhibit 1002-1479

P2P
(Pilot)

85 Petitioner Exhibit 1002-1480

P2P - Pilot

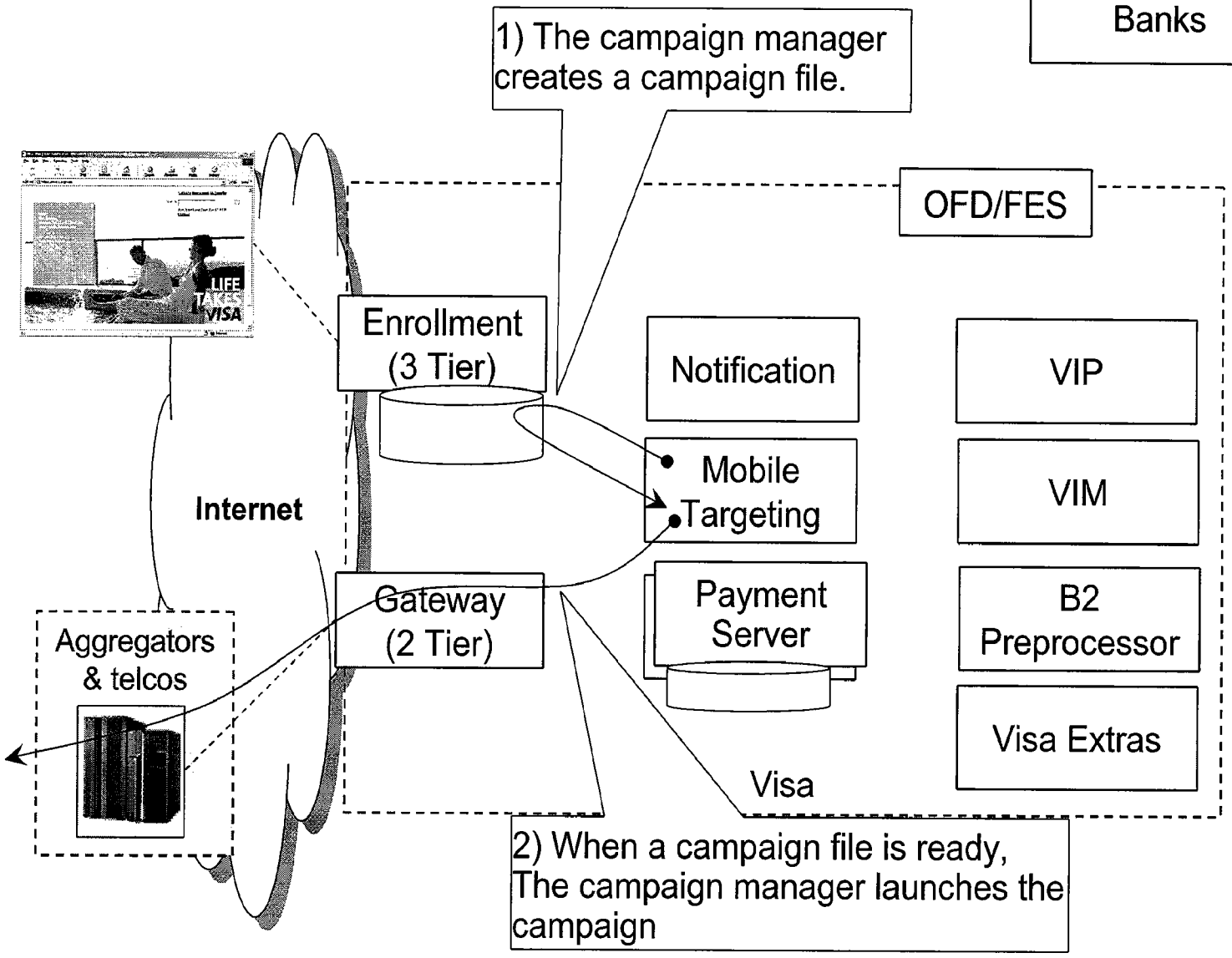


Petitioner Exhibit 1002-1481

Coupon (Pilot)

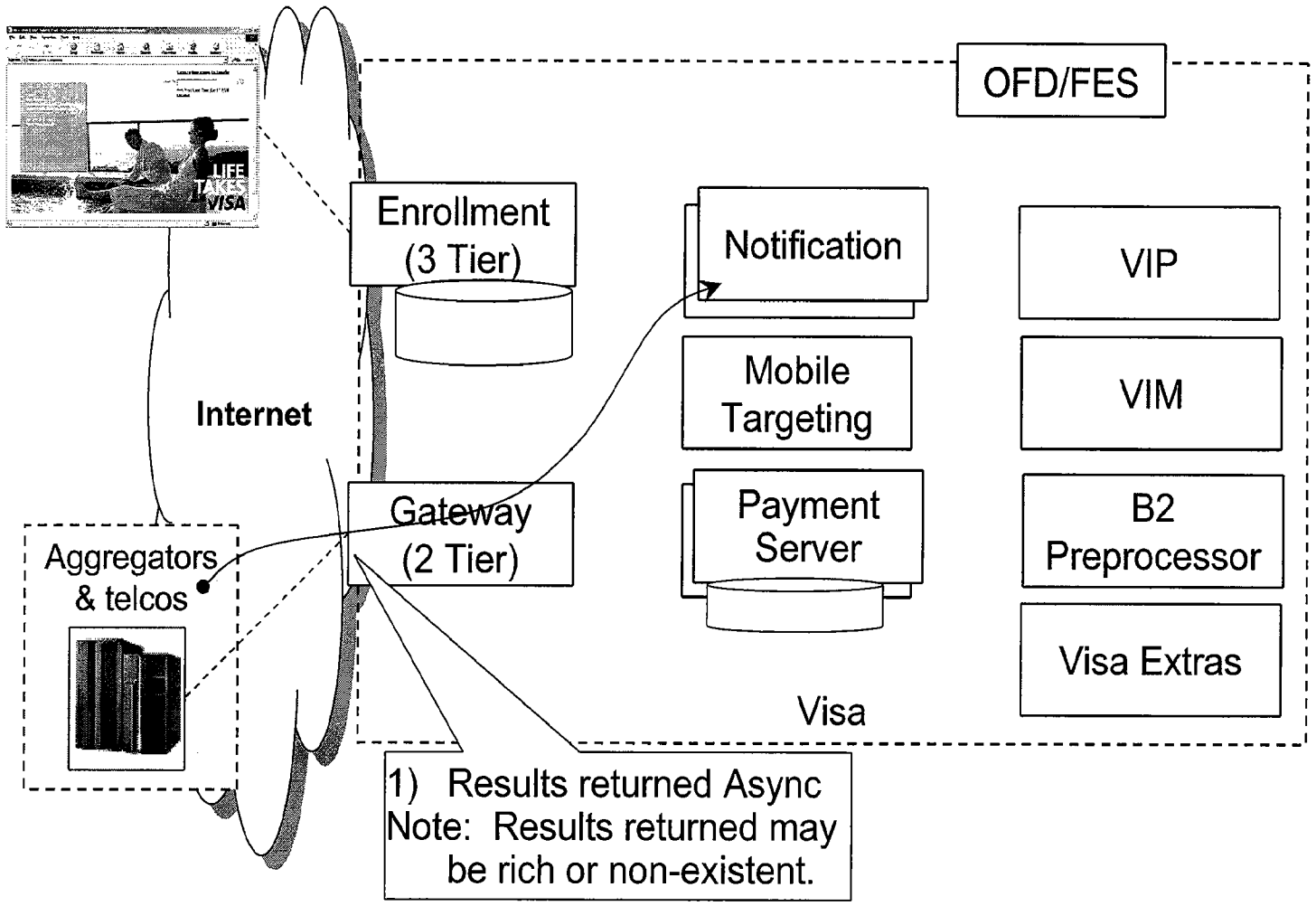
Petitioner Exhibit 1002-1482

Coupon Pilot
Campaign Distribution



& & Petitioner Exhibit 1002-1483

Coupon Pilot
Collect results

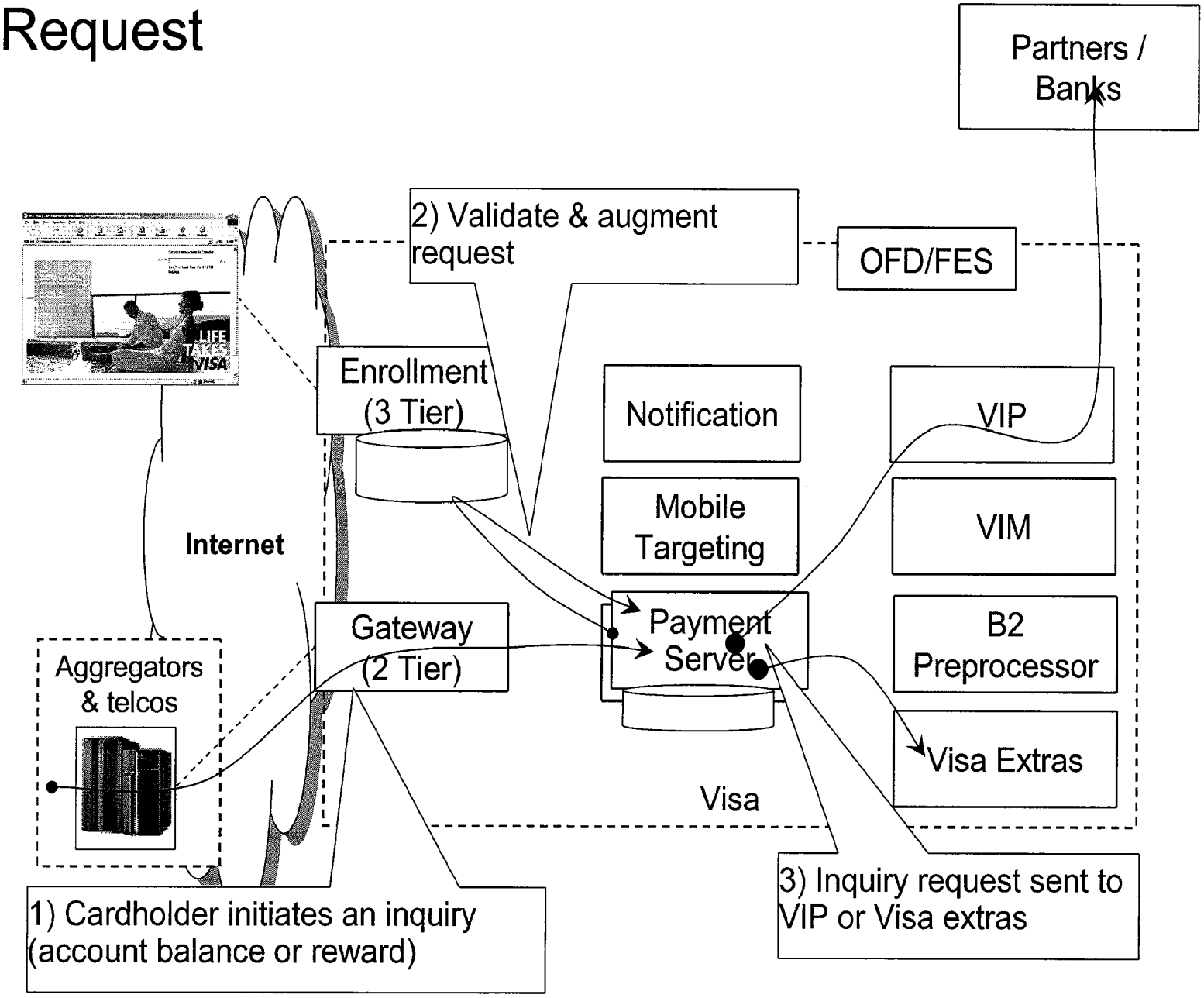


Petitioner Exhibit 1002-1484

Inquiry (Pilot)

