US 20140019340A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2014/0019340 A1

(43) Pub. Date: Jan. 16, 2014

Ruder et al.

(54) **STORING AND FORWARDING PAYMENT TRANSACTIONS**

(71) Applicant: **Square, Inc.**, San Francisco, CA (US)

(72) Inventors: **Edward Ruder**, San Jose, CA (US); **James Puls**, San Francisco, CA (US); **Mehdi Mulani**, San Francisco, CA (US); **Shawn Morel**, San Francisco, CA (US); **Grace Chen**, San Francisco, CA (US); **Christopher R. Clark**, San Francisco, CA (US); **J. Bryan Scott**, San Francisco, CA (US); **Eric Monti**, San Francisco, CA (US)

(73) Assignee: **Square, Inc.**, San Francisco, CA (US)

(21) Appl. No.: **13/797,390**

(22) Filed: **Mar. 12, 2013**

Related U.S. Application Data

(60) Provisional application No. 61/672,228, filed on Jul. 16, 2012.

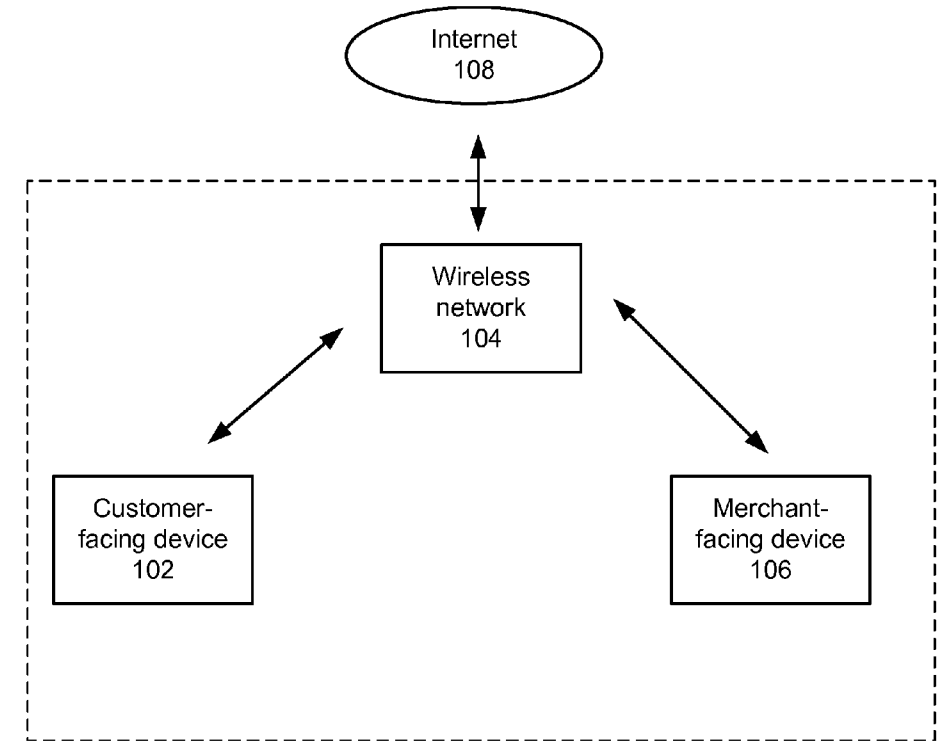
Publication Classification

(51) **Int. Cl.**
G06Q 20/32 (2012.01)

(52) **U.S. Cl.**
CPC *G06Q 20/322* (2013.01)
USPC **705/39**

(57) **ABSTRACT**

Method, systems, and apparatus for a method of processing a payment transaction using a mobile device of a merchant. In one aspect, determining the mobile device does not have a connection to an external network; receiving data indicating a payment transaction between a customer and the merchant; determining whether the payment transaction should be stored, where the determining is based on a risk heuristic model that considers one or more of the following: a number of already stored transactions, a value of the payment transaction, a total value, where the total value is a sum of the value of the payment transaction and values of one or more already stored transactions, and risk factors associated with the customer; and based at least on the determination, storing the payment transaction on the mobile device for future processing.



100

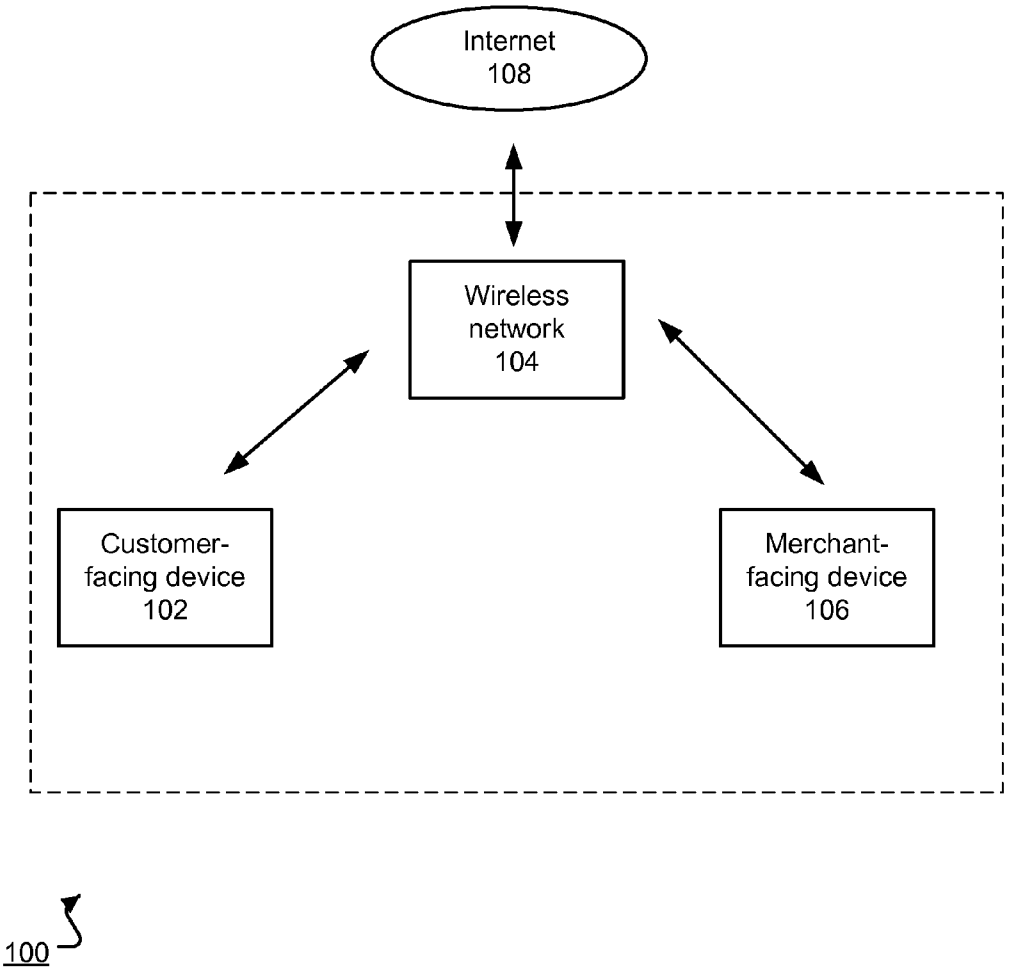

Internet
108
Wireless
network
104
Customer-
facing device
102
Merchant-
facing device
106
100

