US 20150339656A1

(19) **United States**

(12) **Patent Application Publication**

Wilson et al.

(10) **Pub. No.: US 2015/0339656 A1**

(43) **Pub. Date: Nov. 26, 2015**

(54) **VERIFIED PURCHASING BY PUSH NOTIFICATION**

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

(72) Inventors: **Jesse Wilson**, Waterloo (CA); **Brian Grassadonia**, San Francisco, CA (US); **Matthew Rhodes**, San Francisco, CA (US)

(21) Appl. No.: **14/283,504**

(22) Filed: **May 21, 2014**

Publication Classification

(51) **Int. Cl.**

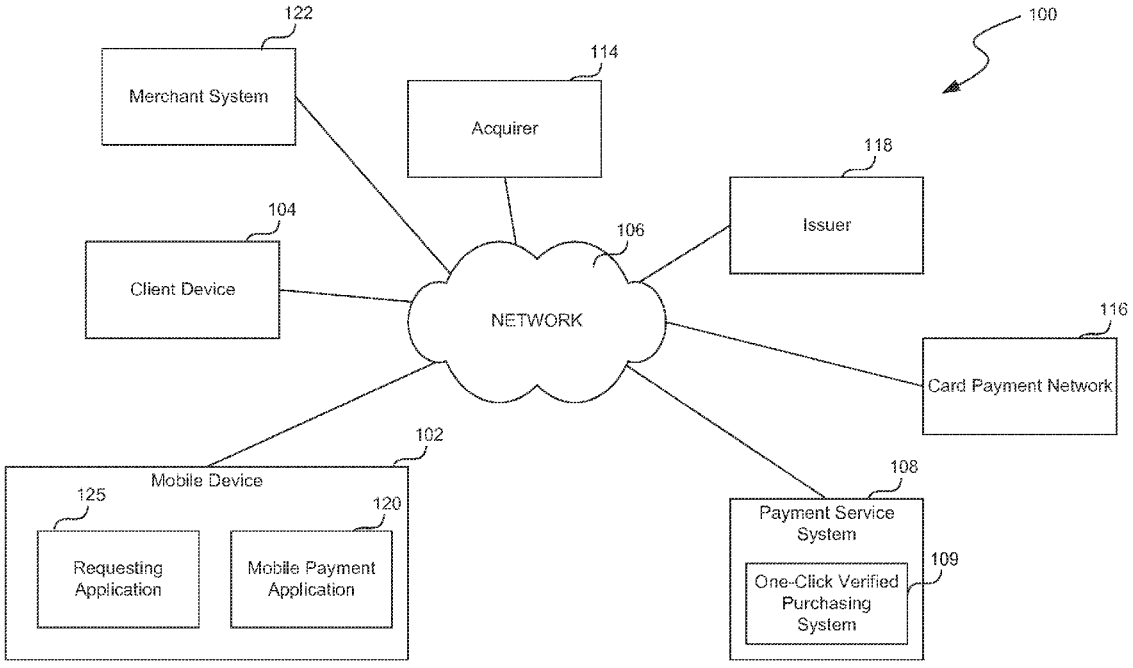
G06Q 20/32	(2006.01)
H04L 29/08	(2006.01)
G06Q 20/40	(2006.01)

(52) **U.S. Cl.**

CPC ***G06Q 20/3226*** (2013.01); ***G06Q 20/40*** (2013.01); ***H04L 67/26*** (2013.01); ***G06Q 20/4016*** (2013.01)

(57) **ABSTRACT**

Disclosed are a system and a method for purchasing items from a merchant system using a single verification action. A user initiates a purchase transaction from a user interface of the merchant system by submitting a communication identifier in lieu of payment information or login credentials. The merchant system then generates a payment request including the communication identifier and sends the request to a payment service system. The payment service system uses the communication identifier to identify a verification device and send a push notification to the verification device to request the user to confirm or cancel the purchase transaction. Upon receiving confirmation from the user, the payment service system initiates a transfer of a payment amount associated with the purchase transaction from a financial account associated communication identifier to a financial account associated with the merchant system to pay for the purchase transaction.