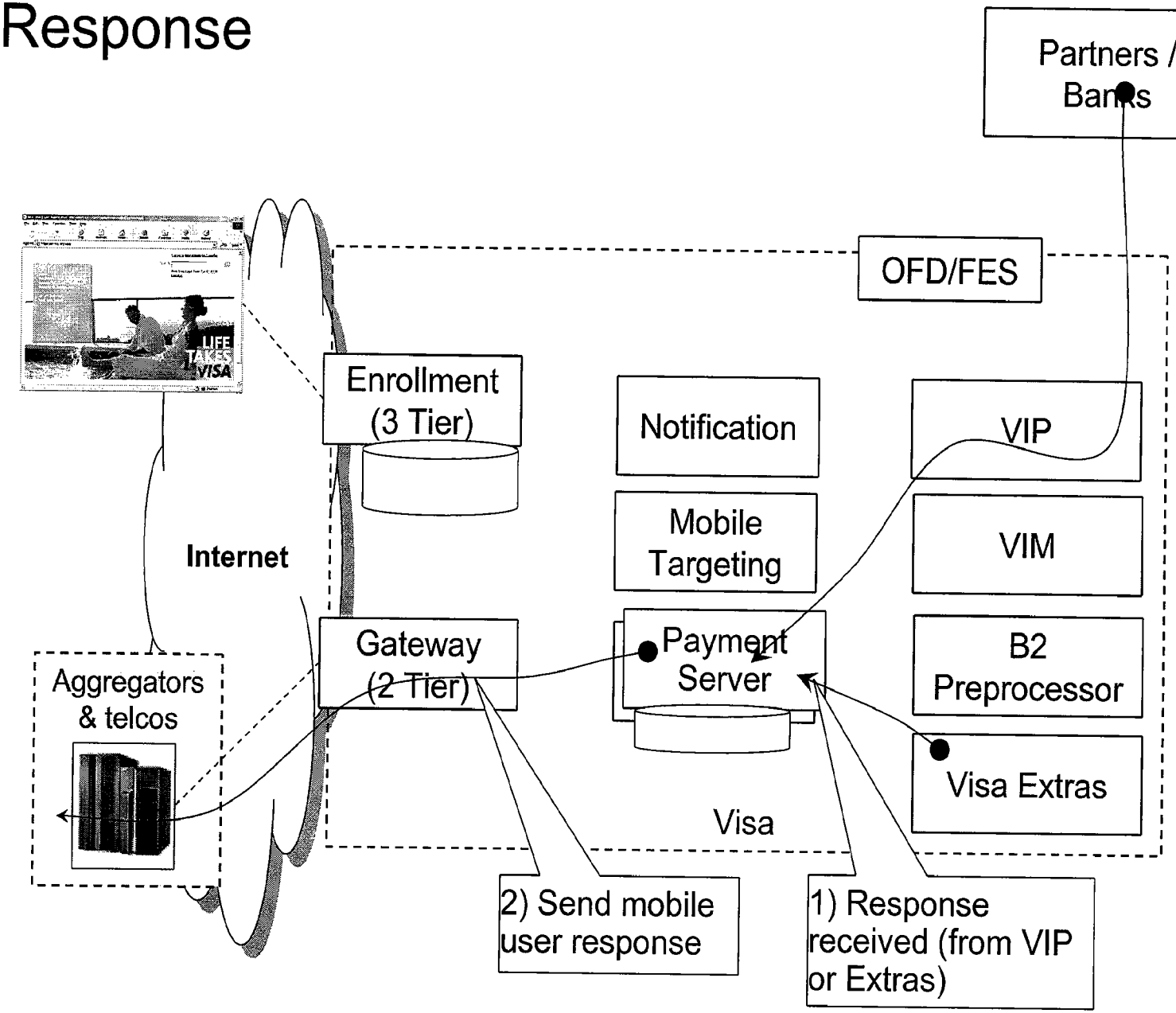
96 Petitioner Exhibit 1002-1485

Inquiry Pilot Request



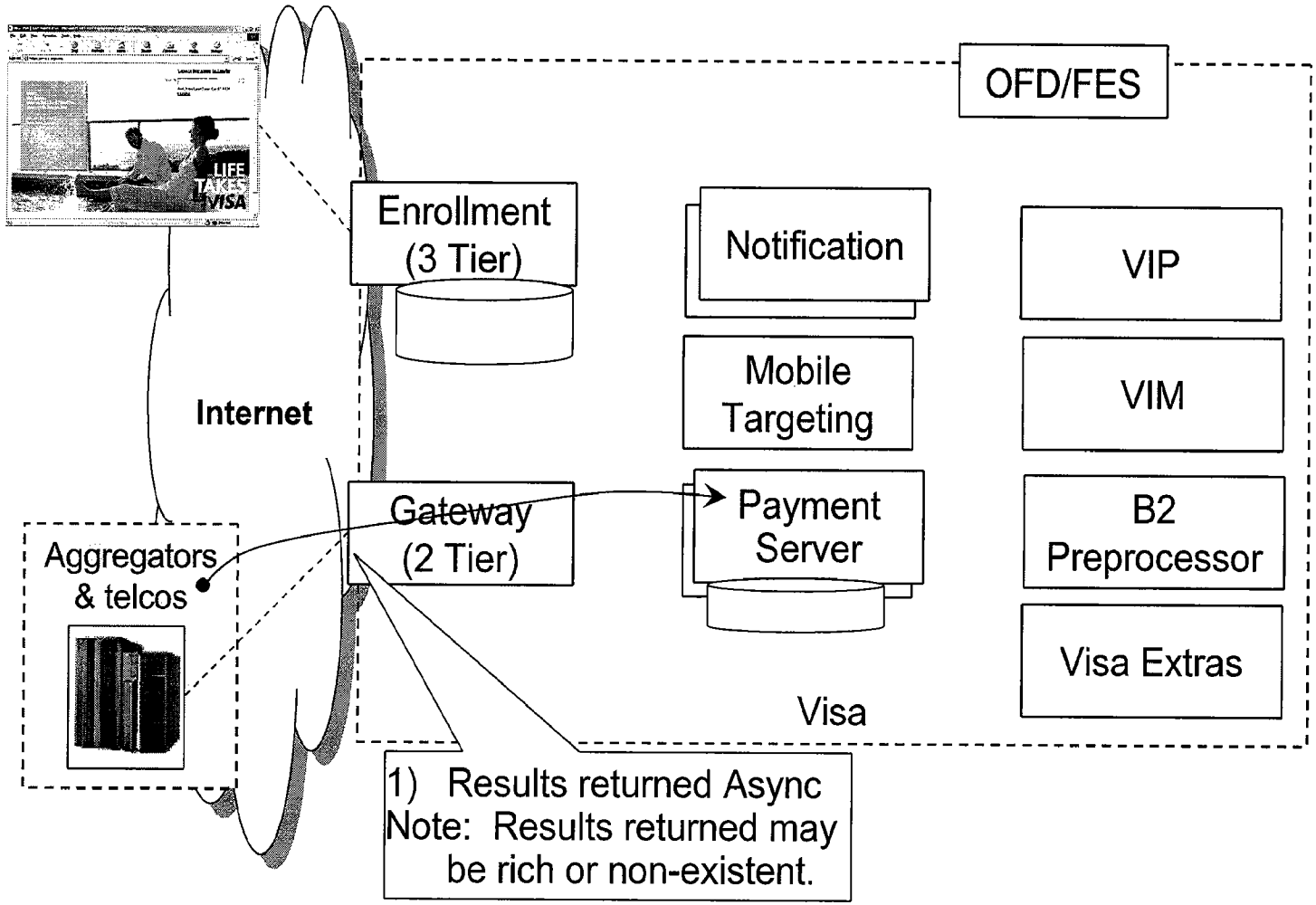
Petitioner Exhibit 1002-1486

Inquiry Pilot Response



Petitioner Exhibit 1002-1487

Inquiry Pilot
Collect results

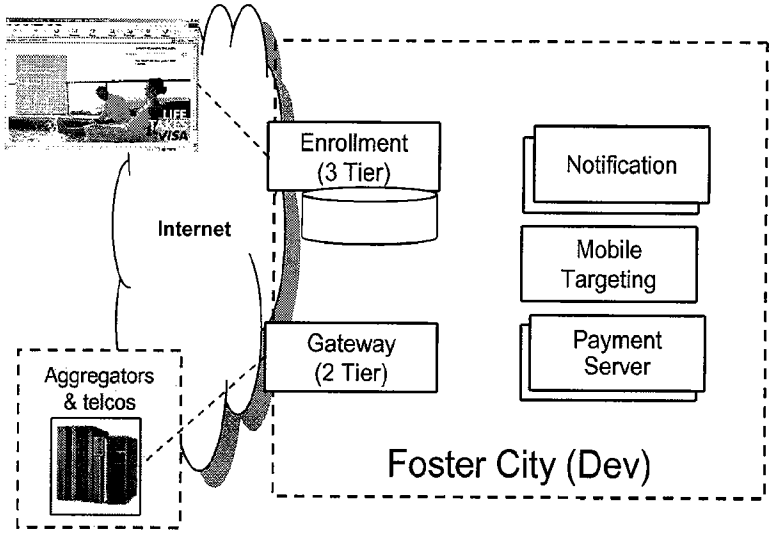


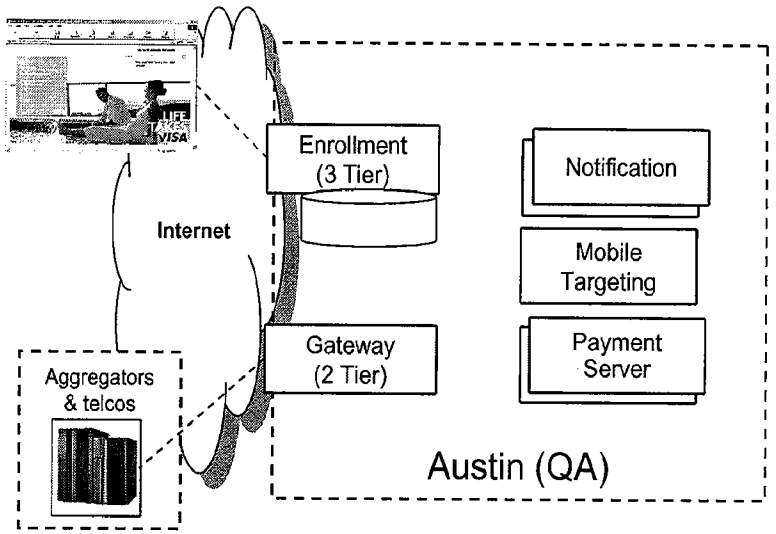
93 Petitioner Exhibit 1002-1488

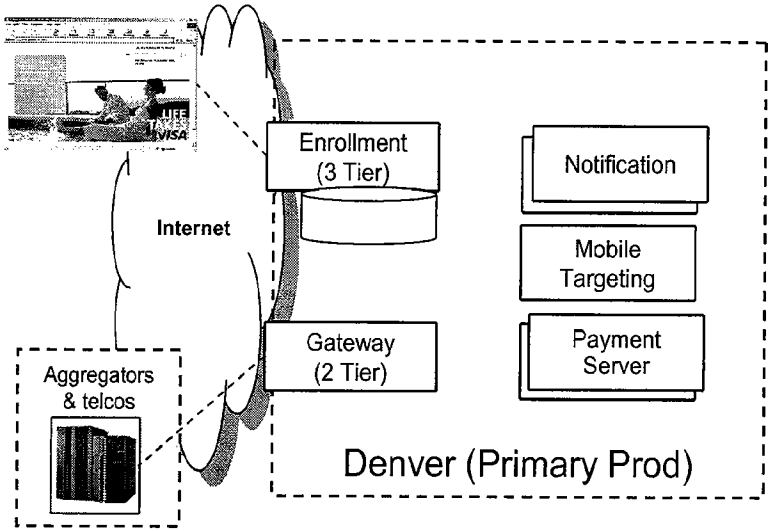
Environments

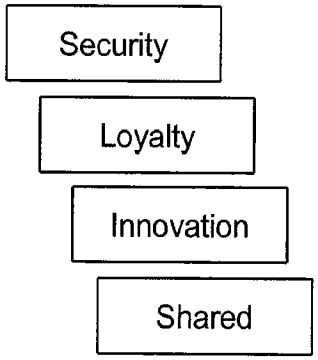
Petitioner Exhibit 1002-1489

Pilot Environment to build out



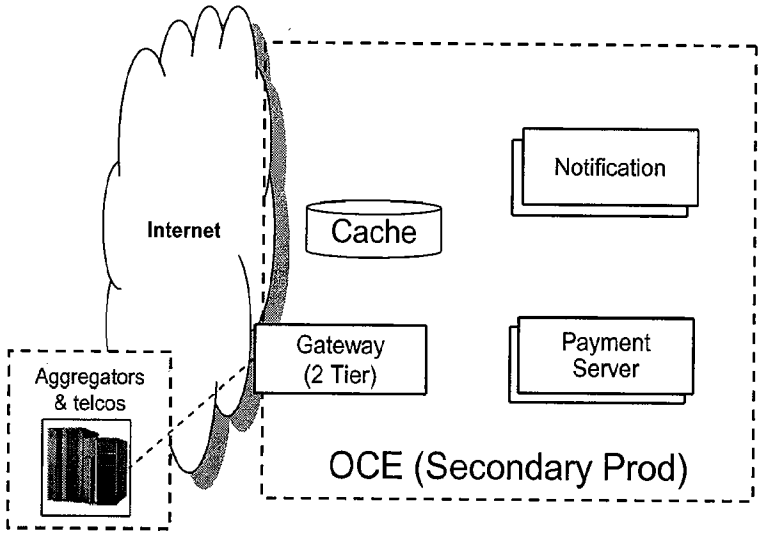






Petitioner Exhibit 1002-1490

Production Topology
Add a 2nd production instance

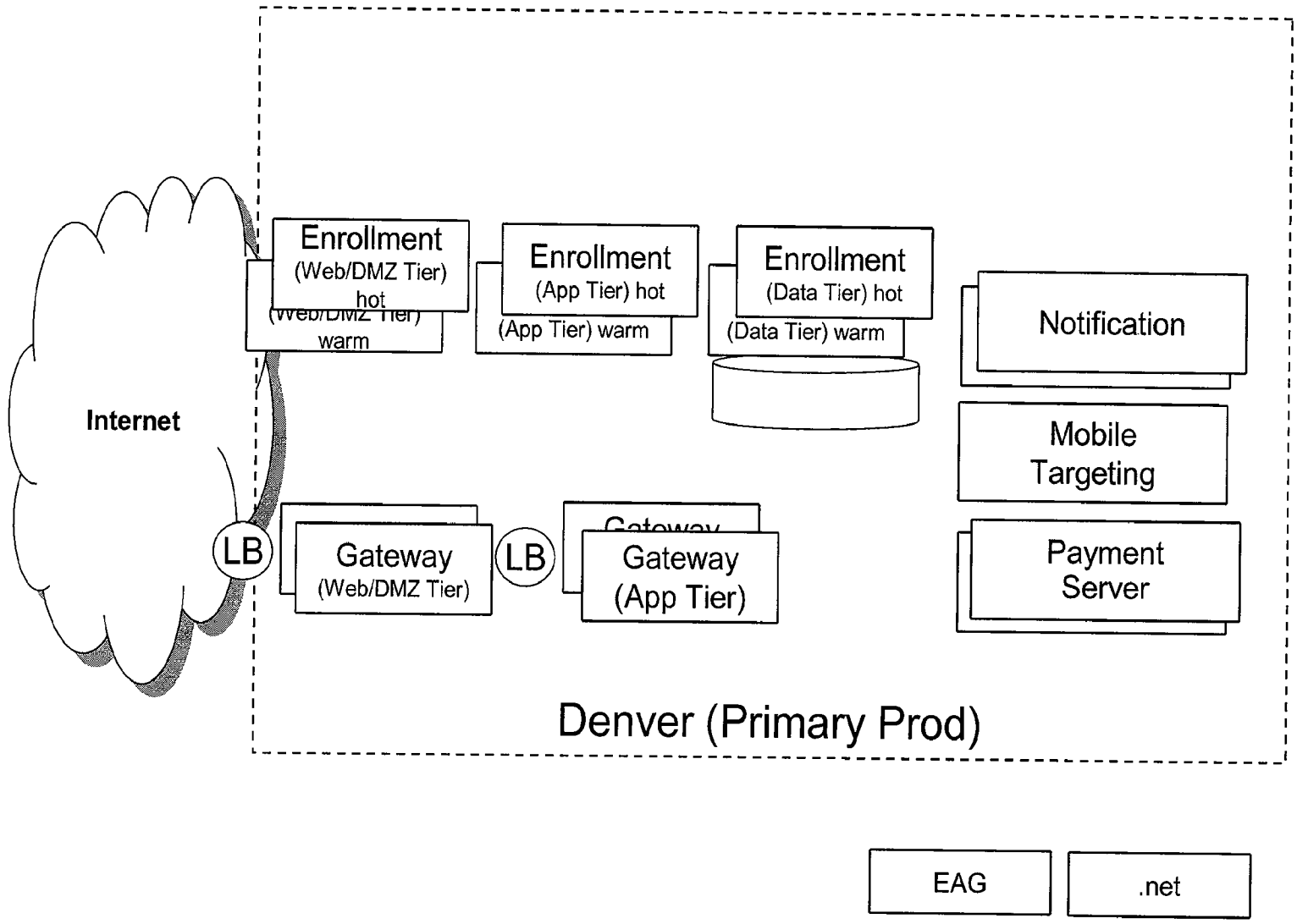


96 Petitioner Exhibit 1002-1491

Detailed Instance

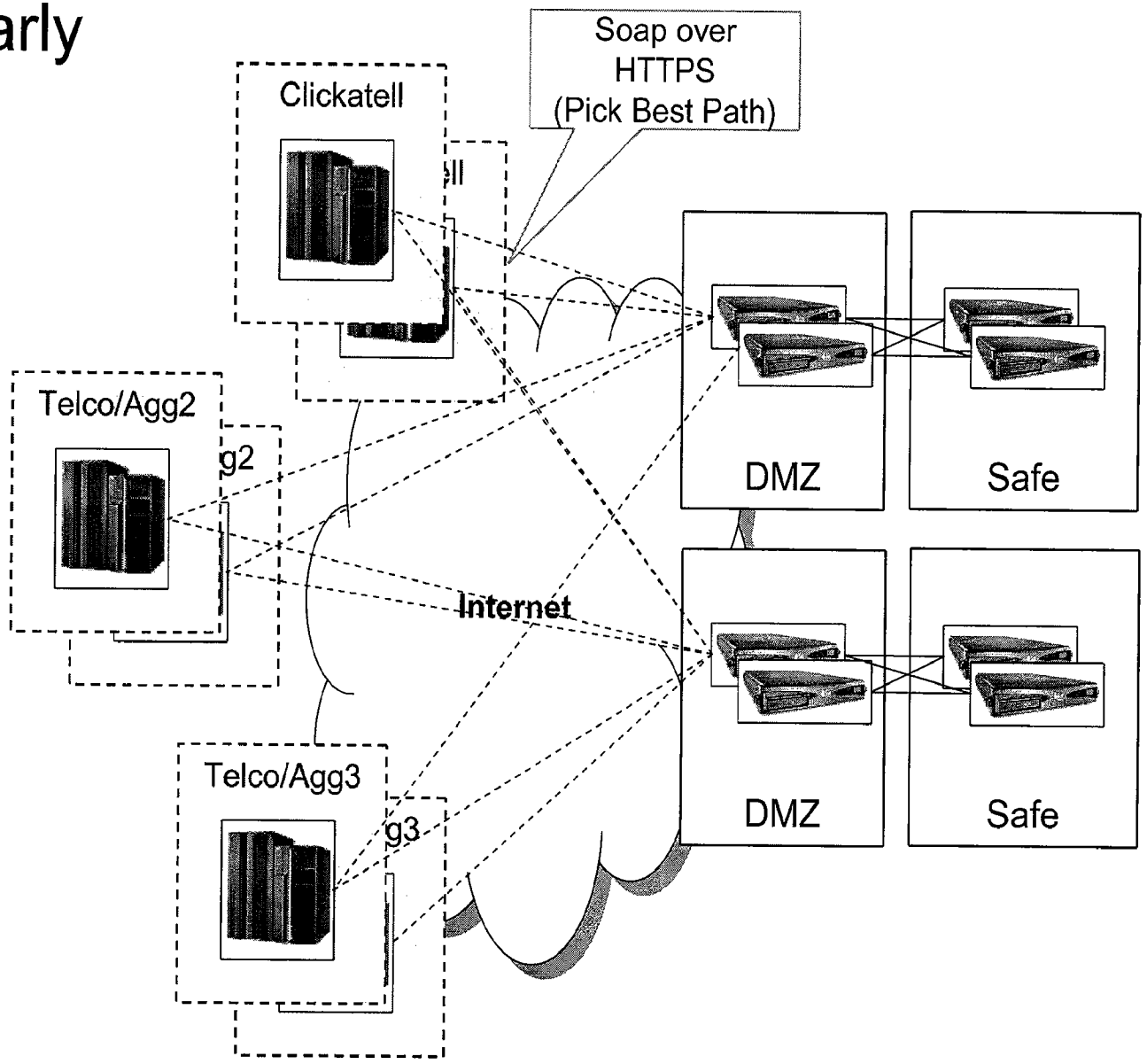
97 Petitioner Exhibit 1002-1492

FY07 Pilot Topology



98 Petitioner Exhibit 1002-1493

Topology Early

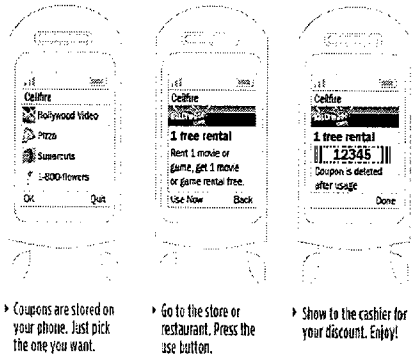


Petitioner Exhibit 1002-1494

Mobile Coupon

Finalize POS Acceptance Method Scanned, Keyed, or Both

- **Acceptance Method for Phase 1b**
- SMS, SMS Link & E-mail
- SMS link will initially be limited to Graphic coupons (no Bar code)



- **Mobile Enrollment Server**
- Excel. Determine initial pilot participants, collect schema info

Mobile Campaign Service
- Generate a coupon
- Craft text message



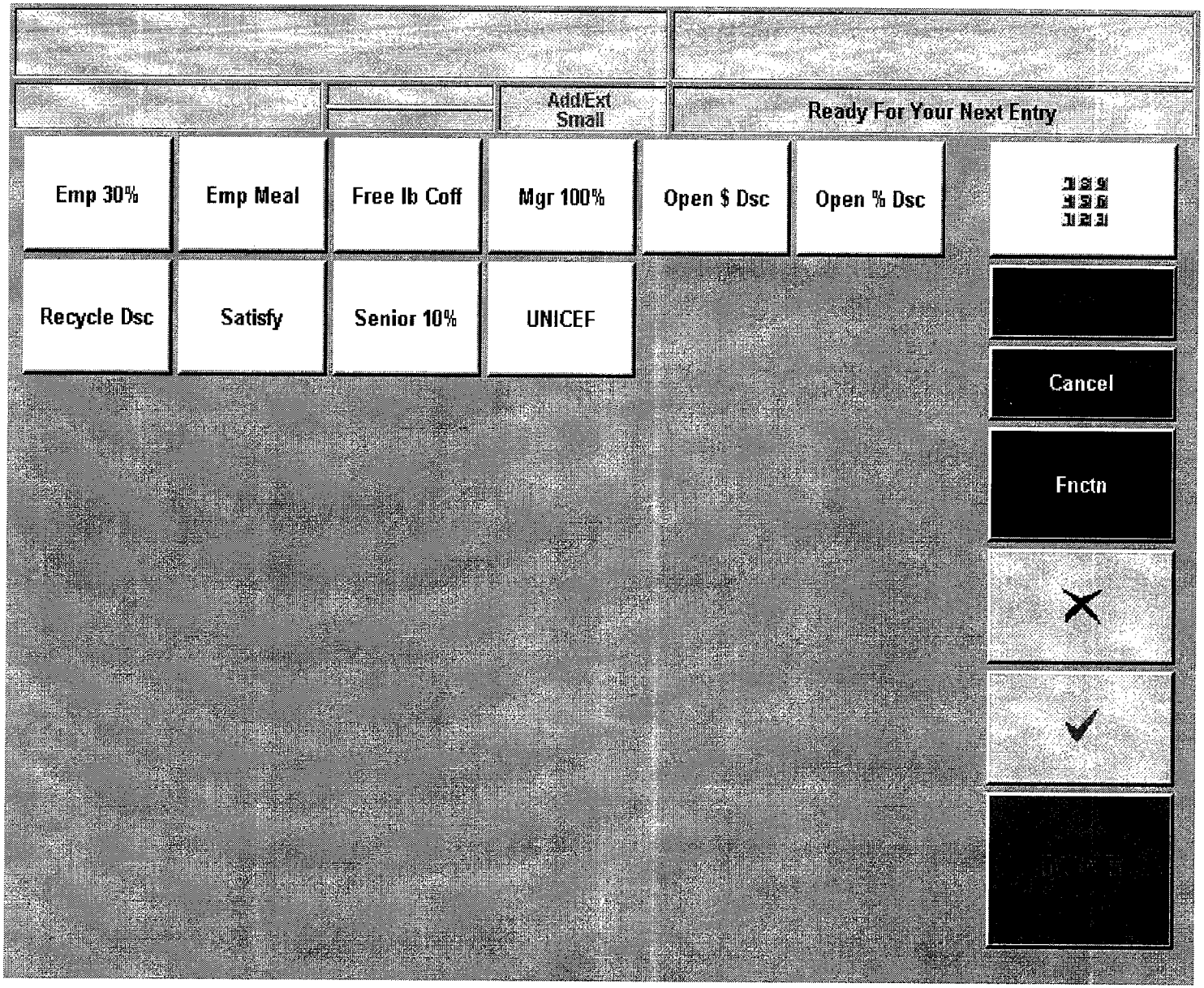
Visa Mobile Gateway
- Place coupon on existing mobile gateway
- Manually send notification messages

- **Aggregator**
- NDA, suggest initial schema for enrollment server & query formats

Visa Confidential

161 Petitioner Exhibit 1002-1496

Discount / coupon Key



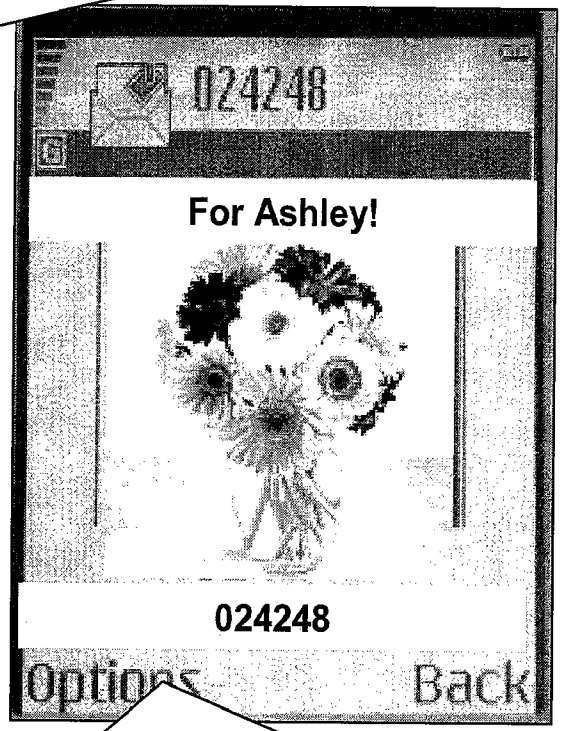
Visa Confidential

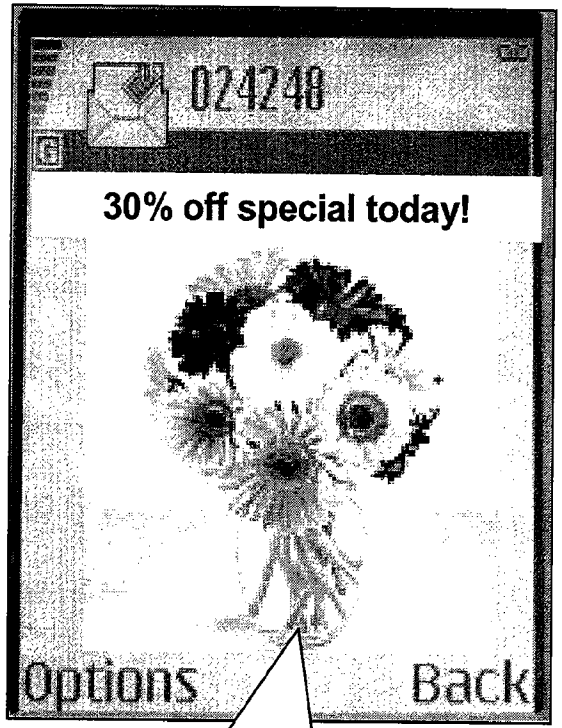
Petitioner Exhibit 1002-1497

Both!

M-Coupon type: Barcode
Input method supported: Scan or keyed
POS programming options: NLU only (for micros)





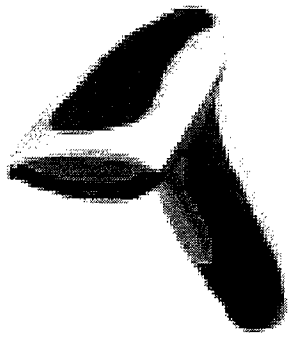


M-Coupon type: Visual w/ NLU #
Input method supported: keyed
POS programming options: Discount key or NLU

M-Coupon type: Visual only
Input method supported: Keyed (discount key)
POS programming options: Discount Key for 30% off

163 Petitioner Exhibit 1002-1498





Bar Scanner

- **CCD Scanners can scan a cell phone.**
- **Our working model (above) is $119**
  http://idautomation.com/scanners/SC5USB.html

- **Laser Scanners can't scan a cell phone. They reflect.**

Visa Confidential

104 Petitioner Exhibit 1002-1499

Service Components



Mobile Enrollment Server

Function: Repository of mobile enrollment info
For Coffee Pilot, users self enroll (or are enrolled).
•For Merchant Pilot, users can self enroll or be batch enrolled. Enrollment service can appear as a Visa service or a "white label" service.



Mobile Campaign Server

Function: Create a campaign file for distribution.
•Extract target names from enrollment DB.
•Administrator selects routing options, text for message, and coupon options.
•A properly formatted Campaign file is generated.

Mobile Gateway

Function: Generic gateway to aggregator or telcos
•Through a message or batch interface, send individual messages

105 Petitioner Exhibit 1002-1500

Visa Confidential

Pilot Phase 2
Automated Description

Mobile Enrollment Server

- Browser interface for Visa employees to enroll on corporate network
- Challenge interface to mobile Gateway (Stretch Goal)
- "Mobile details" Interface to mobile Gateway (Stretch Goal)

Mobile Campaign Server

- Extract selected names from enrollment DB
- Administrator creates coupon greeting text
- Determine Vanities URL & Short code and if they should be used (Business folks)
- Create & associate barcode for each name (same # for batch, or unique # per name)
- When ready to send, handcampaign batch to mobile gateway

Visa Mobile Gateway

- Enable batch Interface from mobile campaign server (accept file from campaign server)
- Enable multi-modal interface (interface to Clickatell) Send & Device query

- **Aggregator**
- Support multi-modal requests (SMS, MMS, e-mail)
- Support device query requests
- Support secure interface / Visa offline Cert
- Work out hyperlink issues with telcos (use existing codes?)
- Work out vanity options selected by business folks

Visa Confidential

Petitioner Exhibit 1002-1501

Pilot Phase 3
Merchant Pilot

Mobile Enrollment Server

- Locate Mobile enrollment server in proper production zone
- Scale, redundancy, and white label capabilities
- Determine and Implement vanity details (and white label details)
- Security requirements
- Additional? TBD controls to support service (reporting, etc)

Mobile Campaign Server

- Per person coupons, coupons optimized for mobile device
- Additional? TBD controls to support service (reporting, etc)

Visa Mobile Gateway

- Same as enrollment server

- **Aggregator**
- Service contract and service levels in place
- Scale, redundancy, and white label capabilities
- Security requirements
- Proper zone
- Additional? TBD to support business (reporting, etc)

167 Petitioner Exhibit 1002-1502

Visa Confidential

Backing

Visa Confidential

Petitioner Exhibit 1002-1503

Gross Use Cases

Visa Confidential

Petitioner Exhibit 1002-1504

Enrollment – Customer Create
UC1.0

- Invoked: Potential mobile customer arrives at enrollment URL
- Collect Schema info
  - Name, Mobile Phone #, E-mail address and distribution options (Webservice, MMS, e-mail)
  - Password/Password (user ID for pilot is mobile number)

- Stretch goals
  - Vanity details (Look & Feel of enrollment pages, URL)
  - Legal notice
  - Before enrollment is complete . . . A test/challenge coupon is sent to the customer for traceability. This also verifies enrolled phone is capable of receiving a coupon.
  - When enrollment is complete, send a "mobile details" query to Clickatell

- Future
  - Accept a formatted file for batch enrollment for white label bulk enrollment

Petitioner Exhibit 1002-1505

Visa Confidential

Enrollment – Customer Modify / Delete UC1.1

- Invoked: Mobile customer arrives at enrollment URL

- Mobile customer signs on with using user ID (Mobile number) & PW.
  - Update schema details
  - Update Password/Password

- Stretch goals
  - User Notified (text or e-mail) an update has been made (using old & new contact info)

- Future
  - KISS . . . bulk enrollment records are treated as "replacements"

Petitioner Exhibit 1002-1506

Visa Confidential

Enrollment – Administrator View / Modify UC1.2

- Invoked: Enrollment administrator arrives at Admin URL
- Admin signs using their user ID & PW
- Bring up enrolled info using mobile # as key
  - Update schema
  - Reset password <temp password is sent via mobile text>
  - Remove account
- Stretch goals
  - User Notified (text or e-mail) an update has been made (using old & new contact info)

Petitioner Exhibit 1002-1507

Visa Confidential

Create Campaign File
UC3

- Invoked: Campaign Manager arrives at Campaign URL

- Campaign manager signs using their user ID & PW

- Campaign manager selects
  - Names from enrolled database "Mark, Michele, Peter, ..."
  - Text Greeting "Hello <Name>, here is a coupon for a free cup of coffee. Good today only."
  - Coupon options. Note: Only group. Future individual, look and feel.

- After options are selected, a Campaign File is generated and stored with a status of pending/None

- Campaign manger selects a time to send file to Mobile Gateway. Status is changed to pending/time

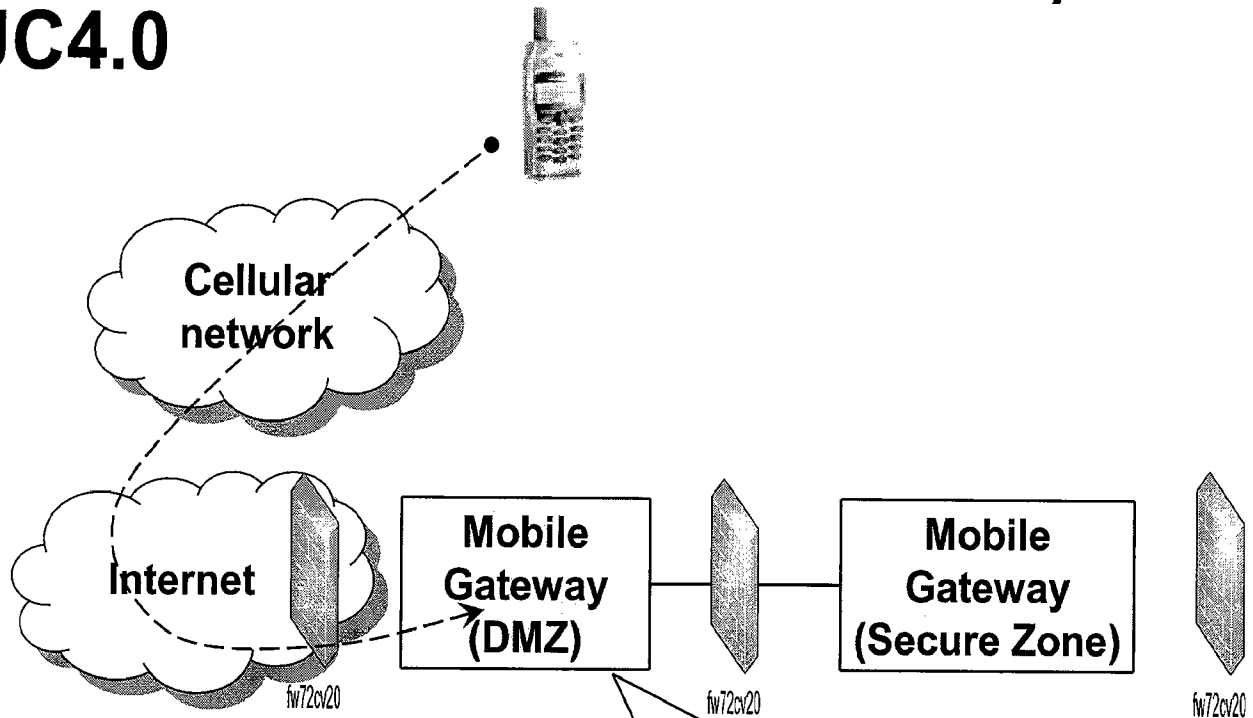
- At selected time Mobile gateway is either handed file or pulls it and status is changed to Sent/time

- Future:
- Get report back from Clickatell on confirmed deliveries, and store with campaign file.

IPR3 Petitioner Exhibit 1002-1508

Visa Confidential

Redemption (Mobile Customer) UC4.0



Customers using web service can pull coupon mobile gateway until expiration date. Try to use MMS so this step can be skipped. Also, no simple way to secure coupon.

114 Petitioner Exhibit 1002-1509

Visa Confidential

Redemption - Scan Gross UC4.1





- Mobile customer orders a cup of coffee
- Cashier rings up coffee
- Customer produces coupon
- Cashier validates coupon is valid
- Cashier scans coupon or hits "negative item" key
- Customer and cashier settle up

Visa Confidential

115 Petitioner Exhibit 1002-1510

Pilot Settlement
Gross UC4.1

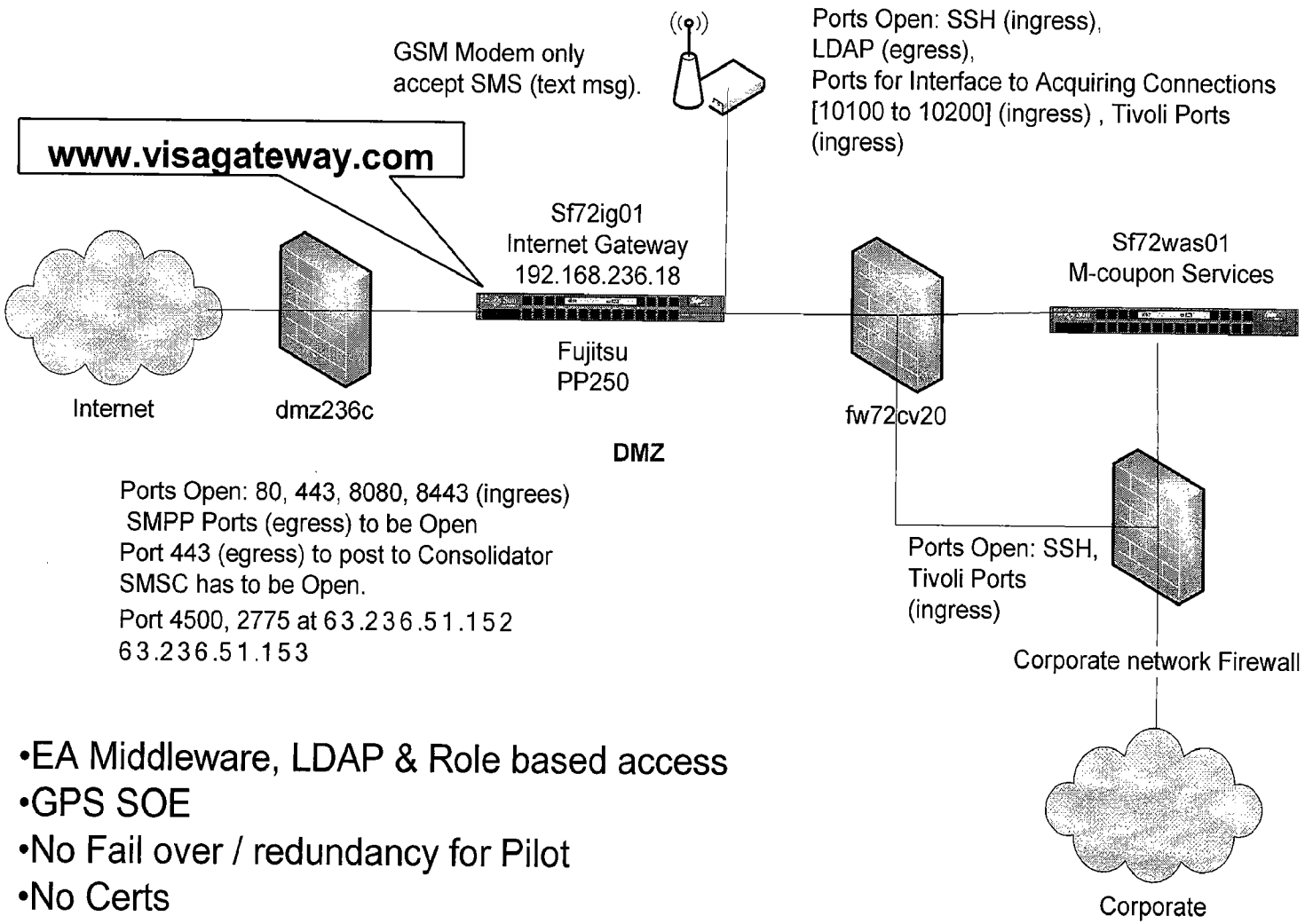
•From "Menu Report" Guckenheimer creates a catering invoice. "Pip Gudry" would be the one submitting the us invoice.

•Determine what controls are needed. All we have to verify this catering invoice is campaign file, and possible delivery report.
•Microsystems can create a "menu report".