FIG. 1

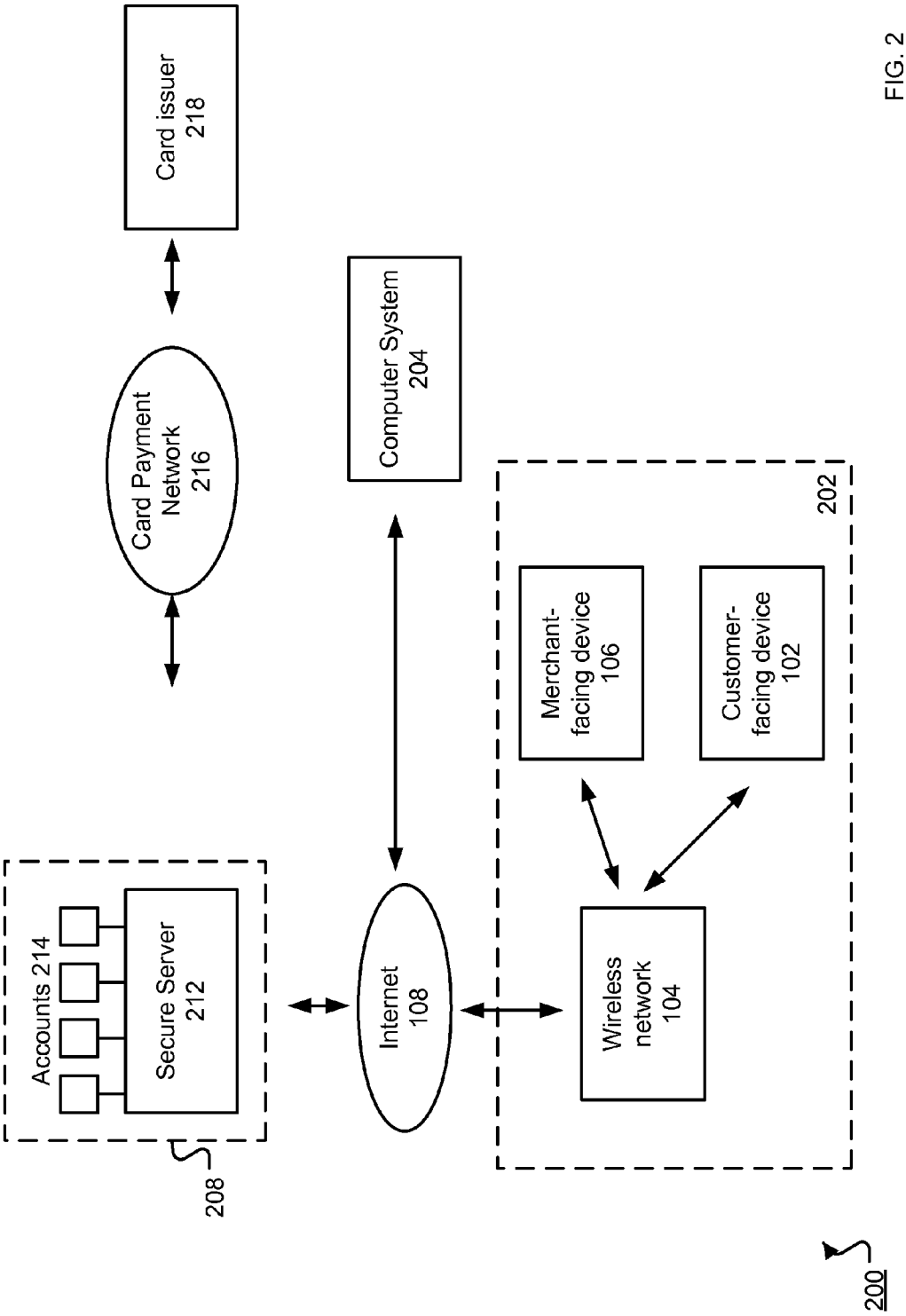

Card issuer
218
Card Payment
Network
216
Computer System
204
202
Merchant-
facing device
106
Customer-
facing device
102
Accounts 214
Secure Server
212
Internet
108
Wireless
network
104
208
200

FIG. 2

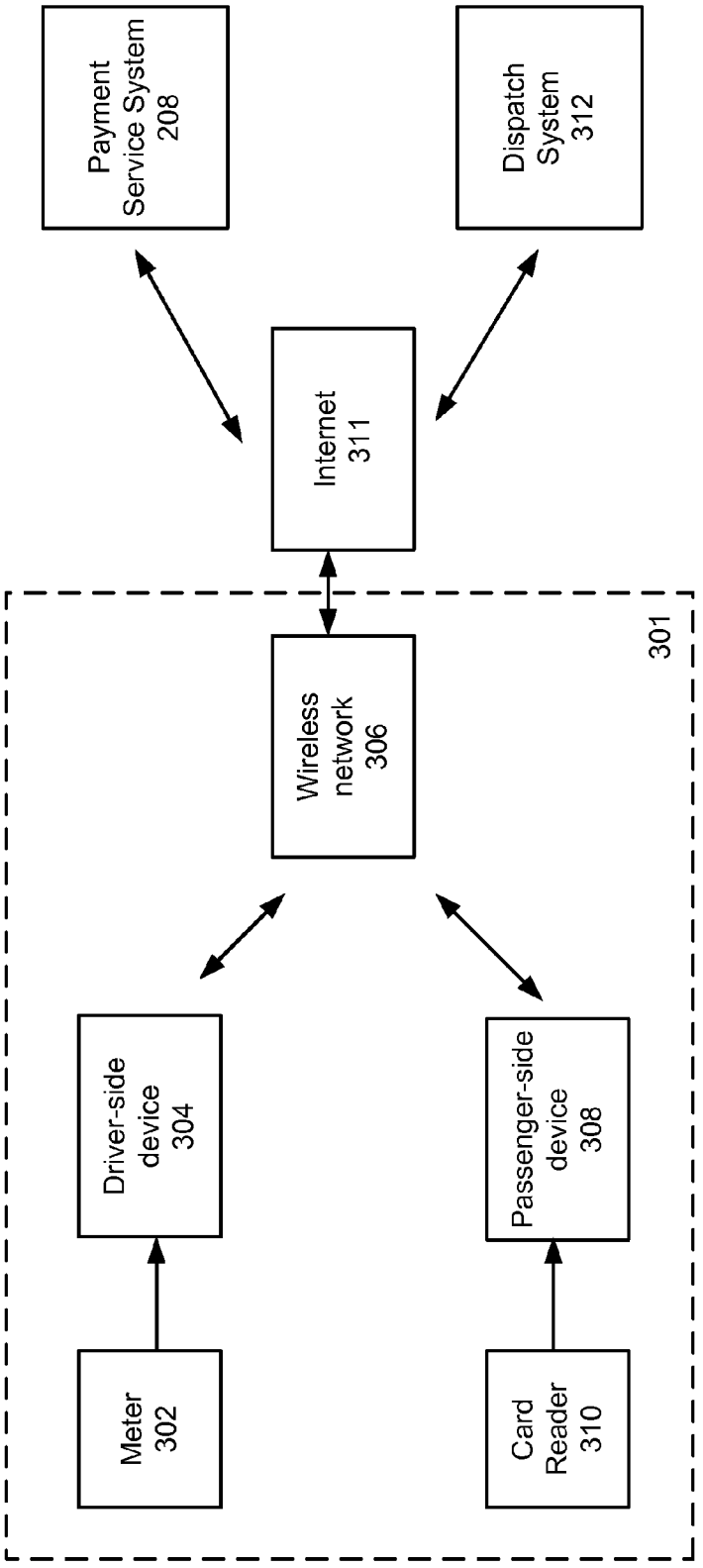

Payment Service System 208
Dispatch System 312
Internet 311
301
Wireless network 306
Driver-side device 304
Passenger-side device 308
Meter 302
Card Reader 310
300

FIG. 3

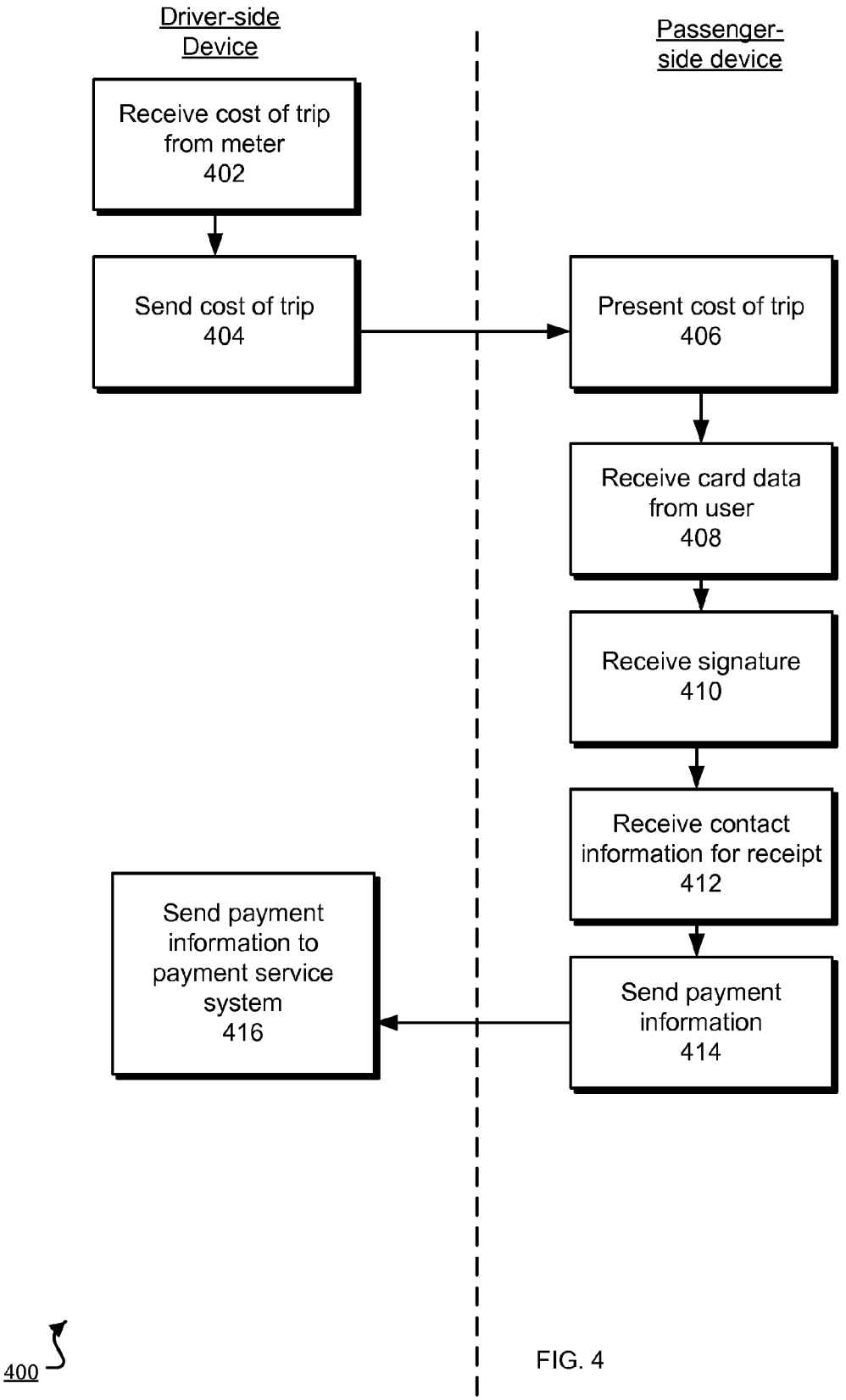

Driver-side Device
Passenger-side device
Receive cost of trip from meter 402
Send cost of trip 404
Present cost of trip 406
Receive card data from user 408
Receive signature 410
Receive contact information for receipt 412
Send payment information 414
Send payment information to payment service system 416
400