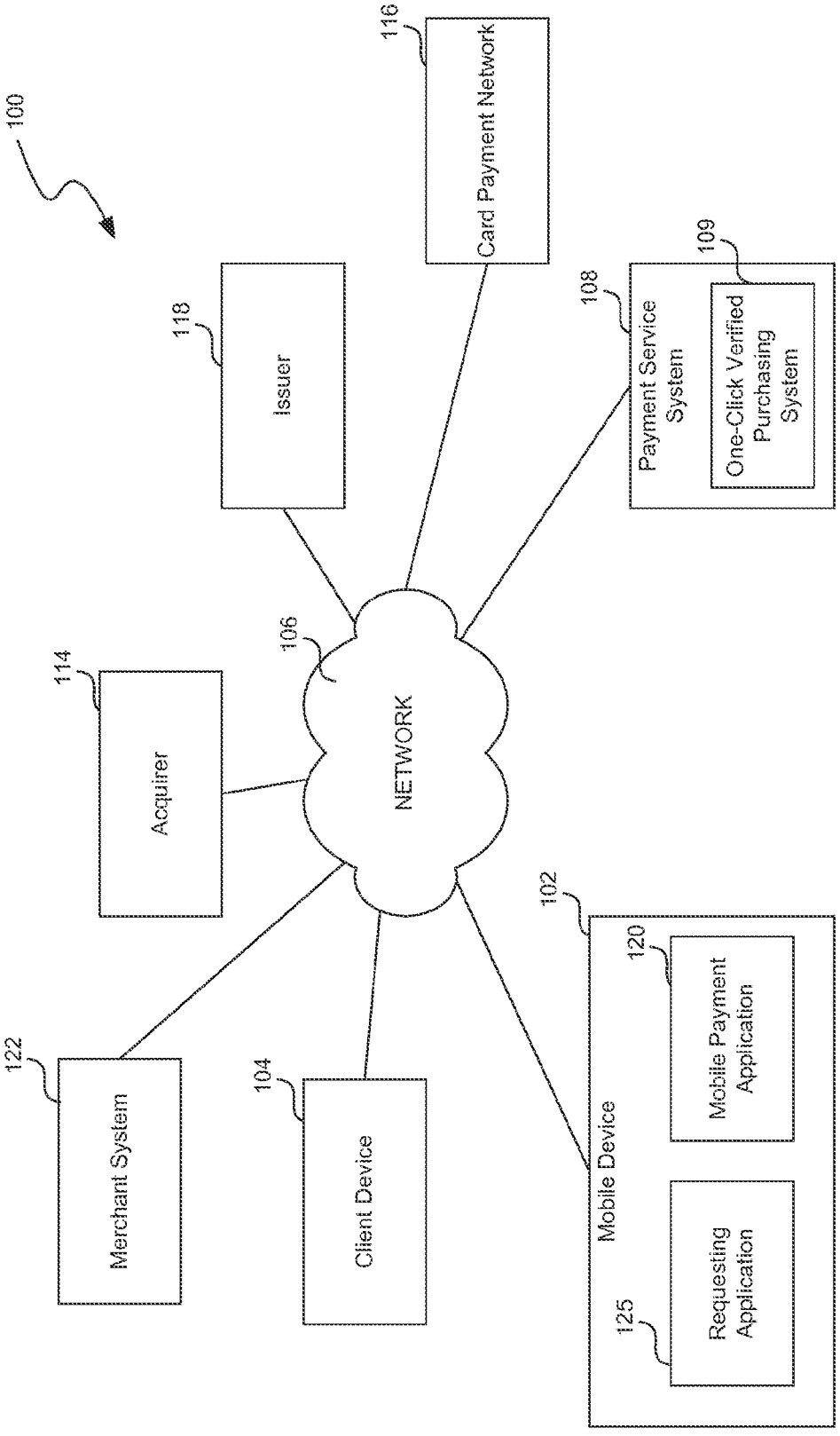

100
116
Card Payment Network
118
Issuer
108
Payment Service System
109
One-Click Verified Purchasing System
106
NETWORK
114
Acquirer
102
Mobile Device
120
Mobile Payment Application
125
Requesting Application
104
Client Device
122
Merchant System

