PAYMENT DEVICE WITH INTEGRATED CHIP

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is a non-provisional of and claims the benefit of the filing date of U.S. Provisional Patent Application No. 61/521,233, filed on August 8, 2011, which is herein incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] For businesses and merchants to improve their goods and services provided to consumers, merchants may gather additional data, such as sensitive or personal data (e.g. geographical location, profile information of the user, transaction history, or any other data from the user etc.) relating to the consumer as well as feedback data about the consumer's experience at a merchant, and analyze the data for future use. Consumers may be asked to fill out surveys or answer questions at a later time, and may be provided incentives for filling out a survey to provide additional feedback. However, such methods risk the additional data falling in to the wrong hands and being used for fraudulent or otherwise undesirable purposes. In addition, the filling out of surveys is often too time consuming and troublesome for consumers.

[0003] Furthermore, when a consumer provides additional data of their experience at the merchant at a later time, the consumer may have forgotten relevant details of the experience. Also, the merchant may not be able to identify a transaction associated with the experience of the consumer, making it difficult for the merchant to target areas of improvement.

[0004] Also, since the additional data is collected by the merchant or the merchant's employee in some cases, the merchant or its employee has access to the additional data. There may be some potential for the merchant or its employee to distribute the additional data and/or to tamper with and falsify the additional data.

[0005] Embodiments of the invention address these and other problems, individually and collectively.

BRIEF SUMMARY

[0006] Embodiments of the invention relate to payment applications, systems, and methods.

[0007] One embodiment of the invention is directed to a method comprising: receiving additional data from a portable consumer device used to conduct a transaction, wherein the additional data is encrypted and is associated with the transaction; generating, by an access device, an authorization request message comprising the encrypted additional data; transmitting the authorization request message comprising the encrypted additional data to a server computer; and receiving an authorization response message from the server computer. Other embodiments are directed to access devices that can perform the method.

[0008] Another embodiment of the invention is directed to a method comprising receiving an authorization request message comprising encrypted additional data for a transaction from an access device operated by a merchant; decrypting, by a server computer, the encrypted additional data associated with the transaction; storing the decrypted additional data associated with the transaction in a database; determining whether the merchant is eligible to receive decrypted additional data; and transmitting an authorization response message to the access device. Other embodiments of the invention are directed to server computers that can perform the method.

[0009] Another embodiment of the invention is directed to a method comprising: generating, by a mobile communication device, a prompt for additional data; receiving, the additional data at the mobile communication device; and transmitting the encrypted data to a server computer. The prompt may be in response in response to an interaction with an access device during a transaction, or may otherwise be associated with the transaction. Other embodiments of the invention are directed to mobile communication devices performing the method.

[0010] These and other embodiments are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 shows a block diagram illustrating a system according to an embodiment of the invention. The system incorporates the use of a mobile communication device such as a phone.

[0012] FIG. 2 shows a flowchart illustrating a method of conducting a transaction according to an embodiment of the invention. FIG. 2 can relate to the system in FIG. 1.

[0013] FIG. 3 shows a block diagram illustrating a system according to an embodiment of the invention. The system incorporates the use of a payment card.

[0014] FIG. 4 shows a flowchart illustrating a method of conducting a transaction according to an embodiment of the invention. FIG. 4 can relate to FIG. 3.

[0015] FIG. 5 shows a block diagram of a system according to an embodiment of the invention. The system incorporates the use of a mobile communication device such as a phone, and encrypted additional data passes to a mobile gateway instead of through an access device.

[0016] FIG. 6 shows a flowchart illustrating a method of conducting a transaction according to an embodiment of the invention. FIG. 6 can be described with reference to FIG. 5.

[0017] FIG. 7 shows a block diagram of an exemplary access device according to embodiments of the invention.

[0018] FIG. 8 shows a block diagram of an exemplary server computer in an exemplary payment processing network according to embodiments of the invention.

[0019] FIG. 9 shows an exemplary database according to embodiments of the invention.

[0020] FIG. 10 shows a block diagram of an exemplary mobile communication device according to embodiments of the invention.

[0021] FIG. 11 shows a block diagram of an exemplary computer readable medium.

[0022] FIG. 12(a) illustrates an exemplary payment card with an integrated chip according to embodiments of the invention.

[0023] FIG. 12(b) shows a block diagram of an exemplary integrated chip of a payment card according to embodiments of the invention.

[0024] FIG. 13 shows an exemplary computer apparatus that may be used in a system according to an embodiment of the invention.

DETAILED DESCRIPTION

[0025] Many merchants or businesses providing products or services may like to collate customer information and receive customer feedback to improve products or services to increase business and revenue. Currently there are means for users to review and rate businesses and merchants, for example, through websites to share their experiences with other users. These review forums allow users to research merchants and businesses to help them determine which merchants to patronize based on other users' reviews and ratings. However, these forums may not be as beneficial for merchants, because it is difficult for the merchant to associate a specific review with a specific transaction and/or user. Thus, the merchant may not be able to find an effective strategy to improve their business because they cannot target areas of improvement if they cannot associate a specific negative review or rating with a specific transaction. Additionally, since anyone can sign up for a review account on existing review websites, a merchant may create false reviews to alter their rating, affecting users' trust in using rating services and motivation to rate merchants. Embodiments of the invention address this and other problems.

[0026] Embodiments of the invention provide a system and method where additional data (e.g., information relating to a user, user feedback, ratings of the merchant by the user, etc.) may be associated with a specific transaction may be received at the time of the transaction, encrypted, transmitted by a portable consumer device such as a mobile phone or a payment card, to an access device, such as a point-of-sale terminal (POS terminal). The encrypted additional data can be transmitted to a server computer operated by a payment processing network (e.g., VisaNet) or entity other than the merchant. The server computer in the payment processing network may decrypt the encrypted additional data, and store

the additional data in a database. At some point in time, the server computer can re-transmit the decrypted additional data to the merchant.

[0027] Since the additional data is encrypted before being transmitted to the access device (e.g., POS terminal) and is only decrypted at the payment processing network (or entity other than the merchant), illegal distribution, merchant tampering and/or falsifying of the additional data can be prevented. For example, using embodiments of the invention, the merchant cannot falsify ratings data (e.g., change an unfavorable review into a favorable one) in an attempt to generate additional business. Additionally, since the additional data is collected at the same time a specific transaction is being conducted, the additional data (e.g., feedback, profile information of the user, etc.) can be directly associated with the specific transaction. This can tie a specific transaction to the additional data, thereby providing the merchant or other party with better analytics. For example, a specific review may be tied to a specific purchase, and a specific payment account number. If, for example, negative reviews are all provided by consumers within a specific time window associated with those purchases, this may indicate that poor customer service may have been provided during this time.

[0028] In embodiments of the invention, payment transactions may be conducted using a portable consumer device that is used by a user. The portable consumer device may be a mobile communication device (e.g., handset, mobile phone, PDA) that has a specific application, or may be a payment card with an integrated chip (e.g., smartcard).

[0029] Also in embodiments of the invention, the portable consumer device may interact with an access device. The access device may be a mobile POS terminal that the merchant may present to the user at the time of the transaction. As will be described below, the user may enter the additional data into the access device and the access device may generate and transmit an authorization request message comprising the encrypted additional data to a payment processing network.

[0030] Embodiments of the invention using a mobile payment application on a portable consumer device, such as a mobile communication device or a card, may include an integrated chip used for cryptographic operations for payment security purposes. This integrated chip may be used in payment applications to conduct

transactions to secure payment, as well as to collect, encrypt, store, and retransmit to a payment processing network (or entity other than the merchant) additional data associated with the transaction.

[0031] Embodiments of the invention further allow the payment processing network or other entity to bundle the decrypted additional data associated with specific transactions for the merchant. The merchant may subscribe to services from the payment processing network or other entity to receive decrypted additional data associated with the transactions and/or corresponding users. By requiring the merchants to subscribe in order to access the additional data, the security of the system is increased. The transaction-specific additional data may be used by the merchant for marketing or business research purposes. The additional data may be user profile information or feedback, such as a rating, which is associated with a specific transaction. Since the feedback is associated with a specific transaction, the merchant can easily determine what users do and do not like and target specific areas of improvement in their business to increase revenue.