FIG. 4

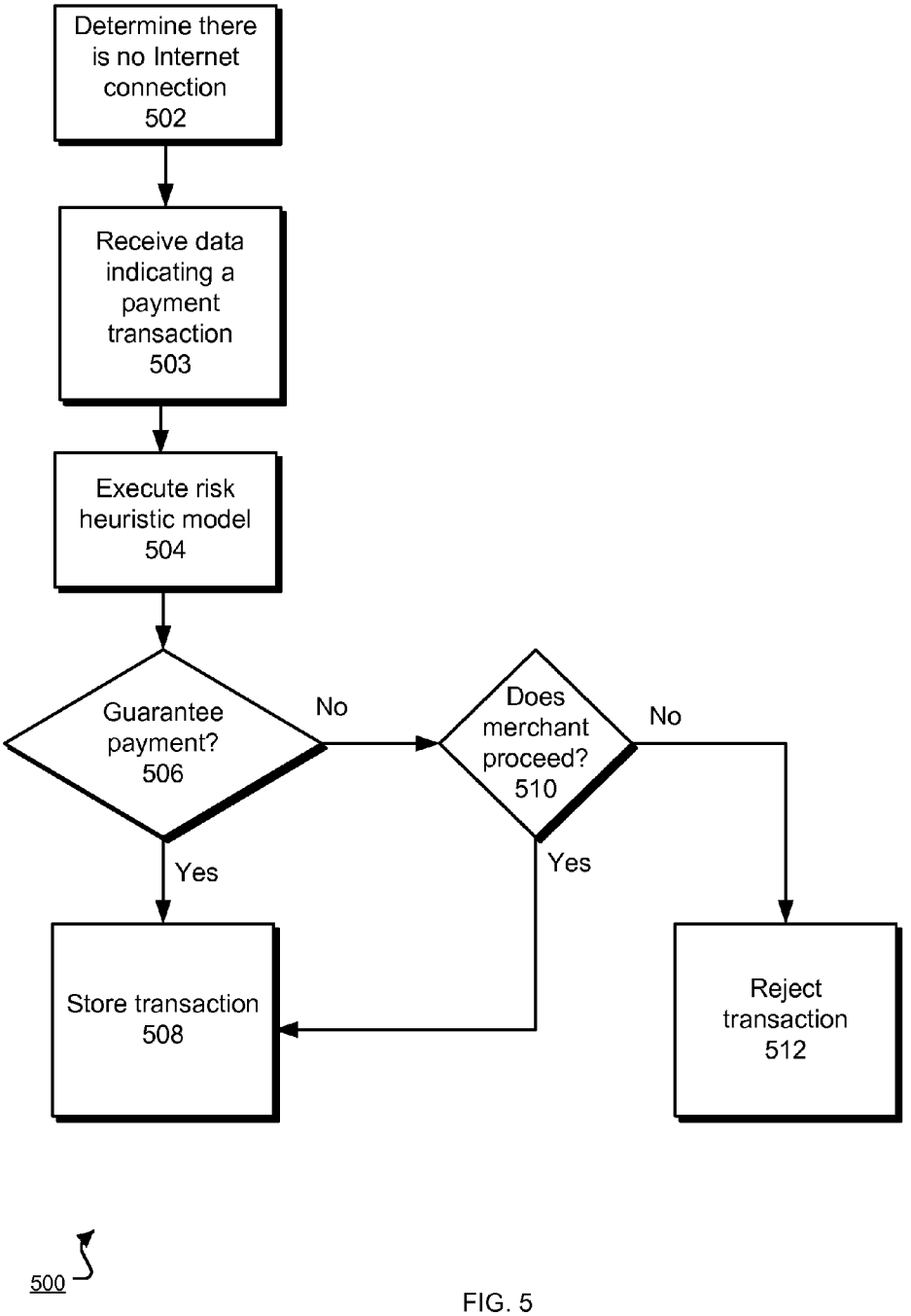

Determine there is no Internet connection 502
Receive data indicating a payment transaction 503
Execute risk heuristic model 504
Guarantee payment? 506
No
Does merchant proceed? 510
No
Yes
Yes
Store transaction 508
Reject transaction 512
500

FIG. 5

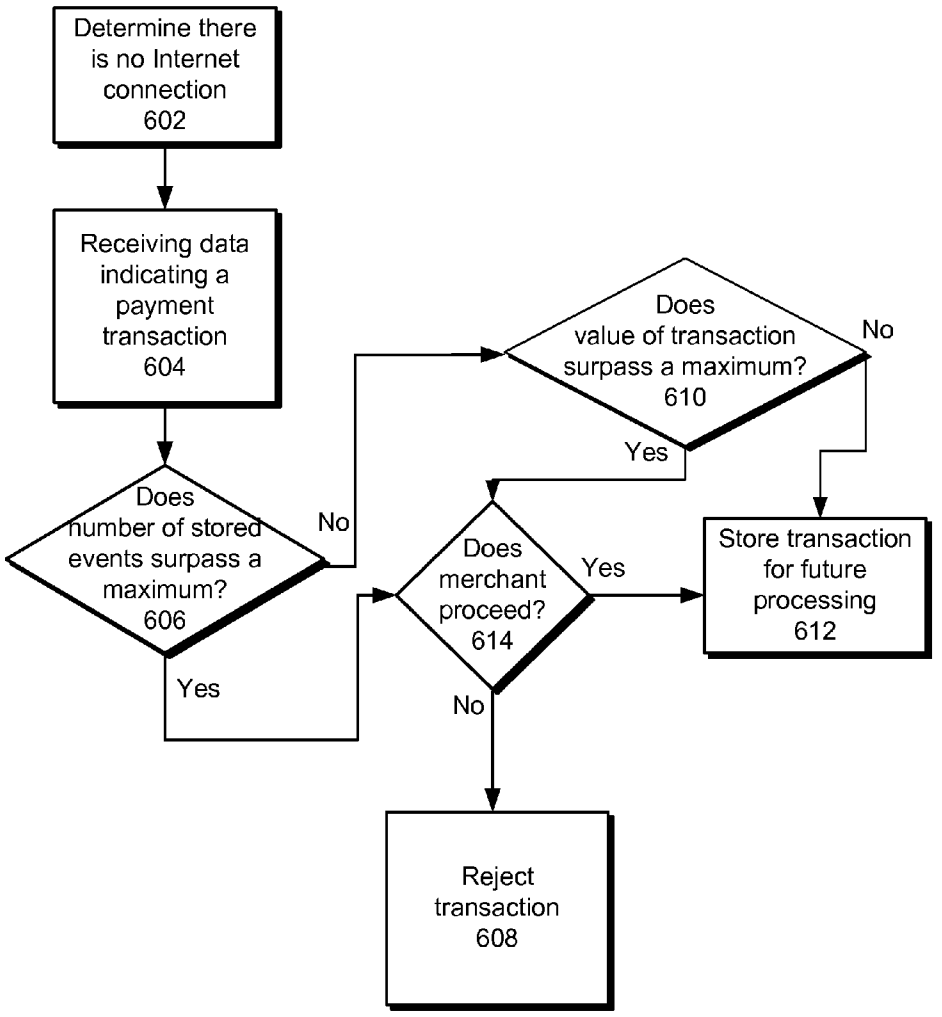

Determine there is no Internet connection 602
Receiving data indicating a payment transaction 604
Does number of stored events surpass a maximum? 606
No
Yes
Does value of transaction surpass a maximum? 610
No
Yes
Does merchant proceed? 614
Yes
No
Store transaction for future processing 612
Reject transaction 608
600

FIG. 6

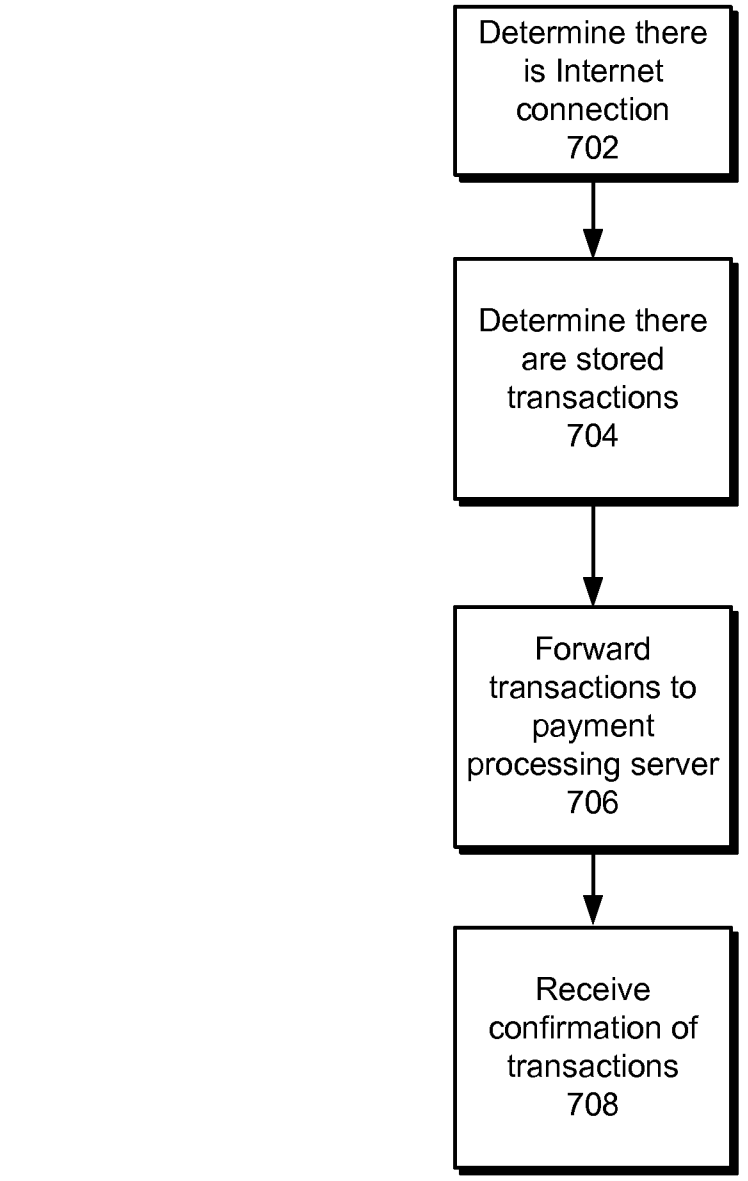

Determine there is Internet connection 702
Determine there are stored transactions 704
Forward transactions to payment processing server 706
Receive confirmation of transactions 708
700