9/1 Petitioner Exhibit 1002-1511

Visa Confidential

Pilot Environment



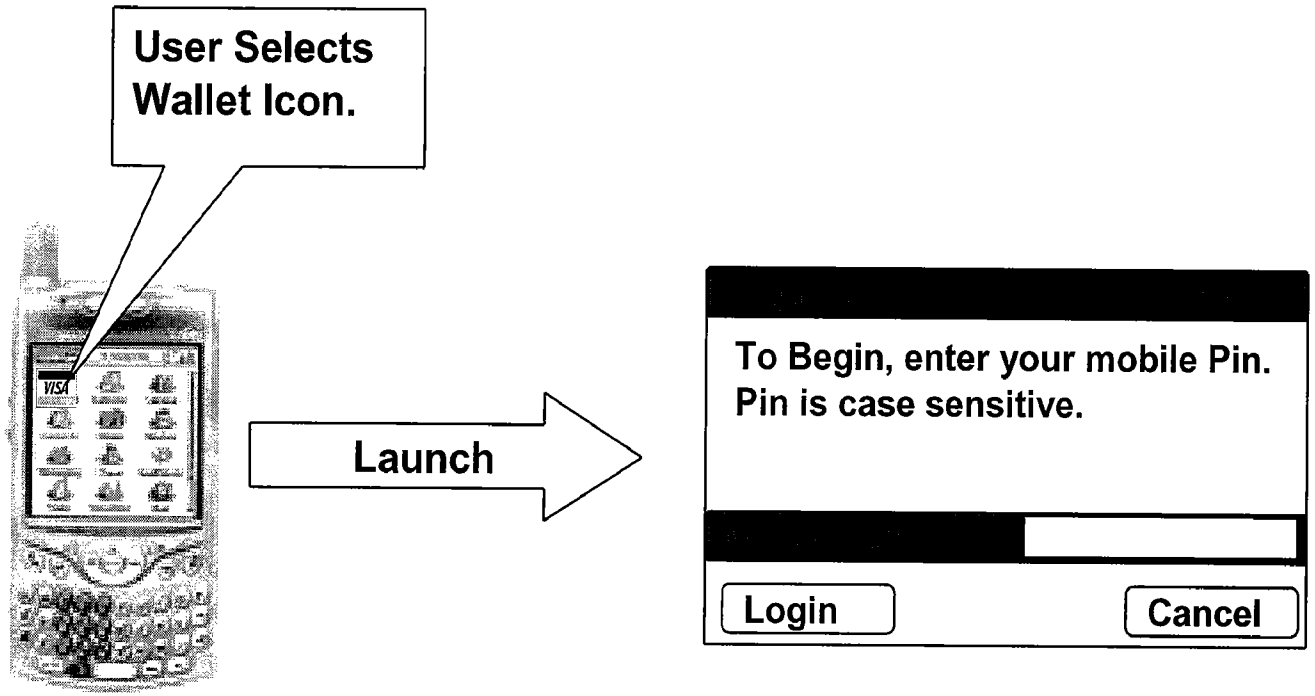
- EA Middleware, LDAP & Role based access
- GPS SOE
- No Fail over / redundancy for Pilot
- No Certs

// 7 Petitioner Exhibit 1002-1512

Visa Confidential

Mobile Wallet

Initial Sign on
Mobile Application pre-configured

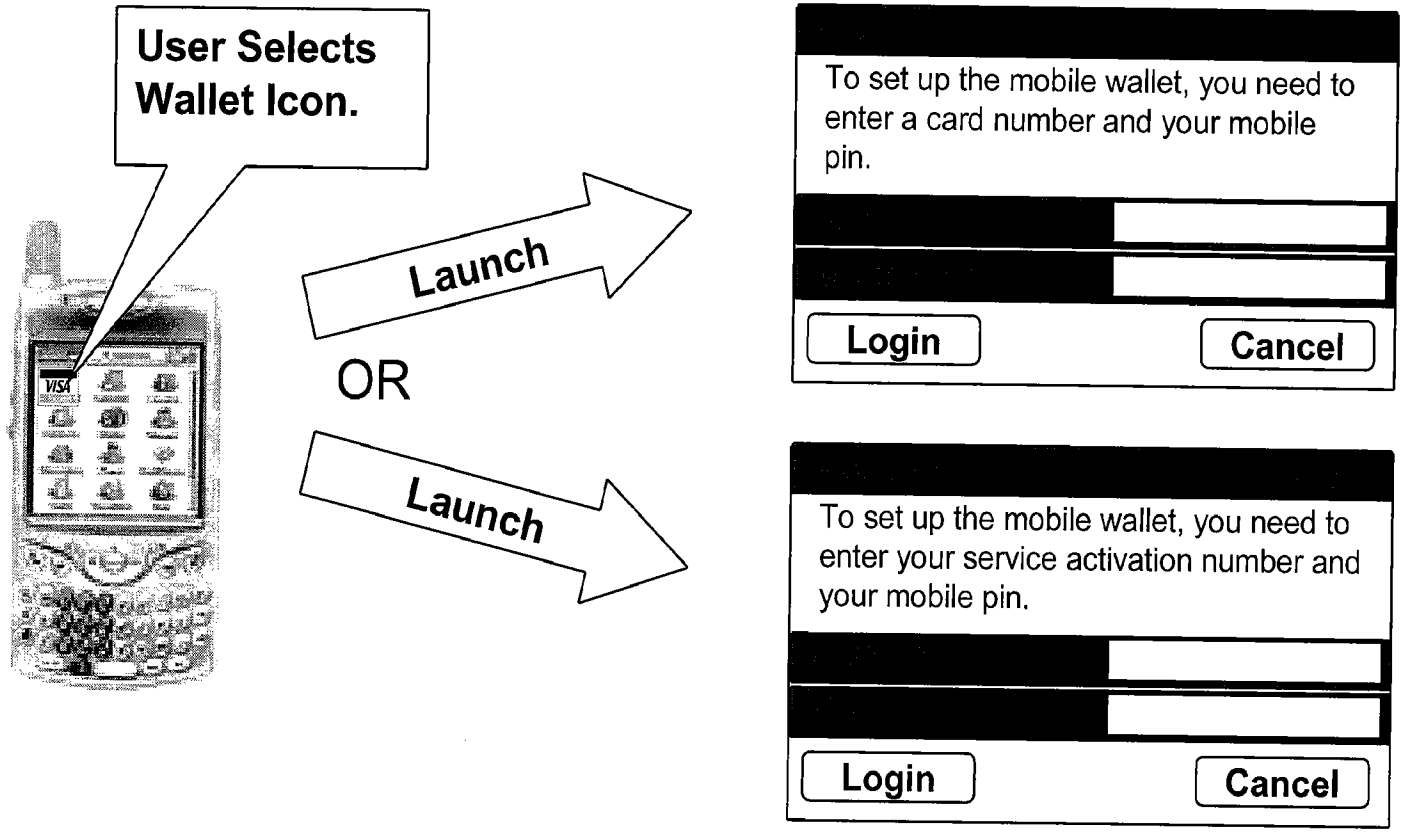


- Application can be "pre-configured" with one or more accounts for an individual user.
- Wallet ICON can be a "Visa" Icon, or any partner Icon

Petitioner Exhibit 1002-1514

119

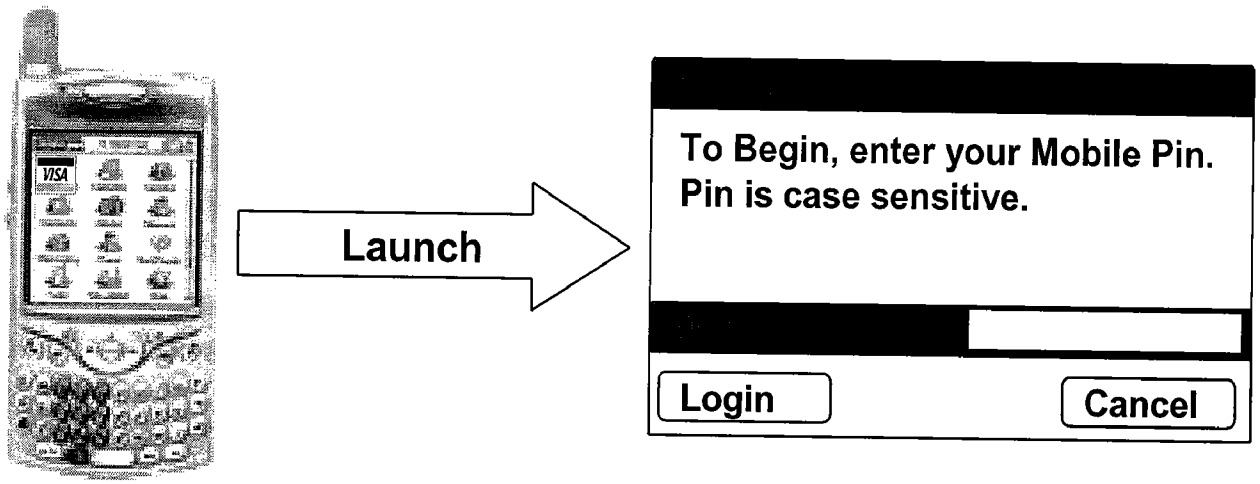
Initial Sign on
Mobile Application NOT pre-configured



- If the application has not been pre-configured, the user could be asked to enter an account number (PAN), or an activation code.
- The mobile application uses the activation code or PAN to identify user and download the user's profile.

Petitioner Exhibit 1002-1515

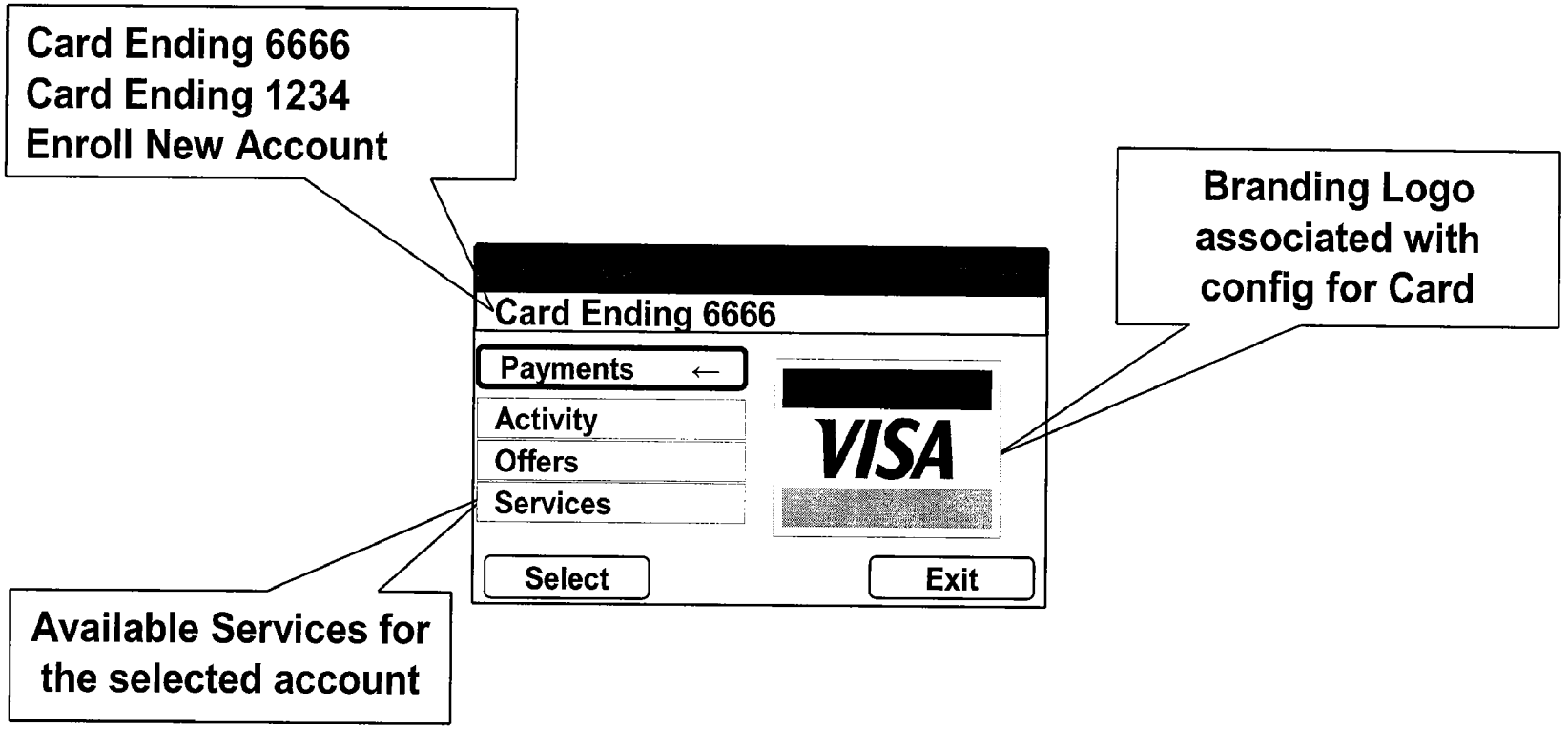
Returning Sign on
For configured applications



- After the application has been configured, the user only needs to enter their mobile Pin when the application is launched.

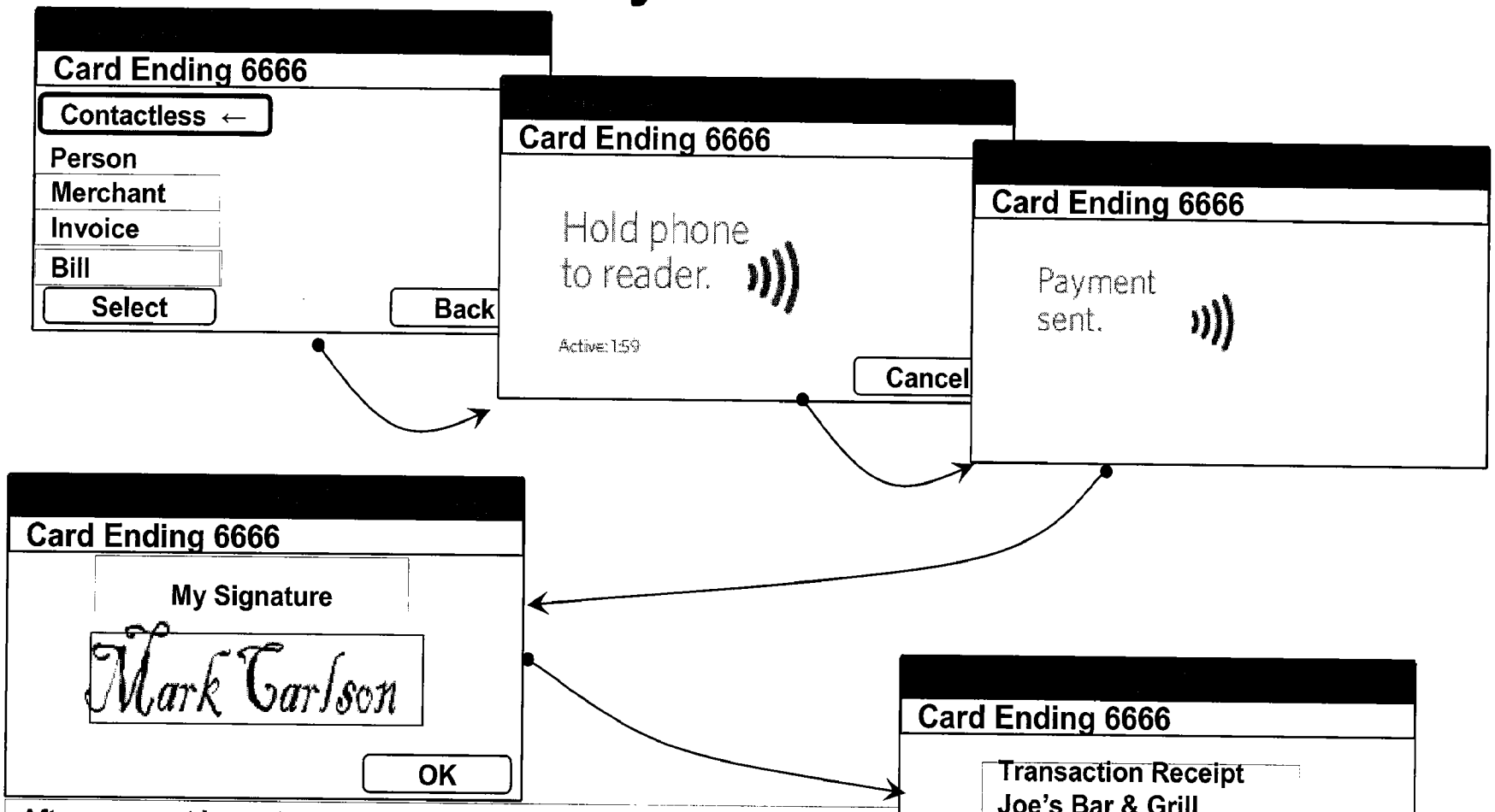
121
Petitioner Exhibit 1002-1516

Landing Page (All Services Configured)



122 Petitioner Exhibit 1002-1517

Payments Page
Contactless P2B Payment

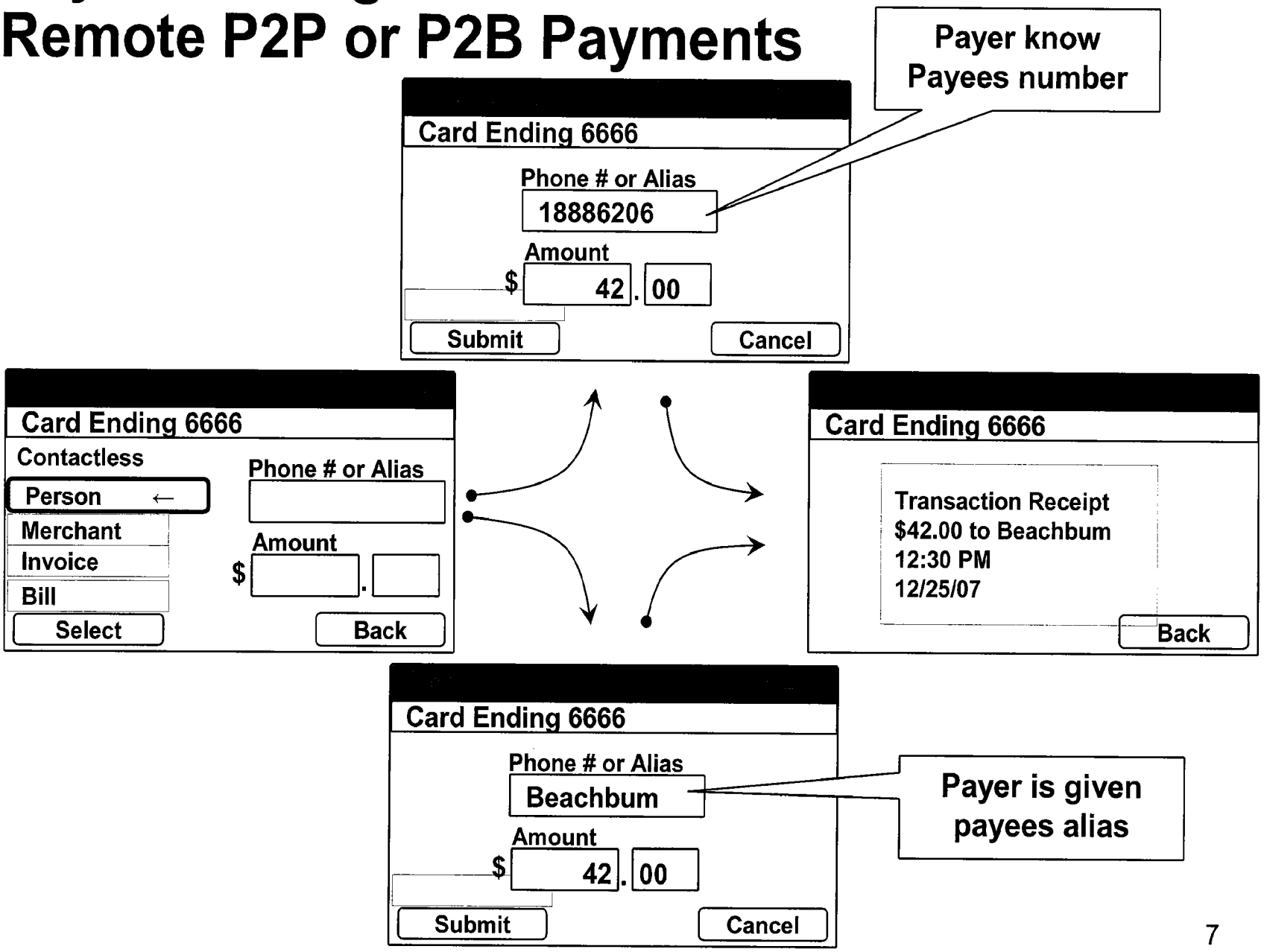


After payment is sent:
- Mobile device displays consumers signature
- Consumer signs at POS
- Consumer can show cashier signature on the phone for comparison
- Receipt available under activity

Visa Confidential

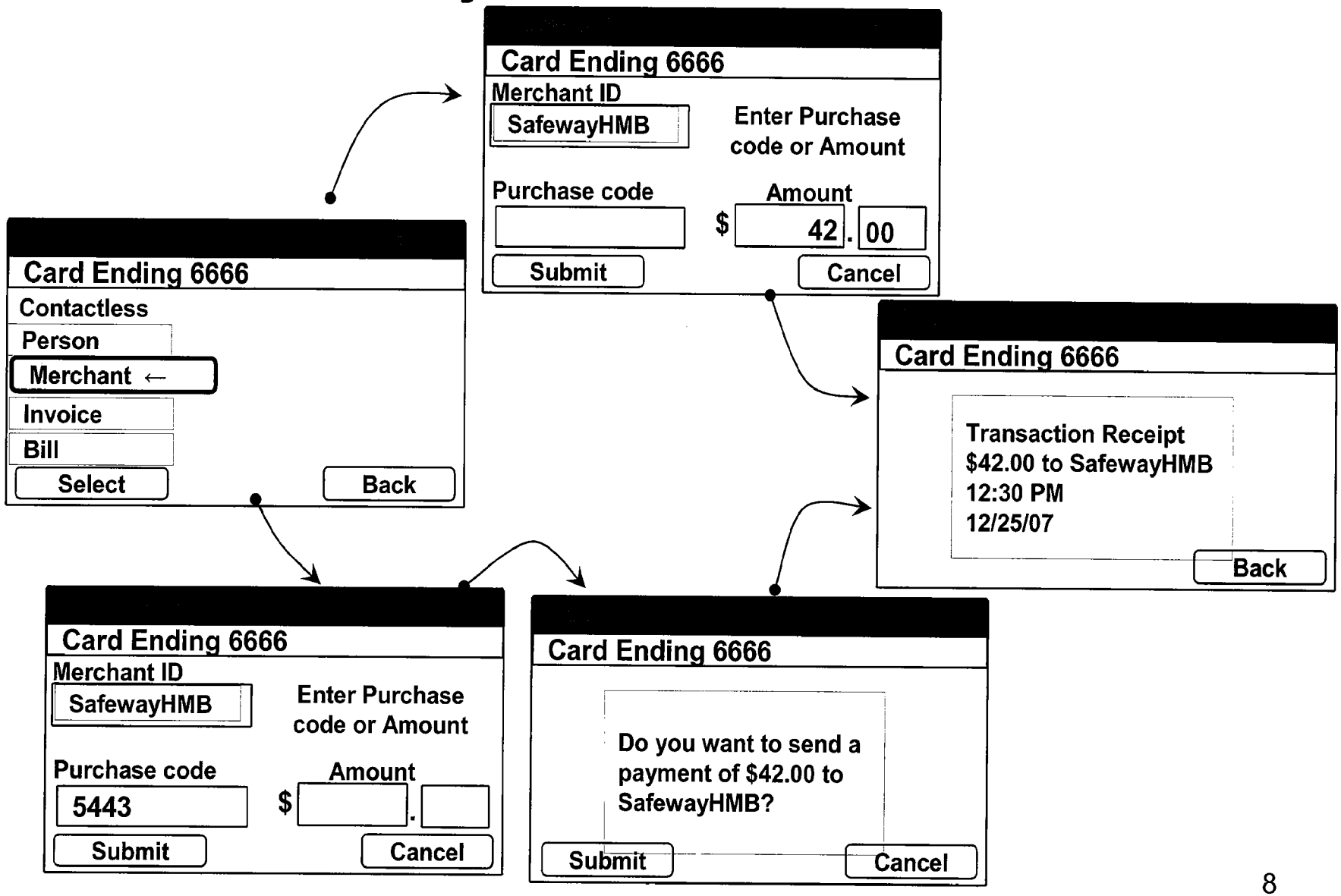
123 Petitioner Exhibit 1002-1518

Payments Page
Remote P2P or P2B Payments



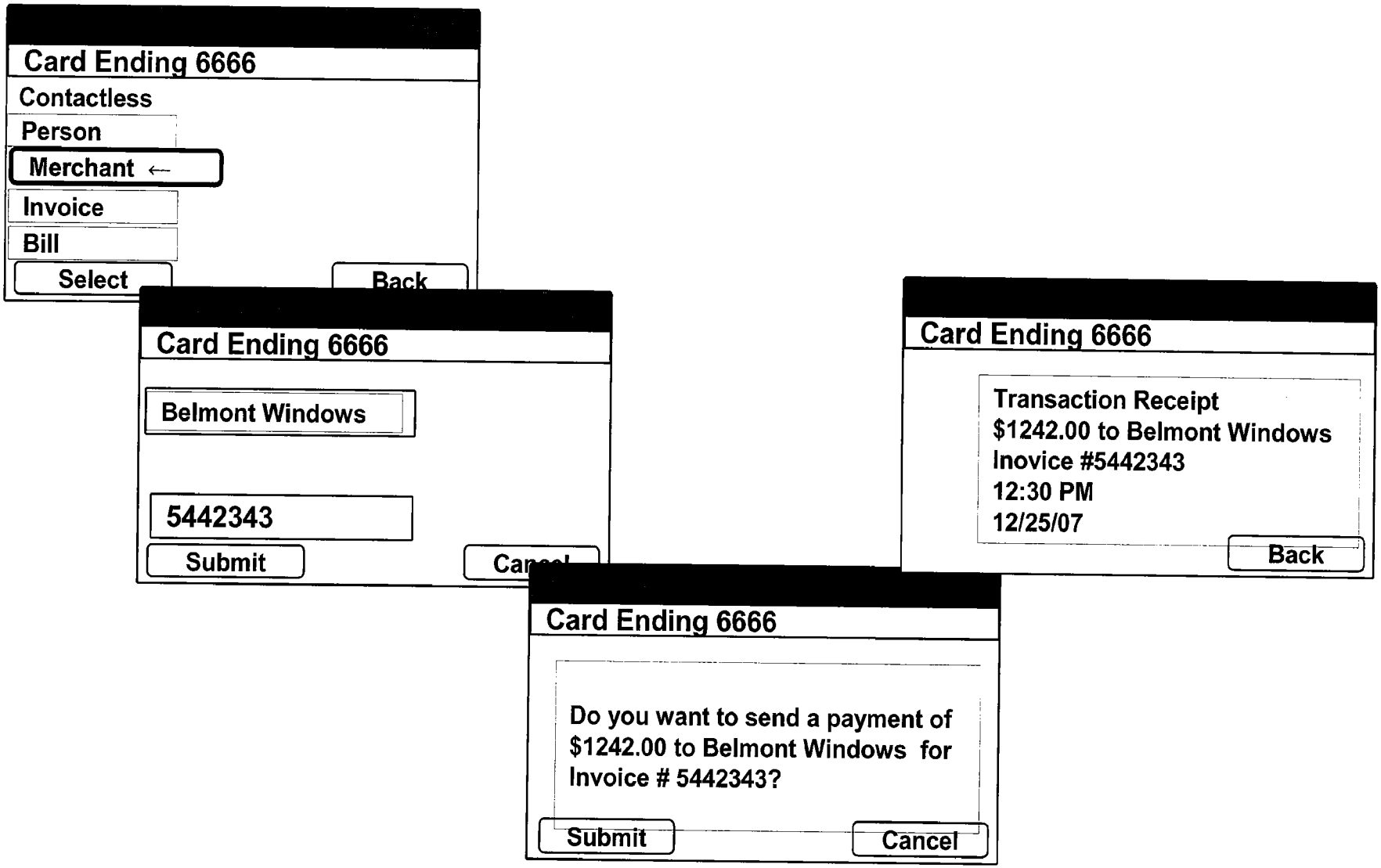
124 Petitioner Exhibit 1002-1519

Payments Page
Remote P2B Payments



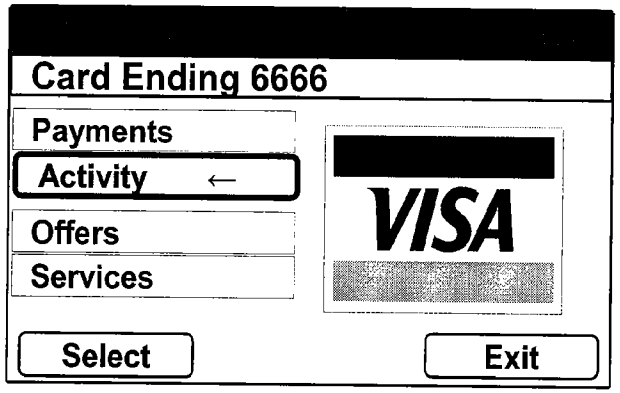
125 Petitioner Exhibit 1002-1520

Payments Page
Remote P2B Invoice Payment



I 24 Petitioner Exhibit 1002-1521

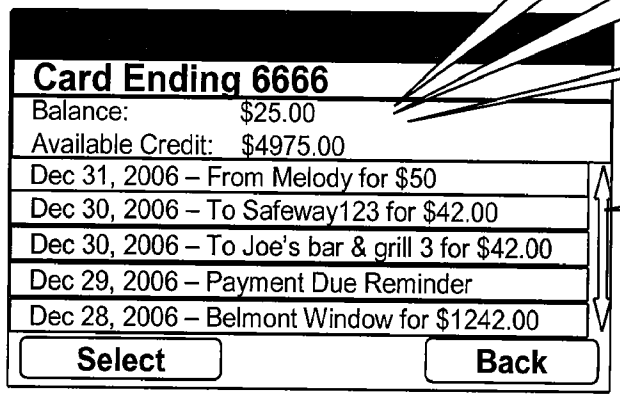
Activity



If 6666 is a credit card.
Balance: $xxx
Available Credit: $xxxx

If 6666 is a prepaid card.
Remaining Balance: $xxx

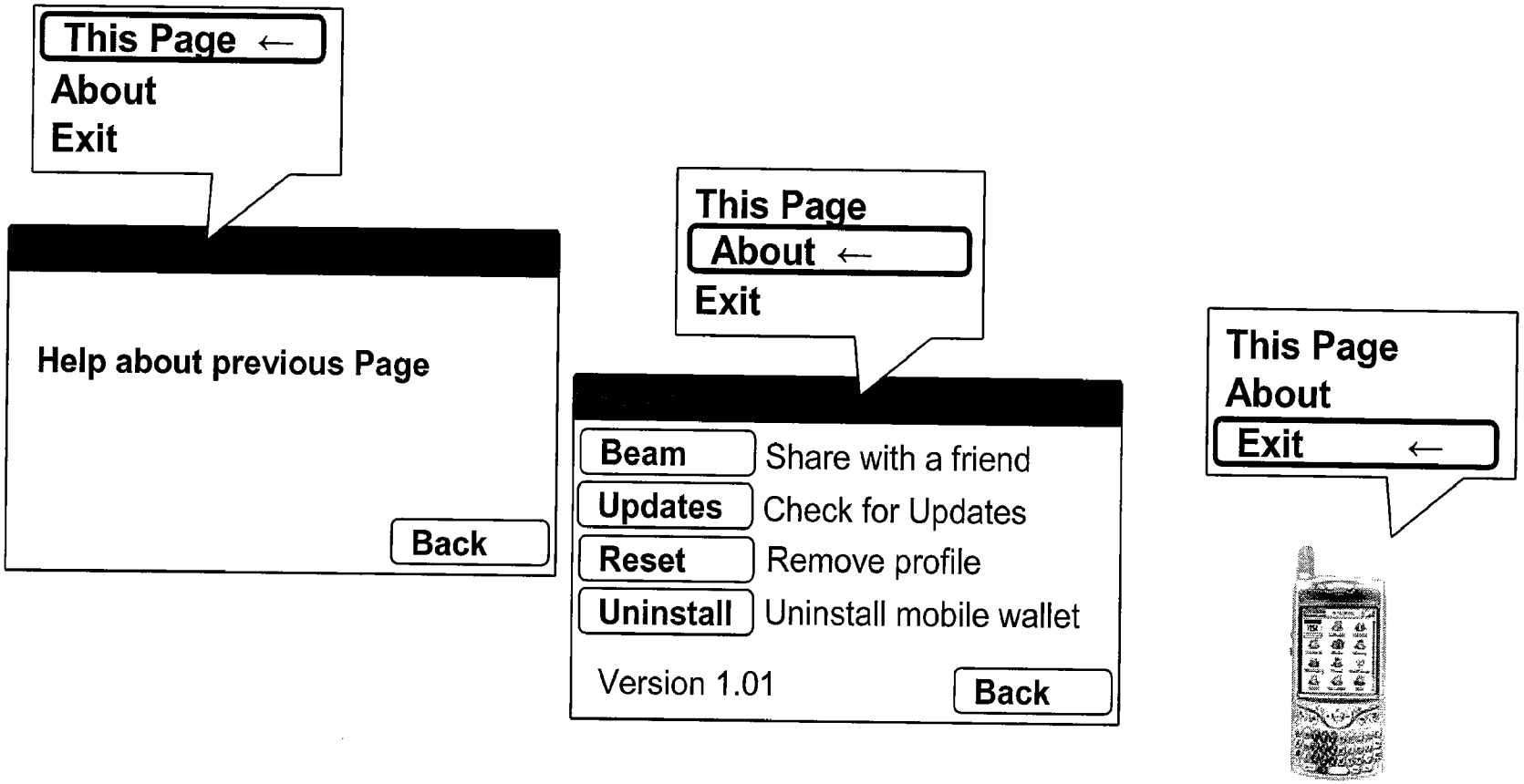
If 6666 is a debit card.
Account Balance: $xxxx



User can scroll through recent activity, alerts, and reminders. User can select an item for more detail.