[0032] Embodiments of the invention provide the payment processing network with additional data related to a transaction conducted by a portable consumer device. As noted above, the additional data may be desirable for merchants to acquire. The payment processing network may sell this additional data to the merchants associated to the transactions. Additional data associated with the transaction may include data such as feedback, ratings, geographical location, profile information of the user, transaction history, or any other data from the user at the time of the transaction that the merchant may not otherwise be able to obtain. Other examples of additional data may include surveys. For example, in embodiments of the invention, the consumer may be prompted to answer a survey to provide preferences on what type of food, shopping, cars, music, etc., the consumer likes. Thus, in some embodiments, the additional data need not relate to the specific merchant at which the current transaction is conducted. The additional data may also have value to entities (e.g., marketers) other than the merchant.

[0033] Prior to discussing various embodiments in greater detail, several terms will be described to provide a better understanding of this disclosure.

[0034] As used herein, a "portable consumer device" may include any suitable device that may be used to conduct a financial transaction. A portable consumer device 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, keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include mobile communication devices, payment cards, security cards, access cards, smart media, transponders, etc. If the portable consumer device is in the form of a debit, credit, or smartcard, the portable consumer device may also optionally have features such as magnetic stripes. Such portable consumer devices can operate in either a contact or contactless mode.

[0035] A "mobile communication device" (or "mobile device") as used herein may include any suitable electronic device that is capable of electronic communication. An exemplary electronic device is capable of being transported to a merchant location and/or capable of being moved to different positions within the merchant location. As discussed below, a mobile communication device may include a computing device, and further may be used to capture images of products at one or more merchant locations. Examples of mobile devices include smart phones, tablet computer, laptop computers, personal digital assistants, etc.

[0036] A "payment card" as used herein may include a card with an integrated chip. It may be capable of communicating with an access device. The payment card may comprise payment data, such as an account identifier, security code, card verification value, dynamic card verification value, and expiration date. Additional information that may be stored on the payment card may include personal data identifying an authorized user of the payment card, such as a photo, or other identifying information. The payment card can also be a debit device (e.g., a debit card), credit device (e.g., a credit card), or stored value device (e.g., a stored value card). They may include smart cards, credit or debit cards (with a magnetic stripe), etc.

[0037] As used herein, an "access device" may be any suitable device for communicating with a merchant computer or payment processing network, and for interacting with a payment device, a user computer apparatus, and/or a user mobile

device. An access device may generally be located in any suitable location, such as at the location of a merchant. An access device may be in any suitable form. Some examples of access devices include POS devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, Websites, and the like. An access device may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a payment device and/or a user mobile device. In some embodiments, where an access device may comprise a POS terminal, any suitable POS terminal may be used and may include a reader, a processor, and a computer-readable medium. A reader may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code readers, or magnetic stripe readers to interact with a payment device and/or mobile device.

[0038] As used herein, "transaction data" may include data relating to a transaction. In some embodiments, transaction data may include data as contained in an authorization request message, contained in an authorization response message, and/or generated by the processing of an authorization message. For example, transaction data can include a unique transaction identifier, transaction date and time, account number, transaction class code (e.g., credit, debit, ATM, prepaid, etc.), merchant code (e.g., MVV, DBA, etc.), ATM code, acquirer code, acquirer processor code, issuer code (e.g., BIN, etc.), issuer processor code, authorization category code (e.g., approved, declined, rejected, etc.), one or more error codes, transaction amount (e.g., settlement amount), cardholder or account holder information (e.g., name, date of birth, address, phone number, etc.), card verification value (CVV), expiration date, loyalty account information, and other information relating to the transaction.

[0039] "Additional data" can include data that is not typically included in conducting a transaction, and is not typically transmitted with the transaction data in an authorization request message. Examples of additional data may include, feedback, ratings, geographical location, personal information of the user (e.g., image), shopping profile of the user, authentication message of the user (e.g., cardholder), device ID, or other data associated with the transaction and/or user.

Additional data may be collected from the user at a time of a transaction, and may be encrypted. Also, in some embodiments, additional data is specifically created and entered by the user at the time of the transaction.

[0040] To prevent tampering or falsifying of the additional data, the additional data may be encrypted. Encryption allows merchants, issuers, acquirers, and other entities to verify the identity of the source of the information (e.g., the additional data is from a valid user), without allowing other parties, such as the merchant, to tamper with the data.

[0041] An "authorization request message" may include an electronic message that is sent to a payment processing network and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a consumer using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to "identification information" including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), an expiration date, etc.

[0042] An "authorization response message" may be an electronic message reply to an authorization request message. The authorization response message may be generated by an issuing financial institution or a payment processing network. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the payment processing network) to the merchant's access device (*e.g.* POS equipment) that indicates approval of the transaction. The code may serve as proof of authorization. As noted above, in some embodiments, a payment processing network may generate or forward the authorization response message to the merchant.

[0043] As used herein, a "payment processing network" 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 transaction, 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.

[0044] As used herein, an "acquirer computer" may be an entity that processes electronic payment transactions on behalf of an acquirer, or that cooperates with an acquirer to process electronic payment transactions.

[0045] As used herein, an "issuer computer" may be an entity that that processes electronic payment transactions on behalf of an issuer, or that cooperates with an issuer to process electronic payment transactions. An issuer processor may include data processing subsystems, networks, and operations used to support and deliver various services such as network gateway, risk management, program management, authorization, exception file, and clearing and settlement services.

[0046] As used herein, a "server computer" may include 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 server computer may be coupled to one or more databases and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

[0047] FIG. 1 shows a block diagram illustrating a system for conducting a transaction according to an embodiment of the invention. System 10 comprises a user 30 with a portable consumer device, such as a mobile device 36, an access device 34, a merchant computer 22, an acquirer computer 24, a payment processing

network (e.g., VisaNet) 26, and an issuer computer 28. One or more of these components can be operatively coupled together. The system 10 may also comprise a ratings server 29 including a ratings database 31. The ratings server 29 and ratings database 31 may be operated by another entity external to the payment processing network 26, or may be operated internally by the payment processing network 26. Further details about each of these components are provide below.

[0048] In an embodiment of the invention, the user 30 may wish to conduct a transaction. At some point during the transaction, the access device 34 may provide a prompt to the user 30 for additional data associated with the transaction. The prompt for the rating 36(a) may be displayed on the access device 34. The user 30 may then enter a rating into the mobile device 36 or the access device 34. For example, the user 30 may choose a rating for the transaction between 1 and 5 stars, and the user 30 may select a 4 star rating for the transaction. The information regarding the 4 star rating may be entered into the access device 34 or the mobile device 36. If the additional data was not entered into the mobile device 36, the access device 34 may transmit the ratings information to the mobile device 36.

[0049] Once received, the mobile device 36 may encrypt the rating and transmit the encrypted rating 36(b) to the access device 34. The mobile device 36 may communicate with the access device 34 in either a wired or wireless (e.g., contactless) mode.

[0050] In other embodiments of the invention, the prompt for rating 36(a) may be any suitable prompt for additional data that is typically not included in a conventional payment transaction. Other examples of additional data include user feedback, geographical location, authentication messages, etc.

[0051] After it receives the encrypted data, the access device 34 generates an authorization request message 34(a) including the encrypted rating 36(b). The authorization request message 34(a) with the encrypted rating 36(b) is then transmitted from the access device 34 to a merchant computer 22, which transmits it to an acquirer computer 24, and to a server computer in the payment processing network 26.

[0052] The server computer in the payment processing network (e.g., VisaNet) 26 may remove the encrypted rating 36(b) from the authorization request message

34(a), and decrypt the encrypted rating. The payment processing network 26 may then generate a second authorization request message 26(a) without the encrypted rating 36(b). The second authorization request message 26(a) comprises typical transaction data for authorization, and is then transmitted to the issuer computer 28. The issuer computer 28 then determines whether or not to approve or decline the transaction.

[0053] In response, the issuer computer 28 generates an authorization response message 28(a), approving or declining the transaction, and transmits the authorization response message 28(a) to the payment processing network 26.

[0054] The payment processing network 26, after removing the encrypted additional data 36(a) from the authorization request message 34(a) and decrypting it, may determine whether or not the merchant has requested the ratings information. The merchant may have subscribed to a subscription service to receive the decrypted additional data (e.g., ratings) associated with the transactions.