FIG. 7

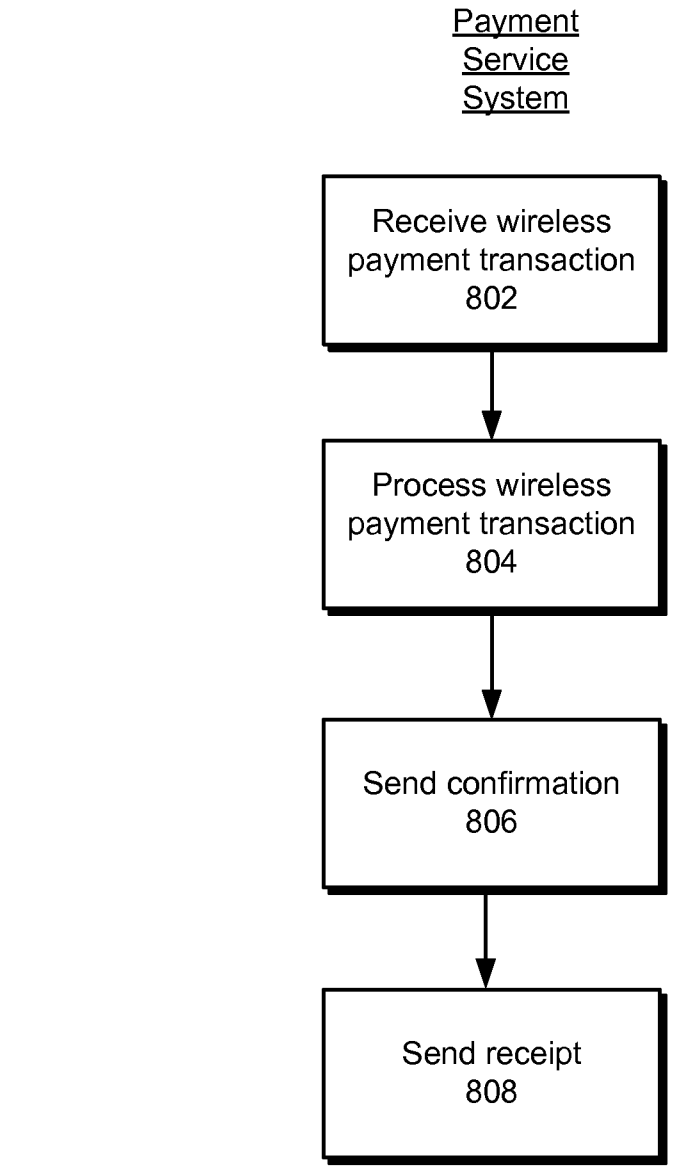

Payment Service System
Receive wireless payment transaction 802
Process wireless payment transaction 804
Send confirmation 806
Send receipt 808
800

FIG. 8

STORING AND FORWARDING PAYMENT TRANSACTIONS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is a non-provisional of and claims priority to U.S. Provisional Patent Application No. 61/672,228, filed on Jul. 16, 2012, the entire contents of which are hereby incorporated by reference.

TECHNICAL FIELD

[0002] This disclosure relates to mobile payment processing using a mobile device.

BACKGROUND

[0003] In a conventional point-of-sale electronic credit card transaction, the transaction is authorized and captured over a network connection during the point-of-sale. In the authorization stage, a physical credit card with a magnetic stripe is swiped through a merchant's magnetic card reader, e.g., as part of a point-of-sale device. A payment request is sent electronically from the magnetic card reader to a credit card processor. The credit card processor routes the payment request to a card network, e.g., Visa or Mastercard, which in turn routes the payment request to the card issuer, e.g., a bank. Assuming the card issuer approves the transaction, the approval is then routed back to the merchant. In the capture stage, the approved transaction is again routed from the merchant to the credit card processor, card network and card issuer, and the payment request can include the cardholder's signature (if appropriate). The capture stage can trigger the financial transaction between the card issuer and the merchant, and optionally creates a receipt. There can also be other entities, e.g., the card acquirer, in the route of the transaction. Debit card transactions have a different routing, but also require swiping of the card.

[0004] Mobile card readers are available. Some mobile card readers use WiFi technology to communicate with the credit card processor via a wireless network access point. Some mobile card readers, e.g., in taxis, use cellular technology to communicate wirelessly with the credit card processor.

SUMMARY

[0005] Although mobile card readers are available, e.g., in taxis, such systems conventionally require an Internet connection to process transactions. However, in some situations, a merchant may be in an area without an Internet connection. For example, a taxi may make a trip to an area with no cellular data network. Therefore, a mobile device can be configured to store a transaction if the mobile device does not have an Internet connection and to forward the transaction to a payment service system when the mobile device reestablishes an Internet connection.

[0006] In one aspect, a method of processing a payment transaction using a mobile device of a merchant, comprising determining the mobile device does not have a connection to an external network; receiving data indicating a payment transaction between a customer and the merchant; determining whether the payment transaction should be stored, where the determining is based on a risk heuristic model that considers one or more of the following: a number of already stored transactions, a value of the payment transaction, a total value, where the total value is a sum of the value of the payment transaction and values of one or more already stored transactions, and risk factors associated with the customer; and based at least on the determination, storing the payment transaction on the mobile device for future processing.

[0007] Implementations may include one or more of the following. After storing the payment transaction, determining the mobile device has a connection to the external network; determining the mobile device has stored payment transactions; forwarding each of the stored payment transactions to a payment service system; and receiving a response for each of the stored payment transactions from the payment service system. Each response is an acceptance or a rejection of the respective stored payment transaction. The risk heuristic model comprises: determining whether a value of the payment transaction or a total value surpasses a maximum value, where the total value is a sum of the value of the payment transaction and values of one or more already stored transactions; and determining whether a number of stored transactions stored on the mobile device surpasses a maximum number. If the number of stored transactions does not surpass the maximum number and the value of the payment transaction or the total value do not surpass the maximum value, storing the payment transaction on the mobile device. If the number of stored transactions surpasses the maximum number, rejecting the payment transaction. If the number of stored transactions does not surpass the maximum number and the value of the payment transaction or the total value surpass the maximum value, further comprising: sending a request to proceed to a user interface of the mobile device; receiving input through the user interface; storing the payment transaction if the input includes an approval of the request to proceed; and rejecting the payment transaction if the input includes a denial of the request to proceed. The payment transaction is encrypted using a key before the storing, where the key is obtained from a payment service system. Storing the payment transaction includes storing a time or user session data of the transaction. Determining whether the mobile device has a connection to the external network after an interval of time. The external network is an Internet network. The already stored transactions are obtained from an internal database. The risk factors include prior transactions or analysis of the prior transactions. The risk factors are updated by a payment service system when the mobile device has a connection to the external network. The risk heuristic model is updated by a payment service system when the mobile device has a connection to the external network.

[0008] Advantages may include one or more of the following. A customer can conduct a point-of-sale electronic payment transaction with a merchant using a mobile device even if the mobile device does not have an Internet connection to immediately process the electronic payment transaction. This allows the merchant to conduct more business with customers without worrying about maintaining a constant Internet connection to a credit card processor. A maximum number of delayed transactions and a maximum value of a delayed transaction can also be established to limit risk to a payment service or to the merchant.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. **1** is a schematic illustration of an example system for communication between mobile devices over a wireless network.

[0010] FIG. **2** is a schematic illustration of an example system for processing distributed payment transactions.

[0011] FIG. **3** is a schematic illustration of an example wireless payment system implemented for a taxi.

[0012] FIG. **4** is a flow chart of an example process conducted with the wireless payment system.

[0013] FIG. **5** is a flow chart of an example process of storing a payment transaction.

[0014] FIG. **6** is a flow chart of an example process of storing a payment transaction using an example risk heuristic model.

[0015] FIG. **7** is a flow chart of an example process of forwarding a payment transaction.

[0016] FIG. **8** is a flow chart of an example process conducted by a payment service system.

[0017] Like reference numbers and designations in the various drawings indicate like elements.

DETAILED DESCRIPTION

[0018] FIG. **1** is a schematic illustration of an example system **100** for communication between mobile devices over a wireless network. The system **100** shown in FIG. **1** is an example of a system that can be configured to establish secure communication between mobile devices over a wireless network using a pairing process in conjunction with a comparison of public keys. The secure communication is described in U.S. patent application Ser. No. 13/353,238, filed on Jan. 18, 2012, entitled "MOBILE CARD PROCESSING USING MULTIPLE WIRELESS DEVICES," which is incorporated by reference herein in its entirety.