1 2 7 Petitioner Exhibit 1002-1522

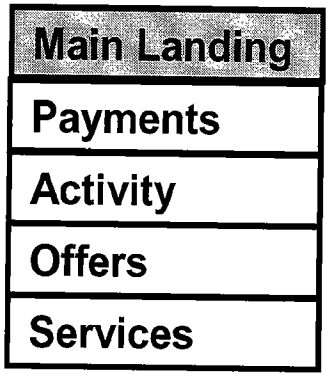
Help

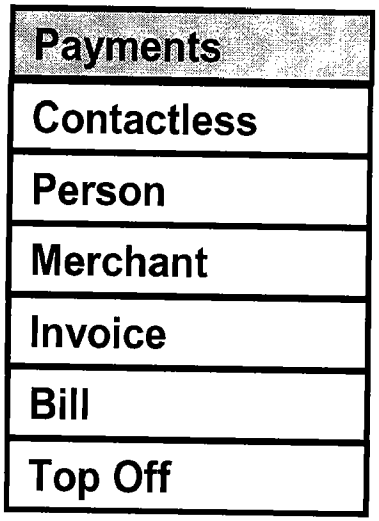


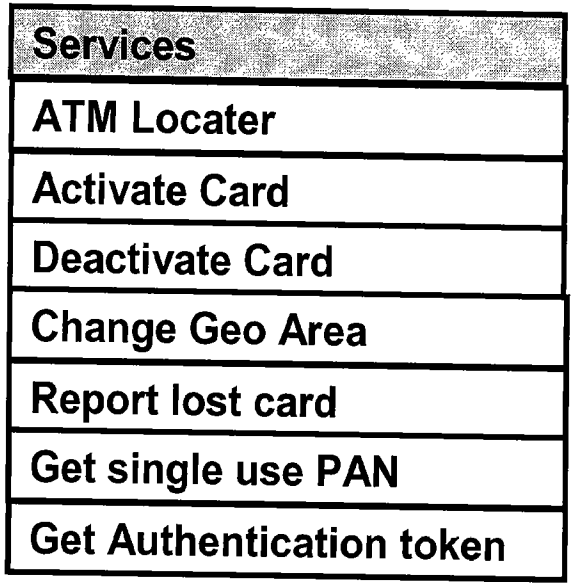
- Help is can be selected on any page. Help is consistent across all pages.
- About page has additional services specific to managing the application
- Beam encourages "viral sharing" of application

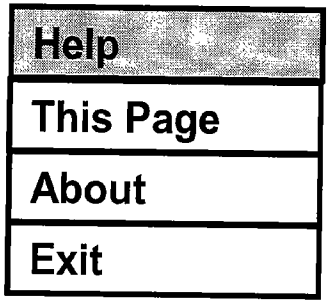
128 Petitioner Exhibit 1002-1523

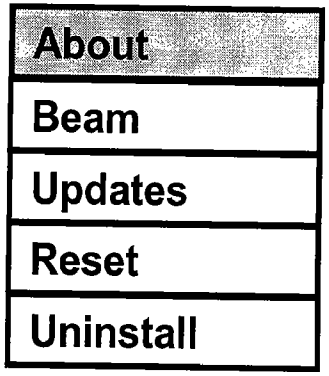
Service Tree

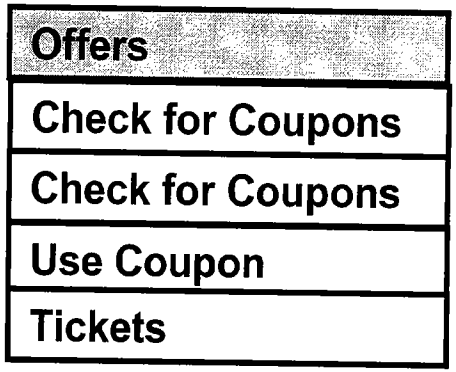












/ 21 Petitioner Exhibit 1002-1524

Tenets

- Key Success goal: Keep as simple, flat & user friendly as possible
- Each enrolled card has a config file. The config file
  - User only sees services which are available for that card
  - Services can be configured to point at different servers
- No sensitive data is left on the phone.
  - Only last 4 digits of card numbers are displayed
  - Mobile Pin is never stored

136 Petitioner Exhibit 1002-1525

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	VALUE BASED OFFERS
First Named Inventor/Applicant Name:	Mark Carlson
Filer:	Patrick Raymond Jewik/Andrea Beck
Attorney Docket Number:	16222U-028500US

Filed as Large Entity

Provisional Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Provisional application filing	1005	1	200	200
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Petitioner Exhibit 1002-1526

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**200**

Electronic Acknowledgement Receipt

EFS ID:	1400034
Application Number:	60871898
International Application Number:	
Confirmation Number:	2152
Title of Invention:	VALUE BASED OFFERS
First Named Inventor/Applicant Name:	Mark Carlson
Customer Number:	66945
Filer:	Patrick Raymond Jewik/Andrea Beck
Filer Authorized By:	Patrick Raymond Jewik
Attorney Docket Number:	16222U-028500US
Receipt Date:	26-DEC-2006
Filing Date:	
Time Stamp:	17:31:48
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$200
RAM confirmation Number	353
Deposit Account	201430
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1		app.pdf	7574140	yes	161

Multipart Description/PDF files in .zip description

Document Description	Start	End
Application Data Sheet	1	3
Specification	4	15
Claims	16	20
Abstract	21	21
Drawings	22	30
Appendix to the Specification	31	161

Warnings:

Information:

2	Fee Worksheet (PTO-06)	fee-info.pdf	8103	no	2

Warnings:

Information:

Total Files Size (in bytes):	7582243

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

01/24/2007 VVAN11 00000010 201430 60871898

01 FC:1085 250.00 DA

PTO-1556
(5/87)

U.S. Government Printing Office: 2003 — 486-267/60033

ASSESSING M-COMMERCE OPPORTUNITIES

Mark N. Frolick and Lei-da Chen

Shortly after the advent of digital mobile phone service, a new innovative way of doing business known as mobile commerce (M-commerce) was created. This article helps organizations gain insight as to whether mobile commerce is a business solution worth exploring. It reviews the technology behind M-commerce and the products and services currently available. It also examines the benefits and challenges of M-commerce, as well as the issues to be addressed when considering implementation of M-commerce solutions.

IN THE EARLY TO MID-1990S, TECHNOlogical buzzwords were "an IP Network," "hypertext," "the 'Net," and "the Web." Not only were executives desperately trying to understand and comprehend these buzzwords, but information technology professionals were confused as well. Today, more and more people are aware of digital technology and how the advancements in the industry are moving toward a more mobile economy. This new mobility can be attributed to the technological advancements in mobile phones, portable computers, and wireless data communications. Due to the rapid advances in these technologies, business foresight is often overlooked. There are many instances where corporate mission statements have been compromised or completely disregarded due to management's confusion regarding the technological buzzwords, hyped-up marketing schemes, and or the flash of the new technology.

Commerce is broadly defined as the buying and selling of goods and services. Many organizations today are selling goods and services on the Internet, which has been referred to as electronic commerce or E-commerce. During the late 1990s, this alternative form of commerce took off like wildfire. Many entrepreneurs investing in E-commerce amassed vast fortunes in less time than it took to build a single Wal-Mart Superstore. With literally every classification of business experimenting with E-commerce, investment bankers and upper management soon discovered which industries prospered from E-commerce, and which industries experienced bankruptcy.

In 1999, Sonera of Finland was the first telecom operator to provide the wireless technology needed to allow its customers to conduct commerce in a wireless fashion (Rasinghani, 2001.) This mode of commerce brought about a new technological buzzword known as mobile commerce (M-commerce). Some professionals define M-commerce as any form of mobile communication with the customer. However, there are others who feel that some form of monetary gain should be achieved. For example, Leung and Antypas (2001) defined M-commerce as both "content delivery (notification and reporting) and transactions (purchasing and data entry) on mobile devices." Another term used for M-commerce is "wireless E-commerce," as such business activities often leverage the existing Internet technologies and infrastructure.

M-commerce should not be confused with mobile information. Mobile information can be defined as providing information between a company and a customer or employee via wireless data communication. The information transmitted can take the form of text, graphics, video, or sound. Monetary gain from providing mobile information does not have to be the motive or intent of this service.

MARK N. FROLICK is the Western & Southern Financial Chair of Information Systems at Xavier University.

LEI-DA CHEN is a doctoral student of MIS at the University of Memphis, Tennessee.

Petitioner Exhibit 1002-1531

By understanding the difference between M-commerce and mobile information, we have a better foundation for determining the type of mobile technology organizations should be offering to their customers.

Nevertheless, mobile information is often indirectly associated with cost savings and increased revenues generated by replacing paper-based processes, improving employee efficiency, and enhancing customer relationships. By understanding the difference between M-commerce and mobile information, we have a better foundation for determining the type of mobile technology organizations should be offering to their customers.

Mobile connectivity by customers and employees is destined to have a much larger communication footprint in the future. If projections hold true, the two billion estimated wireless phone users who participate in M-commerce will increase the M-commerce user base by 25 percent by the year 2005 (Korper and Ellis, 2001). One imperative question to organizations is whether they should offer mobile commerce or simply mobile information to their customers and employees.

The purpose of this article is to help organizations gain insight into whether or not mobile commerce is a business solution worth exploring. A review of the technology behind M-commerce and the products and services currently available are discussed. The benefits and challenges of M-commerce, as well as the issues to be addressed when considering the implementation of M-commerce in an organization, are also addressed.

THE TECHNOLOGY BEHIND M-COMMERCE

Wireless communications begin with the introduction of mobile phone technology. There are three mobile telephone technologies today, of which the first is quickly becoming obsolete. The first mobile service implemented was Advanced Mobile Phone Service (AMPS), which is basically the cellular equivalent to the plain old telephone system (POTS). Second is the Digital-Advanced Mobile Phone Service (D-AMPS), which uses both time division multiplexing and frequency division multiplexing technologies. D-AMPS technology provides increased signal clarity, security, and additional features that are nonexistent in AMPS technology. Third is Personal Communication Systems (PCS) technology, which provides a fully digital signal. The two all-digital mobile phone platforms in the United States are Global System for Mobile Communication (GSM) and Code Division Multiple Access (CDMA).

GSM, although the predominant mobile technology used in Europe, is one of many multiple proprietary technologies used in the United States. The older time division multiple access (TDMA) standard, which is not 100 percent digital, is being phased out as its primary vendors, Cingular and AT&T, are moving to the GSM platform. This switch to GSM is due to the promise of what is known as the third generation (3G) of GSM, which is basically wireless broadband. There is yet another all-digital standard in the United States known as CDMA. This is the standard used by both Sprint and Verizon. The broadband platform for CDMA is wideband-CDMA (W-CDMA).

In addition to wide area wireless network solutions, many companies have invested in wireless local area networks (WLANs) to connect mobile customers and employees on the premises. Currently, the dominant WLAN standard is Wi-Fi. Many organizations have adopted the IEEE 802.11b technology, one of the Wi-Fi standards, to provide wireless access to users within a local geographical area (e.g., a building, campus, airport, coffee shop, or hotel). According to a recent study, the market penetration of WLAN in the United States has reached 10 percent, and users have credited WLAN with convenience, flexibility, mobility, time saving, and productivity gains (Cisco Systems, 2001). While IEEE 802.11b technology is the most popular WLAN solution among U.S. businesses today, new technologies (e.g., IEEE 802.11a) are promising higher data speed and more security in the near future.

For the M-commerce effort to be effective, an organization must select an appropriate way to deliver information wirelessly. The three most common M-commerce information delivery protocols are Wireless Application Protocol (WAP), General Packet Radio Service (GPRS), and Short Messaging Service (SMS).

WAP

The predominant communication protocol used today for M-commerce is the Wireless Application Protocol (WAP) (Rasinghani, 2001). WAP is a specification that allows mobile users to pick up e-mail, synchronize calendars, and access databases instantly over the Internet through handheld wireless devices. WAP is designed to work with most wireless networks and the current mobile communication platforms. WAP has gained broad acceptance because of its leverage of the existing Internet technology and ease of deployment. It is compatible with the majority of handsets currently on the market.

Petitioner Exhibit 1002-1532

SMS allows users of digital wireless handsets to send messages to each other.

WAP, however, is not without its problems. It tends to be rather slow because it was not originally designed for broadband communication. In addition to the lack of high-speed connection, the reliability of the services largely depends on the location of the user. WAP can also be expensive. WAP charges by the minute. As a result, longer connection times mean higher mobile phone charges. Furthermore, the limited display capability and input options of most handsets have made WAP applications less user-friendly and usable. Many companies using WAP have found that the growing pains are more than they want to deal with (Garfinkel, 2002).

GPRS

GPRS, in its basic form, can be thought of as wireless broadband. It is an add-on to GSM and works only with the GSM platform. GPRS is an always-on system that connects a mobile phone to the Internet. Unlike WAP, GSM charges by the kilobyte downloaded. The technological advance of GPRS is that instead of digitizing voice and sending it over a circuit-switched network like WAP, GPRS uses a TCP/IP stack in the phone to send data in high-speed packets, just like the Internet (Garfinkel, 2002).

The most well-known example of this type of service is NTT DoCoMo. This Japanese corporation began offering many different M-commerce products and services such as hotel reservations, online auctions, books, airline tickets, and stock quotes. DoCoMo named its service "i-mode." After two and a half years, the customer base has grown to more than 37 million users (Kolle 2001). i-mode is written in a language known as C-HTML.

On April 16, 2002, AT&T launched a service known as mMode. Is the naming similarity with i-mode a coincidence? Not by any means! DoCoMo now owns 16 percent of AT&T Wireless and has based its global expansion plan on convincing other operators around the globe to deploy i-mode services.

GPRS is much faster than WAP in that it was specifically designed to run on 3G networks. That does not mean, however, that GPRS does not have issues of concern. While, unlike WAP, there is not a per-minute charge for connection, charges are incurred per kilobyte downloaded. If a laptop user starts downloading PowerPoint presentations using a mobile phone as a modem, these charges can become very large.

SMS

True, M-commerce is not for everyone. What if all a company wants to do is deliver information to customers or potential customers? SMS is the answer to this M-information situation. SMS allows users of digital wireless handsets to send messages to each other.

In Europe, WAP has not worked well for many service providers, and 3G has had some serious growing pains (Rose, 2002). Ironically, the M-commerce information delivery protocol that is making the most money is also about as low-tech as you can get. It is known as Short Message Service (SMS). During the summer of 2002, this premium service was netting around $56 million per month for K-Mobile (Rose, 2002).

SMS can be used to generate sales using push marketing strategy. Wireless push marketing refers to the business situation in which the vendor initiates the communication and proactively delivers time-sensitive or location-specific promotional messages to consumers' mobile devices. The authors have coined the term "message and mortar" to describe this phenomenon. Nowhere can this be better demonstrated than in Singapore. At the Jurong Point shopping center, customers create a short text message and send it to the opt-in number advertised in the mall. Within a minute, customers receive a welcome message from the management of the shopping center. While shopping, customers' mobile phones beep intermittently signaling that another discount coupon has been received. The system allows shoppers to selectively receive coupons from the shopping center's merchants in the form of an SMS message (Thayer, 2002b). Many companies are hoping that Global Positioning Systems (GPS) will be used synergistically with SMS to deliver the timely promotional information to consumers at the right time and the right place in the near future.

BENEFITS OF MOBILE COMMERCE TO BUSINESSES AND CONSUMERS

M-commerce provides organizations with the means to sell products and services to customers and to deliver vital information to employees at any time and from most locations. This alternate means of connectivity provides an avenue to allow customers and employees to be anywhere and not have to be physically connected by a wire to the Internet. The technology allows instant communications with both customers and employees if needed, which has

Petitioner Exhibit 1002-1533

By utilizing mobile communications, corporations can eliminate expensive wiring in the offices connecting their workstations.

merit in a competitive situation. While M-commerce is still in its infancy, its strategic implications to businesses are endless. The benefits of M-commerce and existing M-commerce applications discussed in this section serve as starting points for managers to explore how their organizations can use wireless technology to achieve competitive advantage.

Wireless technology provides great value to businesses when it allows employees to access real-time data to make timely decisions that either decrease costs or increase revenues. For example, a field salesperson could access a wide range of information, including customers' purchase history and availability of products. If the product the customer wants is not in stock, a suitable alternative could be recommended at that time. One international corporation based in Memphis, Tennessee, is currently working on a sales order application for the sales executives to obtain digital signatures using PDAs in the field, which would allow immediate uploading of the order to the corporate office for processing and billing. The speed of processing with wireless sales transactions and the reduced error rate, when compared to handwritten orders, are phenomenal. As this example demonstrates, mobile commerce has the potential to reengineer the less efficient business processes and make them more streamlined; business can leverage wireless technology to reduce costs and increase worker productivity.

Businesses are using mobile devices to create more contact points with their customers and improve customer services by bringing the products and services directly to the customers. Toronto Blue Jays staff members, armed with wireless touch-screen displays with mobile credit card processing equipment, roam parking lots, shopping malls, and other areas adjacent to the Toronto Sky Dome looking for fans to attend games. These cyber-sellers then print out tickets on the spot (Thayer, 2002a). In the hospitality industry, hotels have not only installed WLANs to make it convenient for their customers to connect to the Internet, but have also adopted technology that allows their employees to register check-in guests in the lobby, parking lot, and conference rooms (McGarvey, 2002).

M-commerce provides a valuable channel for enhancing customer relationships as well as direct marketing and promotional activities. Experts pointed out that the key to effective mobile marketing is to fully exploit the time-critical, location-based, and personal nature of the mobile channel (Jimenez, 2002). Directory services offered via mobile devices (e.g., wireless restaurant guide and movie guide) are directing consumers to business venues that are close to the consumers' location. Location technologies, such as GPS, will enable M-commerce applications that take a user's location into account and provide users with access to localized and personalized information. For example, a service that delivers targeted promotional messages to mobile devices when the potential customers are within the business' vicinity will prove to be valuable.

By utilizing mobile communications, corporations can eliminate expensive wiring in the offices connecting their workstations. Wireless networks will also help conserve a valuable metal (copper), which is used in all communication and network wiring.

To consumers, M-commerce applications offer unprecedented convenience and access to information. A new service called Wireless Rebidding is a joint venture of the popular online auction service eBay and InPhonic. The service sends an SMS alert to a mobile phone anytime a subscriber's bid is outbid (Martin, 2001). Fidelity Investments and Etrade have implemented equity trading services to allow customers to trade stocks and bonds from anywhere. In China, the government sells lottery tickets directly to individuals' handsets that completely bypass the retailer (Friesen, 2002). Furthermore, the technology enhances consumers' bargaining power by diminishing the information asymmetry between the buyers and sellers.

Wireless devices are proliferating as new tools to support mobile payment (M-payment) and micropayments. An interesting example of M-commerce involves individuals purchasing soft drinks from vending machines utilizing a mobile handset (Johnson, 2002). In some European cities, one's mobile phone can be used to not only find the nearest parking space, but also to pay for it. AT&T Wireless has released an M-wallet feature that allows subscribers to add purchases to their monthly bills or charge them to a credit card (Smith, 2002).

CHALLENGES POSED BY MOBILE COMMERCE

Implementing M-commerce can lead to significant benefits for both businesses and consumers. However, there are many challenges that should be considered when developing an M-commerce strategy. Some challenges outlined

Petitioner Exhibit 1002-1534

Organizations must educate their employees about security risks and means of prevention.

here may or may not be considered critical to every class of business. Each class of business should respectfully take each disadvantage into consideration when determining their relevancy.

According to a survey of 270 IT professionals in May 2002, the most prominent barriers to wireless technologies adoption were a lack of security, unproven benefits/ROI, and high start-up costs (Ware, 2002). Many aspects of security have not been thoroughly addressed, as was the problem with the wired Internet until the implementation of 128-bit encryption. A cautious employee with the TRW Company consulted with an outside firm regarding their wireless network. The consulting firm provided an evaluation stating that a hacker could literally drive into their parking lot with the proper equipment and intercept their data (Sherman, 2002). Of course, the management began implementing the proper encryption keys. It was, however, unfortunate that this was not done at the beginning. Wireless security is still in need of improvement to meet the requirements of M-commerce. Businesses and consumers must feel safe transmitting sensitive transaction-related data over wireless media. Like wired networks, wireless networks must be designed to provide the authentication, privacy, integrity, and non-repudiation required for secure online transactions.

The small size and portability of wireless devices have raised the concern of physical security. Cell phones, PDAs, and laptops can be easily lost or stolen. Only a small portion of wireless users utilize the built-in security features, such as password protection and locking keypads, to protect information in case of loss or theft. Furthermore, data on handheld devices is seldom encrypted. Organizations must educate their employees about these risks and means of prevention.

Another risk regarding security concerns which party is responsible should a financial or data theft occur. The blame could be cast to the wireless service provider or to the financial institution's software application. When it comes to financial loss, customers rely on banks or financial institutions to protect their money. It may not, however, be the fault of the bank or financial institution (DeZoysa, 2001).

The weakened economy has placed an enormous burden on IT managers to justify new investment in wireless technology for M-commerce. However, determining the ROI from M-commerce efforts is not always easy. The intangible benefits, such as increased productivity and customer satisfaction, provided by M-commerce applications cannot be easily measured. Therefore, a large number of planned wireless projects failed to materialize, according to a recent CIO survey (Worthen, 2002). On the other hand, organizations must avoid the danger of investing in M-commerce solely based on media hype instead of its potential strategic impact on the organization. IT managers must realize that not all business activities are good candidates for M-commerce. For example, one retirement financial services company abandoned a project to extend its company's Web site to handheld devices because it failed to see the demand for a service that enables customers to trade their 401(k) as they walk through the airport (Worthen, 2002). Therefore, the *first* step in planning for any M-commerce project should always be that of making a business case for such an investment.

At the present time, the cost for consumers to participate in M-commerce remains relatively high. One downside of GPRS is cost. This particular M-commerce technology charges by the kilobyte of data transferred. To add to this problem, even if a user only transmits a partial kilobyte of data, most GPRS vendors round up to the next full kilobyte on a daily basis. This has the potential to add up significantly over a billing cycle (Parker, 2002).

Airtime minutes should also be considered if transactions take an extremely long time. Situations that cause customers to exceed their allotted minutes may invoke frustration and resentment toward the company. The reliability of the mobile service provided to customers in Europe far exceeds that in the United States. In the United States, users can be standing perfectly still and lose connection from their service providers. Transaction speed, text in lieu of graphic screens, and battery life of mobile devices are other challenging issues in M-commerce.

M-commerce application developers are facing a growing array of client devices for which applications are designed. Applications developed for general consumer use must be compatible with a wide range of devices, including mobile phones, PDAs (both Palm and Window CE devices), pagers, and laptops. These devices are constrained by their display capabilities, input options, limited processing power, memory, or battery life. As one expert pointed out, the wide adoption of an M-commerce application requires its compatibility with multiple devices (Worthen, 2001). Understanding the strengths and constraints of these

Petitioner Exhibit 1002-1535

The organization must be able to identify the real business drivers for mobile technologies and demonstrate how M-commerce solutions will help it solve existing problems, capitalize new opportunities, or create a competitive edge.

client devices and designing effective user interfaces for M-commerce application will continue to be a major challenge to developers. Furthermore, new emerging technologies and lack of standardization make it even more difficult for IT managers to determine the choice of technical platform for M-commerce applications.

ISSUES TO CONSIDER

When considering the implementation of M-commerce to a business model, management should pay close attention to both the technical and business issues. While some of these issues are similar to those that need to be considered while implementing E-commerce, wireless technologies have presented many new opportunities and challenges. Some of the most important issues that reflect the unique characteristics of M-commerce are discussed below.

Making the Business Case

The first and the most important step in developing a mobile strategy is *building the business case*. The organization must be able to identify the real business drivers for mobile technologies and demonstrate how M-commerce solutions will help it solve existing problems, capitalize new opportunities, or create a competitive edge. For starters, the organization needs to consider the following items. These items have been outlined in a question form and should be analyzed in-depth as to their validity in each occurrence.

- What business problems can be solved by mobile technologies?
- Are our customers and employees likely to use mobile devices?
- Will the mobile platform primarily be used to deliver information (i.e., M-information) or facilitate transactions (i.e., M-commerce)?
- Is the product or service time sensitive or location sensitive?
- How many of my potential users feel secure in transmitting sensitive information via wireless networks?
- Can the company make a profit or reduce costs from the investment of M-commerce technology, or will the initial investment, transaction cost, and support exceed the profit of the product or service sold?
- Will the investment in M-commerce technology produce any intangible benefits, such as improved customer service or employee morale?

Providing M-commerce with real business incentives behind it should be ranked with the highest priority in the decision process. Companies should avoid adopting new technology just because it is a great new toy. The feasibility of M-commerce can be detrimental or place extreme pressure on a company's assets. Office Depot experienced the pressures of wireless technology. Upon implementing the wireless logistics and distribution tracking system OD STAR, Office Depot lost significant profits annually on customer disputes resulting prior to offering M-commerce (Goldman, 2001). QVC, the home shopping network, put M-commerce this way: "You shouldn't just do things because you can do them. We can list our products for sale on cell phones and PDAs, but why should we? It wouldn't enhance sales enough to be worth the headaches." (Anonymous, 2002).

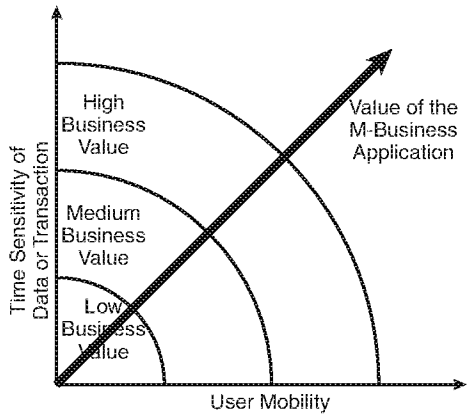
As Chen and Nath (2003) pointed out in their study, the value of M-commerce is a function of the time sensitivity of the data or transaction, and the mobility of the information user. The value of M-commerce increases with an increase in user mobility and time sensitivity of the required data or transaction (see Figure 1). Using time sensitivity of data or transaction and user mobility as the two dimensions, managers can categorize business activities into classes of applications that have the potential to contribute a low, medium, or high level of value to the business by making these applications wireless. This approach allows managers to identify those business processes where wireless applications are likely to bring the most value to the company.

Being an Early Adopter?

Organizations that find that an M-commerce strategy makes business sense are recommended to use a step-wise implementation plan to edge into this uncharted territory. A pilot project designed for a small business unit where M-commerce can deliver obvious benefits (e.g., e-mail and sales force automation) will provide management with valuable lessons to improve the chance of success for more ambitious M-commerce projects in the future. While capitalizing on the "first-to-market" advantage is considered important sometimes, the history of E-commerce has taught us that competitive advantages created by IT were often unsustainable and could be easily duplicated by competitors. As Porter (2001) pointed out, technology

Petitioner Exhibit 1002-1536

FIGURE 1 The Business Value of M-Business Applications



[Adapted from Chen and Nath (2003)]

acts as a neutral competitive tool due to the ease of acquisition and replication by competitors. A company will gain competitive advantages more effectively through strategic positioning rather than chasing the waves of technology. Furthermore, competitors that wait and take advantage of the new and improved technologies and business processes often surpass first-movers in this dynamic technical and business environment.