FIG. 1

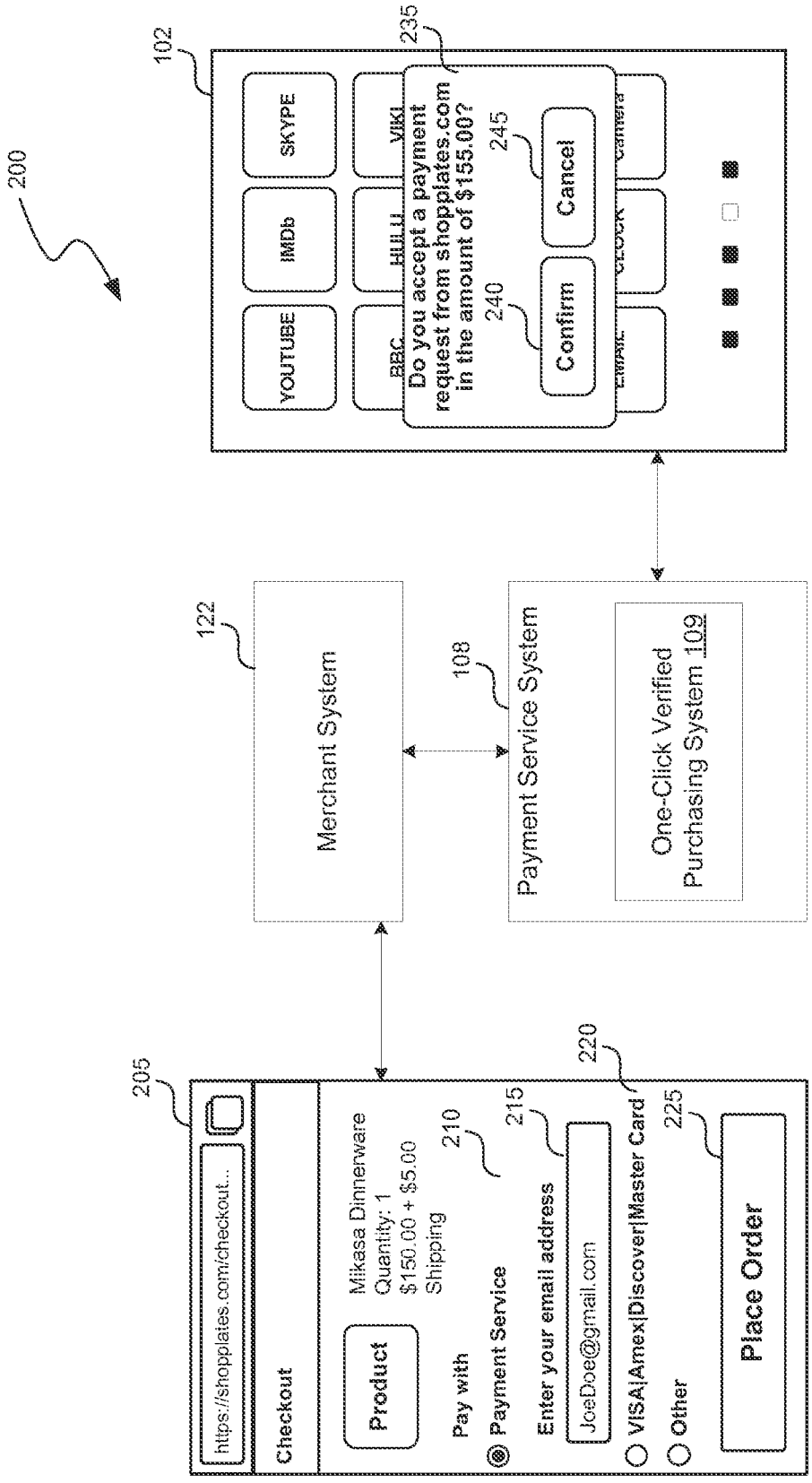

200
102
235
YOUTUBE
IMDb
SKYPE
BBC
HULU
VIKI
Do you accept a payment request from shopplates.com in the amount of $155.00?
240
245
Confirm
Cancel
122
Merchant System
108
Payment Service System
One-Click Verified Purchasing System 109
205
https://shopplates.com/checkout...
Checkout
Product
Mikasa Dinnerware
Quantity: 1
$150.00 + $5.00 Shipping
210
Pay with
Payment Service
215
Enter your email address
JoeDoe@gmail.com
220
VISA|Amex|Discover|Master Card
Other
225
Place Order