[0055] In some embodiments, the payment processing network 26 may generate and transmit a subscription query 26(c) to a ratings server computer 29 or other entity, coupled to a ratings database 31. If the ratings server computer 29 determines that the merchant is a subscriber, and is therefore eligible to receive the decrypted additional data, the decrypted rating and an associated transaction ID 29(a) are stored in the ratings database 31. In other embodiments, it is desirable to store the data even if the merchant is not subscribed, because other parties may desire access to the data. Other transaction data may be stored and associated with the decrypted rating, including an account identifier, merchant ID, transaction details (e.g., products purchased or services received), and transaction amount. The ratings server computer 29 may generate and transmit a subscription response 29(b) to the payment processing network 26 to confirm whether or not the merchant is a subscriber.

[0056] Although the ratings server 29 and the ratings database 31 are shown as being outside of the payment processing network 26, the ratings server 29 and the ratings database 31 may be present in the payment processing network 26 in other embodiments of the invention.

[0057] When the server computer in the payment processing network 26 receives the subscription response 29(b) with confirmation that the merchant is subscribed and is therefore eligible to receive the decrypted additional data (e.g., decrypted ratings), the payment processing network 26 incorporates the decrypted rating 36(c) with the authorization response message 28(a) from the issuer computer 28 to generate a modified authorization response message 26(b). The authorization response message 26(b) comprises the decrypted rating 36(c) and is transmitted through the acquirer computer 24, and to the merchant computer 22. The merchant computer 22 can remove the decrypted rating 36(c) from the authorization response message 26(b), store it in a local database (not shown) along with the transaction data for future analysis. It can also forward the authorization response message 26(b) to the access device 34.

[0058] In some embodiments of the invention, the decrypted rating may be transmitted directly to the merchant computer 22 from the payment processing network 26, and may be transmitted separately from the authorization response message.

[0059] FIG. 2 shows a flowchart illustrating a method of conducting a transaction according to the embodiment of the invention described above. A user 30 may possess a mobile device 36 to conduct the transaction with a merchant 22 at an access device 34.

[0060] In step A1, the user 30 initiates a payment transaction with the merchant at the access device 34. For example, the user 30 may bring items at a retail store to a checkout counter to initiate a transaction to purchase the items.

[0061] In step A2, the user 30 may be requested by an access device 34 to present the mobile device 36 for payment. For example, after all the items have been scanned and the transaction details, including total amount, are displayed on the access device 34, the access device 34 may request a form of payment to complete the transaction to purchase the items.

[0062] In step A3, the user 30 presents the mobile device 36 for payment. The mobile device 36 may communicate with the access device 34 by tapping or touching the mobile device on the access device 34, or holding the mobile device 36

in proximity of the access device 34 so that they can communicate with each other wirelessly or through other contactless means.

[0063] In step A4, the user 30 may be prompted for additional data, such as a rating or other feedback. The prompt could happen before or after the start of the transaction. The additional data may also include additional payment, personal user, or other additional data associated with the transaction. In some embodiments, the user 30 may receive a prompt on the access device 34 to interact the mobile device 36 with the access device 34. The user's mobile device 36, when in contact with the access device 34, may communicate with the access device 34 to display the prompt onto the mobile device 36. The mobile device 36 may communicate with the access device 34 by contactless means (e.g., wireless communication).

[0064] In step A5, the additional data (e.g., rating) from the user 30 is encrypted by the mobile device 36 and the encrypted data is transmitted to the access device 34.

[0065] In step A6, the access device 34 receives the encrypted additional data from the portable consumer device (e.g., mobile device 36) of the user, and generates an authorization request message to transmit to the payment processing network 26. The authorization request message may include transaction data typically contained in an authorization request message. Transaction data may include payment information (e.g., payment card identifier, card verification value, etc.) In embodiments of the invention, the encrypted additional data (e.g., rating) is bundled and included with the transaction data in the authorization request message transmission. In this way, the additional data may be collected in a secure manner without increasing the number of messages that are required to be transmitted or received. As such, only minimal additional demand is placed on computing resources in the system. In addition, it allows existing systems to perform methods in accordance with the invention, while requiring no, or minimal, modification.

[0066] In step A7, the payment processing network (e.g., VisaNet) 26 receives the authorization request message with the encrypted additional data (e.g., rating). The payment processing network 26 initiates authorization of the transaction using transaction data from the authorization request message. Additionally, the encrypted additional data (e.g., rating) is optionally removed from the authorization request

message and decrypted, associated with the specific transaction using a transaction ID, and stored in a database with the associated transaction. The payment processing network 26 also determines if the merchant is subscribed to receive decrypted additional data (e.g., rating) from the payment processing network 26. In other variations of the invention, the payment processing network 26 may communicate with another entity comprising a server computer (e.g., ratings server 29 of FIG. 1) and a database (e.g., ratings database 31 of FIG. 1) to determine whether the merchant is subscribed and therefore eligible to receive decrypted additional data associated with the transaction.

[0067] In step A8, after receiving the authorization request message including the encrypted additional data, the payment processing network 26 (e.g., VisaNet) removes the encrypted additional data, and generates an authorization request message without the encrypted additional data. The authorization request message without the encrypted additional data is transmitted to an issuer computer 28. The issuer computer 28 determined whether to authorize the transaction, and generates an authorization response message indicating whether the transaction is approved or declined.

[0068] In step A9, the issuer computer 28 transmits the authorization response message to the payment processing network 26, in which the authorization response message contains an indication of whether the transaction is approved or declined.

[0069] In step A10, the payment processing network 26 generates an authorization response message to be transmitted to the merchant computer 22. If in step A7 it has been determined that the merchant is a subscriber, the payment processing network 203 will bundle the decrypted additional data with the authorization response message. The payment processing network 26 will then transmit the authorization response message with the decrypted additional data (e.g., rating) to the merchant computer 22. If the merchant is not a subscriber, then the payment processing network 26 will generate and transmit the authorization response message to the merchant computer 22 without the decrypted data.

[0070] The decrypted additional data is removed from the authorization response message and stored at the merchant computer for the merchant to analyze and use. An authorization response message without the decrypted additional data is then

forwarded to the access device 34 to be displayed to the user 30 that the transaction is complete.

[0071] FIG. 3 shows a block diagram illustrating a system for conducting a transaction according to an embodiment of the invention. System 30 comprises a user 30 with a payment card 32. An access device 34, a merchant computer 22, an acquirer computer 24, a payment processing network (e.g., VisaNet) 26, and an issuer computer 28 may all be operatively coupled together. The system 10 may also comprise an additional data server 40 and an additional data database 42. Further details about each of these components are provided below.

[0072] In an embodiment of the invention, the user 30 may wish to conduct a transaction. At some point during the transaction, the access device 34 may provide a prompt to the user 30 for additional data associated with the transaction. The prompt for the additional information 46(a) may be displayed on the access device 34. The user 30 may then enter the additional information into the access device 34. For example, the user 30 may provide additional information such as authentication data (e.g., a password) to the access device 34. It might be useful to encrypt additional information such as a password, so that the merchant is unable to obtain the password. This increases the level of security in case the merchant or the merchant's employee is deemed untrustworthy.

[0073] In other embodiments, the prompt could come from the payment card 32 to be displayed on the access device 34. The access device 34 then sends the collected additional data to the payment card 32 so that it can be encrypted.

[0074] Once received, the payment card 32 may encrypt the additional information and can transmit the encrypted additional data 46(b) to the access device 34. The payment card 34 may communicate with the access device 34 in either a wired or wireless (e.g., contactless) mode.

[0075] In other embodiments of the invention, the prompt for the additional information 46(a) may be any suitable prompt for additional data that is typically not included in a conventional payment transaction. Other examples of additional data include user feedback, geographical location, authentication messages, etc.

[0076] After it receives the encrypted additional data, the access device 34 generates an authorization request message 34(a) including the encrypted additional data 46(b). The authorization request message 44(a) with the encrypted additional information 46(b) is then transmitted from the access device 34 to a merchant computer 22, which transmits it to an acquirer computer 24, and to a server computer in the payment processing network 26.

[0077] The server computer in the payment processing network (e.g., VisaNet) 26 may remove the encrypted additional information 46(b) from the authorization request message 44(a), and may decrypt the encrypted additional data. The payment processing network 26 may then generate a second authorization request message 48(a) without the encrypted additional data 46(b). The second authorization request message 48(a) comprises typical transaction data for authorization, which is then transmitted to the issuer computer 28. The issuer computer 28 then determines whether or not to approve or decline the transaction.

[0078] In response, the issuer computer 28 generates an authorization response message 48(b), approving or declining the transaction, and transmits the authorization response message 48(b) to the payment processing network 26.