Identifying Applications before Selecting Devices

Dazzled by a wide variety of wireless gadgets, managers are often tempted to start their M-commerce efforts with the selection of devices. However, this approach contradicts the traditional systems design and development framework, in which the identification, analysis and logical design of applications happen before the selection of tools (physical design). The rationale behind this approach is that the system development process should be application driven rather than tool driven. Tools are selected based on their ability to meet the requirements of the application, instead of the other way around. Wireless devices differ in many aspects, such as size, display, memory, battery life, technology platform, and expansion capabilities; therefore, selecting the device before identifying the application will seriously limit the functionalities of the future application. In many accounts, a less popular and more proprietary device may be the device of choice due to the unique requirements of the application. In the case of a German hospital that provides its heath-care staff with wireless devices, the hospital chose to adopt Palm devices with Bluetooth capabilities instead of the more popular pocket PCs and the IEEE 802.11b solution because it felt that the ease-of-use of Palm devices and the low power consumption of Bluetooth technology best suited the requirements of the intended applications. Therefore, an organization must take into account the unique requirements of its mobile applications while selecting mobile devices.

For organizations that already have various devices in use in the field, *standardization* should be the next step. The diversity of mobile devices has far surpassed the diversity of PCs. Therefore, standardizing the device while at the same time trying to satisfy varied functional requirements is a daunting task. Nevertheless, managers will find that the advantages of standardizing outweigh its repercussions, as standardizing client devices will help reduce application development complexity and maintenance costs, and ensure the availability and reliability of services.

Technology Selection

Many of the technical considerations relevant to M-commerce were discussed in previous sections of this article. In general, IT managers should follow the following principles when making technology selection decisions: scalable and flexible infrastructure, well-supported protocols and applications, strong security measures, and standardized and functional devices.

To quickly deploy their mobile solutions, many organizations turn to system integrators and application service providers (ASPs) instead of acquiring internal expertise. The former is favored by large enterprises, which plan to implement mobile solutions that span across multiple business units, and the latter is often employed by organizations to mobilize a single business unit or application. While outsourcing is a viable and highly recommended approach to help an organization improve its applications' time-to-market, the volatile technology industry sector has added an additional layer of concerns. The volatility of the mobile technology market can be demonstrated by the case of the world's largest brick-and-click bookseller, Barnes and Noble. During the implementation of wireless capabilities, its key wireless technology partner, NetMorph, filed for bankruptcy (Prior, 2001).

Petitioner Exhibit 1002-1537

To help corporations continue to find prosperity, each product and service offered should be evaluated on an individual basis as to whether M-commerce is viable.

User Acceptance

Experience has shown that the diffusion of new technologies has not always been smooth sailing. While M-commerce is a very exciting prospect, many questions have emerged. Will users accept the new technology-based services? Will a new mobile application be able to effortlessly diffuse itself into the user community? Will employees who are equipped with mobile capabilities accept the responsibilities and self-discipline that come with the ability to work anywhere at anytime? User acceptance and innovation diffusion have been two recurring issues in the IT field. When a technology is not accepted and used effectively by users, only a fraction of its potential benefit is realized. An application rollout plan must be included as an indispensable part of the M-commerce strategy. Managers should consult the technology acceptance model (TAM) (Davis, 1986) and innovation diffusion theory (IDT) (Rogers, 1995) when designing a rollout strategy. Based on these classic theoretical models, a number of application-specific acceptance models were developed, including the wireless technology diffusion model (Gera and Chen, 2003), which can be readily applied in this situation. These frameworks offer a comprehensive theoretical paradigm that takes into account the technological, psychological, and sociological factors that influence the acceptance of new technologies.

CONCLUSION

Some organizations have found that by capitalizing on new digital technology quickly, significant profits can be earned. The idea of whether mobile commerce should be provided to all customers for all products and services is a farce. There are too many products and services where the mobile technology would only drive the cost of the item higher and possibly add more frustration for the customer. To help corporations continue to find prosperity, each product and service offered should be evaluated on an individual basis as to whether M-commerce is viable. The mobile commerce technologies will improve exponentially, and the analysis of the technology will need to be revised in relationship to the improvements. As of this writing, however, caution should be exercised by any organizations before treading on M-commerce waters. ▲

References

1. Anonymous. "Use Tech as a Tool," *Men's Health,* September 2002, p. 64.
2. Chen, L.D. and Nath, R. "A Framework for Mobile Business Applications," *International Journal of Mobile Communications,* 2003 (forthcoming).
3. Cisco Systems. "Wireless LAN Benefit Study," NOP World-Technology, 2001. Available at http://newsroom.cisco.com/dlls/tln/WLAN_study.pdf.
4. Davis, F.D. A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results, Doctoral dissertation, 1986. MIT Sloan School of Management, Cambridge, MA.
5. DeZoysa, S. "Who Do You Trust?," *Telecommunications,* 35(12), 70–72, December 2001.
6. Friesen, G.B. "M-commerce mmm-good?" *Consulting to Management,* 13(2), 26–29, June 2002.
7. Garfinkel, S. "What is GPRS," *Wired,* September 2002, p. 40.
8. Gera, K. and Chen, L.D. "Wireless Technology Diffusion: An Evaluation Model for Wireless Services," *Proceedings of Association for Information Systems Annual Conference,* 2003.
9. Goldman, C. "Data on Aisle Six!," *Overland Park,* 18(17), 11A–15A, September 2001.
10. Jimenez, H. "B2C E-Commerce Gaining Foothold," *Business World,* April 2002.
11. Johnson, T. "Project Canned," *Communications International,* February 2002, p. 14.
12. Kolle, C. "The Wireless Age," *Asian Business,* 37(11), 25, November 2001.
13. Korper, S. and Ellis, J. *The E-Commerce Book: Building the E-Empire (2nd ed.),* San Diego, CA: Academic Press, 2001.
14. Leung, K. and Antypas, J. "Improving Returns on M-Commerce Investments," *Journal of Business Strategy,* 22(5), 12–16, Sept.–Oct. 2001.
15. Martin, Z. "Stairway to the Future: Mobile Commerce Special Report," Thomson Publishing Corporation, January 2001.
16. McGarvey, R. "Hospitality Checks Out Wireless," *Mbusiness,* March 2002, pp. 18–23.
17. Raisinghani, M.S. "WAP: Transactional Technology for M-Commerce," *Information Systems Management,* 18(3), 8–16, 2001.
18. Parker, T. "SMS, Romance, and Other Sexy Topics: Wireless Phones Become Ever More Personal," *Pen Computing,* 9(45), 34–35, July 2002.
19. Porter, M.E. "Strategy and the Internet," *Harvard Business Review,* March 2001, pp. 63–78.
20. Prior, M. "M-Commerce Infancy No Day in the Park," *Dsn Retailing Today,* 40(16), 1, p. 35, August 2001.
21. Rogers, E.M. *The Diffusion of Innovations, 4th ed.,* New York: Free Press, 1995.

Petitioner Exhibit 1002-1538

22. Rose, F. "Why Premium SMS Took Off," *Wired,* September 2002, p. 40.
23. Sherman, E. "The Next Setup Forward," *Newsweek,* 139(11), 38B–38D, March 2002.
24. Smith, B. "Under the Radar: Wireless Internet," *Reed Business Information,* August 2002.
25. Thayer, G. "M-Commerce: Long Trek to the Promised Land," *Pen Computing,* 9(45), 17, July 2002a.
26. Thayer, G. "Shopping in Singapore? Don't Forget your Mobile," *Pen Computing,* 9(45), 20, July 2002b.
27. Ware, L.C. "Wireless Update — Slow and Steady Progress," *CIO,* September 30, 2002. Available at http://www2.cio.com/research/surveyreport.cfm?id=36.
28. Worthen, B. "Will You Still Love It Tomorrow," *CIO,* October 15, 2001. Available at http://www.cio.com/archive/101501/tomorrow.html.
29. Worthen, B. "When Wireless Works," *Computerworld,* December 4, 2002. Available at http://www.computerworld.com/mobiletopics/mobile/story/0,10801,76397,00.html.

Petitioner Exhibit 1002-1539

Copyright of Information Systems Management is the property of Auerbach Publications Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.

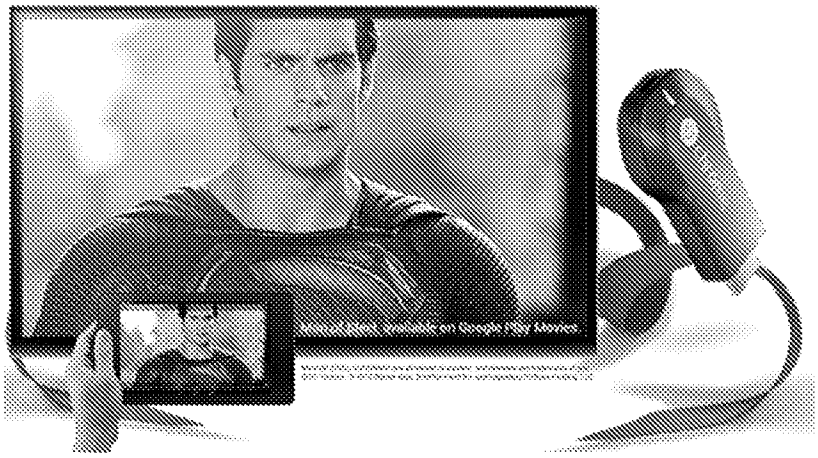
chrome

MENU

Chromecast

The easiest way to enjoy online video and music on your TV.

$35 Buy now



Sit back, watch together

With Chromecast, you can easily enjoy your favorite online entertainment on your HDTV—movies, TV shows, music, and more from Netflix, YouTube, HBO GO, Hulu Plus, Google Play Movies and Music, and Chrome. No more huddling around small screens and tiny speakers. Chromecast automatically updates to work with a growing number of apps.

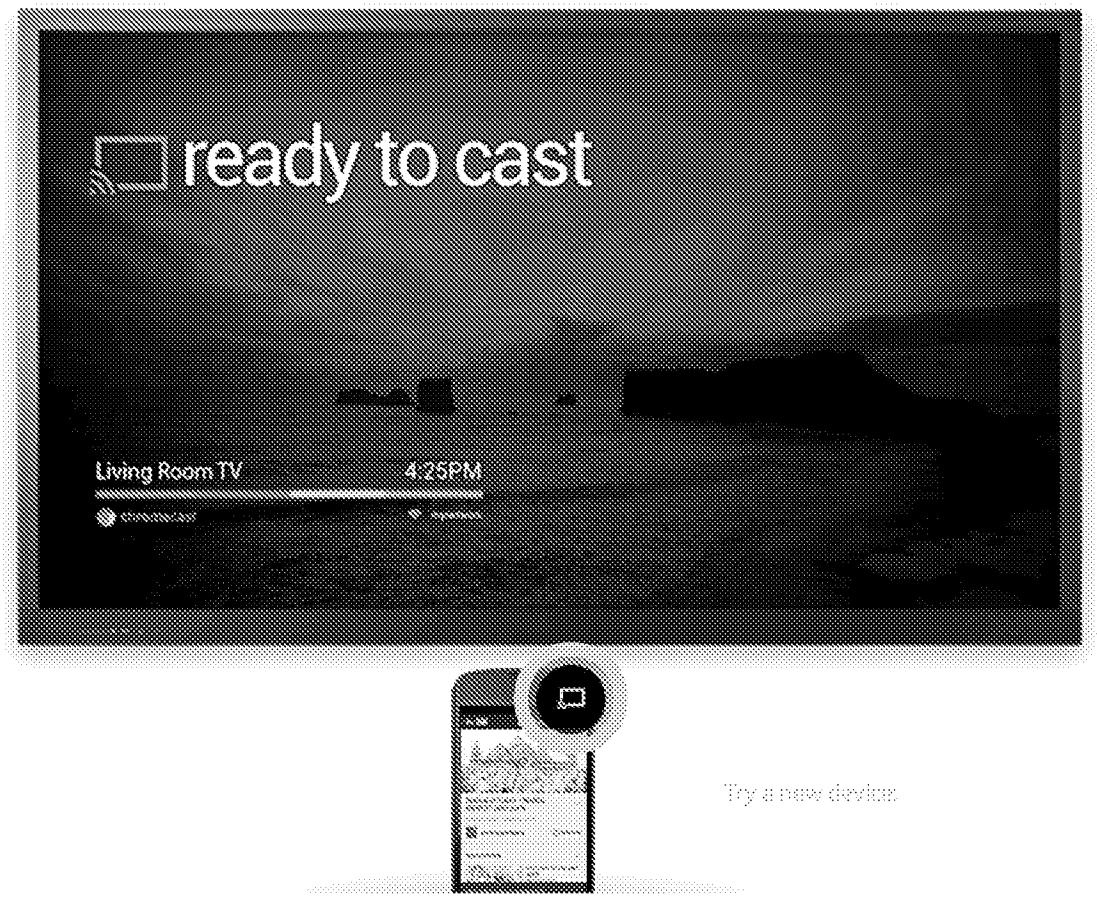
Petitioner Exhibit 1002-1541



Watch thousands of TV shows and movies on your TV.
See everything you can enjoy with Chromecast

Remote free

Chromecast works with devices you already own, including Android tablets and smartphones, iPhones®, iPads®, Chrome for Mac® and Chrome for Windows®. Browse for what to watch, control playback, and adjust volume using your device. You won't have to learn anything new.



Plug in and play

Get started in 3 easy steps: plug Chromecast into any HDTV, connect it to WiFi, then send videos and more from your smartphone, tablet or laptop to your TV with the press of a button.

See it in action

plug in

connect

enjoy





Chromecast

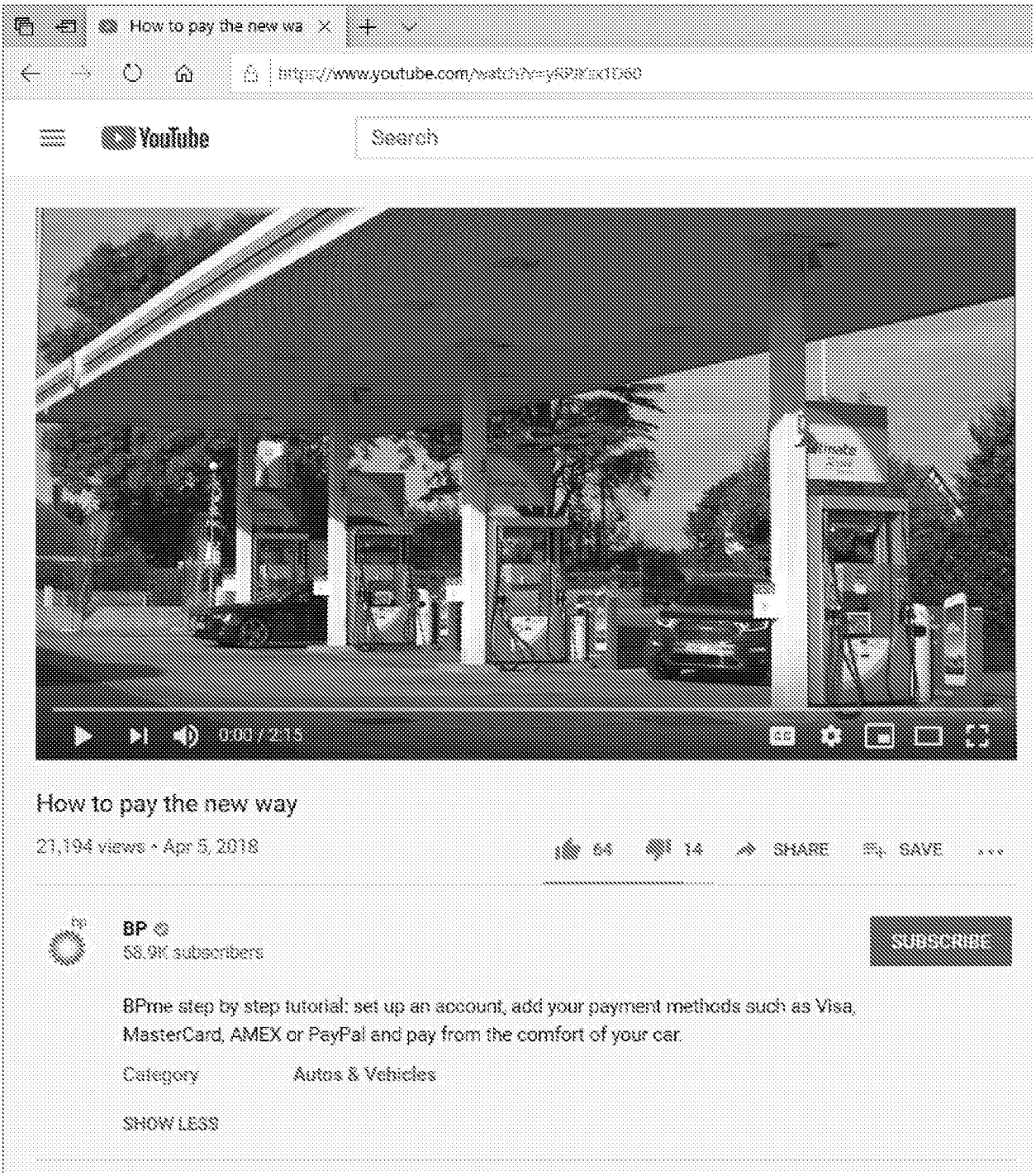
Everything you love, now on your TV.

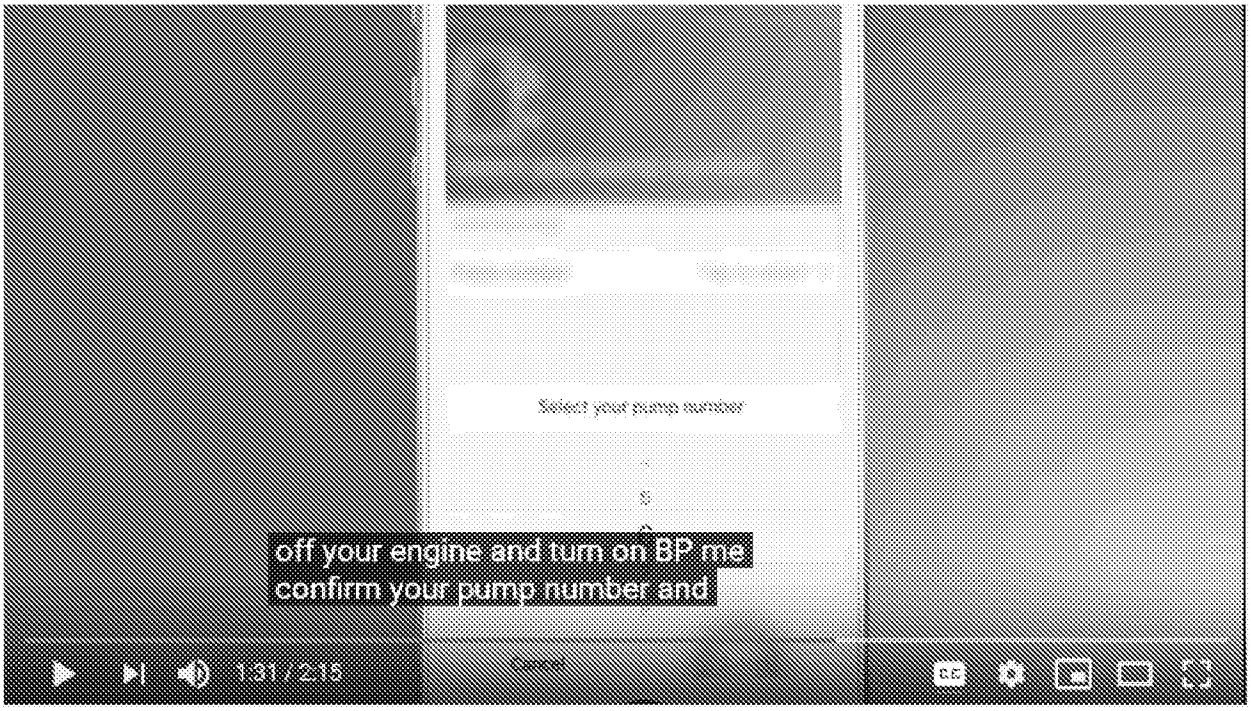
$35 Buy now

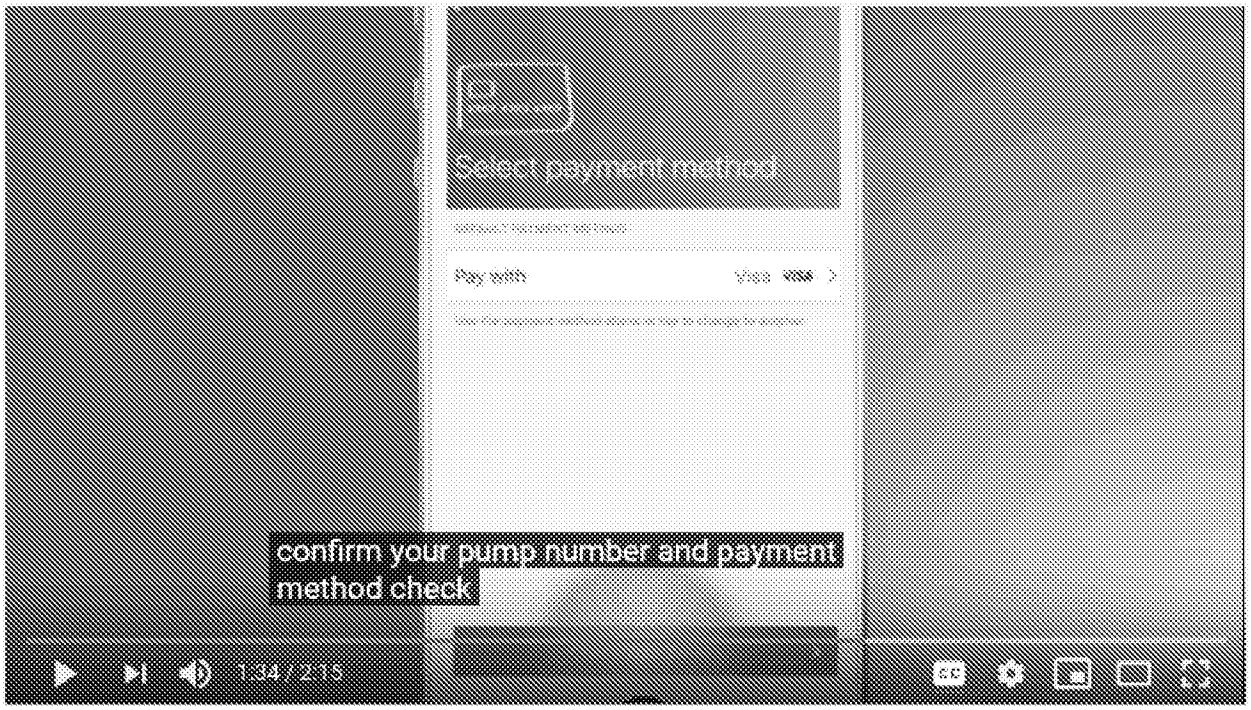
Subscriptions may be required to use with certain content providers. Chromecast is compatible with WiFi-enabled Android 2.3+ smartphones and tablets; iOS 6.0+ iPhones, iPads, and iPods; Chrome for Mac® and Chrome for Windows®; and Chromebook Pixel.

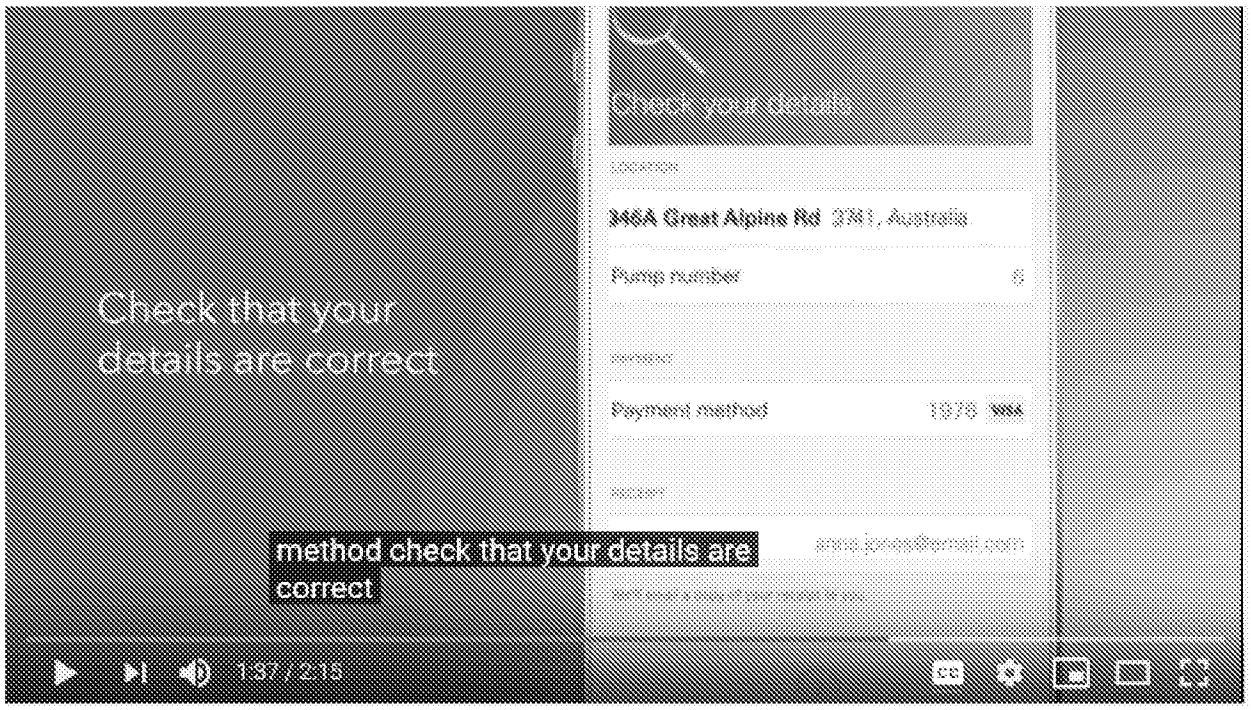
Petitioner Exhibit 1002-1544

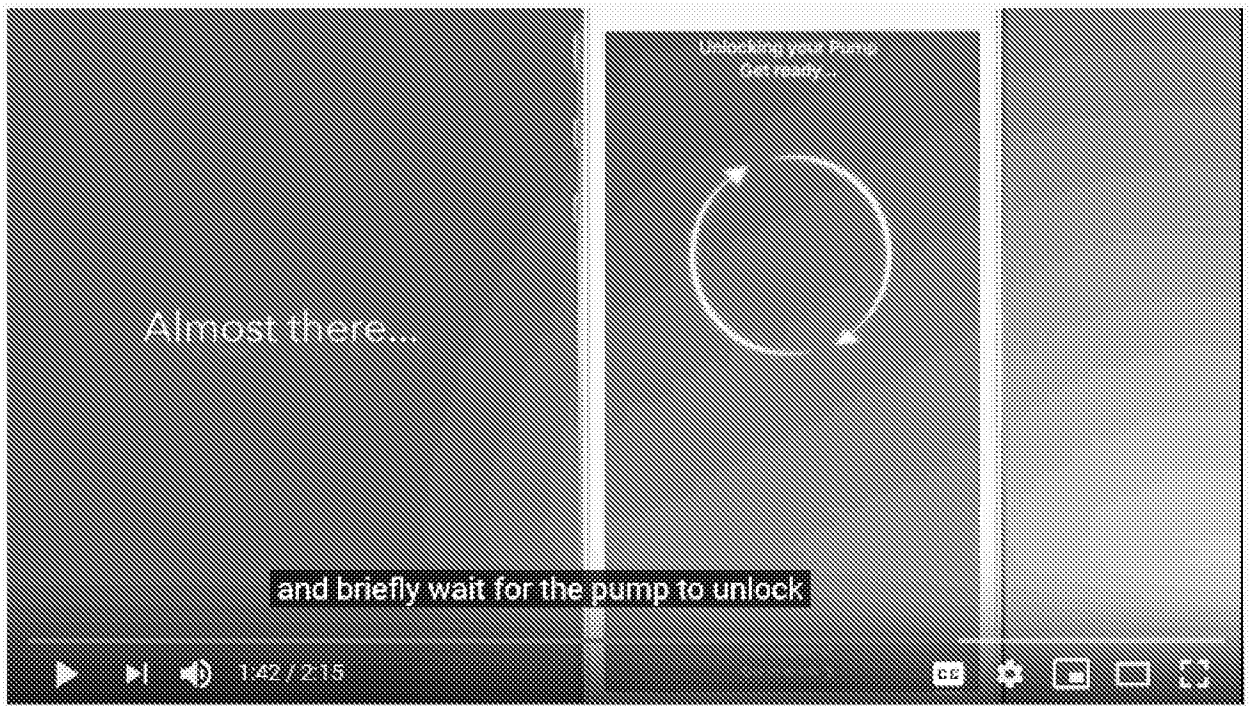
"How to pay the new way." *YouTube*, uploaded by BP, 5 April 2018, www.youtube.com/watch?v=yRPJKsx1D60

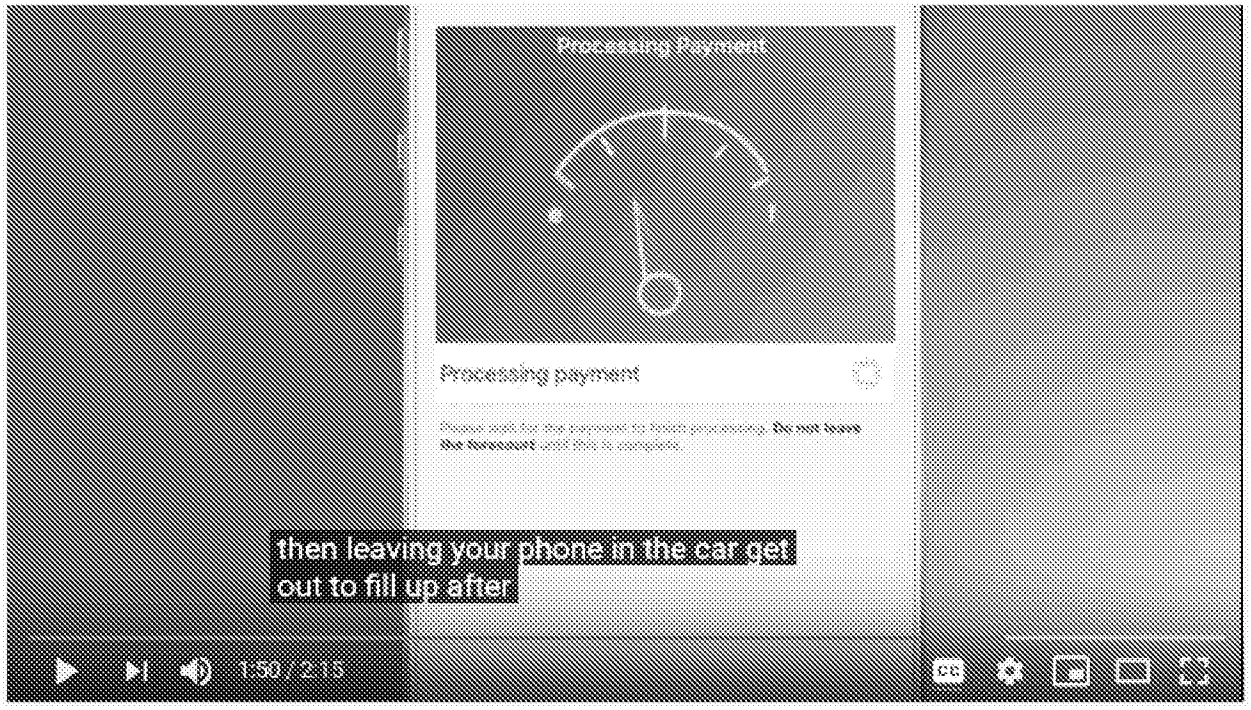



Select your pump number
off your engine and turn on BP me
confirm your pump number and
1:31 / 2:15


Select payment method
Pay with
confirm your pump number and payment
method check
1:34 / 2:15


Check that your details are correct
346A Great Alpine Rd 3741, Australia
Pump number 6
Payment method 1976
method check that your details are correct
137 / 215


Almost there...
and briefly wait for the pump to unlock
142 / 215

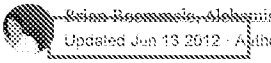

Processing Payment
Processing payment
then leaving your phone in the car get
out to fill up after
1:50 / 2:15

Search for questions, peo Ask New Question Sign In

Apps by Apple Wallet (iOS app) Online and Mobile Payment Startups Digital Wallets

How will Apple's new mobile wallet Passbook impact other mobile wallets?