FIG. 2

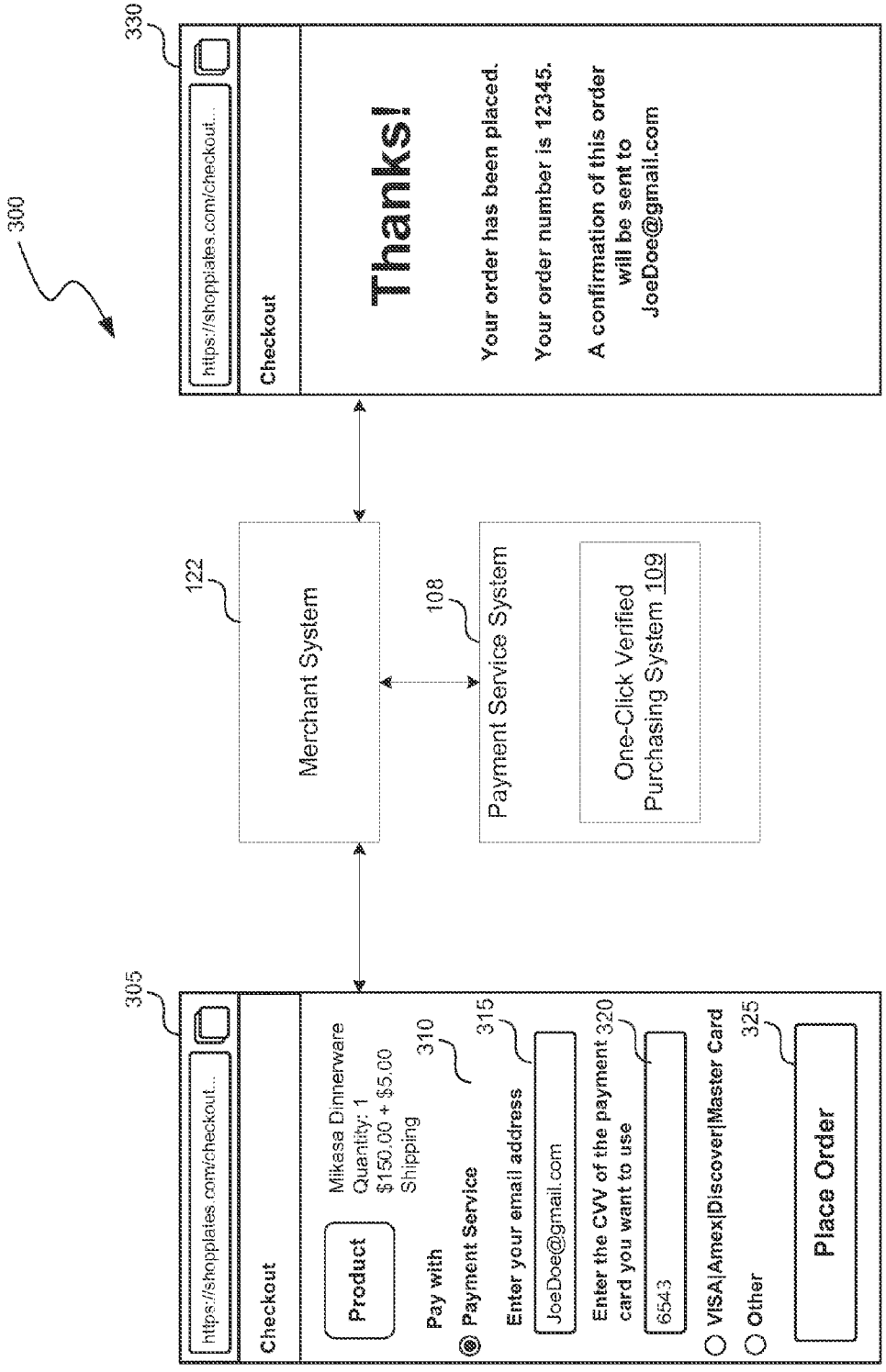

300
330
https://shopplates.com/checkout...
Checkout
Thanks!
Your order has been placed.
Your order number is 12345.
A confirmation of this order will be sent to JoeDoe@gmail.com
122
Merchant System
108
Payment Service System
One-Click Verified Purchasing System 109
305
https://shopplates.com/checkout...
Checkout
Product
Mikasa Dinnerware
Quantity: 1
$150.00 + $5.00 Shipping
310
Pay with
Payment Service
315
Enter your email address
JoeDoe@gmail.com
Enter the CVV of the payment card you want to use 320
6543
VISA|Amex|Discover|Master Card
Other
325
Place Order