[0079] The payment processing network 26, after removing the encrypted additional data 34(a) from the authorization request message 44(a) and decrypting it, may determine whether or not the merchant has requested the additional information. The merchant may have subscribed to a subscription service to receive the additional data associated with the transactions.

[0080] In some embodiments, the payment processing network 26 may generate and transmit a subscription query 40(c) to an additional data server computer 40 or other entity, coupled to an additional data database 42. If the additional data server computer 40 determines that the merchant is subscribed, and is therefore eligible to receive the decrypted additional data, the decrypted additional data and an associated transaction ID 40(b) are stored in the additional data database 42. Other transaction data may be stored and associated with the decrypted additional data including an account identifier, merchant ID, transaction details (e.g., products purchased or services received), and transaction amount. The additional data server computer 40 may generate and transmit a subscription response 40(c) to the

payment processing network 26 to confirm whether the merchant is subscribed or not.

[0081] Although the additional data server computer 40 and the additional data database 42 are shown as being outside of the payment processing network 26, they may be present in the payment processing network 26 in other embodiments of the invention.

[0082] When the server computer in the payment processing network 26 receives the subscription response 40(c) with confirmation that the merchant is subscribed and is therefore eligible to receive the decrypted additional data (e.g., decrypted ratings), the payment processing network 26 incorporates the decrypted additional data 46(c) with the authorization response message 48(b) from the issuer computer 28 to generate a modified authorization response message 48(c). In other embodiments, other entities including a payment processing network may generate an authorization response message on behalf of an issuer. The authorization response message 48(b) comprises the decrypted additional data 46(c) and is transmitted through the acquirer computer 24, and to the merchant computer 22. The merchant computer 22 can remove the decrypted additional data 36(c) from the authorization response message 48(c), and store it in a local database (not shown) for future analysis. It can also forward the authorization response message 48(c) to the access device 34.

[0083] In some embodiments of the invention, the decrypted rating may be transmitted directly to the merchant computer 22 from the payment processing network 26, and may be transmitted separately from the authorization response message.

[0084] FIG. 4 shows a flowchart illustrating a method of conducting a transaction according to the embodiment of the invention described above corresponding to FIG. 3. A user 30 may possess a payment card 32 to conduct the transaction with a merchant at an access device 34.

[0085] In step B1, the user 30 initiates a payment transaction with the merchant at the access device 34. For example, the user 30 may have just finished a meal at a restaurant and is ready to pay for the meal, thus asking a waiter for a bill.

[0086] In step B2, the user 30 may be presented with the bill, and an access device 34, such as a mobile merchant POS terminal, in which a payment card 32 is requested.

[0087] In step B3, the user 30 presents the payment card 32 for payment. In some embodiments the payment card 32 may communicate with the access device 34 by tapping or touching payment card 32 on the access device 34, or inserting the payment card 32 into the access device. Where the payment card 32 is a contactless payment card with an integrated chip, B3 may include holding the payment card 32 with integrated chip in proximity of the access device so that they can communicate with each other wirelessly or through other contactless means.

[0088] In step B4, the user 30 may be prompted for additional data, such as geographical location, preferences, user image, shopping profile, or other additional data associated with the transaction. The additional data may also include additional payment information, personal user information, etc., or other additional data associated with the transaction. In some embodiments, the additional data may be obtained directly from the payment card 32 without a prompt to the user (e.g., geo-location data may be transmitted by a payment card or mobile device, encrypted and sent to the access device). In some embodiments, the user 30 may receive a prompt on the access device 34 to enter the additional data and then interact the payment device 32 with the access device 34, such that the user's payment card 32, when in contact with the access device 34, may communicate with the access device 34 to receive the additional data from the access device 34. The payment card 32 may communicate with the access device 34 by contactless means (e.g., wireless communication).

[0089] In step B5, the additional data entered by user 30 on the access device 34 and received by the payment card 32 is encrypted by the payment card 32 and the encrypted additional data is transmitted to the access device 34. The user's payment card 32 encrypts and transmits the encrypted additional data to the access device 34. No data from the user 30 or the user's payment card 32 is stored at the access device 34.

[0090] In step B4, the access device 34 transmits the additional data to the payment card 32. In step B5, the access device 34 receives the encrypted data from

the payment card 32. These steps can coincide with a standard request for a cryptogram from the payment card 32, and the subsequent transmission of the cryptogram from the card 32 to the access device 34. In the cryptogram request, terminal data (e.g., a terminal unpredictable number and a transaction amount) may be transmitted from the access device 34 to the payment card 32. A processor in the payment card 32 may then generate a cryptogram using an application transaction counter on the payment card and the terminal data. This cryptogram is then transmitted from the payment card to the access device 32. By incorporating the transmission of the additional data to the card with the cryptogram request, and by incorporating the transmission of the encrypted additional data with the transmission of the cryptogram, the additional data encryption process can be efficiently incorporated into an pre-existing communication process without requiring the creation of additional communication processes.

[0091] Further details regarding known interaction protocols between a payment card and an access device (e.g., a payment terminal) can be found in U.S. Patent Application No. 11/536,307, filed on September 28, 2006, which is herein incorporated by reference in its entirety.

[0092] In step B6, the access device 34 receives the encrypted additional data from the payment card 32 of the user, and generates an authorization request message to transmit to the payment processing network 26. The authorization request message may include transaction data typically contained in an authorization request message. Transaction data may include user information (e.g., name, billing address, mobile device identifier, etc.), and payment information (e.g., payment card identifier, card verification value, etc.) In embodiments of the invention, the encrypted additional data is bundled and included with the transaction data in the authorization request message transmission.

[0093] In step B7, the payment processing network (e.g., VisaNet) 26 receives the authorization request message with the encrypted additional data. The payment processing network 26 initiates authorization of the transaction using transaction data from the authorization request message. Additionally, the encrypted additional data is removed from the authorization request message and decrypted, associated with the specific transaction using a transaction ID, and stored in a database with the associated transaction. The payment processing network 26 also determines if the

merchant is subscribed to receive decrypted additional data from the payment processing network 26. In other variations of the invention, the payment processing network 26 may communicate with another entity comprising a server computer (e.g., additional data server 40 of FIG. 3) and a database (e.g., additional data database 42 of FIG. 3) to determine whether the merchant is subscribed and therefore eligible to receive decrypted additional data associated with the transaction.

[0094] In step B8, after receiving the authorization request message including the encrypted additional data, the payment processing network 26 (e.g., VisaNet) removes the encrypted additional data, and generates an authorization request message without the encrypted additional data. The authorization request message is transmitted to an issuer computer 28. The issuer computer 28 determined whether to authorize the transaction, and generates an authorization response message indicating whether the transaction is approved or declined.

[0095] In step B9, the issuer computer 28 transmits the authorization response message to the payment processing network 26, in which the authorization response message contains an indication of whether the transaction is approved or declined. In other embodiments, the payment processing network 26 may generate and transmit the authorization response message on behalf of the issuer.

[0096] In step B10, the payment processing network 26 generates an authorization response message to be transmitted to the merchant computer 22. If in step B7 it has been determined that the merchant is a subscriber, the payment processing network 26 will bundle the decrypted additional data with the authorization response message. The payment processing network 26 will then transmit the authorization response message with the decrypted additional data to the merchant computer 22. If the merchant is not a subscriber, then the payment processing network 26 will generate and transmit the authorization response message to the merchant computer 22 without the decrypted additional data.

[0097] The decrypted additional data is removed from the authorization response message and stored at the merchant computer for the merchant to analyze and use. An authorization response message without the decrypted additional data is then forwarded to the access device 34 to be displayed to the user 30 that the transaction

is complete in step B11. In some embodiments, the authorization response message may pass from the access device 34, back to the payment card.

[0098] FIG. 5 shows a block diagram illustrating a system according to an embodiment of the invention. System 50 comprises a user 30 with a portable consumer device such as a mobile device 36. An access device 34, a merchant computer 22, an acquirer computer 24, a payment processing network (e.g., VisaNet) 26, and an issuer computer 28 are operatively coupled together. The mobile device 36 may be enabled to communicate over a mobile gateway 27 to the payment processing network 26. The system 50 may also comprise a ratings server computer 29 including a ratings database 31. The ratings server computer 29 and ratings database 31 may be operated by another entity external to the payment processing network 26, or may be operated internally by the payment processing network 26.