17 Answers



Updated Jun 13 2012 · Author has 1.3k answers and 11.4m answer views

Apple has entered into the mobile wallet marketplace by sticking just a toe in the ocean of mobile payments. In the process Apple will change just about all aspects of discounts, ticketing and payments.

Meet Passbook

Today 6/11/2012, is the moment that many have waited for, the beginning signs of the Apple mobile wallet called Passbook. Passbook is an iOS 6 app fully integrated into iOS 6 with developer APIs to extend current features to other iOS apps. Passbook will have APIs for centrally locating just about all gift cards, loyalty cards, reward cards, incentive cards and ticketing. Much like the iOS Newsstand and Books apps this is more of a conduit for innovations.

Passbook is partly the work of the designer of Starbuck's very successful 2D barcode mobile payment solution, the mobile wallet and NFC genius Benjamin Vigier now working at Apple. This guy is a powerhouse that designed Paypal Mobile, Sprint MyMoneyManager, Mobile Wallet applications for 2 top #5 US carriers, mFoundry Mobile Banking WAP platform, NFC Wallet for a top 3 US bank and led SanDisk mobile commerce and NFC activities. We will see a great deal of his work at Apple in the coming months.

I have had some time to digest my early exposure and early information about Passbook and can say with rather high certainty we are seeing the first brick in Apple's "mobile wallet" system.

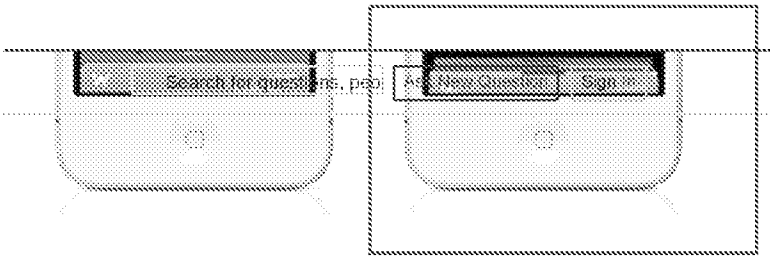


Related Questions

- Can I get my FD without a passbook?
- Is Apple Wallet safe?
- Which mobile wallet is the best?
- What is the best mobile wallet?
- What is the best mobile wallet for Ethereum?
- What is a mobile wallet loan?
- How do mobile wallets make money?
- If I want to develop a new mobile wallet. What should I do?
- Which merchants accept Google wallet?
- What are the top mobile wallets in India?

Ask New Question

Petitioner Exhibit 1002-1549



Related Questions

Can I get my FD without a passbook?

Is Apple Wallet safe?

Which mobile wallet is the best?

What is the best mobile wallet?

What is the best mobile wallet for Ethereum?

What is a mobile wallet loan?

How do mobile wallets make money?

If I want to develop a new mobile wallet. What should I do?

Which merchants accept Google wallet?

What are the top mobile wallets in India?

Ask New Question

Beautiful Passbook UI.

Passbook, An IOS Wallet API

By creating Passbook Apple will establish a secure standard for storing and sorting virtual cards, tickets and offers in iOS devices. There will be a number of features included on the launch date but many more will be unveiled as the product becomes more integrated with Payment Cards. Apple has already established an impressive number of large retailers to use and integrate Passbook into existing iOS apps, for example Starbucks massively successful mobile payments app (Brian Roemmele's answer to What retailer is the most successful in mobile payments? What can be learned by this success?). More retailers will announce how they will use Passbook in the summer as they realign front end systems and back end systems.

Passbook's user interface presents the user's personal items in a card-like interface that is updated live as things change. This skeuomorphism (http://en.wikipedia.org/wiki/Ske...) visual design is very much like the former Square Card Case (How important is Square's new stand-alone Card Case app?) that has been replaced by the "Pay With Square" app. Passbook goes far beyond this concept by being a truly open system that any retailer can use regardless of what payment card company is processing the payment. There will also be a rich feature set of controls that allows the user to finely tune the use of the system covering access to personal data and location information on to prior purchase history.

Passbook displays an image that is related to the functionality of the items in the wallet. For example, a coupon has a serrated edge showing graphically that it is a discount. In another example tickets will have a half circle cut at the top to present the image of a Ticket Stub. Each item in the wallet will come with a number of user and merchant set perimeters.

We are really seeing the stage being set for the framework on how Apple will integrate with Visa, MasterCard and the other Payment Card networks.

Notable Features

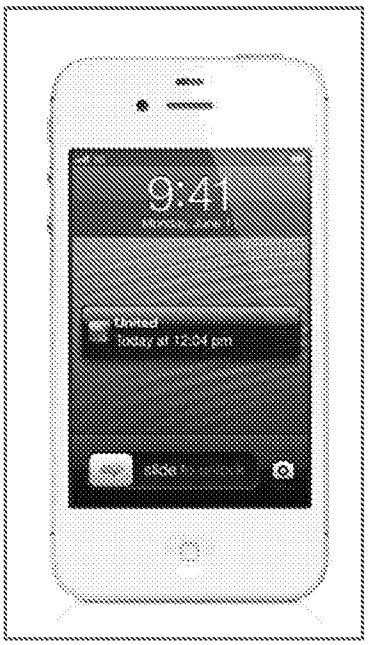
Petitioner Exhibit 1002-1550

Search for questions, peo Ask New Question Sign in

Geolocation- The appropriate reward/incentive/gift card/ticket will be automatically presented for use as the iOS user enters the retail location. **Passbook is integrated with the lock screen so that when the device is near a retailer, a message pops up alerting the user that he or she has a ticket or rewards card that can be redeemed.** This very powerful feature will allow users to have instant access to Passbook functions, however in the future retailers will be able to push offers/credits/incentives to users based on a number of criteria including location.

Examples:

- Starbucks will integrate their wildly popular Payment System that will open a card in Passbook app when within a preset distance from a store location. The users will have instant access to the Starbucks Payment Card barcode and present the iPhone to scan as normal.
- Target will be able to present an instant coupon as the user enters the store. The can also notify the user of the balance on registered gift cards.
- When entering an Amtrak train (CalTrain, Path, Subway) platform, Passbook will notify the user of the amount of credit/rides that are available and present a barcode to be scanned by the ticketing agent.
- Eventbright, for example could create a "daily deal" integration to help fill local events in the last days or hours of the event maximizing attendance.



Live Updates- All cards will have a dynamical update function that allows for up to the second changes to be made and pushed to Passbook and through the a standard iOS notification. Using geolocation and live tracking it will be possible to allow tickets

Examples:

Related Questions

Can I get my FD without a passbook?

Is Apple Wallet safe?

Which mobile wallet is the best?

What is the best mobile wallet?

What is the best mobile wallet for Ethereum?

What is a mobile wallet loan?

How do mobile wallets make money?

If I want to develop a new mobile wallet. What should I do?

Which merchants accept Google wallet?

What are the top mobile wallets in India?

Ask New Question

Petitioner Exhibit 1002-1551

Search for questions, peo Ask New Question Sign In

User interest in Passbook is huge, since the release of iOS6 we've seen website views for Passbook increase 10 fold.

NFC has a big problem in that it is a technical specification and not a solution. For Apple to make NFC work, they would need to provide solutions down to the POS level, and clearly this is not a business that they are in.

Instead, Apple has decided to make updatable Passes easily available in people's phones - they have effectively decided to concentrate on the user experience problem and are leaving third parties to concentrate on the full integration.

Because for many businesses, they will need to integrate passbook use-flows into their businesses and into their customer-facing systems. In one sense, this is a lot of work, but in another sense it's much easier enabling thousands to of companies to do this on their own than trying to create a standard for NFC working with banks, visa/mastercard, national organizations (Interac in Canada, Proton in Belgium, Switch in the UK etc), airlines, movie theatres etc.

Richard Beck.
Digital Possibilities Passbook Specialist Centre:
http://digital-possibilities.com...

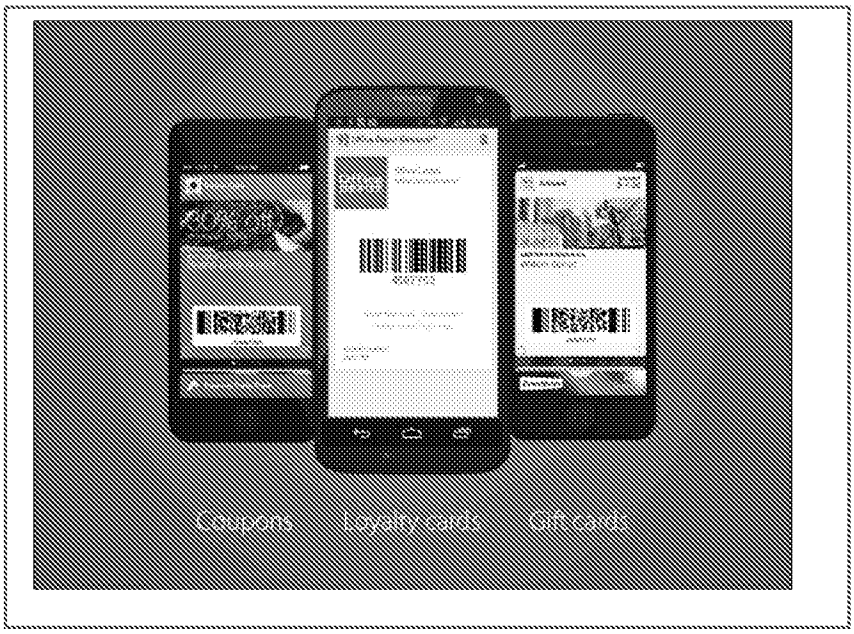
781 Views · View Upvoters



Drew Giovannoli, Techstars Alum. Sales and Marketing @ Fosbury.co, Mobile Wallet Expert, Foodie, Musician, Traveler
Updated Nov 25 2013

Over a year since the Passbook release, and I wanted to chime in on the impact Passbook has made in the mobile wallet ecosystem, specifically for the use of mobile coupons, loyalty cards, and gift cards.

These forms of "branded currency" make up $165 billion dollars in purchasing power each year (http://blogs.hbr.org/2013/07/the...), only 5% of which is digital. No one doubts that there is a tremendous opportunity here, and Passbook has certainly led the way with usability & adoption.



Related Questions

- Can I get my FD without a passbook?
- Is Apple Wallet safe?
- Which mobile wallet is the best?
- What is the best mobile wallet?
- What is the best mobile wallet for Ethereum?
- What is a mobile wallet loan?
- How do mobile wallets make money?
- If I want to develop a new mobile wallet. What should I do?
- Which merchants accept Google wallet?
- What are the top mobile wallets in India?

Ask New Question

Petitioner Exhibit 1002-1552

Passbook. Just the ticket.
And the boarding pass, card, and coup



Beautiful Passbook UI.

Near-Field Communication-Based Secure Mobile Payment Service

Kiran S. Kadambi[1]
Hewlett-Packard Company
19447 Pruneridge Avenue
Cupertino, CA 95014
972-693-4062
kiran.kadambi@gmail.com

Jun Li
Hewlett-Packard Laboratories
1501 Page Mill Road
Palo Alto, CA 94304
650-857-4087
jun.li@hp.com

Alan H. Karp
Hewlett-Packard Laboratories
1501 Page Mill Road
Palo Alto, CA 94304
650-857-3967
alan.karp@hp.com

ABSTRACT
The loss of customer account information makes headlines all too often. The Payment Card Industry (PCI) Data Security Standard (DSS) has generated resistance from merchants because of its cost and complexity. Unfortunately, innovating in the Point of Sale (PoS) space is hard because the protocols have been standardized, tightly constraining new ideas. Using mobile phones as payment devices opens up some opportunities, but any solution must minimize changes in the back-end processing. This paper describes a Near Field Communication (NFC) based mobile phone payment solution in a service-oriented environment, which provides the needed data protection without requiring costly changes to the payment processing infrastructure. In the payment transaction path, a personal mobile phone is viewed as a single, user-trusted touch point. Compared to other solutions available, our approach better protects user credentials, provides better user control over the transaction, and supports both proximity and remote transactions. The prototype has been integrated with an in-store kiosk application and a HP multi-channel banking platform to demonstrate its value in the retail environment.

Categories and Subject Descriptors
K.4.4 [**Computers and Society**]: Electronic Commerce–Security
H. 3.5 [**Information Storage and Retrieval**]: Online Information Services–Web-based Services

General Terms
Management, Design, Security, Human Factors

Keywords
NFC, mobile payment, payment authorization, SOA

1. INTRODUCTION
With the increase in mobile ownership and cheaper data services, the mobile commerce market was expected to generate close to $55 billion in revenue in 2008, with significant growth predictions for the future [3]. The growth of the mobile banking channel provides opportunities for various players in this emerging market, including mobile phone manufacturers and carriers, banking institutions, and service providers. For example, this channel introduces a new revenue stream for banks from mobile micro-payments and reduces customer churn due to the convenience provided by mobile payments [churn reduction of 10% was reported in [3]). To the service providers in retail, online music download, public transportation, *etc.*, it offers new, more convenient touch points to the customers and enhanced security features compared to traditional plastic credit or debit cards. This new channel provides customers with a single point of spending once personal mobile devices become wallet replacements.

The loss of customer account information makes headlines all too often [6, 7]. To protect cardholder data, merchants and service providers are required to comply with the Payment Card Industry (PCI) Data Security Standard (DSS) [24]. Merchants, or their service providers (such as payment gateways), are subject to the PCI DSS compliance if they store, collect and transmit cardholder data on their systems or the systems of their service providers. To meet compliance requirements, merchants and their service providers often have to implement costly upgrades to reinforce systems that are already complex enough. This also puts small and medium sized merchants and e-commerce startups at a competitive disadvantage.

To explore and develop this mobile banking channel and its integration with systems from other players, such as network carriers and retailers, while at the same time striving for a solution that provides needed data protection for cardholder data, we[1] started with a contact-less mobile payment scheme based on Near-Field Communication (NFC) and integrated it with a retailer-based service framework prototyped within HP. An NFC-enabled phone is a cell phone with a smartcard microchip embedded that can communicate with a local host computer within a small range (<10 cm) over a RF channel (13.6 MHz). The NFC-based microchips have two key security features: Public Key Infrastructure (PKI) based cryptographic functionalities, and a well-controlled, point-to-point, short-range communication channel. The commercially available NFC-based chips follow the widely adopted EMV [9], a standard that defines the interaction

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
ICEC'09, August 12–15, 2009, Taipei, Taiwan.
Copyright © 2009 ACM 978-1-60558-586-4/09/08...$10.00.

[1] Kiran Kadambi's present address: Darden School of Business, University of Virginia.

Petitioner Exhibit 1002-1554

between IC cards (i.e., microchip cards) and IC card processing devices, such as Point-of-Sale (POS) terminals and ATMs, to authenticate credit and debit card payment transactions.

Compared to other mobile payment services and systems, the NFC-based mobile payment end-to-end solution that we developed exhibits the following core technical innovations:

- **End-To-End Secure Transaction Protocol:** Other solutions rely on the mobile phone to communicate the user's payment information, which includes the payment amount and credit card number, to the transaction issuer device (*e.g.,* an in-store self-service terminal) over a point-to-point secure communication channel. The merchant may want to hold such sensitive information for various reasons, even long after the transaction occurs [11]. In our protocol, the phone issues a payment authorization token with payment information such as credit card number completely opaque to the merchant. The backend transaction is performed after the token is validated. Thus, our protocol mitigates the customer data breach risk at the merchant and significantly reduces the effort to (if not completely removes) the PCI DSS compliance requirement, because PCI DSS does not apply if primary account number (card number) are not stored, processed, or transmitted [24, 25]. Furthermore, because the authorization token is linked to the transaction identifier at both the merchant and the bank, the merchant is able to defend itself in a dispute.

- **Personal Cell Phone as the Single User-Trusted Touch Point:** As a personal trusted device equipped with sufficient display capabilities, the mobile phone is used to present and interpret the payment amount, confirm the payment, and issue the payment-specific authorization token. No personal information ever gets revealed to the transaction issuer owned by the merchant, which is occasionally open to compromise as reported in [6], and thus not fully trusted by the customer.

- **Support of Proximity Transaction and Remote Transaction:** The existing NFC payment systems are designed to serve only transaction requests issued from a nearby device. Our solution supports online purchases by having downloadable software installed to a local computer, which mediates the interaction between the mobile phone and the remote web application. As a result, aside from an in-store service terminal, our solution can use the same secure transaction protocol from a home shopping station such as a PC desktop or special home appliance like the HP TouchSmart, with the personal mobile phone being the transaction authorization token issuer.

- **Flexible and Multiple Payment Options:** Due to the banking infrastructure's multi-channel support, mobile payments can be routed directly to an account provided by the bank, or to a digital wallet offered by the phone carrier that maintains shadow balances to the chosen banking account [17]. Thus, the mobile phone can become a single point of spending.

The rest of the paper is structured as follows. In Section 2, we introduce the PCI DSS standard to help understand merchant specific compliance requirements for data protection. In Section 3, we then describe the two solutions systems that we developed in HP, namely Adaptive Bank and Retail Store Assistant (RSA), upon which our mobile payment system was built. We then detail the NFC based mobile payment solution architecture in Section 4, and have Sections 5, 6, 7 cover the core technical aspects, namely, the secure transaction protocol, the interaction between the phone and the local machine, and the interaction between the phone and the remote service mediated by a local machine, respectively. We report our prototype implementation in Section 8, which details the hardware we used for our prototype, the SDK that we used for development, and how we managed to use different middleware to integrate the mobile phone, the retail solution based on the RSA kiosk, and the Adaptive Bank to form a complete end-to-end payment system prototype. In Section 9 we contrast our mobile payment solution with existing mobile payment solutions. The paper is concluded in Section 10.

2. PCI DSS

The Payment Card Industry (PCI) Data Security Standard (DSS) [24] specifies regulatory compliance requirements for merchants (retail store, mail order, e-commerce sites, *etc.*) and service providers (payment gateways, e-commerce host providers, credit report agencies, *etc.*) that involve payment processing, and thus store, process, or transmit cardholder information. The Point-of-Sale (POS) terminal environment may be excluded from merchant's compliance validation, if it is not IP network based or has no access to the merchant location [25]. Merchants are subject to different levels of compliance, from a high of level 1 to a low of level 4, depending on annual payment transaction volumes (level 1 for more than 6 million credit card transactions per year).

Information subject to protection consists of *cardholder data* that further includes Primary Account Number (PAN), cardholder name, service code and expiration Date, and sensitive *authentication data* that further includes full magnetic stripe data, validation code, and PIN. Following the defined storage and protection requirements, cardholder data is allowed to be stored on some storage medium with sufficient measures to ensure the protection of the PANs. Other cardholder data mentioned above need only be protected if it is stored in conjunction with the PANs. The sensitive authentication data mentioned above must not be stored at all.

The PCI DSS is divided into six categories, with twelve high-level requirements that govern network security, data protection, access control, access monitoring, *etc.* A template of assessment procedures is described in [25]. The high-level requirement on cardholder data protection is further refined into: (1) keep cardholder data storage to a minimum, with the necessary data retention and disposal policies; (2) no storing of sensitive authentication data after payment authorization (even if encrypted); (3) mask PANs when displayed; (4) render PAN unreadable anywhere it is stored, including truncation, encryption, *etc.* (5) protect the cryptographic keys used for encryption of cardholder data; (6) document and implement key-management processes and procedures for cryptographic keys used for encryption of cardholder data.

Note that the standard [25] states that *".... PCI DSS, however, does not apply if PANs are not stored, processed, and transmitted".* Clearly, the data protection requirement will be effectively satisfied with minimum risk if cardholder data is not stored at all. We interpret the statement to mean that the

Petitioner Exhibit 1002-1555

requirement is satisfied if the data is stored in a form that the merchant cannot interpret, which in our solution is achieved by applying strong public-key based crypto support to encrypt card holder data into payment authorization tokens that are transmitted across the end-to-end payment system.

3. RETAIL STORE ASSISTANT & ADAPTIVE BANK

Our mobile payment system is built on two Service Oriented Architecture (SOA) based solution systems: the Retail Store Assistant (RSA) that delivers personalized shopping services and experiences to in-store customers, and the Adaptive Bank platform that supports multiple front-end banking channels to the core banking process. Both systems are interoperable at the Web Service SOAP messaging level. Our mobile payment system uses the RSA as a front-end customer touch point and the Adaptive Bank for backend payment processing.

3.1 Retail Store Assistant (RSA)

The RSA system is designed to uniformly support shopping-related kiosk applications at different touch points (in physical stores, at home, and through mobile devices). The kiosk-based application prototype is currently accessible for online demonstration [27]. These touch points serve as the front-end to a network of services provided by the retailer and its business partners, which include manufacturers and financial institutions. The system aims to reduce or eliminate common shopping frustrations and to help buyers with shopping rather than only helping retailers sell. The RSA application prototype currently provides in-store personalized coupon offering, product information search, personal event management, voice and image based shopping reminders, *etc.* The mobile version of the RSA system has also been prototyped [16].

NFC mobile payment is a key part of the integrated solution to improve the shopping experience, not only because it is convenient for customer payment transactions, but also because it naturally pulls other shopping and purchase related applications together onto the personalized mobile phones, primarily due to its secure wireless communication protocol and the "tap-and-go" simple phone usage model. Examples of these applications can include the storing of accepted personalized coupons and subsequently redeeming the coupons at check out, the on-the-phone storing of transaction receipts to keep track of shopping purchases, *etc.*

3.2 Adaptive Bank

Adaptive Bank is a SOA-based, multi-channel integration framework that was developed within HP to integrate front office applications with the backend business services and systems by a uniform connectivity and messaging interface [1].

The infrastructure framework of Adaptive Bank is shown in Figure 1. It supports multiple channel applications that include teller, call center, ATM, web, *etc.* Each channel application is associated with a different communication mechanism (TCP/IP, HTTP and Web-Services, *etc.*) and message formats that includes Fixed Length, XML and IFX (following the Interactive Financial eXchange standard). Adaptive Bank exposes a uniform channel messaging and connectivity interface to integrate different channel applications with the backend infrastructure. The business events generated from all these different channels are

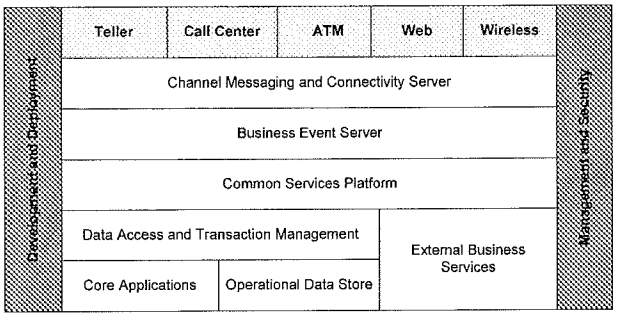


Figure 1. Adaptive Bank multiple channel applications and its layered infrastructure.

routed through the business event server for further backend processing. These events are also collected for business activity monitoring, which can be either a common service from the common services platform or provided by external business services.

Seamless customer experiences are offered over multiple banking channels. Specifically, the operational data store hosts the data model and integration technology essential to creating a unified customer view across the channels by integrating various data sources that span the infrastructure stack, such as host customer transactions, customer profile, customer activity monitoring, and targeted customer offerings. Each channel application can fully leverage comprehensive customer behavior information aggregated from all different channels.

4. MOBILE PAYMENT SOLUTION ARCHITECTURE

The entire secure mobile payment solution spans the NFC-enabled cell phone, the service terminal (such as an in-store kiosk enabled by the RSA) with its backend services, and the Adaptive Bank platform. The overall system is shown in Figure 2.

We introduced a mobile banking channel to Adaptive Bank. The Adaptive Bank provides front-end processing of the *issuing* bank (*i.e.,* the bank that issues the payment card to the card holders, who then use the issued card at the merchant [26]). In our system, the issuing bank owns the mobile user account. This channel receives the transaction request from the *acquiring* bank (*i.e.*, the bank that takes care of payment processing for the merchant [26]), processes the request, and forwards the processed result to the core banking processor of the issuing bank, where the credit/debit processing updates the mobile user accounts to reflect payment transaction. The merchant account can be either immediately credited in this credit/debit processing, or deferred to later bank-to-bank reconciliation with the settlement bank involved. The payment transaction request originates at the local transaction issuer, which can be a kiosk or a point-of-sale terminal at a retail store.