FIG. 3

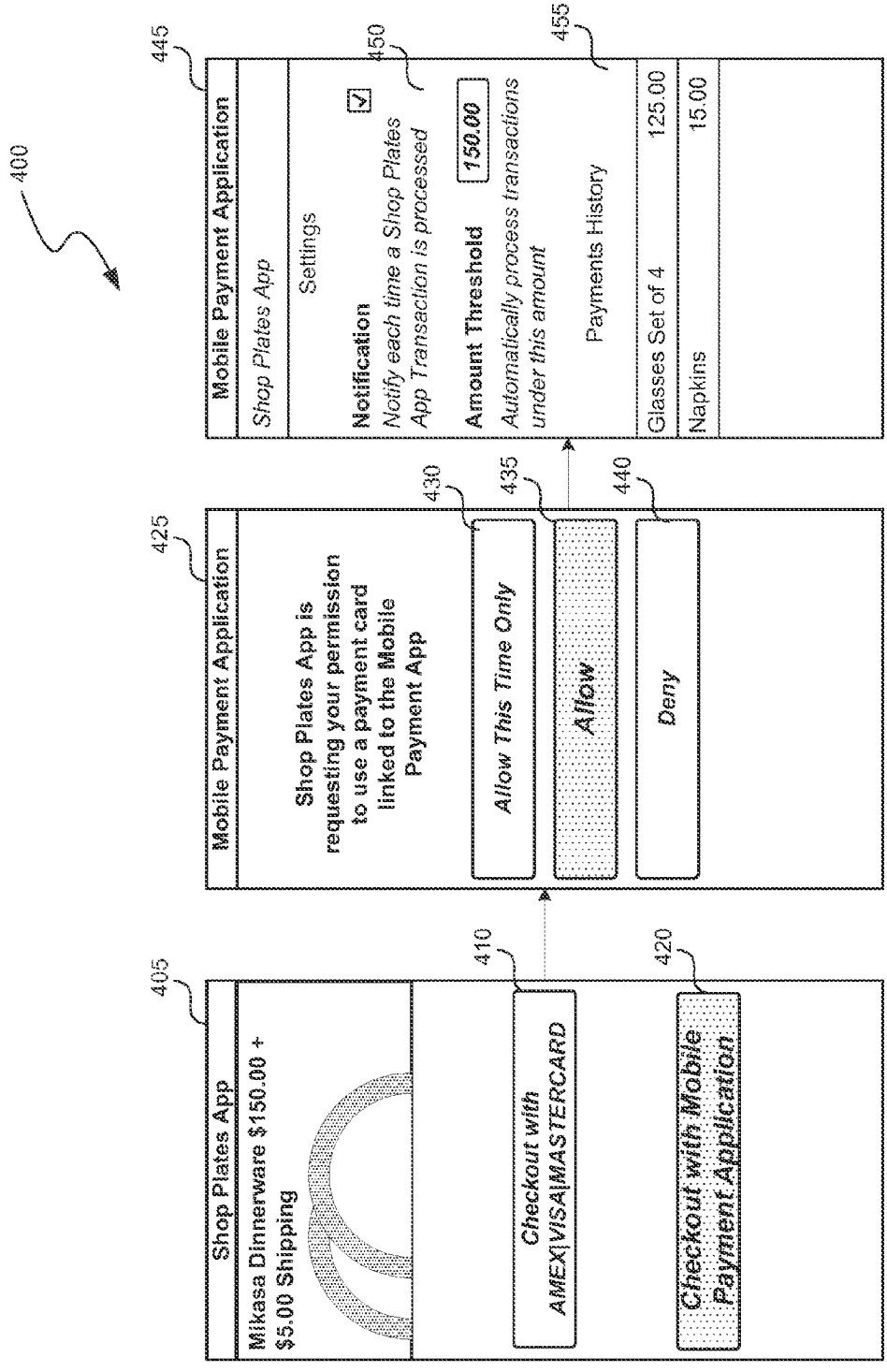

400
405
Shop Plates App
Mikasa Dinnerware $150.00 +
$5.00 Shipping
410
Checkout with
AMEX|VISA|MASTERCARD
420
Checkout with Mobile
Payment Application
425
Mobile Payment Application
Shop Plates App is
requesting your permission
to use a payment card
linked to the Mobile
Payment App
430
Allow This Time Only
435
Allow
440
Deny
445
Mobile Payment Application
Shop Plates App
Settings
450
Notification
Notify each time a Shop Plates
App Transaction is processed
Amount Threshold
150.00
Automatically process transactions
under this amount
455
Payments History
Glasses Set of 4
125.00
Napkins
15.00