[0099] In an embodiment of the invention, the user 30 may wish to conduct a transaction. The user 30 may use a mobile communication device 36 to interact with the access device 34. The access device 34 and the mobile communication device 36 can communicate via a short range (e.g., less than 5 feet, and preferably less than 0.5 feet) contactless communication protocol (e.g., short range RF, Bluetooth™, IR, etc.), or may operate in a contact mode. The access device 34 generates an authorization request message 34(a). The authorization request message 34(a) is then sent from the access device 34 to a merchant computer 22, transmitted to an acquirer computer 24, and to a payment processing network 26.

[00100] The payment processing network 26 may then provide a prompt for additional data associated with the transaction to the mobile device 36 of the user 30, communicating via a mobile gateway 27. For example, the mobile device 36 may display a prompt for additional data, such as a rating of the transaction. A prompt for a rating 36(a) may be displayed on the mobile device 36, and the user 30 may enter a rating into the mobile device 36. For example, the user 30 may choose a rating for the transaction between 1 and 5 stars, and the user 30 may select a 4 star rating for the transaction. The mobile device 36 may encrypt the rating and transmit the encrypted rating 36(b) to the payment processing network 26 via the mobile gateway 27. The mobile device 36 may communicate with a server computer in the payment processing network 26 using a long range communication protocol.

For instance, the mobile device 36 may comprise an antenna which will allow it to communicate with the server computer in the payment processing network 26 via a cellular telecommunications network.

[00101] In other embodiments of the invention, the prompt for rating 36(a) may be any prompt for additional data typically not included in transactional data, such as user feedback, geographical location, authentication messages, or other user data.

[00102] The payment processing network (e.g., VisaNet) 26 may decrypt the encrypted rating. The payment processing network 26 may then forward an authorization request message 26(a) comprising typical transaction data for authorization, and transmit it to an issuer computer 28, wherein the issuer computer determines whether to approve or decline the transaction. In response, the issuer computer 28 generates an authorization response message 28(a), approving or declining the transaction, and transmits the authorization response message 28(a) to the payment processing network 26. In other embodiments, the payment processing network 26 may generate and send an authorization response message on behalf of the issuer.

[00103] The payment processing network 26, after receiving the encrypted additional data 36(b) from the mobile device 36 and decrypting it, may determine whether the merchant is subscribed to receive decrypted additional data, such as ratings, associated with the transactions. The payment processing network 26 may generate and transmit a subscription query 26(c) to a ratings server 29 or other entity, coupled to a ratings database 31. If the ratings server 29 determines that the merchant is subscribed, and therefore is eligible to receive decrypted additional data, the decrypted rating and an associated transaction ID 29(a) are stored in the ratings database 31. In some embodiments, the additional data is stored and/or processed whether or not there are active subscribers so such additional data. Other transaction data may be stored and associated with the decrypted rating, including an account identifier, merchant ID, transaction details (e.g., products purchased or services received), and transaction amount. The ratings server 29 may generate and transmit a subscription response 29(b) to the payment processing network 26 to confirm whether the merchant is subscribed or not.

[00104] In other embodiments of the invention, the ratings server 29 and ratings database 31 may be operated by the payment processing network, thus determining whether the merchant is a subscriber may be done internally within the payment processing network.

[00105] When the payment processing network 26 receives the subscription response 29(b) with confirmation that the merchant is subscribed and is therefore eligible to receive decrypted additional data, such as ratings, the payment processing network 26 directly transmits the decrypted additional data (e.g., ratings) to the merchant computer 22. The decrypted additional data may be transmitted separately from the authorization response message 26(b). The payment processing network 26 forwards the authorization response message 26(b) to the access device 34 via the acquirer computer 24 and merchant computer 22. The decrypted rating 36(c) may be stored and used by the merchant computer 22 for analysis.

[00106] FIG. 6 shows a flowchart illustrating a method of conducting a transaction according to the embodiment of the invention described above corresponding to FIG. 5. A user 30 may possess a mobile device 36 to conduct the transaction with a merchant 22 at an access device 34.

[00107] In step C1, the user 30 initiates a payment transaction with the merchant at the access device 34. For example, the user 30 may bring items at a retail store to a checkout counter to initiate a transaction to purchase the items. After all the items have been scanned and the transaction details, including total amount, are displayed on the access device 34, the access device 34 may initiate processing the transaction.

[00108] In step C2, the access device generates an authorization request message to transmit to the payment processing network 26. The authorization request message may include transaction data typically contained in an authorization request message. Transaction data may include payment information (e.g., payment card identifier, card verification value, etc.) The payment processing network (e.g., VisaNet) 26 receives the authorization request message.

[00109] In step C3, after the payment processing network receives an authorization request message from the access device 34, the payment processing

network 26 transmits a prompt to the mobile device 36 of the user 30 to request additional data. For example, the mobile device 36 may operate an application which is activated when a transaction is initiated with an access device 34, such that after the payment processing network 26 receives an authorization request message, the mobile device 26 receives a prompt from the payment processing network 26 to display to the user 30 requesting additional data, such as a rating of the transaction.

[00110] In step C4, the user 30 enters additional data into the mobile device 36. The additional data may also include additional payment, personal user, or other additional data associated with the transaction. The additional data (e.g., rating) from the user 30 is encrypted by the mobile device 36 and the encrypted additional data is transmitted to the payment processing network 26, bypassing the merchant computer 22 and the access device 34. The encrypted additional data may pass through a mobile gateway 27.

[00111] In step C5, the payment processing network 26 initiates authorization of the transaction using transaction data from the authorization request message. Additionally, the encrypted additional data (e.g., rating) received from the mobile device 36 is decrypted, associated with the specific transaction using a transaction ID, and stored in a database with the associated transaction. The payment processing network 26 also determines if the merchant is subscribed to receive decrypted additional data (e.g., rating) from the payment processing network 26. In other variations of the invention, the payment processing network 26 may communicate with another entity comprising a server computer (e.g., ratings server 29 of FIG. 5) and a database (e.g., ratings database 31 of FIG. 5) to determine whether the merchant is subscribed and therefore eligible to received decrypted additional data associated with the transaction.

[00112] In step C6, after receiving the authorization request message, the payment processing network 26 (e.g., VisaNet) prepares an authorization request message to forward to an issuer computer 28. The issuer computer 28 determined whether to authorize the transaction, and generates an authorization response message indicating whether the transaction is approved or declined. In other embodiments, the payment processing network 26 may act on behalf of the issuer.

[00113] In step C7, the issuer computer 28 transmits the authorization response message to the payment processing network 26, in which the authorization response message contains an indication of whether the transaction is approved or declined.

[00114] In step C8, the payment processing network 26 generates an authorization response message to be transmitted to the merchant computer 22. If in step A5 it has been determined that the merchant is a subscriber, the payment processing network 26 may bundle the decrypted additional data with the authorization response message. In other embodiments, the decrypted additional data may be sent to the merchant computer 22 without being present in an authorization response message. The payment processing network 26 will then transmit the authorization response message with the decrypted additional data (e.g., rating) to the merchant computer 22. If the merchant is not a subscriber, then the payment processing network 26 will generate and transmit the authorization response message to the merchant computer 22 without the decrypted additional data.

[00115] The decrypted additional data is removed from the authorization response message and stored at the merchant computer for the merchant to analyze and use. An authorization response message without the decrypted additional data is then forwarded to the access device 34 to be displayed to the user 30 that the transaction is complete, in step C9. In some embodiments, the authorization response message may pass back to the mobile device 36 (e.g., via a mobile gateway 27 or through the access device 34).

[00116] Although the embodiments of the invention described with reference to FIGS. 5-6 include encrypting additional data in mobile device and then transmitting that encrypted data to a central server computer, such encryption is not required in this embodiments. For example, if the additional data is a rating, this additional data may be transmitted to a central server operating a review Website (e.g., Yelp™). The additional data may be linked to actual transaction data so that the review Website can verify that the reviews that are posted are tied to actual transactions and are not posted by people who did not conduct actual transactions.

[00117] Provided below are descriptions of some devices (and components of those devices) that may be used in the systems and methods described above. These devices may be used, for instance, to receive, transmit, process, and/or store

data related to any of the functionality described above. As would be appreciated by one of ordinary skill in the art, the devices described below may have only some of the components described below, or may have additional components.

[00118] With reference to FIG. 7, an exemplary access device 34 is shown. The exemplary access device 34 is illustrated as comprising a plurality of hardware elements and software modules (301-310). However, it should be appreciated that this is provided for illustration purposes only, and each of the modules and associated functionality may be provided and/or performed by the same or different components.