The transaction request message over this mobile banking channel carries two parts: the *payment information* and the *authorization token* issued from the mobile phone. The payment information can include, for example, the merchant bank account number, the payment amount to be collected from the customer's account, and a transaction identifier issued by the merchant for future tracking purposes, *e.g.*, when the purchased items are returned and a

Petitioner Exhibit 1002-1556

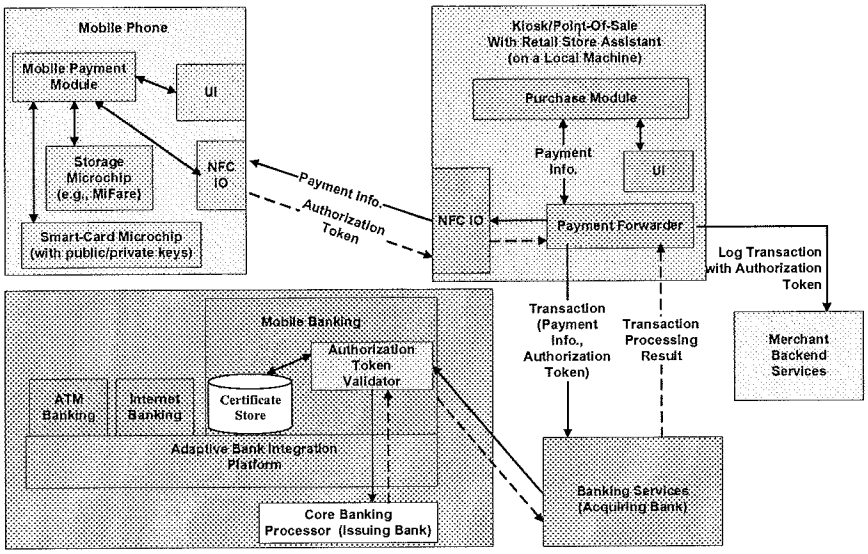


Figure 2. The overall NFC-enabled mobile payment system.

refund is issued. The authorization token is constructed by the mobile phone based on the payment information sent from the local transaction issuer (detailed in the description of the secure transaction protocol in Section 5), and is tamper-resistant with strong public-key based cryptographic support built into the mobile phone's smart-card microchips.

While our payment message conforms to the traditional payment processing protocol, our proposal replaces the sensitive information, such as bank account number (PAN) and password (PIN), with an authorization token.

The processing of the transaction request at the mobile banking channel involves the validation of the authorization token (the validation procedure will be detailed in Section 5). The credit/debit transaction relies on a validated authorization token to ensure the correct customer account and actual payment amount specified by the mobile user.

Each purchase transaction and the associated authorization token are logged by the local transaction issuer and the logs are stored at the merchant's backend services. The transaction can be either a purchase transaction or a refund transaction. For a refund transaction, the authorization token is not issued from the mobile phone. Instead, the merchant relies on the recorded transaction identifier to retrieve the authorization token issued for the previous purchase transaction. Afterwards, the retrieved authorization is incorporated into the refund transaction request. A transaction data flow similar to that shown in Figure 2 happens and ultimately the issuing bank credits the customer the refund amount, and the acquiring bank deducts the corresponding amount from the merchant account.

In a typical merchant-based deployment environment, a dedicated secure communication payment network is established between the merchant's transaction issuer and Adaptive Bank to handle actual payment transactions. For example, the merchant has its local transaction issuer (such as a POS terminal) connect to the acquiring bank. The acquiring bank then forward the transaction request to the payment network that it belongs to, such as VisaNet or BankNet, for transaction routing. The transaction request eventually reaches the Adaptive Bank, because the issuing bank belongs to the same payment network, or because the two payment networks that the issuing bank and the acquiring bank are associated with can be bridged through a payment processing gateway [26].

In other deployment environments that are more open, such as a home-based remote transaction (detailed later in Section 7), a secure communication channel like HTTPS is required between the local machine and the merchant's backend with the above mentioned dedicated communication channel.

The merchant's acquiring bank serves as only a middleman in the banking network to forward mobile payment transaction requests. Its functionalities can be logically encapsulated by some merchant's backend services, as shown in Figure 2. In the remainder of this paper, we are only interested in the issuing bank, at which the Adaptive Bank is hosted. We refer to the issuing bank as simply the *bank*.

Note that the end-to-end payment processing network described in Figure 2 involves only the NFC communication channel and the traditional payment processing network. Thus no mobile carrier networks are required in our mobile payment solution.

5. SECURE TRANSACTION PROTOCOL

5.1 Payment Authorization Token

The smart-card chip embedded in the phone holds a public/private key pair assigned to the user, as well as the public key of the user's bank. The local transaction issuer sends the required payment amount to the user's device via the NFC channel. After the user confirms the payment amount, a digital signature is created from the user's private key and the user-side payment information that includes the user's bank account number, the payment amount, a transaction counter (to prevent replay attacks), and a time stamp. The payment standards require that all

Petitioner Exhibit 1002-1557

transactions have to be time stamped to the second with GMT offsets.

The digital signature and the user-side payment information are then encrypted with the bank's public key. The encrypted result can not be interpreted by the merchant, and thus we need a clear-text part to specify: (1) the payment amount that the mobile user promises, such that the merchant can know beforehand the amount that the user claims to be willing to pay and (2) the bank's routing number, because the payment network needs the number to route the transaction request to the correct bank.

The overall data structure that includes both the encrypted part and the clear-text part is called an *authorization token*, as shown in Figure 3.

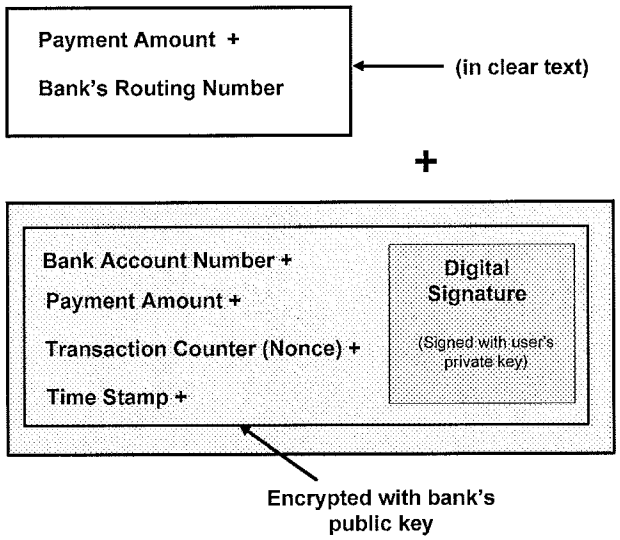


Figure 3. Payment authorization token issued from mobile phones.

Note that there are two payment amounts encapsulated in the authorization token: the amount in clear-text, which the merchant can check, and the amount in encrypted form, which is the true amount that the mobile user agrees to pay. The Adaptive Bank's mobile banking channel will detect if the two payment amounts differ, perhaps because the merchant deliberately or inadvertently changed the clear-text part, and will refuse to forward the transaction request down to the issuing bank's core banking processor. Similarly, if the customer lies to the merchant by deliberately setting the amount in clear-text larger that what is put in the encrypted form, although the merchant will proceed to issue the transaction request to the backend payment network, the merchant will be notified about transaction failure by the Adaptive Bank's mobile banking channel. Consequently, the merchant will not release what is to be purchased by the customer. Thus the customer gains nothing from such cheating.

It is up to the merchant to protect the integrity of the clear text message part and the authorization token in the same way that the merchant would have to protect a check made out to "Cash". If the communications channel is secure, there is no risk that the token will be stolen. If not, it is as likely that attackers can subvert the key exchange process as it is that they will steal the token. The mobile users never expose their identities, or even their public keys, to the merchant. As a result, we do not have the mobile phone sign the entire authorization token, since the merchant is not able to verify this signature.

5.2 Detailed Communication Protocol

The authorization token is issued by the mobile phone to the transaction requester from the local transaction issuer over the NFC channel. The local transaction issuer inspects the clear text part to check the amount the user agrees to pay. After checking, the authorization token is incorporated into the transaction request message by the local transaction issuer for backend payment processing. This token finally arrives at the Adaptive Bank's mobile banking channel through necessary routing network, guided by the bank's routing number embedded in the transaction request. The authorization token is then decrypted using the bank's private key. The digital signature that is included in the decrypted authorization token is checked, after the mobile banking channel using the decrypted bank account number to retrieve the corresponding customer's public key from the bank's central certificate store. After the valid digital signature is confirmed by the mobile banking channel, at the bank's core banking processor, the user account is debited the specified amount. For the core banking processor to make the final decision, other bank account information is evaluated as well, such as whether the account is blocked or frozen, whether the card is stolen, and whether the transaction is over the limit. The end-to-end payment transaction result eventually returns to the transaction issuer at the local machine right next to the mobile phone.

The end-to-end secure transaction spanning the mobile phone, the merchant, and Adaptive Bank, is illustrated by the sequence diagram in Figure 4.

All customer personal information is in the encrypted part of the authorization token, which is opaque to the merchant. Thus, with our secure payment solution, customer related data breach incidents, such as the one at T.J. Maxx [6], will not compromise customer account numbers. Since the authorization token is not designated to a particular merchant, the merchant that receives the token has an incentive to protect it from being tampered with, lost or stolen. In the case of a return or refund, the merchant can retrieve from its backend office the original authorization token and provide the retrieved token to the bank, along with the refund amount that the merchant is to pay. The bank decrypts the authorization token, validates the authorization token, extracts the embedded user's account number, and credits the refund amount to the user from the merchant's account.

With respect to the PCI DSS regulatory compliance described in Section 2, because the authorization tokens that come out of the mobile phone are encrypted with the bank's public key, the merchants can never obtain sensitive card holder information, in particular, the primary account number (PAN) embedded in the authorization token. Therefore, with the NFC mobile banking channel, the merchants should be relieved from the compliance requirements imposed by the PCI DSS.

5.3 Key Management

The user's public/private key pair is generated locally within the mobile phone during the initial mobile application installation,

Petitioner Exhibit 1002-1558

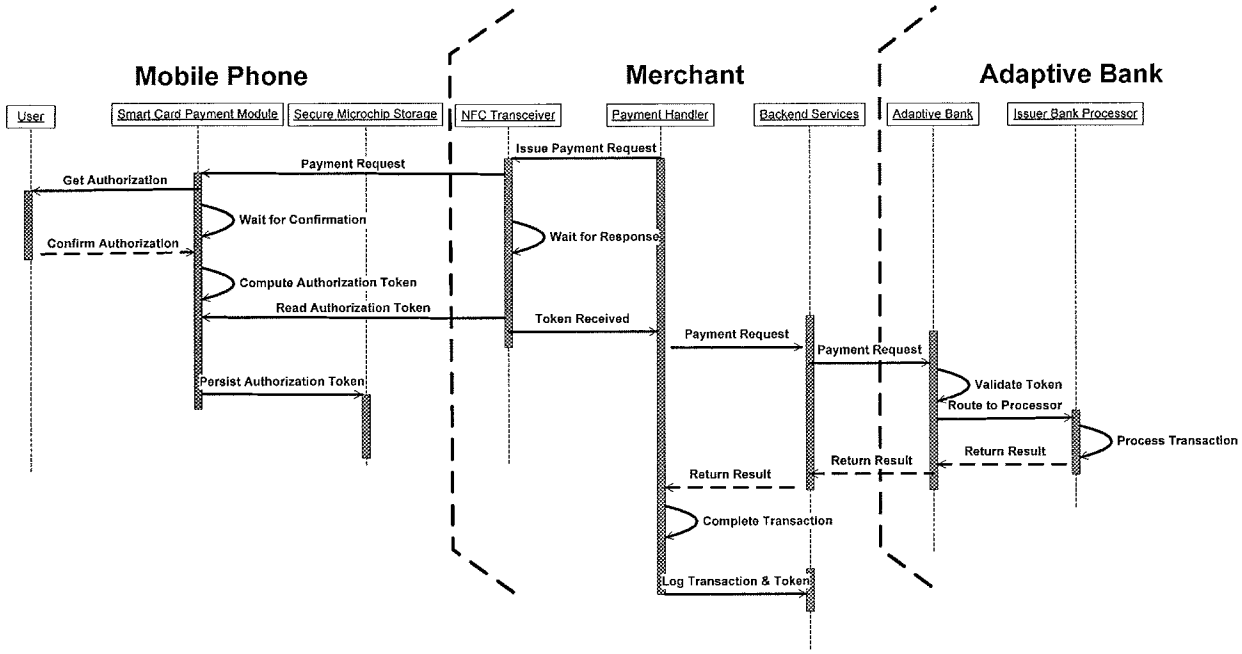


Figure 4. Sequence interaction on mobile phone, local machine and Adaptive Bank.

which can take place at a bank branch office. The private key never leaves the mobile phone. The bank's public key is also imported to the mobile phone's local certificate store (on the NFC chip) during software installation. Once the mobile payment application is installed on the phone, user registration can take place at the bank's branch as well. The mobile phone exports the user's public key to a local machine at the bank's branch, from which the public key is eventually stored in the bank's central certificate store and associated with the user's bank account number. When the user's bank account is closed, the corresponding public key at the central certificate store is revoked, disallowing further mobile payment transaction processing.

If the user has multiple accounts at the bank (e.g., checking and saving), he or she can select the desired account to associate with the authorization token. However, they share the same public/private key pair in the mobile phone. The mobile payment solution can support multiple banks as well as multiple accounts in one bank. Under this situation, each bank will supply its own public key and bank routing number to the mobile payment software installed at the mobile phone.

6. USER INTERACTION COORDINATION AND MANAGEMENT

The mobile phone and local machine exchange data over the NFC channel, as shown in Figure 4. Due to the NFC proximity requirement, the mobile phone needs to be positioned close to the local machine's NFC reader to enable message exchange twice: to receive the payment amount for user verification, and to send back the authorization token. Correspondingly, the customer is prompted to do the following steps by the transaction issuer device (local machine):

(1) Put the mobile phone close to the NFC reader so that the payment amount can be written to the NFC IO accessible storage (shown as smart-card microchip in Figure 2) on the mobile phone by the local machine;

(2) Confirm payment amount on the mobile phone and ultimately the authorization token is written to the NFC IO accessible storage on the mobile phone;

(3) Put the mobile phone close to the NFC reader again so that the local machine can read mobile phone's NFC IO accessible storage that contains the latest authorization token.

The send/receive status at the transaction issuer (local machine)'s NFC IO is communicated to its payment processing UI, as shown in Figure 5 (left-hand side), to keep human in the loop. Figure 5 (right-hand side) shows the payment confirmation step on the mobile phone.

Notice that the UI of the mobile phone is critical in our solution, a concept called Splitting Trust [2]. The mobile phone is personally owned and trusted by the consumer but not the merchant. The local machine that issues the transaction request is trusted by the merchant, but not the user. By having the phone UI show the required payment amount and then allow user to confirm the amount, the local machine cannot cheat or alter the actual amount that the merchant includes into its transaction request to the bank, because the authorization token is only valid for the amount confirmed by the customer.

Petitioner Exhibit 1002-1559

A user profile hosted on the phone simplifies the interaction and provides further payment protection. The user profile is created when the mobile payment software is installed to the phone and can be updated later by the user. The user profile can support the following payment related configuration information. A payment threshold can be defined to skip the verification step for small amounts, or to activate password or biometric based authentication on the mobile device for large transactions. A limit can be also set for the total amount that can be issued from the phone within a day. A payment choice can be given to the user to debit a different banking account or a digital wallet [17]. Because the mobile phone is viewed as a personal device, rather than being shared among multiple users, our system only supports a single user profile.

refunds. As a result, online merchants and traditional brick-and-mortar merchants share the same customer data retention behavior and thus potential risk of a data breach. Our secure transaction protocol can help online merchants avoid such risk. The security provided by our solution is similar to what Citi's Virtual Account Numbers provide [5], but we eliminate the effort of acquiring the virtual account number over the web for every online purchase.

The detailed protocol for NFC enabled online payment transaction is shown in Figure 6. The user makes an online purchase from a web site. The shopping session is linked to a *global payment session identifier* at the backend. At the payment web page, once a payment button is clicked, a certified .NET ClickOnce application [21] or a Java applet, called a *mediator*, is downloaded to and then launched from the machine that hosts the

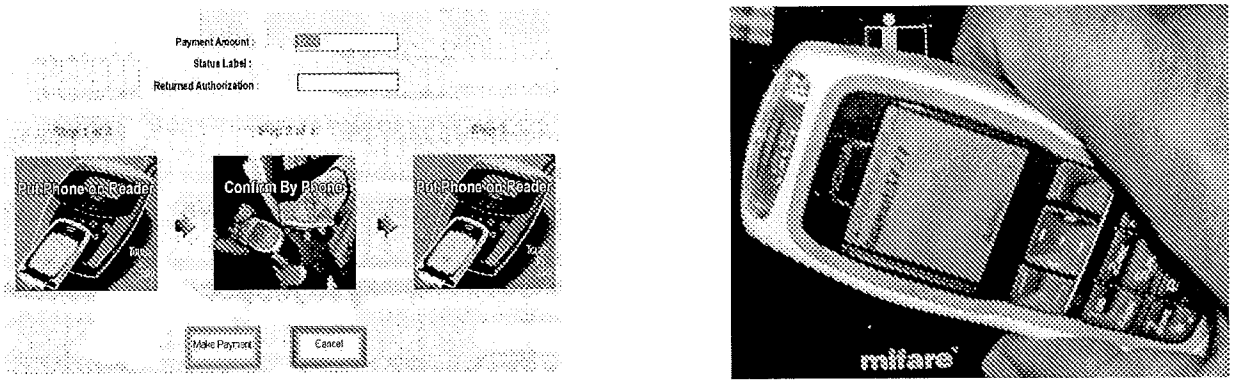


Figure 5. Mobile phone to local machine interaction (the left-hand side screenshot shows the steps displayed on the RSA based kiosk to guard user interaction, and the right-hand side screenshot shows payment confirmation on the mobile phone).

Apart from the smart-card chip, a second micro-chip (called storage micro-chip in Figure 2) can be installed in the phone for secure storage, allowing mobile users to store more shopping-related information on the phone, such as transaction receipts, coupons, *etc.*, when other mobile services (*e.g.*, coupon offering) are provided as part of the integrated solution package to enrich consumer mobile experiences.

7. REMOTE TRANSACTION ENABED BY NFC

The proximity interaction detailed in Section 6 occurs when the transaction issuer is an in-store kiosk or point-of-sale, *i.e.*, a machine close to the mobile phone. Our solution also supports remote transactions by extending the solution architecture detailed in Section 4 with a web browser located at the store and a remote web-based payment application, while following the secure transaction protocol detailed in Section 5. Such remote transactions enable secure online shopping, such as from a home PC or a home multimedia appliance like HP TouchSmart. A typical online shopping site nowadays requires full credit card information. Even though the payment transaction is done via HTTPS and thus protected during message transmission, the online merchant will receive and then store the user's full credit card information, for example, for future shopping purchases or web browser. Once the mediator detects that a NFC reader is attached to the local computer, it starts a local payment session. The local payment session will inherit the global payment session identifier at the time the mediator is launched. For example, in .NET, the ClickOnce application can accept input parameters at the time it is launched as environment variables that are then retrievable in the launched ClickOnce application.

The local session handles the exchange of the payment information and authorization token between the mobile device and the local machine through a local NFC reader, following the same procedure described previously. Once the authorization token is acquired, the downloaded mediator migrates the purchase session back to the remote purchase web site and terminates itself at the local machine. The session migration is achieved by having the mediator invoke the backend session management service, whose end-point reference is pre-specified in the downloaded mediator application. This web service invocation is done via the HTTPS channel, with input parameters that include the global payment session identifier and the authorization token. Once the session management service receives the global payment session identifier and the authorization token, the previous online shopping application that had been suspended will resume.

At this point, the transaction continues at the online purchase site, through the merchant backend and then Adaptive Bank, following

Petitioner Exhibit 1002-1560

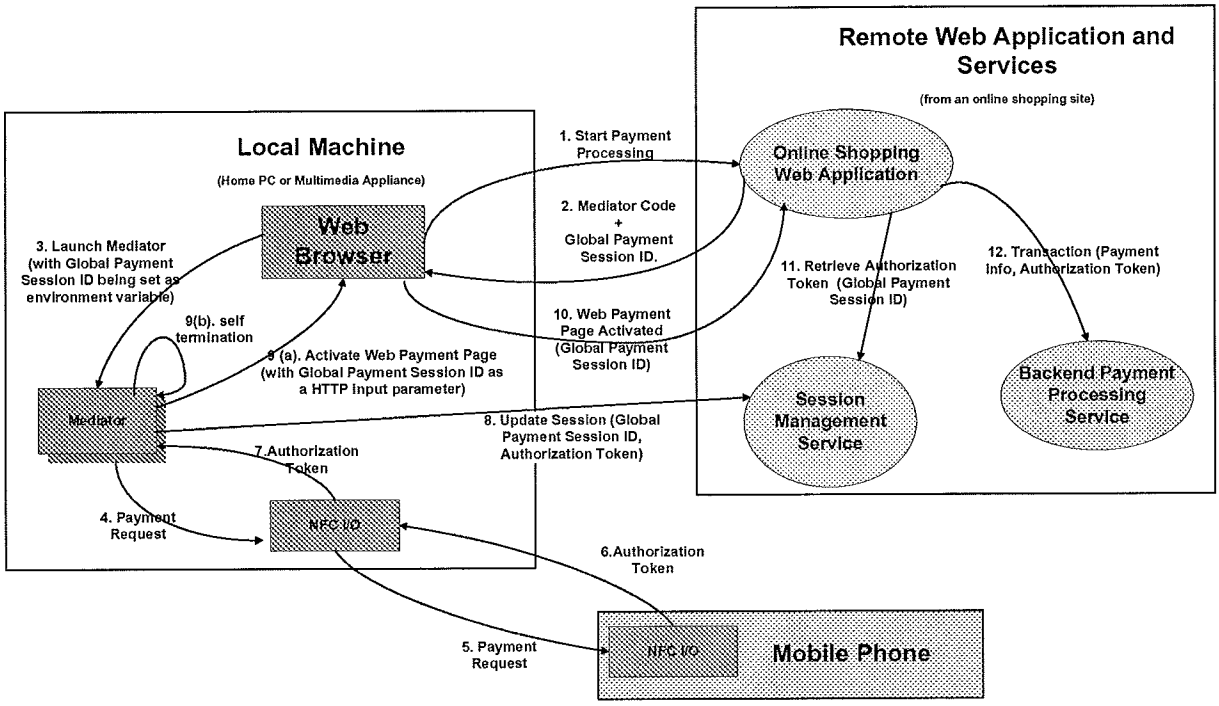


Figure 6. Remote web-based payment transactions enabled by local NFC.

the steps described previously in Section 5. Ultimately, the transaction result is acknowledged to the user through a web page from the online purchase site.

The downloaded mediator's security guarantee is rooted at the trusted .NET runtime installed at the local machine. Code integrity is checked before the mediator is launched. Restriction on local resource access is enforced by the .NET runtime through the Code Access Security mechanism (CAS) [21]. The access control policies enforced by CAS consist of the ones that are defined by the local machine, and the ones that are embedded in the downloaded code and defined by the code publisher (for example, to restrict remote communication only back to the publisher site). In our solution, the code publisher is the online purchase site that supports NFC-based payment solution.

Note that this protocol is not subject to keystroke loggers because critical information is passed via the NFC channel, not the keyboard.

8. PROTOTYPE IMPLEMENTATION

In our prototype, we used a Nokia 3220 mobile phone with a NFC enabled jacket and a secure Mifare memory chip. The RSA web-based application serves the same function as the in-store kiosk touch point for store purchases. The web-based kiosk application is implemented in ASP.NET and it communicates with the merchant backend via .NET web services. The merchant backend directly interacts with the Adaptive Bank mobile banking channel for transaction requests, by using the XML document exchange supported by the .NET Web Service Enhancement (WSE) 3.0. The Adaptive Bank mobile channel has a special HTTP listener installed to handle mobile payment transaction requests.

On the mobile phone, the payment application consists of two parts. The UI is a Java-based Midlet designed to run on the J2ME virtual machine. The payment module is a Java card Applet application [13] developed in Java using the JCOP API's from IBM and the NFC-related SDK from Nokia. We also used the JetZ API from NXP for secure access to the Philips' Mifare chip, which works as our secure storage chip. Since the kiosk application is web-based, it relies on our remote transaction technique (with .NET ClickOnce application download) to communicate with the mobile phone. The NFC reader on the kiosk was developed in Java. A CORBA communication framework [19] enables the cross-language communication between the NFC reader and the .NET ClickOnce application. Should a .NET based NFC reader SDK become available, we will not need the CORBA-based cross-language communication.

9. RELATED WORK

There is a large collection of mobile banking applications that has been developed, piloted and deployed since late 1990's. Here we only contrast our work with other mobile payment solutions, with or without the NFC enablement.

The contactless smart card relies on NFC to send data stored on the smart card to host devices equipped with NFC readers. The Sony Felica Card is one of the most successful contactless smart cards [10]. A Felica card stores an integer counter representing a pre-paid credit. The reader reduces the amount of available credit through a secret-key sharing protocol. Different data access rights

Petitioner Exhibit 1002-1561

are granted based on the secret presented by the reader. The services supported by Felica include transportation passes, electronic wallets, loyalty programs. Such contactless cards are very convenient and ease-to-use, due to their tap-and-go interaction with the reader. The payment process is completely local and no backend processing is involved. Because the card lacks a UI, users must fully trust the host devices to deduct only the agreed amount.

Contactless smart cards (NFC chips) can be combined with mobile phones to form NFC-enabled mobile phones. Such mobile phones, including NTT DoCoMo's i-mode Felica [15] and Nokia NFC phones [20], use the phone UI to display secure data (for example, the remaining credit) stored on the attached chip, and allow or disallow the payment transaction based on UI commands. However, secure transactions still go through the NFC chip's local data store, as done on the i-mode Felica. Alternatively, in MasterCards's NFC pilot with Nokia [3], the NFC chip allowed the reader to fetch the customer's Primary Account Number (PAN). By contrast, in our solution, the payment transaction processing happens at the backend, and the NFC chip only issues authorization tokens. No transaction data is updated on the mobile phone. Hence, our solution is more flexible for the merchant, because the merchant is not required to have the secret keys pre-distributed for access to the NFC chips [14]. That means the merchant is not locked into a particular payment service provider. Furthermore, since only the authorization tokens, but not NFC stored personal data are revealed to the merchant, our solution is more secure as well.

NFC-enabled mobile phones do not require mobile carrier networks for payment transactions. There are alternative payment solutions that do. Some are based on SMS text messaging [8]. Others are either mobile browser applications or mobile device applications, which all rely on the WAP enabled internet [23, 22]. All of these payment solutions require a mobile carrier to provide the wireless communication channel. In SMS messaging based solutions, the payment request (payer's phone number, amount, and even PIN) is carried in one SMS message. A major disadvantage is that such SMS payment solutions are inherently not real-time.

The mobile browser or device applications mentioned above are no different from what is already provided in today's online payment services, such as PayPal or Google Checkout, except that such applications run on mobile devices. The user's password is typically presented to the service provider for authentication. Although the mobile payment process is secured by HTTPS, it is suitable only for online purchases, *i.e.*, the ones with the transaction requests being originally issued from the mobile environment and completed in the mobile environment. They are not designed to have the mobile device to be inserted into the transaction path in which the transaction is an in-store purchase issued from an in-store POS terminal, or an online purchase issued from a browser running on a home desktop. In contrast, our NFC solution works for both in-store purchase terminals and home desktops via the same secure transaction protocol.

In all mobile payment schemes, a virus could take full control of the phone and communicate with a malicious party within and beyond the carrier network, as reported by the mobile phone-based Trojan named Redbrowser.a [29] that attacked mobile devices that run the J2ME version of the Java virtual machine. The only protection our protocol provides is the confirmation step, but it is not clear that a virus cannot simulate a button press. The best solution is to provide a more secure operating system that better isolates applications running on the phone [28].

Finally, with respect to secure payment protocol, Hamann et al. [12] described a Java-based online transaction technique that relies on a smart card device attached to the local machine through a particular wiring protocol (*e.g.*, USB) for online transaction authorization. Fundamentally, the local machine is viewed as a trusted machine and thus the system is designed to have PIN number entered from the local machine in order to activate the smart card authorization process. Chaum's digital cash protocol [4] is designed for anonymous cash in which the bank that issues the cash can not distinguish the cash holders. Although our payment solution has the authorization tokens anonymous to the merchants, the tokens have to be decrypted and then validated by the bank, and thus the tokens in our solution can be fully tracked by the bank.

Overall, our solution significantly differs from the work described above. It provides integrated features that include the trusted personal phone UI, the authorization-based secure transaction protocol that relies on signing the customer account number and then obfuscating it using the bank's public key, the dual support of proximity and remote transactions to bring the same mobile payment experience to both in-store shopping and online shopping, and the flexible payment integration powered by Adaptive Bank.

10. CONCLUSIONS

We have designed and implemented the NFC-based mobile payment solution. It demonstrates the integration of the mobile devices with current existing Point-of-Sale (POS) retail payment solutions. By issuing payment authorization tokens from the mobile devices, the solution eliminates the transfer of any sensitive user information over the public networks, such as bank account number (PAN) and user passwords (PIN). The prototype has been showcased to various HP prospective customers. In our next steps, we plan to perform end-to-end system performance and mobile user evaluation to better character our solution architecture. To enrich the solution features, we plan to integrate the digital wallet [17] as a special payment option in our solution. To further assess the solution's practicality, we will investigate how to adopt our secure transaction protocol and security tokens in the current VisaNet routing network, which routes the transactions between the acquiring banks and the issuing banks. Finally, to improve security and privacy of our solution, we will look into anonymous digital cash, and explore the mobile Trusted Platform Module (TPM) for building secure mobile applications [18].