[0019] The system **100** includes a first mobile device **102** and a second mobile device **106** that can communicate over wireless network **104**. The system **100** can also include additional mobile devices. The system **100** and the wireless network **104** can be connected to an external network, e.g., the Internet **108**. For example, the wireless network **104** can be a WiFi hot spot that includes a wireless access point for wireless connection to the mobile devices **102** and **106**. The wireless network **104** can also include a wired or cellular, e.g., 3G or 4G, connection the Internet **108**. Alternatively or in addition, one or both of the mobile devices **102**, **106** could have a wireless connection to the Internet, e.g., over a cell network. However, the Internet **108** is not needed for the two devices **102** and **106** to establish secure communications. The two devices **102** and **106** can establish secure communication solely through the wireless network **104**. Establishing secure communications through a pairing process and a comparison of public keys can be implemented with more than two devices.

[0020] In some implementations, described further below, the first device **102** serves as a customer-facing device, and the second device **106** serves as a merchant-facing device **106**. A "customer facing" device is a device that is configured with applications to display messages to and receive input from the customer. For example, the customer facing device can display a total for a transaction, display an interface for the customer to set a tip, and display a message that a credit card should be swiped. A "merchant facing" device is a device that is configured with applications to display messages to and receive input from the merchant. For example, the merchant facing device can display an interface for the merchant to enter a transaction, calculate a total amount due for the transaction, and display an interface for the merchant to request that the transaction be submitted for authorization.

[0021] FIG. **2** is a schematic illustration of the architecture **200** of an example system for processing distributed payment transactions. The system **200** includes a wireless payment system **202**. The wireless payment system **202** includes multiple devices, e.g., a customer facing device **102** and a merchant facing device **106**, connected to the wireless network **104**. The wireless network **104** is connected at least intermittently to an external network **108**, e.g., the Internet. The wireless network **104** can be a wireless access point. In some implementations, the wireless network **104** is a Wi Fi hotspot.

[0022] The system **100** or the system **300** can be used in implementing the wireless payment system **202**. The customer facing device **102** can be implemented using the first device **102**, but with additional programming to enable the device for use in the distributed payment transaction. Similarly, the merchant facing device **106** can be implemented using the second device **106**, but with additional programming to enable the device for use in the distributed payment transaction. The wireless network **104** can be implemented using the wireless network **104**.

[0023] In some implementations, devices connected to the wireless network **104** can securely communicate with each other, e.g., through a process of establishing secure communication as described above. In particular, once secure communication is established, the devices connected to the wireless network **104** can securely communicate with each other without data passing through the external network **108**, e.g., through the Internet.

[0024] The customer facing device **102** can be a mobile computing device, i.e., a hand held computing device, capable of running a customer-facing portion of a merchant application. For example, the customer facing device **102** can be a smart phone, tablet computer, laptop, or other data processing apparatus. The customer facing device **102** can include a display, e.g., a touch screen display. In some implementations, the customer facing device **102** and the display are two devices connected to each other.

[0025] The customer facing device **102** can include or be attached to a credit card reader. For example, the card reader can be attached to an input, e.g., an audio jack, of the customer facing device **102**.

[0026] The merchant facing device **106** is also a mobile computing device, capable of running a merchant-facing portion the merchant application. For example, the merchant facing device **106** can be a smart phone, tablet computer, laptop, or other data processing apparatus. The merchant facing device **106** can also include a display, e.g., a touch screen display. In some implementations, the wireless payment system **202** includes more than one customer facing device or more than one merchant facing device.

[0027] In some implementations, the merchant application has a login and logout functionality such that multiple merchants, each having a separate account with the payment service system **208**, can use the same device **106** for processing distributed payment transactions. The functionality allows a driver to login and logout of the payment service system **208**. Association by the payment service system **208** of the device **106** with the appropriate merchant account can be done by conventional login techniques.

[0028] In some implementations, the system **200** includes a computer system **204** connected to the network **108**. The computer system **204** can process or store data related to the transaction for analysis by the merchant or another third party that has a right to the data related to the transaction. For example, the merchant can be a franchisee and the third party can be the franchisor. As another example, the third party can

be responsible for coordinating jobs between various merchants who are themselves independent contractors, e.g., the merchant can be a taxi driver and the third party can be a dispatcher.

[0029] When a merchant submits a transaction to the payment service system **208**, the transaction can include sufficient information, e.g., the name or id number of the merchant, to associate the merchant with the third party. The payment service system **208** can maintain a database associating merchants with third parties, and when the payment service system **208** receive this information, it can identify the associated third party from the information. This allows the payment service system **208** to send data about transactions to the computer system **204** of the associated third party.

[0030] For example, if the system **200** is implemented in a restaurant, a customer can pay a restaurant using the wireless payment system **202** after a waiter at the restaurant brings the customer the final tab of the meal. After conducting the transaction, the system can send data about the meal to a computer system **204**, e.g., a meal tracking system. The data can include which items were ordered, the cost of the meal, the tip included, the date and time of the meal, or which waiter served the customer.

[0031] In some implementations, the customer facing device **102** receives transaction details from the merchant facing device **106** and displays the details on the display of the merchant facing device **106**. In particular, the merchant facing device **106** can calculate an amount for the transaction, e.g., based on purchase of individual items, and the amount can be sent to the customer facing device **102** and displayed.

[0032] The wireless payment system **202** can communicate with a payment service system **208** using the network **108**.

[0033] In some implementations, the merchant facing device **106** receives transaction details from the customer facing device **102** and communicates with the payment service system **208** to submit a request for authorization of the transaction. In particular, when the customer swipes the card through the card reader, the card information can be sent to the merchant facing device **106**. Similarly, a signature, PIN, or other data required for authorization of the transaction can be input by the customer into the customer facing device **102**, e.g., entered on the touch screen display, and this data can be sent to the merchant facing device **106**.

[0034] In some implementations, the customer facing device **102** does not send transaction details to the merchant facing device **106**. Instead, the customer facing device **102** receives the amount for the transaction from the merchant facing device **106**, and receives the card information from the card reader when the customer swipes the card. The customer facing device **102** communicates with the payment service system **208** to submit a request for authorization of the transaction.

[0035] The payment service system **208** includes a secure server **212** to processes all transactions from the wireless payment system **202**. The secure server **212** handles secure information such as credit card numbers, debit card numbers, bank accounts, user accounts, user identifying information or other sensitive information.

[0036] The payment service system **208** can communicate electronically with a card payment network **216**, e.g., Visa, Mastercard, or the like. The payment service system **208** can communicate with a card payment network **216** over the same network **108** used to communicate with the wireless payment system **202**, or over a different network. The computer system **216** of the card payment network can communicate in turn with a computer system **218** of a card issuer, e.g., a bank. There can also be computer systems of other entities, e.g., the card acquirer, between the payment service system **208** and the card issuer.

[0037] Before a transaction between the user and the merchant can be performed using the wireless payment system **202**, the merchant must create a merchant account with the payment service system **208**. The merchant can sign up using a mobile application or using an online website, and can use a device within the wireless payment system **202** or another computing device, e.g., a home computer. At some point prior to the transaction, one or more applications are downloaded to the devices within the wireless payment system **202**, e.g., a merchant facing device and a customer facing device. The merchant facing and customer facing devices may run the same application or customized applications to each device (e.g. a merchant application and a customer application). In some implementations, the applications are downloaded through an application store. Creation of the merchant account can be handled through the application, or through another application, e.g., a generic web browser. The merchant enters a name, account password, and contact information, e.g., email address, and physical location information (if applicable), e.g., an address, into the payment service system **208**. The merchant can also provide other information, e.g., a list of goods or services available, operating hours, phone number, a small identifying image logo or mark, to the payment service system **208**. The data associated with the merchant account **214** can be stored at the secure server **212**, e.g., in a database. In some implementations, the merchant can provide information sufficient to establish communication with the computer system **204** and this information can be stored in the payment service system **208**.

[0038] Eventually, in order to receive funds from the transaction, the merchant will need to enter financial account information into the payment service system **208** sufficient to receive funds. For example, in the case of a bank account, the user can enter the bank account number and routing number. However, the merchant's financial account can also be associated with a credit card account or another third party financial account. In addition, in some implementations, if the merchant has not entered the financial account information, the payment service system **208** can hold the received funds until the financial account information is provided.

[0039] FIG. **3** is a schematic illustration of a wireless payment system implemented in a taxi environment. The wireless payment system **301** includes a meter **302**, a mobile driver side (i.e., merchant facing) device **304**, a passenger side (i.e., customer facing) device **308**, a card reader **310**, and the wireless network **306**. The wireless network **306** can include wireless access point mounted in the vehicle that provides a WiFi hot spot. The wireless network **306** can include a transceiver that provides a cellular connection, e.g., 3G or 4G, to the external network **306**.

[0040] In some implementations, the driver side device **304** is physically connected to the meter **302**, e.g., by a data cable, such as a USB cable. The driver side device **304** can be positioned next to the taxi driver in the front of the taxi. The driver side device **304** is wirelessly connected to the wireless network **306**. The driver side device **304** can be a smart phone or tablet computer having a display onto which the driver has loaded an appropriate application. The driver side device **304** can also display a passenger fare for the taxi ride.

[0041] The passenger side device **308** can be positioned in the back of the taxi where a customer can interface with the device. For example, the passenger side device **308** can be affixed to the back of the front seat of the taxi, or to the back of the barrier separating the driver compartment from the passenger compartment. The card reader **310** is attached to an input, e.g., an audio jack, of the passenger side device **308**. The passenger side device **308** is wirelessly connected to the wireless network **306**. The passenger side device **308** can be a tablet computer onto which an appropriate application has been loaded. As a tablet computer, the passenger side device **308** includes a display, e.g., a touch screen display.