[00119] The access device 34 comprises a processor 301, system memory 302 (which may comprise any combination of volatile and/or non-volatile memory such as, for example, buffer memory, RAM, DRAM, ROM, flash, or any other suitable memory device), and an external communication interface 303. It may also include a display 304, a contactless element 305, input elements 306, and a printer 307, all operatively coupled to a processor 301. In other embodiments, the access device 34 may also have a contact element (not shown) for contact based transactions, where the access device 34 contacts a portable consumer device.

[00120] The access device 34 may comprise software modules, such as a calculation module 308, using the transaction data to calculate transaction amounts, such as a subtotal, tax, discount, and total amount for the transaction. This transactional data may also be used to generate a receipt, performed by the receipt generation module 309. Further, a printer 307 may print the receipt or other relevant transactional data, such as a coupon.

[00121] The access device 34 may also comprise a contactless element 305 to communicate with suitable portable consumer devices. The access device 34 may receive information via input elements 306, such as a keypad, from a user. Any received information may be transmitted to an appropriate module within the computer 300 (*e.g.* via a data bus line 350).

[00122] The access device 34 may also receive additional data from a payment card, portable consumer device, or mobile device, communicating through the contactless element 305. The received information, transaction information, and additional data may be used to generate an authorization request message in an

appropriate data format in conformance with a transmission protocol so that the message may be sent to an issuer or payment processing network. The authorization request message may be generated by the authorization request generation software module 310, and may then be passed to the external communication interface 303 for transmission. Thus, the access device 34 is capable of generating an authorization request message, and in some embodiments, the authorization request message comprises encrypted additional data. The access device 34 may then transmit the authorization request message to a server computer operated by a payment processing network, acquirer, and/or issuer. The external communication interface 303 may receive authorization response messages, or transmit an authorization request message to an issuer, acquirer, or payment processing network. Thus, the access device may also receive an authorization response message from the server computer operated by the payment processing network, issuer, and/or acquirer.

[00123] With reference to FIG. 8, an exemplary server computer 200 in payment processing network 26 is shown. The exemplary server computer 200 is illustrated as comprising a plurality of hardware and software modules (201-211).

[00124] The exemplary server computer 200 comprises a processor 201, system memory 202 (which may comprise any combination of volatile and/or non-volatile memory such as, for example, buffer memory, RAM, DRAM, ROM, flash, or any other suitable memory device), and an external communication interface 203. Moreover, one or more of the modules 204-211 may be disposed within one or more of the components of the system memory 202, or may be disposed externally.

[00125] The communication module 204 may be configured or programmed to receive and generate electronic messages. When an electronic message is received by the server computer 200 via external communication interface 203, it may be passed to the communications module 204. The communications module 204 may identify and parse the relevant data based on a particular messaging protocol used in the system 10. The received information may comprise, for instance, identification information, transaction information, and/or any other information that the payment processing network 26 may utilize in authorizing a financial transaction or performing a settlement and clearing procedure. The communication module 204 may then transmit any received information to an appropriate module within the server

computer 200 (*e.g.* via a data bus line 250). The communication module 204 may also receive information from one or more of the modules in server computer 200 and generate an electronic message in an appropriate data format in conformance with a transmission protocol used in the system 10 so that the message may be sent to one or more components within the system 10. to an issuer computer 28 or merchant computer 22). The electronic message may then be passed to the external communication interface 203 for transmission. The electronic message may, for example, comprise an authorization response message (*e.g.* to be transmitted to a merchant conducting a transaction) or may be an authorization request message to be transmitted or forwarded to an issuer.

[00126] The database look-up module 205 may be programmed or configured to perform some or all of the functionality associated with retrieving information from one or more databases. In this regard, the database look-up module 205 may receive requests from one or more of the modules of server 200 (such as communication module 204, authorization module 208, or settlement module 209) for information that may be stored in one or more of the databases. The database look-up module 205 may then determine and a query an appropriate database.

[00127] The report generation module 207 may be programmed or configured to perform some or all of the functionality associated with generating a report regarding a user, an account, a transaction or transactions, or any other entity or category of information with regard to system 10. This may include, for instance, identifying patterns (such as patterns that indicate a fraudulent transaction or transactions) and generating one or more alerts that may be sent (*e.g.* via communication module 204 and external communication interface 203) to one or more entities in the system 10, including the user, merchant, or issuer. The report generation module may also, for example, request information from one or more of the databases via database look-up module 205.

[00128] The authorization module 208 may be configured or programmed to perform some or all the functionality associated with authorizing a financial transaction associated with an authorization request message.

[00129] The payment processing network 26 may further comprise a decryption module 210, which can receive encrypted additional data, and decrypt the additional

data. In some embodiments of the invention, the additional data can be a rating of the transaction. The payment processing network 26 may also include a ratings module 211, to parse, process, and interpret the decrypted ratings. For example, some ratings may be on a scale of 1 to 10, or 1 star to 5 stars. Additionally, the ratings module is not limited to only ratings, but the payment processing network 26 may include other modules for processing other types of additional data that may be encrypted/decrypted.

[00130] FIG. 9 illustrates an exemplary ratings database 31, or additional data database 42. The ratings database 31 may comprise a look-up table of different fields 2202-2218. Each field may include data relating to the transaction and/or the user, such as transaction ID 2202, account identifier (e.g., PAN) 2204, a rating of the transaction (or other additional data) 2206, merchant ID 2210, payment data (e.g., payment card information) 2212, transaction amount 2214, and/or transaction data (e.g., items purchased, services provided) 2208.

[00131] As shown in FIG. 9, additional data such as ratings, authentication data, surveys, etc. may be stored in a database with actual transaction data. By doing this, the additional data is more meaningful and authentic.

[00132] FIG. 10 shows a block diagram showing components of an exemplary mobile device 36. The exemplary mobile device 36 shown in FIG. 10 may comprise a computer readable medium 36(b) that be present within the body (or outer casing) 36(h), or the computer readable medium 36(b) could be detachable from the device The computer readable medium 36(b) may be in the form of a memory that stores data. The memory may store information such as financial information, transit information (*e.g.*, as in a subway or train pass), access information (*e.g.*, access badges), serial numbers, mobile account information, and any other suitable information. In general, any of this information may be transmitted by the mobile device 36 (such as to an access device 34), via any suitable method, including the use of antenna 36(a) or contactless element 36(g). The body 36(h) may be in the form a plastic substrate, housing, or other structure.

[00133] In some embodiments, the mobile device 36 may further include a contactless element 36(g), which is typically implemented in the form of a semiconductor chip (or other data storage element) with an associated wireless

transfer (e.g., data transmission) element, such as an antenna (for long range communication). Contactless element 36(g) may be coupled to (*e.g.*, embedded within) the mobile device 36 and data or control instructions that are transmitted via a cellular network may be applied to the contactless element 36(g) by means of a contactless element interface (not shown). The contactless element interface functions to permit the exchange of data and/or control instructions between the mobile device circuitry and an optional contactless element 36(g), or between another device having a contactless element (e.g., a POS terminal or a payment device). Contactless element 36(g) may be capable of transferring and receiving data using a short range wireless communication capability. As noted above, mobile device 36 may comprise components to both be the interrogator device (*e.g.* receiving data) and the interrogated device (*e.g.* sending data). Thus, the mobile device 36 may be capable of communicating and transferring data or control instructions via both cellular network (or any other suitable wireless network - *e.g.* the Internet or other data network) and short range communications.

[00134] The mobile device 36 may also include a processor 36(c) (*e.g.,* a microprocessor) for processing the functions of the phone 36 and a display 36(d) to allow a consumer to see phone numbers and other information and messages. The mobile device 36 may further include input elements 36(e) to allow a user to input information into the device, a speaker 36(f) to allow the user to hear voice communication, music, etc., and a microphone 36(i) to allow the user to transmit her voice through the mobile device 36. The mobile device 36 may also include an antenna 36(a) for wireless data transfer (*e.g.*, data transmission).