11. ACKNOWLEDGEMENTS

Bob Lyons introduced the digital wallet concept and provided insightful suggestions.

12. REFERENCES

[1] Adaptive Bank, http://h71028.www7.hp.com/enterprise/cache/255537-0-0-225-121.html.

Petitioner Exhibit 1002-1562

[2] D. Balfanz and E. W. Felten, "Hand-Held Computers Can Be Better Smart Cards," Proceedings of the 8th USENIX Security Symposium, 1999.

[3] Celent, "Mobile Commerce: Dealing with the Devil in the Details—How Banks, Carriers, and Device Manufacturers Are Gearing Up for Mobile Commerce," Feb. 2006.

[4] D. Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," *Commun. ACM* 28, 10 (Oct. 1985), 1030-1044.

[5] Citibank Virtual Account Numbers, https://www.citibank.com/us/cards/vanpromo/cmc_pop/index2.htm.

[6] CNET news: T. J. Maxx Hack Exposes Consumer Data, available at http://www.news.com/T.J.-Maxx-hack-exposes-consumer-data/2100-1029_3-6151017.html.

[7] Computerworld security news: Heartland data breach could be bigger than TJX's, available at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9126379.

[8] R. Dodin, "Text Message Payment," Google's United States Patent Application, No. US 2007/0203836, published on Aug. 30, 2007.

[9] EMV, http://en.wikipedia.org/wiki/EMV.

[10] Felica Product Information, accessible at http://www.sony.net/Products/felica/.

[11] Forrester Consulting, "The State of PCI Compliance," Sept. 2007.

[12] E. Hamann, H. Henn, T. Schack, and F. Seliger, "Securing e-Business Applications using Smart Card," *IBM System Journal*, Volume 40, Number 3, 2001. http://www.research.ibm.com/journal/sj/403/hamann.pdf.

[13] Java Card, http://java.sun.com/products/javacard/.

[14] M. Jurgensen, S. B. Guthery, *Smart Cards: The Developer's Toolkit*, Prentice Hall, 2002.

[15] A. Kumar and D. Jaffe, "Mobile Payments in Asia: Breaking New Ground," Financial Insights, April 2006.

[16] J. Li, I. Ari, J. Jain, A. H. Karp and M. Dekhil, "Mobile In-Store Personalized Services," Proceedings of International Conference on Web Services, 2009.

[17] B. Lyons and R. Murthy, "Method and System for Managing Monetary Value on A Mobile Device," HP Patent Application (Ref. 200501925-1).

[18] Mobile Phone Work Group in Trusted Computing Group, https://www.trustedcomputinggroup.org/groups/mobile.

[19] K. Moore, and E. Kirshenbaum, "Building Evolvable Systems: the ORBlite Project," Hewlett-Packard Journal, pp. 62-72, Vol. 48, No.1, Feb. 1997.

[20] Nokia NFC Phone Web Site, http://www.forum.nokia.com/Resources_and_Information/Explore/Mobile_Technologies/Near_Field_Communication/.

[21] B. Noyes, *Smart Client Deployment with ClickOnce: Deploying Windows Forms Applications with ClickOnce*, Addison Wesley Professional, Dec. 2006.

[22] Obopay, http://www.obopay.com/

[23] PayPal Mobile Checkout, https://cms.paypal.com/us/cgi-bin/?cmd=_render-content&content_ID=developer/howto_api_mobile_checkout

[24] PCI DSS (Version 1.2), Oct. 2008. https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html.

[25] PCI DSS Requirements and Security Assessment Procedures (Version 1.2), Oct. 2008. https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf.

[26] C. Radu, *Implementing Electronic Card Payment Systems*, Artech House, 2003.

[27] RSA in-store web-based kiosk application, accessible at http://opra.hpl.hp.com/RSALaunch/flash.html (required: 1280x1024 for display setting; pop-up enabled on Internet Explorer).

[28] D. Toll, P. Karger, E. Palmer, S. McIntosh, S. Weber, "The Caernarvon Secure Embedded Operating System," SIGOPS Operating Systems Review , Vol. 42, Issue 1, Jan. 2008.

[29] Trojan.Redbrowser.A, http://www.symantec.com/security_response/writeup.jsp?docid=2006-022814-5027-99.

Petitioner Exhibit 1002-1563

Near Field Communication based Mobile Payment System

Gerald Madlmayr, Josef Langer
University of Applied Sciences of Upper Austria, Hagenberg
{gmadlmay, jlanger}@fh-hagenberg.at

Josef Scharinger
Johannes Kepler University
josef.scharinger@jku.at

Abstract: In daily life, ordinary cash is more and more replaced by electronic means of payment. Where on the one hand side macro payment systems are well covered by credit cards, micro payment systems still suffer from different technological and usability issues. Besides usability, security in payment systems has always been a hot topic ever since.

In this paper we present a new, promising approach for a purse-based micro payment system. Our system relies on a prepaid wallet having the money stored in a secure chip in the mobile phone. The proximity technology Near Field Communication (NFC) is used to conduct contactless payment transactions at the point of sale (POS). Additionally the wallet can be topped up over the air (OTA), anywhere and anytime.

The combination of OTA top-up and NFC payment transactions make this system very convenient as the data acquired during an eight month trial shows. Users benefit from the system as they do need to head for an ATM to load money into the wallet. This system is also advantageous for banks and payment providers as there is no need to issue smartcards. Besides the technological aspects of NFC and the implementation of the payment system, this paper also presents the results of an eight month trial with 75 participants.

1 Introduction

The use of mobile communication and wireless networks has a huge impact on the daily life. Due to the raise of participants in mobile networks, operators and application providers are searching for new applications and services to serve the consumer. Using the mobile phone for payment transaction has ever since been a hot topic [Va02]. Whereas card based payment systems are well established, mobile payment is far behind as the market so far has been unstructured with lots of proprietary solutions competing with each other [DMOZ06].

Chi Po et al. point out the four major criteria for the acceptance of mobile payment systems: Security, Cost, Convenience and Universality [CPCL07]. Khodawandi et al. show in their consumer report [KPW03] that *avoiding counting/carrying coins*, the *easy of use* as well as *time needed for a payment transaction* are among the most critical ones for using a mobile payment system in everyday life. Out of this criteria set we implemented a prepaid payment system in combination with Near Field Communication (NFC) technology

Petitioner Exhibit 1002-1564

to provide a new payment experience to the consumer.

In prepaid systems there are usually two processes needed for the user in terms of cash transactions: A top-up process and a payment process. Keeping the time needed low for both transactions is the major goal of our system. We propose the implementation of a micro payment system with a prepaid wallet on the mobile phone. The money is kept in a stored value account (SVA) in the mobile device. The SVA can be recharged over-the-air (OTA). The clearing and settlement of the transactions is performed by a bank. NFC is used at the point of sale (POS) to perform the payment transaction in a quick and convenient way. Money can be topped up OTA within seconds, anytime and anywhere. Additionally users can instantly query the amount of money available and the last transactions performed on their mobile phone without establishing an online connection.

The presented payment system was tested by 75 users during an eight-month field trial. The findings show, that this system is a fast and convenient implementation of a mobile payment system. A major focus of this paper is also the implemented security. We propose a public key infrastructure (PKI) and certificates for authentication and AES encryption for secure communication during OTA top-up transactions, as security concerns are the major argument for not using a mobile payment system. Linck et al. discuss this topic extensively in [LPW06].

Section 2 of this paper introduces the reader to the functionality and integration of NFC technology in systems and applications. Moreover the implementation and the architecture of a mobile payment system are lined out in section three. In this section also covers security aspects of the system. The findings section in section four provides the reader with information on the usage data acquired during a field trial. The paper closes with a conclusion.

2 Background Related Work

2.1 NFC - Near Field Communication

NFC is a wireless communications technology for proximity transactions. NFC is defined in ISO 18092 [In04] and backward compatible to the smartcard standard ISO14443. Hence NFC devices can be integrated in already existing smartcard based infrastructures easily. NFC allows contactless transactions over a distance of up to 10 centimetres. This is a reasonable operating range for transaction at ticketing gates and POS terminals, whereas logistics and health care make use of long-range radio frequency identification (RFID) technology. Both, NFC as well as RFID, base on the same physical technology: electro magnetic waves. Whereas RFID uses several different frequency domains for communication, NFC is located in the 13.56 MHz band.

RFID is mainly used for remote tracking, tracing and identification of goods and persons without a line of sight. NFC on the other hand is used for more sophisticated and secure transactions like contactless access or payment. The benefit of the short operating distance is that transactions are usually only caused on purpose [BHS+07].

Petitioner Exhibit 1002-1565

An NFC enabled device features the following operating modes [MDL+07]:

Reader/Writer Mode (Proximity Coupling Device, PCD): Operating in this mode, the NFC device can read and alter data stored in NFC compliant passive (without battery) transponders. Such tags can be found on *SmartPoster* e. g., allowing the user to retrieve additional information by reading the tag with the NFC device.

Card Emulation (Proximity Inductive Coupling Card, PICC): An NFC device can also act as smart card after being switched into card emulation mode. In this case an external reader can not distinguish between a smartcard and an NFC device. This mode is useful for payment and ticketing applications for example.

Peer-to-Peer (Near Field Communication, NFC): The NFC peer-to-peer mode allows two NFC enabled devices to establish a bidirectional connection in order to exchange contacts, Bluetooth pairing information or any other kind of data.

The protocol handling as also the conversion of the analogue into a digital signal and vice versa is performed by the NFC controller. Besides this integrated circuit, the mobile device – usually a cell phone – additionally contains a secure chip to store sensitive data. There are various ways to implement this secure chip: using the SIM Card, adding an additional smart card chip or storing data on a secure memory card [BJ05]. The data in such a secure data container – also referred to as secure element (SE) – can be access on the one hand side through the NFC interface (NFC controller chip in tag emulation mode) but also by the host controller. For example, data received over the mobile network (GSM e.g.) can be stored in the secure element then be queried over the NFC interface [MDL+07]. The secure element itself is designed to be tamper proof. Figure 1 shows the architecture of an NFC device.

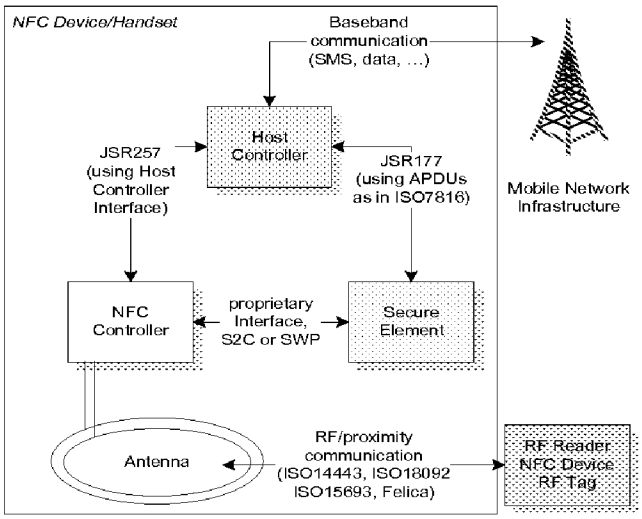


Abbildung 1: Integration of NFC into a mobile handset and communication flows/interfaces.

A major benefit of NFC is the quick setup up time (200 ms) of the communication in comparison to Bluetooth or WiFi. Usually there is no user interaction or PIN code required

Petitioner Exhibit 1002-1566

to establish a connection between to NFC devices. But the data rate of an NFC connection (max. 424 kbit/sec) is significantly lower than these technologies.

Industry and academia are quite excited about NFC technology being integrated into mobile devices. As Mark Weiser mentions in [We95] it is important that the technology itself disappears and only the interaction respectively the application should be visible to the user. NFC has a good chance to meet this criteria with its *Touch and Go* philosophy. NFC enabled handsets allow the users to interact with their environment like never before [ABPW07]. Additionally the integrated secure element stores identification information for the user in a secure way, like Satyanarayanan proposes already in [Sa05].

2.2 Mobile Payment

Mobile payment refers to a system where a wireless electronic device is used for a payment transaction. Gao et al line out the extensive literature available in their work [GCPS05] for example.

A good classification of payments is given in [La06]:

- Amount of money spent: micro (<5 USD) vs. macro payment (>5 USD)
- Point of Sale: local (vending machine e.g.) or remote payment (internet e.g.)
- Clearing and settlement: prepaid, post-paid, in-time paid
- Operation method: online (centralized) or offline (distributed)

A very interesting approach for an m-payment system was presented by Fujitsu Lab's in [LAJ+04] called *Wireless Wallet*. The proposed framework allows different implementation of an online payment system with various clearing methods and POS types. They also presented a unique hardware development for an m-payment device using WLAN to conduct transaction with wireless merchants. Additionally a J2ME version for a mobile phone was implemented. In this case the mobile network was used to process payment transaction with the backend server system.

In [GCPS05], [GES05] Gao et al. propose a wireless payment system based on Bluetooth for the local transaction with a server for online verification of payer and payee. The system is capable of POS payment as well as peer-to-peer transaction in a secure way.

Both systems, the *Wireless Wallet* and the Bluetooth based implementation, require a server in the backend. Either the payer or the payee needs an online connection to verify the authenticity of the instances involved in the payment transaction. Regarding online payment systems Bao et al. give an extensive overview and related references in [BDZ00].

Offline wallets and terminals as mentioned in [MR01] follow a different approach. In such a system the individual information – usually money or tickets – is stored highly secured in a remote device/integrated circuit. Transactions do not require an online connectivity to a server and thus save time during the transaction. Although, wallets and terminals need to

Petitioner Exhibit 1002-1567

be synchronized from to time to time in order to perform the clearing and settlement or to recharge the wallet with money. The implementation and management of the distributed paychip system *QUICK* is outlined by Holzmann in [Ho96]. The system is based on a contacted smartcard and is designed for micro payment transactions. The smartcard contains a secure wallet to store money. This prepaid wallet is topped up at an ATM before usage. At the POS the smartcard is inserted into the terminal and the amount due is deducted from the wallet. The terminal does not require the user to enter a PIN code to perform a payment transaction. Although, from a user's point of view, prepaid system are not very popular as Dahlberg et al. line out in [DMOZ07], this is the only technical solution of a secure offline payment system.

Akio et al. give details on a distributed public transport ticket payment system implemented by Japan Rail [WDL06]. The wallet is located on a contactless smartcard using *Sony's FeLiCa* technology. This purse – similar to *QUICK* – needs to be recharged at an ATM. Akia et al mention the following reasons for choosing a distributed purse based approach over a centralized one: better scalability, less cost for implementation and maintenance as well as simpler system architecture.

The idea of integrating a wallet in the secure element of an NFC device, using the contactless interface for payment, is self-evident [At06]. This fact in combination with the ability to alter the information in the secure element is a promising approach for new applications like payment and ticketing. Also Zmijewska lines out in [Zm05] that NFC is a promising technology for mobile payment.

3 Implementation

We implemented the system in a way that it is backwards compliant to the card based payment system at our campus. The payment infrastructure itself is a proprietary and closed ecosystem and relies on the following processes:

- Top-up of money into the SVA
- Payment Transaction at the POS
- Clearing and settlement

The already established system forces the user to go to an ATM on campus to load money into the wallet on the smartcard. Our system only modifies this process of topping up money and does not influence the other two processes (payment, clearing). In the following we describe how this process was improved by using an NFC handset.

The implementation, as shown in Fig. 2, bases on four different components:

A wallet application on the mobile phone to top-up the SVA: The application acts as a proxy between a security applet in the secure element and the backend server. This application also tells the user how much money there is available on the mobile

Petitioner Exhibit 1002-1568

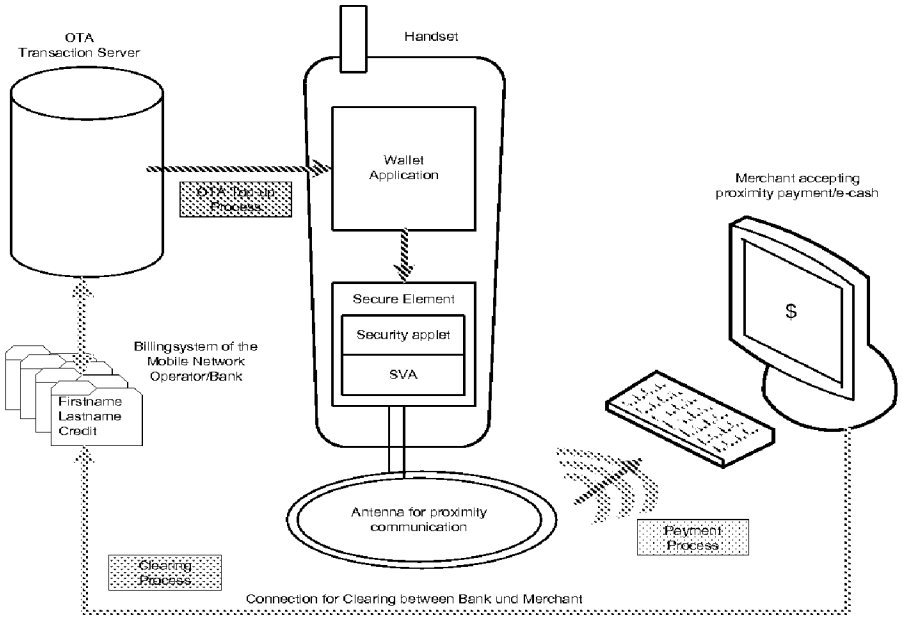


Abbildung 2: The system architecture shows the different process of the payment system: OTA top-up, payment transaction and clearing.

phone. The wallet application does not hold any keys nor does any de- or encryption. We used J2ME for the implementation (Fig. 4).

A security applet to process cryptographic functions: The security applet holds the

- public and the private key of the user, a certificate to authenticate against the server during OTA top-up,
- an AES key used for encryption during the OTA transaction,
- a certificate in order to verify the authenticity of the server and
- the keys to read and write the amount of data in the SVA.

The keys stored in the secure element can neither be read by an attacker nor will leave the security applet. The security applet uses Java Card technology.

A SVA with a contactless interface: We made use of a contactless memory card in the SE based on ISO14443-A, to be backwards compatible to our existing payment ecosystem. Besides the amount of money, the SVA stores the last 10 transactions, the last top-up date and the last payment date. The SVA contains a unique number used for anti-collision during the ISO14443 communication.

Backend: A Server in the backend to process the OTA top-up transactions.

Petitioner Exhibit 1002-1569

3.1 OTA top-up Process

The OTA top-up process is used to load money into the SVA in the handset (Fig. 3). The process is implemented as a pull service and has to be triggered by the user consciously (Fig. 3, 1.1). After starting wallet application, it establishes a connection to the secure element and requests the amount of money stored in the SVA (Fig. 3, 1.2 - 1.6) which is displayed on the screen (Fig. 4, Step 1). The read operation on the SVA (Fig. 3, 1.3) is performed by the security applet as the wallet applications does not hold the keys to do so. The security applet returns the amount of money stored (Fig. 3, 1.5 and 1.6).

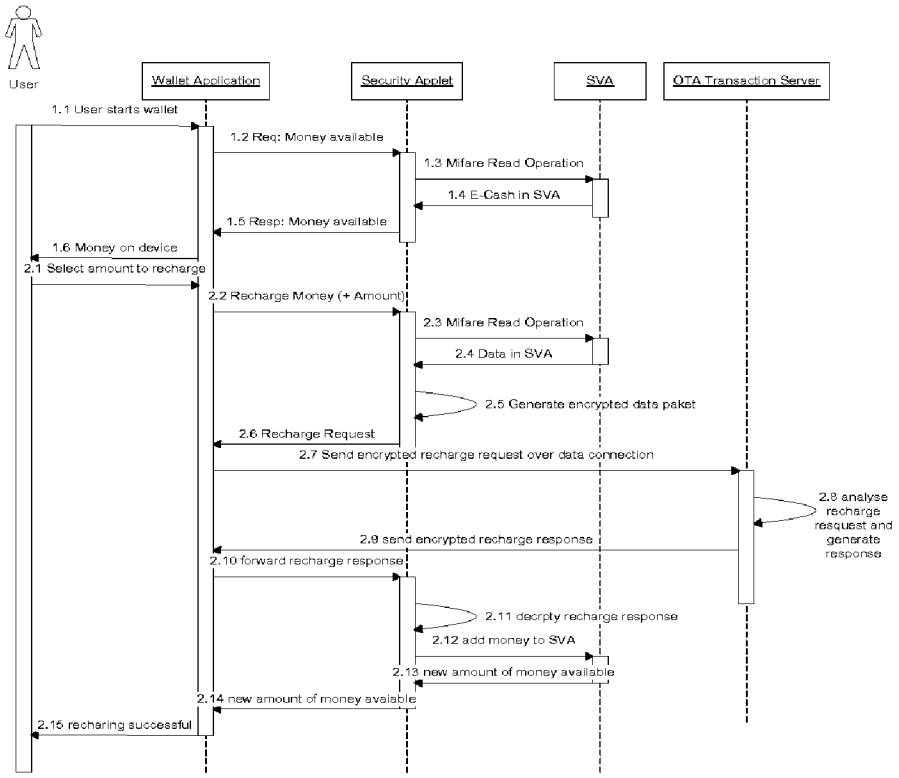


Abbildung 3: Process of recharging money: The figure shows the communication between the four components: wallet application, security applet, SVA and OTA transaction server.

The user can top-up the wallet (Fig. 3, 2.1) by selecting the amount from a list box (Fig. 4, Step 2) and confirms the operation (Fig. 4, Step 3). The amount of money selected to be topped up is handed over to the security applet (Fig. 3, 2.2). The security applet reads the information stored in the SVA, (Fig. 3, 2.3) and generates a secure random number as a session key for this transaction. This information is combined with the amount of money to be topped up. The whole data set is encrypted (AES) and signed (RSA) using the private key of the user stored in the security applet (Fig. 3, 2.5). As the secure element is optimized for cryptographic functions, encrypting and signing the data is performed without notice. Finally the wallet application receives the encrypted data packet from the security applet (Fig. 3, 2.6).

Petitioner Exhibit 1002-1570

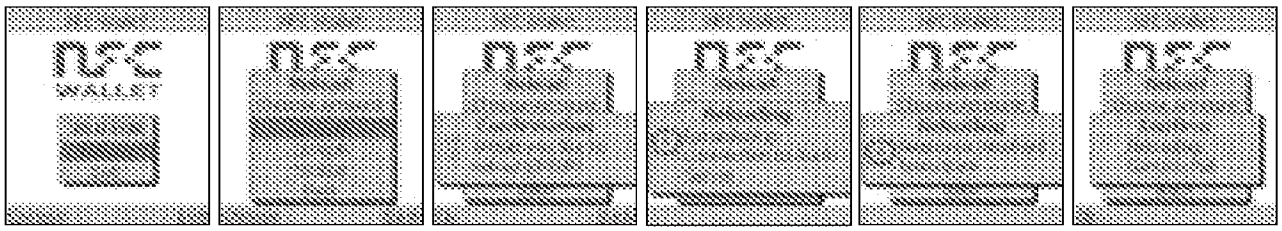


Abbildung 4: User interface at the mobile device during top-up process.

The next step taken by the wallet application is to establish an IP connection to the transaction server and hand over the encrypted data packet (Fig. 3, 2.7). The transaction server validates the signature of the packet using the public key of the wallet. Then the data packet is decrypted and an authentication of the user is performed through the IP address. This is done by querying the mobile network operator's GPRS/GSM database. The transaction server is able to match the mobile subscriber ISDN (MSISDN) number of the user with the IP address of the data package received. The transaction server also compares the ID and the date of the last top-up from the SVA with the information stored in a database (Fig. 3, 2.8).

If everything is correct the transaction server ties up a data packet with the top-up information, encrypts and signs it. A correct response is only given by the payment server if the credit line of the customer is not exceeded. Then this packet is sent back to the mobile device (Fig. 3, 2.9).

The wallet application receives the data and hands it over the security applet (Fig. 3, 2.10). The applet decrypts the data and checks the signature of the server (Fig. 3, 2.11). Additionally the applet checks the session key and the correctness of the new amount of money. If the tests are passed satisfactorily the SVA is updated (Fig. 3, 2.12). Finally the security applet confirms that everything worked out fine and sends the current amount of money available to the wallet application. The wallet application then displays the new amount of money to the user (Fig. 3, 2.13 and 2.14). This recharging process takes about 10 seconds.

3.2 Payment Process

The payment process itself is not different to using a smart card. In order to pay with the mobile phone the device must be in card emulation mode. Therefore the host controller has not to communicate with the secure element. Thus the wallet application in our case needs to close the connection to the secure element. Deducting money from the SVA takes about 0.2 seconds.

Petitioner Exhibit 1002-1571

3.3 Clearing and Settlement Process

The institution in charge of the transaction server receives the money collected at the terminals. Such a transaction can be performed in different ways. In case the terminals are operating online, the transaction server receives the money spent without delay through a secure IP connection. On the other hand, offline terminals send the data after a certain period of time to the central system. In case the terminals are not wired at all, the money from the the secure access modules (SAM) in the terminals is collected in person (using a smartcard for example) and sent to the backend system through a specially designed application. At the end of an accounting period the clearing institution credits the e-cash received to the merchant's bank accounts.

4 Trial Results

The trial phase started in November 2006 and last until June 2007. 75 persons participated in the trial. Among the participants there were 50 students and 25 full time employees at the campus. 1/3 of them were female, 2/3 were male. At the campus there are two cafeterias, five coffee and one drink vending machine accepting contactless payment. For legal reasons the cash handling is performed by the bank of the mobile network operator (MNO) during our trial. In our case the MNO provides a banking license and therefore its bank is able to issue *e-cash*. At the beginning of the trial the participants had to sign a contract with the bank and decide whether the money topped-up was credited to the customer's telephone bill or credit card. MNOs without a banking license would be able to offer this service through a 3rd party payment provider.

The NFC enabled mobile phone was used as access token, as loyalty card and to use information services by the participants as well.

4.1 Findings

In order to collect feedback on the applications in the trial, a combination of three complementary studies was chosen: Diary Study, Online Survey and Idea Development Workshop. Details on the whole user study conducted during the trial can be found here [GF07].

Diary Study: At the beginning of the trial, a 7-day online diary was kept by a group of 11 users. They provided information on the services used (quantity and quality). It turned out, that the access functionality was the feature used most often, followed by payment and information services. 75 % of the participants indicated that they were *very satisfied* or *rather satisfied* with the quality and availability of the NFC services on a five point scale.

Online Survey: All participants of the trial were asked to participate in an online survey (CAWI - Computer assisted web interview). Out of them, 60 persons returned

Petitioner Exhibit 1002-1572

a complete questionnaire. 83 % of the participants indicated that they were *very satisfied* or *rather satisfied* with the quality and availability of the NFC services on afive point scale. 19 % used the payment service daily and 41 % at least three times a week. 91 % of the user indicated that they were *very satisfied* or *rather satisfied* with the payment service. 89 % rated NFC payment as faster than payment in cash, 95 % as more convenient, 90 % as better, 90 % as more user friendly, and 95 % as more stylish (Fig. 5(a)). Only 40 % think, that the NFC payment system is at least as secure as cash-payment. With regards to attributes, NFC services were ranked as innovative, easy to use and simple. Also negative attributes like too technical and unpredictable were associated with NFC.

Idea Development Workshop: The 10 most active users during the first period of the trial were invited to participate in an idea workshop in order to improve the services given and come up with ideas on new services. Users explained how they like the services and which parts to be improved. On the positive side the contactless payment system was mentioned, on the negative side a lake of information on payment security. The possibility of topping up OTA was lined out as the most innovative feature of the system.

Generally, consumers are happy with the high transaction speed at the POS as also the OTA top-up functionality. The trial participants mention the time saving as the most convenient factor of this system. The users like the easy-to-use wallet application on the phone. 95 % of the users prefer the NFC payment system to using coins at automated vending machines. This is true for both students and full time employees. The major part of the users is satisfied with the system and would like to have more POS and more NFC services on campus.

With regard to the amount of money topped up, there are two different groups. There is one group which tops up a big amount of money (50 EUR e. g.). They say that they won't bother with topping up too often. This user group correlates well with the user group that is convinced that this means of payment is secure. The other group, usually topping up only 10 to 20 EUR at a time, is skeptical of technology and security. Both groups say that they are in favor of the NFC solution as they only need their handset for their every-day-life on campus as a replacement for an ordinary wallet. This is the case as the NFC device is also used as access token and loyalty card.

Out of the data collected (around 5000 transaction records) we were able to classify three different groups of user with regard to amount and value of transactions. The data was extracted form the transaction server.

Low revenue/high amount of transactions: This group has lots of transactions and uses the handset mainly for automated vending or small payments at the cafeteria. The users top-up between 10 and 20 EURs, but as the transaction value is not very high, topping up once last even up to a month or more. The speed at the POS is much more important than the time needed to top-up. The avoidance of coins is the most important argument for this group to use NFC payment.

Petitioner Exhibit 1002-1573