[0042] In some implementations, the driver application has a login and logout functionality such that multiple taxi drivers, each having a driver account, can use the same device **304** for processing distributed payment transactions. The functionality allows a driver to login and logout of the payment service system **208**. Association by the payment service system **208** of the device **304** with the appropriate driver account can be done by conventional login techniques.

[0043] The driver side device **304** can read data from the meter **302**, e.g. fare of a trip, while the passenger side device **308** can read card data, i.e., card information such as the card number, or cardholder name, from the card reader **310**. The wireless payment system **301** can communicate with the payment service system **208** over the external network **311**, e.g., the Internet.

[0044] The wireless payment system **301** can also communicate with a computer system **312**, e.g., a dispatch system, of a dispatcher. The computer system **312** can process or store data about taxi rides, as discussed below.

[0045] In the taxi environment, when a driver submits a transaction to the payment service system **208**, the transaction can include sufficient information, e.g., the name or id number of the driver, to associate the driver with the dispatcher. The payment service system **208** can maintain a database associating drivers with dispatchers, and when the payment service system **208** receive this information, it can identify the associated dispatcher from the information. This allows the payment service system **208** to send data about the taxi ride to the computer system **312** of the associated dispatcher.

[0046] For example, if the system **200** is implemented in a taxi, a customer can pay a taxi driver using the wireless payment system **202** after the taxi driver brings the customer to the customer's destination. After conducting the transaction, the system can send data about the taxi ride to a computer system **204**, e.g., the computer system of the dispatcher. The data can include a start location and an end location of the taxi ride, the duration of the trip, the distance of the trip, the date and time of the trip, total cost of the trip (e.g., passenger fare and tip), or which taxi cab performed the service.

[0047] FIG. **4** is a diagram of an example flow chart of a process **400** conducted with the wireless payment system **102** implemented in a taxi environment. For example, a customer can enter a taxi and ask a taxi driver to take the customer to a destination. The taxi driver starts a meter that determines the fare of the trip based at least on the distance and duration of the trip. In some implementations, when the driver starts the meter, the meter generates a signal that is sent to the driver side device indicating that the ride has started.

[0048] Once the taxi driver arrives at the destination, the taxi driver stops the meter, which causes the meter to finalize the fare of the trip. The driver side device then receives the amount of the fare of the trip from the meter (step **402**). The driver side device can send the amount of the fare of the trip to the passenger side device (step **404**). In some implementations, the driver side device sends the amount of the fare to the passenger side device after receiving a signal from the meter (e.g., the driver stops the meter) indicating an end of the trip.

[0049] Once the passenger side device receives the amount of the fare of the trip through the wireless network, the passenger side device can display the amount of the fare of the trip (step **406**) to the customer. The customer can pay by swiping a card through the card reader attached to the passenger side device. The passenger side device can receive card data, e.g., the card number, from the card reader (step **408**). In some implementations, the passenger side device can receive card data from a customer that manually inputs in a card number, e.g., using the touch screen of the passenger side device. After receiving card data, the passenger side device can optionally display a request for a signature and receive a signature approving the transaction (step **410**). The passenger side device can display a request to enter a tip amount, and can receive passenger input selecting a tip amount. The passenger side device can calculate a total transaction amount (the fare plus the tip) and display the total transaction amount. The passenger side device can also receive contact information for a receipt (step **412**). The passenger side device can receive this information through customer input into the passenger side device, e.g., through a graphical user interface on the touch screen display.

[0050] In some implementations, the passenger side device initiates the request for authorization of the transaction. In this case, the passenger side device sends the payment information, which includes at least the transaction amount and the card data (e.g., the card number), but may also include the signature and contact information, directly to the payment service system, e.g., using an Internet connection.

[0051] In some implementations, the driver side device initiates the request for authorization of the transaction. In this case, the passenger side device sends the payment information, including at least the card data received from the card reader, to the driver side device (step **414**). The signature, tip amount or total transaction amount, and contact information can also be sent to the driver side device. The driver side device can then send the payment information to the payment service system (step **416**/**806**), e.g., using an Internet connection.

[0052] In some implementations, neither the driver side device nor the passenger side device has access to an external network connection, e.g., an Internet connection. That is, because the mobile device cannot connect to the payment service system using an Internet connection, the request for authorization cannot be initiated at the end of the trip, e.g., when the customer is about to pay using a credit card and leave the taxi. Instead, the mobile device can store the transaction and process the transaction later. Processing the transaction later can be accomplished by forwarding the transaction to the payment service system when the mobile device reestablishes an Internet connection.

[0053] In order to encourage merchants that are likely to enter areas without an external network connection, e.g., taxis, to use the payment system **200**, the payment service may decide to cover some transactions (i.e., pay the merchant) even if the transactions are not approved.

[0054] FIG. **5** is a diagram of an example flow chart **500** of storing a payment transaction. The mobile device, e.g., a

merchant device, e.g., the merchant-facing device, determines there is no connection to an external network, e.g., the Internet (step **502**). The mobile device can test whether a connection can be made to a resource, e.g., a web page, located on the external network. There may be no cellular Internet connection in areas with poor cellular data reception or with too many cellular data connections concentrated in one area.

[0055] The mobile device receives data indicating a payment transaction (step **503**). For example, a merchant facing device can receive, over a WiFi network, the data from a customer facing device, which receives data from a user swiping a card at a card reader attached to the mobile device. The data can include payment information, a signature, a tip amount, or a total transaction amount as described above in reference to FIG. **4**.

[0056] The mobile device can execute a risk heuristic model to determine whether the payment service covers a transaction (step **504**). The risk heuristic model can use a number of already stored transactions, a value of the proposed stored transaction, and/or a total value for all stored transactions in evaluating the risk and determining whether the payment service will cover the transaction. For example, the risk heuristic model can compare a number of already stored transactions, a value of the proposed stored transaction, and/or a total value for all stored transactions to, respectively, a maximum number of stored transactions, a maximum individual value for an individual stored transaction, and a maximum total value for all stored transactions. Where the number or value exceeds the maximum, the mobile device can determine that the payment service will not cover the transaction. These numbers, values, and their respective maximums can be stored on a mobile device, e.g., in an internal database.

[0057] The risk heuristic model can also use risk factors associated with a cardholder of the mobile device. For example, the risk factors can include prior transactions or analysis of the prior transactions. In some implementations, when there is a connection, e.g., prior to a store and forward transaction, the payment service system sends the risk factors to the mobile device, e.g., whenever the payment service system determines new or updated risk factors. Therefore, the mobile device can update its risk heuristic model to consider the risk factors.

[0058] The risk heuristic model can be dynamically modified by the payment service system. For example, the maximum number of stored transactions or the maximum value of a payment transaction can be modified through a communication, e.g., in the background when there is an Internet connection, with the payment service system. Some risk factors can also be updated to weigh more than others.

[0059] The mobile device can determine whether the payment service system will guarantee payment to the merchant based on the risk heuristic model (step **506**). If payment will be guaranteed, the mobile device stores the transaction for future processing (step **508**). If the payment will not be guaranteed, e.g., the risk heuristic model deems the transaction as too risky, the mobile device prompts the merchant for an approval to proceed (step **510**). That is, the mobile device indicates to the merchant, e.g., using a user interface of the device, that the transaction will not be covered if the transaction is denied upon future processing. Thus, the merchant will be taking a risk of non-payment if the transaction is denied upon future processing. If the merchant approves, the mobile device stores the transaction (step **508**). If the merchant does not approve, the mobile device rejects the transaction (step **512**). Steps **506**-**512** will be described further below in reference to FIG. **6**.

[0060] FIG. **6** is a diagram of an example flow chart **600** of storing a payment transaction using an example risk heuristic model. The example risk heuristic model considers a number of already stored transactions, a value of a proposed transaction, and a total value of previously stored transactions and does not consider risk factors. In some other implementations, a different combination or subcombination of the above considerations, e.g., including or excluding the risk factors, are used for the risk heuristic model.

[0061] The mobile device can determine there is no connection to an external network and receive data indicating a payment transaction (steps **602**/**604**), as described above in reference to FIG. **5**.

[0062] The mobile device determines whether a number of already stored transactions surpass a maximum number of stored transactions (step **606**). The maximum number of stored transactions can be established to limit the number of times a mobile device can store a transaction for future processing. If the number of stored transactions surpasses the maximum number, the mobile device prompts the merchant for approval (step **614**), which will be described further below. In some implementations, determining whether the number of stored transactions surpasses the maximum number is an optional step.

[0063] If the number of stored transactions does not surpass the maximum number, the mobile device determines whether the value of the proposed payment transaction surpasses the maximum value for the individual stored transaction and/or whether the total value of the proposed payment transaction plus the value of the already stored transactions exceeds the maximum total value for all stored transactions (step **610**). The value of the payment transaction can be obtained from the data indicating the payment transaction. If the value of the proposed payment transaction surpasses the maximum individual value, or if the total value of the proposed payment transaction plus the value of the already stored transactions exceeds the maximum total value, the mobile device displays a message that the merchant will be taking the risk of non-payment if the transaction is not approved, and request merchant approval before proceeding (step **614**). The merchant can approve or deny the request, e.g., through a user interface of the mobile device. If the merchant approves the request, the mobile device stores the transaction for future processing (step **612**), e.g., in an internal database. An indication that the transaction was one which exceeded a maximum can be stored in the internal database.

[0064] In some implementations, the mobile device encrypts the transaction, e.g., using a key or a signature on the mobile device, before storing the transaction. The key can be obtained from the payment service system. The key can also be short lived and discarded after a single use. For example, after the mobile device uploads a collection of stored transactions, the payment service system can provide the mobile device with a new key. If the merchant denies the request, the mobile device rejects the transaction (step **608**). A notification of the rejection of the transaction can be sent to a user interface of the mobile device.