[00135] FIG. 11 shows an exemplary non-transitory computer readable medium 36(b) of the mobile device 36. The computer readable medium 36(b) may comprise several software modules. The mobile device 36 may be executing an operating system 3600 in operative association with a communication module 3602. The operating system 3600 may enable the communication module 3602 to activate mobile communication capability on the mobile device, for example, enabling Wi-Fi or telecommunications connectivity. Further, the operating system 3600 may also be linked to a mobile application 3604, to enable the mobile device to run the application to perform tasks. The mobile application 3604 according to embodiments of the invention may also include several software modules, including, but not limited

to, a transaction module 601, a payment card module 602, a ratings module 603, and an encryption module 604. The transaction module 601 may process transaction details when the mobile device is being used to conduct a transaction. The payment card module 602 may store and manage payment cards (e.g., credit card, debit cards, bank accounts) for payment of the transaction conducted. The ratings module 603 may display and receive the rating, or alternatively in other embodiments, additional data associated with the transaction. Then the ratings module 603 may send the rating collected to the encryption module 604 to be encrypted before it is transmitted either to a payment processing network 26 or an access device 34. The encryption module 604 (and any other encryption module described herein) may be use any suitable encryption process including DES, AES, etc. to encrypt the above-described additional data.

[00136] FIG. 12(a) shows an example of a payment device 32" in the form of a card. As shown, the payment device 32" comprises a plastic substrate 32(m). In some embodiments, an integrated chip 32(o) (e.g., contactless chip) for interfacing with an access device 34 may be present on, or embedded within, the plastic substrate 32(m). Consumer information 32(p) such as an account number, expiration date, and/or a user name may be printed or embossed on the card. A magnetic stripe 32(n) may also be on the plastic substrate 32(m). In some embodiments, the payment device 32" may comprise a microprocessor and/or memory chips with user data stored in them.

[00137] As noted above and shown in FIG. 12(a), the payment device 32" may include both a magnetic stripe 32(n) and an integrated chip 32(o). In some embodiments, both the magnetic stripe 32(n) and the integrated chip 32(o) may be in the payment device 32". In some embodiments, either the magnetic stripe 32(n) or the integrated chip 32(o) may be present in the payment device 32".

[00138] As shown in FIG. 12(b), the integrated chip 32(o), according to embodiments of the invention may also include several software modules, including, but not limited to, a payment data module 1306, a ratings module 1308, a contactless module 1304, and an encryption module 1302. The encryption module may have similar functionality as the encryption module 604 in FIG. 11. The contactless module 1304 may enable the payment card 32 to communicate with the access device 34, in a wireless manner, such that holding the payment card in near

proximity of the access device enables communication to conduct a transaction. The payment data module 1306 may store and manage payment data (e.g., credit card, debit cards, bank accounts) for payment of the transaction conducted. The additional data module 1308 may receive additional data associated with the transaction. Then the additional data module 1308 may send the additional data collected to the encryption module 1302 to be encrypted before it is transmitted to an access device 34.

[00139] FIG. 13 shows an exemplary computer apparatus according to embodiments of the invention, in which various embodiments may be implemented. The system 400 may be used to implement any of the computer systems described above (e.g., client computer, a server computer at the payment processing network, a computer apparatus at the merchant, etc.). The computer system 400 is shown comprising hardware elements that may be electrically coupled via a bus 424. The hardware elements may include one or more central processing units (CPUs) 402, one or more input devices 404 (e.g., a mouse, a keyboard, etc.), and one or more output devices 406 (e.g., a display device, a printer, etc.). The computer system 400 may also include one or more storage devices 408. By way of example, the storage device(s) 408 can include devices such as disk drives, optical storage devices, solid-state storage device such as a random access memory ("RAM") and/or a read-only memory ("ROM"), which can be programmable, flash-updateable and/or the like.

[00140] The computer system 400 may additionally include a computer-readable storage media reader 412, a communications system 414 (e.g., a modem, a network card (wireless or wired), an infra-red communication device, etc.), and working memory 418, which may include RAM and ROM devices as described above. In some embodiments, the computer system 400 may also include a processing acceleration unit 416, which can include a digital signal processor DSP, a special-purpose processor, and/or the like.

[00141] The computer-readable storage media reader 412 can further be connected to a computer-readable storage medium 410, together (and, optionally, in combination with storage device(s) 408) comprehensively representing remote, local, fixed, and/or removable storage devices plus storage media for temporarily and/or more permanently containing, storing, transmitting, and retrieving computer-readable information. The communications system 414 may permit data to be exchanged with

the network and/or any other computer described above with respect to the system 400.

[00142] The computer system 400 may also comprise software elements, shown as being currently located within a working memory 418, including an operating system 420 and/or other code 422, such as an application program (which may be a client application, Web browser, mid-tier application, RDBMS, etc.). It should be appreciated that alternate embodiments of a computer system 400 may have numerous variations from that described above. For example, customized hardware might also be used and/or particular elements might be implemented in hardware, software (including portable software, such as applets), or both. Further, connection to other computing devices such as network input/output devices may be employed.

[00143] Embodiments of the invention have many advantages. In embodiments of the invention, user feedback or additional data regarding a transaction and/or a merchant is protected from tampering by the merchant by encrypting the feedback at the time of the transaction before being transmitted to the merchant. This is accomplished by having the user enter additional data (e.g., rating) on a mobile device (or the information may originate in some other way from the mobile device) where it is encrypted. The encrypted additional data is then sent to a payment processing network (e.g., VisaNet) through an authorization request message from the merchant or by some other means (e.g., directly from the mobile device), as a proprietary additional data of the transaction.

[00144] One example of such additional data is a rating of the merchant showing purchase experience (e.g., 0 - 5 stars). At the time of payment, a mobile payment application may display a menu on the mobile device display, where the user can enter or select 0 to 5 stars. In other embodiments, the user may use a payment device, such as a smartcard, that when communicating with a merchant POS terminal, can initiate the menu or other prompt for data to display on the merchant POS terminal.

[00145] One advantage is that this additional data (e.g., rating) could be of value to the merchant accepting the payment transaction, but to prevent the merchant from tampering with the additional data, the additional data is encrypted, and the payment processing network controls access to the decrypted additional data. Only by

subscribing to receive the decrypted additional data, the merchant may be allowed to access the data.

[00146] The user benefits from providing additional data, such as rating his or her experience and sharing the rating with other users for future reference of where and with whom to conduct transactions with. There are existing means that allow users to rate and share their ratings with other users (e.g., Yelp, TripAdvisor, Google Latitude, and other similar services). However, user ratings are not fully protected from or for the merchant in currently existing services. Encrypting the additional data (e.g., rating) from the merchant ensures the security and protects the authenticity of user ratings, thus encouraging users to provide feedback and trust that their (and other users') feedback will be accurate and untampered with.

[00147] In embodiments of the invention, the merchant can benefit from a rating associated with a single transaction and can be encrypted to ensure that it is not modified in transit, thus assuring the merchant that the rating is provided by a real consumer, rather than one who has signed into a review service and provides fraudulent ratings because that person was never a recent customer or was never a customer at all.

[00148] Other advantages of embodiments of the invention relate to the merchant. Additional data, such as feedback or ratings from the user, may be of value to the merchant. In existing user feedback services (e.g., Yelp), user ratings are minimally useful to merchants because depending on the detail provided by the user in a review, the merchant may or may not be able to determine the specific transaction that the rating or review refers to. In embodiments of the invention, the data (e.g., rating) provides the merchant with more detail, since the user rating is directly associated to a specific transaction, unlike the ratings or reviews merchants may see on Yelp, or other rating services. Hence, this data is very valuable to the merchant because it may be used for more targeted marketing and/or improvements to the merchant's business to increase revenue.

[00149] Other advantages of embodiments of the invention relate to the payment processing network. The payment processing network may operate a subscription service where the merchants are provided with various levels of access to the collected decrypted additional data (e.g., ratings), with the highest level of

subscription providing a raw rating received at the time of the transaction, and with lower levels of subscription providing batched data that might relate merchant terminal IDs with ratings but not to individual purchases. Thus, merchant are encouraged to subscribe to the services provided by the payment processing network, increasing revenue for the payment processing network.

[00150] Embodiments of the invention also establish and build the relationships between the user, the merchant, and the payment processing network, by providing protection, benefits, and advantages to all parties during a transaction. Furthermore, strengthening the relationship with the user establishes user loyalty with the merchant and the payment processing network, thus increasing repeated business with the merchant and other merchants who are subscribers and revenue for both merchants and the payment processing network.

[00151] Embodiments of the invention may use existing technology and systems for payment processing, with no or minimal changes. In existing payment processing systems and methods, an authorization request message may contain a supplemental data field (e.g., Field 55), in which an encrypted additional data element (e.g., rating) may be stored. Thus, the merchant POS terminal may transmit the authorization request message to the payment processing network with the encrypted additional data contained in Field 55. The payment processing network may be enabled to (1) understand Field 55 or other supplemental data field, (2) decrypt the encrypted additional data, and (3) store the decrypted additional data and/or send the decrypted additional data back in a generated authorization response message, depending on a subscription status of the merchant. The subscription status of the merchant may be determined by looking up a merchant identifier in a table or database at the payment processing network.

[00152] In other embodiments of the invention, additional data may be collected from the user during a transaction. Examples of additional data are described below.

[00153] The user or mobile device may provide where a transaction was last conducted. This may enable marketers, merchants, and/or other interested parties to gather data and trace patterns of where the user conducts transactions and how they may relate to types of transactions that are conducted.

[00154] The mobile device may provide a picture of its registered user or account holder of a payment device used in the transaction, allowing the merchant to verify instantly with the person conducting the transaction to ensure that the mobile device has not been stolen. The picture may be digitally signed by an integrated chip in the mobile device or smartcard, so that the picture's integrity is protected and cannot be replaced with a new picture if stolen. The picture may be validated at the POS terminal with suitable software using the signature on the picture and displayed on the POS terminal.

[00155] In embodiments of the invention, the payment processing network may comprise a system and process to manage, encrypt/decrypt, and sell the data received. This may be performed by a server computer comprising a processor and a computer-readable medium comprising code executable by the processor.

[00156] In other embodiments of the invention, the payment processing network may be associated with a publisher of ratings, such as Yelp, Trip Advisor, Google (Latitude), Yahoo, Microsoft, Facebook or other entity. This may be beneficial so that users can go anywhere and see how merchants rate via multiple venues based on the user's preference. Further, the ratings data can be used by such sites to verify that comments are actually associated with real purchase transactions. This can make the reviews more authentic and reliable.

[00157] In other embodiments, an electronic wallet may be used with a mobile communication device or other device, in conjunction with embodiments of the invention. The wallet may be used to conduct a transaction. An electronic wallet may be used in a variety of transactions, including but not limited to eCommerce, social networks, money transfer/personal payments, mobile commerce, proximity payments, gaming, and/or the like. For example, users may engage in eCommerce via the electronic wallet for retail purchases, digital goods purchases, and utility payments. Users, for example, may also use the electronic wallet to purchase games or gaming credits from gaming websites, and transfer funds to friends via social networks. Further, for example, users may also use the electronic wallet on a smart phone for retail purchases, buying digital goods, NFC/RF payments at point of sale (POS) terminals.

[00158] In an exemplary transaction involving an electronic wallet, a consumer may submit an indication to purchase or transfer funds. For example, the consumer may visit a merchant website (e.g., Facebook.com, Amazon.com, etc.), and request to purchase an item from the website, transfer funds to a friend, and/or the like. The merchant website may determine whether the electronic wallet is authorized on its website, and may provide a list of payment options. If the merchant is registered with an electronic wallet server, the electronic wallet server may authorize the merchant to collect consumer credentials for login to the electronic wallet, and the merchant website may prompt the consumer to login to the electronic wallet. Otherwise, the merchant website may request the consumer to provide payment details for alternative payment options (e.g., credit card, debit card, PayPal account).

[00159] The consumer may authorize submission of their wallet consumer credentials, such as, but not limited to a Wallet/User ID, a password, and/or the like. For example, the consumer may enter the Wallet/User ID and password into a pop-up window provided from the merchant website and/or electronic wallet server. In another example, the consumer may authorize the merchant website to provide the consumer credentials (e.g., previously stored in HTML5, cookies, etc.), to the electronic wallet server. In yet another example, the consumer may authorize the electronic wallet server, via a remote component running on the merchant website (e.g., a Java applet, etc.) to provide consumer credentials to the electronic wallet server for verification.

[00160] When the consumer submits consumer credentials to log into the electronic wallet, the merchant website may forward the consumer credentials and transaction details to the electronic wallet server, which may determine the validity of the consumer credentials. If the consumer's credentials are not valid, the electronic wallet server may deny the payment request and send a notification of denial to the merchant website. In other embodiments, if the consumer provided credentials are valid, the electronic wallet server may process payment from the electronic wallet. For example, the electronic wallet server communicates with the consumer's bank account associated with the electronic wallet and requests a fund transfer of an indicated amount. The electronic wallet server may then store a transaction record.

[00161] In some embodiments, after processing the payment, the electronic wallet server sends a payment confirmation notice to the merchant website, which in turn completes the order and stores the transaction record in the database. The merchant website may provide a confirmation page comprising transaction confirmation to the consumer.

[00162] 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.

[00163] 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.

[00164] 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 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.

[00165] 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.

[00166] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving additional data from a portable consumer device used to conduct a transaction, wherein the additional data is encrypted and is associated with the transaction;

generating, by an access device, an authorization request message comprising the encrypted additional data;

transmitting the authorization request message comprising the encrypted additional data to a server computer; and

receiving an authorization response message from the server computer.

2. The method of claim 1, further comprising:

generating, by the access device, a prompt for the additional data.

3. The method of claim 1, wherein the portable consumer device displays a prompt for the additional data.

4. The method of claim 3, wherein the portable consumer device encrypts the additional data, and transmits the encrypted additional data from portable consumer device to an access device.

5. The method of claim 1, wherein the additional data comprises a rating associated with the transaction.

6. The method of claim 1, wherein the additional data comprises transaction profile data of a user, a geographical location, an image, or an authentication message.

7. An access device comprising a processor and a non-transitory computer readable medium, wherein the non-transitory computer readable medium comprises code executable by the processor to implement a method, the method comprising:

receiving additional data from a portable consumer device used to conduct a transaction, wherein the additional data is encrypted and is associated with the transaction;

generating an authorization request message comprising the encrypted additional data;

transmitting the authorization request message comprising the encrypted additional data to a server computer; and

receiving an authorization response message from the server computer

8. The access device of claim 8, wherein the method further comprises generating a prompt for the additional data.

9. The access device of claim 8, wherein the additional data is a rating associated with the transaction.

10. A method comprising:

receiving an authorization request message comprising encrypted additional data for a transaction from an access device operated by a merchant;

decrypting, by a server computer, the encrypted additional data associated with the transaction;

storing the decrypted additional data associated with the transaction in a database;

determining whether the merchant is eligible to receive decrypted additional data; and

transmitting an authorization response message to the access device.

11. The method of claim 10, further comprising:

removing the encrypted additional data from the authorization request message, thereby generating a second authorization request message;

transmitting the second authorization request message to an issuer; and

receiving the authorization response message from the issuer.

12. The method of claim 10 wherein the authorization response message comprises the additional data.

13. The method of claim 10, further comprising:

transmitting the decrypted additional data associated with the transaction to the access device when the merchant is eligible to receive decrypted additional data.

14. The method of claim 10, wherein the additional data is a rating associated with the transaction.

15. The method of claim 10, wherein the additional data is transaction profile data of the user, a geographical location, an image, or an authentication message associated with the transaction.

16. A server computer comprising a processor and a non-transitory computer readable medium, wherein the non-transitory computer readable medium comprises code executable by the processor to implement a method, the method comprising:

receiving an authorization request message comprising encrypted additional data for a transaction from an access device operated by a merchant;

decrypting the encrypted additional data associated with the transaction;

storing the decrypted additional data associated with the transaction in a database;

determining whether the merchant is eligible to receive decrypted additional data; and

transmitting an authorization response message to the access device.

17. A method comprising:

generating, by a mobile communication device, a prompt for additional data, the prompt associated with a transaction conducted with an access device;

receiving, the additional data at the mobile communication device; and

transmitting the additional data to a server computer.

18. The method of claim 22, wherein the additional data comprises a rating, and wherein the rating is provide on a review Website.

19. The method of claim 22 wherein the mobile communication device interacts with the access device using a short range communication protocol and the encrypted data is transmitted to the server computer using a long range communication protocol, and wherein the generated prompt is in response to an interaction with the access device during the transaction.

20. A mobile communication device comprising a processor and a non-transitory computer readable medium, wherein the non-transitory computer readable medium comprises code executable by the processor to implement a method, the method comprising:

generating a prompt for additional data, wherein the prompt is associated with an interaction with an access device during a transaction;

receiving the additional data; and

transmitting the additional data to a server computer.

21. The mobile communication device of claim 24 wherein the prompt is in response to an interaction between the mobile communication device and the access device.