[0065] In some implementations, when the mobile device stores the transaction, the mobile device includes storing a time or user session data of the transaction. The time or user session data can identify the merchant associated with the

transaction. For example, in a taxi environment, if a first taxi driver changes shifts with a second taxi driver, comparing a time of a stored transaction with a time of the shift change can indicate which taxi driver should be associated with the stored transaction. Similarly, the second taxi driver can sign in using a respective personal account on the mobile device. This starts a new user session between the mobile device and the second taxi driver. As a result, subsequent stored transactions will be associated with the second driver.

[0066] Once the mobile device stores the transaction, the mobile device can increment the number of stored transactions, e.g., in an internal database. In some implementations, the number of stored transactions is reset after all stored transactions are forwarded to a payment service system. In alternative implementations, the number of stored transactions is decreased when one or more stored transactions are forwarded.

[0067] FIG. **7** is a diagram of an example flow chart **700** of forwarding a payment transaction. The mobile device, e.g., a merchant device, can periodically determine whether the mobile device can access an external network, e.g., the Internet. This determination can occur during, before, or after a transaction. For example, the mobile device can ping a resource every few minutes or through an exponential backoff algorithm. If the mobile device eventually determines it can access the Internet (step **702**), the mobile device determines whether there are stored transactions on the mobile device (step **704**). If there are stored transactions that have not yet been forwarded, the mobile device forwards each transaction to a payment service system for processing (step **706**), e.g., using the reestablished Internet connection. In some implementations, the stored transactions are batched and sent to the payment service system for processing. Processing forwarded transactions by a payment service system can occur as described below above in reference to FIGS. **8**A-B. Once the forwarded transactions are processed, the mobile device can receive a response for each transaction (step **708**). The responses can be acceptances or rejections of the respective transactions. The responses can also include receipts for each respective transaction.

[0068] FIG. **8** is a diagram of an example flow chart of a process **800** conducted by a payment service system **208** after receiving a distributed payment transaction from the wireless payment system **102**. The payment service system **208** can receive the distributed payment transaction, e.g., a stored transaction, from the wireless payment system (step **802**). The distributed payment transaction can include card data, a signature, and other payment information (e.g., payment amount) provided by the customer.

[0069] The payment service system **208** then processes the distributed payment transaction (step **804**) by sending a record to the computer system of the card payment network **216**, e.g., Visa or MasterCard, and the card payment network **216** then sends the record to the card issuer, e.g., the bank, as described above in FIG. **1**.

[0070] If the transaction is approved and the payment service system **208** receives approval from the card payment network **216**, the payment service system **208** communicates this to whichever device (driver side or passenger side) that initiated the request for authorization (step **806**). For example, in the case of a stored transaction, the approval can be displayed on the driver side device. The driver side and/or passenger side device then captures the transaction. In the capture stage, the approved transaction is again routed from the capturing device to the card processor, card network and card issuer. The record of the transaction in the capture stage can include the cardholder's signature (if appropriate), or other information. The capture state can trigger the financial transaction between the card issuer and the merchant. On receipt of an indication from the card network that the transaction has been captured, the payment service system **208** optionally creates receipts to send to the customer, e.g., through the customer application and/or through the previously provided contact email, and to the merchant (step **808**). For example, if the wireless payment system **202** is implemented in a taxi environment, before signing for the transaction, the customer can input an email address to which the payment service system can send the receipt. Both devices can then display the receipt in each of their applications.

[0071] If the transaction is not approved because it would exceed the credit limit or there are insufficient funds in the customer's financial account, the payment service system **208** notifies the application on whichever device (driver side or passenger side) that initiated the request for authorization. For example, in the case of a stored transaction, a notification can be displayed on the driver side device.

[0072] As noted above, the payment service may decide to cover some transactions (i.e., pay the merchant) even if the transactions are not approved. In particular, the payment service may determine whether the stored transaction is for an amount less than the maximum individual amount, and/or whether the total amount of all the stored transactions is less than the maximum total amount. If it is, the payment service can pay the merchant for the amount of the stored transaction. However, if the transaction is not approved and the transaction exceeds the individual or total amount, then the payment service system **208** notifies the merchant that the transaction was not approved and that the payment service is not covering the transaction. The message can be sent to whichever device (driver side or passenger side) that initiated the request for authorization.

[0073] Embodiments of the subject matter and the operations described in this specification can be implemented in digital electronic circuitry, or in computer software, firmware, or hardware, including the structures disclosed in this specification and their structural equivalents, or in combinations of one or more of them. Embodiments of the subject matter described in this specification can be implemented as one or more computer programs, i.e., one or more modules of computer program instructions, encoded on a non-transitory computer storage medium for execution by, or to control the operation of, data processing apparatus. Alternatively or in addition, the program instructions can be encoded on an artificially-generated propagated signal, e.g., a machine-generated electrical, optical, or electromagnetic signal, that is generated to encode information for transmission to suitable receiver apparatus for execution by a data processing apparatus. A computer storage medium can be, or be included in, a computer-readable storage device, a computer-readable storage substrate, a random or serial access memory array or device, or a combination of one or more of them. Moreover, while a computer storage medium is not a propagated signal, a computer storage medium can be a source or destination of computer program instructions encoded in an artificially-generated propagated signal. The computer storage medium can also be, or be included in, one or more separate physical components or media (e.g., multiple CDs, disks, or other storage devices).

[0074] The operations described in this specification can be implemented as operations performed by a data processing apparatus on data stored on one or more computer-readable storage devices or received from other sources.

[0075] The term "data processing apparatus" encompasses all kinds of apparatus, devices, and machines for processing data, including by way of example a programmable processor, a computer, a system on a chip, or multiple ones, or combinations, of the foregoing The apparatus can include special purpose logic circuitry, e.g., an FPGA (field programmable gate array) or an ASIC (application-specific integrated circuit). The apparatus can also include, in addition to hardware, code that creates an execution environment for the computer program in question, e.g., code that constitutes processor firmware, a protocol stack, a database management system, an operating system, a cross-platform runtime environment, a virtual machine, or a combination of one or more of them. The apparatus and execution environment can realize various different computing model infrastructures, such as web services, distributed computing and grid computing infrastructures.

[0076] A computer program (also known as a program, software, software application, script, or code) can be written in any form of programming language, including compiled or interpreted languages, declarative or procedural languages, and it can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, object, or other unit suitable for use in a computing environment. A computer program may, but need not, correspond to a file in a file system. A program can be stored in a portion of a file that holds other programs or data (e.g., one or more scripts stored in a markup language resource), in a single file dedicated to the program in question, or in multiple coordinated files (e.g., files that store one or more modules, sub-programs, or portions of code). A computer program can be deployed to be executed on one computer or on multiple computers that are located at one site or distributed across multiple sites and interconnected by a communication network.

[0077] The processes and logic flows described in this specification can be performed by one or more programmable processors executing one or more computer programs to perform actions by operating on input data and generating output. The processes and logic flows can also be performed by, and apparatus can also be implemented as, special purpose logic circuitry, e.g., an FPGA (field programmable gate array) or an ASIC (application-specific integrated circuit).

[0078] Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any kind of digital computer. Generally, a processor will receive instructions and data from a read-only memory or a random access memory or both. The essential elements of a computer are a processor for performing actions in accordance with instructions and one or more memory devices for storing instructions and data. Generally, a computer will also include, or be operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data, e.g., magnetic, magneto-optical disks, or optical disks. However, a computer need not have such devices. Moreover, a computer can be embedded in another device, e.g., a mobile telephone, a personal digital assistant (PDA), a mobile audio or video player, a game console, a Global Positioning System (GPS) receiver, or a portable storage device (e.g., a universal serial bus (USB) flash drive), to name just a few. Devices suitable for storing computer program instructions and data include all forms of non-volatile memory, media and memory devices, including by way of example semiconductor memory devices, e.g., EPROM, EEPROM, and flash memory devices; magnetic disks, e.g., internal hard disks or removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks. The processor and the memory can be supplemented by, or incorporated in, special purpose logic circuitry.

[0079] To provide for interaction with a user, embodiments of the subject matter described in this specification can be implemented on a computer having a display device, e.g., a CRT (cathode ray tube) or LCD (liquid crystal display) monitor, for displaying information to the user and a keyboard and a pointing device, e.g., a mouse or a trackball, by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback, e.g., visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, or tactile input. In addition, a computer can interact with a user by sending resources to and receiving resources from a device that is used by the user; for example, by sending web pages to a web browser on a user's client device in response to requests received from the web browser.

[0080] Embodiments of the subject matter described in this specification can be implemented in a computing system that includes a back-end component, e.g., as a data server, or that includes a middleware component, e.g., an application server, or that includes a front-end component, e.g., a client computer having a graphical user interface or a Web browser through which a user can interact with an implementation of the subject matter described in this specification, or any combination of one or more such back-end, middleware, or front-end components.

[0081] The computing system can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other. In some embodiments, a server transmits data (e.g., an HTML page) to a client device (e.g., for purposes of displaying data to and receiving user input from a user interacting with the client device). Data generated at the client device (e.g., a result of the user interaction) can be received from the client device at the server.

[0082] A system of one or more computers can be configured to perform particular operations or actions by virtue of having software, firmware, hardware, or a combination of them installed on the system that in operation causes or cause the system to perform the actions. One or more computer programs can be configured to perform particular operations or actions by virtue of including instructions that, when executed by data processing apparatus, cause the apparatus to perform the actions.

[0083] While this specification contains many specific implementation details, these should not be construed as limitations on the scope of any inventions or of what may be claimed, but rather as descriptions of features specific to particular embodiments of particular inventions. Certain features that are described in this specification in the context of separate embodiments can also be implemented in combination in a single embodiment. Conversely, various features that

are described in the context of a single embodiment can also be implemented in multiple embodiments separately or in any suitable subcombination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a subcombination or variation of a subcombination.

[0084] Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Moreover, the separation of various system components in the embodiments described above should not be understood as requiring such separation in all embodiments, and it should be understood that the described program components and systems can generally be integrated together in a single software product or packaged into multiple software products.

[0085] In some cases, the actions recited in the claims can be performed in a different order and still achieve desirable results. In addition, the processes depicted in the accompanying figures do not necessarily require the particular order shown, or sequential order, to achieve desirable results. In certain implementations, multitasking and parallel processing may be advantageous.

[0086] Thus, particular embodiments of the subject matter have been described. Other embodiments are within the scope of the following claims. For example, usage of wireless payment system may not be limited to a taxi environment but could also be applied to other environments, such as a restaurant. Moreover, usage of the techniques to establish secure communication may not be limited to mobile devices, but could also be applied to non-mobile or wired devices connected to a network. Although the swiping of a card through a reader is described above, other techniques for scanning a card, e.g., chip reading or near field communication, could be used to read data from the card.

[0087] Although FIGS. **1** and **2** illustrate a system **200** in which customer-facing and merchant-facing functions are distributed between a first device **102** and a second device **106**, the techniques for storing and forwarding transactions are applicable if there is only a single device. In this case the same device provides the customer-facing functions, e.g., displaying a request for the credit card swipe and receiving the card information from the card reader, and the merchant-facing functions, e.g., entering the transaction and calculating a total amount for the transaction.

1. A method of processing a payment transaction using a mobile device of a merchant, comprising:

determining the mobile device does not have a connection to an external network;

receiving data indicating a payment transaction between a customer and the merchant;

determining whether the payment transaction should be stored, where the determining is based on a risk heuristic model that considers one or more of the following: a number of already stored transactions, a value of the payment transaction, a total value, where the total value is a sum of the value of the payment transaction and values of one or more already stored transactions, and risk factors associated with the customer; and

based at least on the determination, storing the payment transaction on the mobile device for future processing.

2. The method of claim **1**, further comprising:

after storing the payment transaction, determining the mobile device has a connection to the external network;

determining the mobile device has stored payment transactions;

forwarding each of the stored payment transactions to a payment service system; and

receiving a response for each of the stored payment transactions from the payment service system.

3. The method of claim **2**, where each response is an acceptance or a rejection of the respective stored payment transaction.

4. The method of claim **1**, where the risk heuristic model comprises:

determining whether a value of the payment transaction or a total value surpasses a maximum value, where the total value is a sum of the value of the payment transaction and values of one or more already stored transactions; and

determining whether a number of stored transactions stored on the mobile device surpasses a maximum number.

5. The method of claim **4**, where if the number of stored transactions does not surpass the maximum number and the value of the payment transaction or the total value do not surpass the maximum value, storing the payment transaction on the mobile device.

6. The method of claim **4**, where if the number of stored transactions surpasses the maximum number, rejecting the payment transaction.

7. The method of claim **4**, where if the number of stored transactions does not surpass the maximum number and the value of the payment transaction or the total value surpass the maximum value, further comprising:

sending a request to proceed to a user interface of the mobile device;

receiving input through the user interface;

storing the payment transaction if the input includes an approval of the request to proceed; and

rejecting the payment transaction if the input includes a denial of the request to proceed.

8. The method of claim **1**, where the payment transaction is encrypted using a key before the storing, where the key is obtained from a payment service system.

9. The method of claim **1**, where storing the payment transaction includes storing a time or user session data of the transaction.

10. The method of claim **1**, further comprising determining whether the mobile device has a connection to the external network after an interval of time.

11. The method of claim **1**, where the external network is an Internet network.

12. The method of claim **1**, where the already stored transactions are obtained from an internal database.

13. The method of claim **1**, where the risk factors include prior transactions or analysis of the prior transactions.

14. The method of claim **1**, where the risk factors are updated by a payment service system when the mobile device has a connection to the external network.

15. The method of claim **1**, where the risk heuristic model is updated by a payment service system when the mobile device has a connection to the external network.

16. A computer program product, tangibly embodied in a machine readable storage media, comprising instructions for causing a processor to perform operations comprising:

determining the mobile device does not have a connection to an external network;

receiving data indicating a payment transaction between a customer and the merchant;

determining whether the payment transaction should be stored, where the determining is based on a risk heuristic model that considers one or more of the following: a number of already stored transactions, a value of the payment transaction, a total value, where the total value is a sum of the value of the payment transaction and values of one or more already stored transactions, and risk factors associated with the customer; and

based at least on the determination, storing the payment transaction on the mobile device for future processing.

17. The computer program product of claim **16**, further comprising:

after storing the payment transaction, determining the mobile device has a connection to the external network;

determining the mobile device has stored payment transactions;

forwarding each of the stored payment transactions to a payment service system; and

receiving a response for each of the stored payment transactions from the payment service system.

18. The computer program product of claim **17**, where each response is an acceptance or a rejection of the respective stored payment transaction.

19. The computer program product of claim **16**, where the risk heuristic model comprises:

determining whether a value of the payment transaction or a total value surpasses a maximum value, where the total value is a sum of the value of the payment transaction and values of one or more already stored transactions; and

determining whether a number of stored transactions stored on the mobile device surpasses a maximum number.

20. The computer program product of claim **19**, where if the number of stored transactions does not surpass the maximum number and the value of the payment transaction or the total value do not surpass the maximum value, storing the payment transaction on the mobile device.

21. The computer program product of claim **19**, where if the number of stored transactions surpasses the maximum number, rejecting the payment transaction.

22. The computer program product of claim **19**, where if the number of stored transactions does not surpass the maximum number and the value of the payment transaction or the total value surpass the maximum value, further comprising:

sending a request to proceed to a user interface of the mobile device;

receiving input through the user interface;

storing the payment transaction if the input includes an approval of the request to proceed; and

rejecting the payment transaction if the input includes a denial of the request to proceed.

23. The computer program product of claim **16**, where the payment transaction is encrypted using a key before the storing, where the key is obtained from a payment service system.

24. The computer program product of claim **16**, where storing the payment transaction includes storing a time or user session data of the transaction.

25. The computer program product of claim **16**, further comprising determining whether the mobile device has a connection to the external network after an interval of time.

26. The computer program product of claim **16**, where the external network is an Internet network.

27. The computer program product of claim **16**, where the already stored transactions are obtained from an internal database.

28. The computer program product of claim **16**, where the risk factors include prior transactions or analysis of the prior transactions.

29. The computer program product of claim **16**, where the risk factors are updated by a payment service system when the mobile device has a connection to the external network.

30. The computer program product of claim **16**, where the risk heuristic model is updated by a payment service system when the mobile device has a connection to the external network.

31. A system comprising:

a processor; and

computer-readable medium coupled to the processor and having instructions stored thereon, which, when executed by the processor, cause the processor to perform operations comprising:

determining the mobile device does not have a connection to an external network;

receiving data indicating a payment transaction between a customer and the merchant;

determining whether the payment transaction should be stored, where the determining is based on a risk heuristic model that considers one or more of the following: a number of already stored transactions, a value of the payment transaction, a total value, where the total value is a sum of the value of the payment transaction and values of one or more already stored transactions, and risk factors associated with the customer; and

based at least on the determination, storing the payment transaction on the mobile device for future processing.

32. The system of claim **31**, further comprising:

after storing the payment transaction, determining the mobile device has a connection to the external network;

determining the mobile device has stored payment transactions;

forwarding each of the stored payment transactions to a payment service system; and

receiving a response for each of the stored payment transactions from the payment service system.

33. The system of claim **32**, where each response is an acceptance or a rejection of the respective stored payment transaction.

34. The system of claim **31**, where the risk heuristic model comprises:

determining whether a value of the payment transaction or a total value surpasses a maximum value, where the total value is a sum of the value of the payment transaction and values of one or more already stored transactions; and

determining whether a number of stored transactions stored on the mobile device surpasses a maximum number.

35. The system of claim **34**, where if the number of stored transactions does not surpass the maximum number and the value of the payment transaction or the total value do not surpass the maximum value, storing the payment transaction on the mobile device.

36. The system of claim **34**, where if the number of stored transactions surpasses the maximum number, rejecting the payment transaction.

37. The system of claim **34**, where if the number of stored transactions does not surpass the maximum number and the value of the payment transaction or the total value surpass the maximum value, further comprising:

sending a request to proceed to a user interface of the mobile device;

receiving input through the user interface;

storing the payment transaction if the input includes an approval of the request to proceed; and

rejecting the payment transaction if the input includes a denial of the request to proceed.

38. The system of claim **31**, where the payment transaction is encrypted using a key before the storing, where the key is obtained from a payment service system.

39. The system of claim **31**, where storing the payment transaction includes storing a time or user session data of the transaction.

40. The system of claim **31**, further comprising determining whether the mobile device has a connection to the external network after an interval of time.

41. The system of claim **31**, where the external network is an Internet network.

42. The system of claim **31**, where the already stored transactions are obtained from an internal database.

43. The system of claim **31**, where the risk factors include prior transactions or analysis of the prior transactions.

44. The system of claim **31**, where the risk factors are updated by a payment service system when the mobile device has a connection to the external network.

45. The system of claim **31**, where the risk heuristic model is updated by a payment service system when the mobile device has a connection to the external network.

* * * * *