FIG. 4

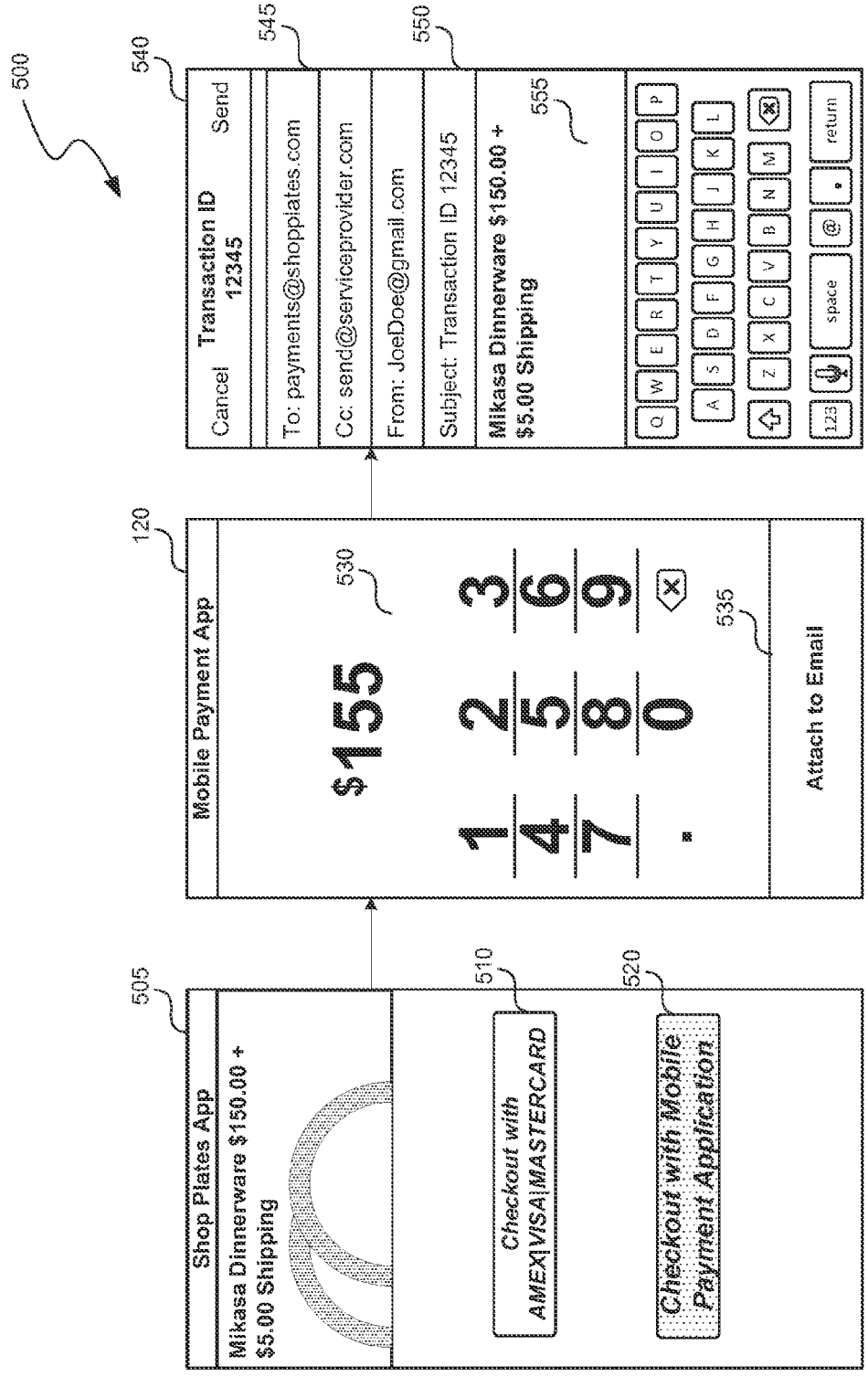

500
505
Shop Plates App
Mikasa Dinnerware $150.00 + $5.00 Shipping
510
Checkout with AMEX|VISA|MASTERCARD
520
Checkout with Mobile Payment Application
120
Mobile Payment App
$155
530
1 2 3
4 5 6
7 8 9
. 0
535
Attach to Email
540
Cancel
Transaction ID 12345
Send
545
To: payments@shopplates.com
Cc: send@serviceprovider.com
From: JoeDoe@gmail.com
550
Subject: Transaction ID 12345
Mikasa Dinnerware $150.00 + $5.00 Shipping
555
space
return

FIG. 5

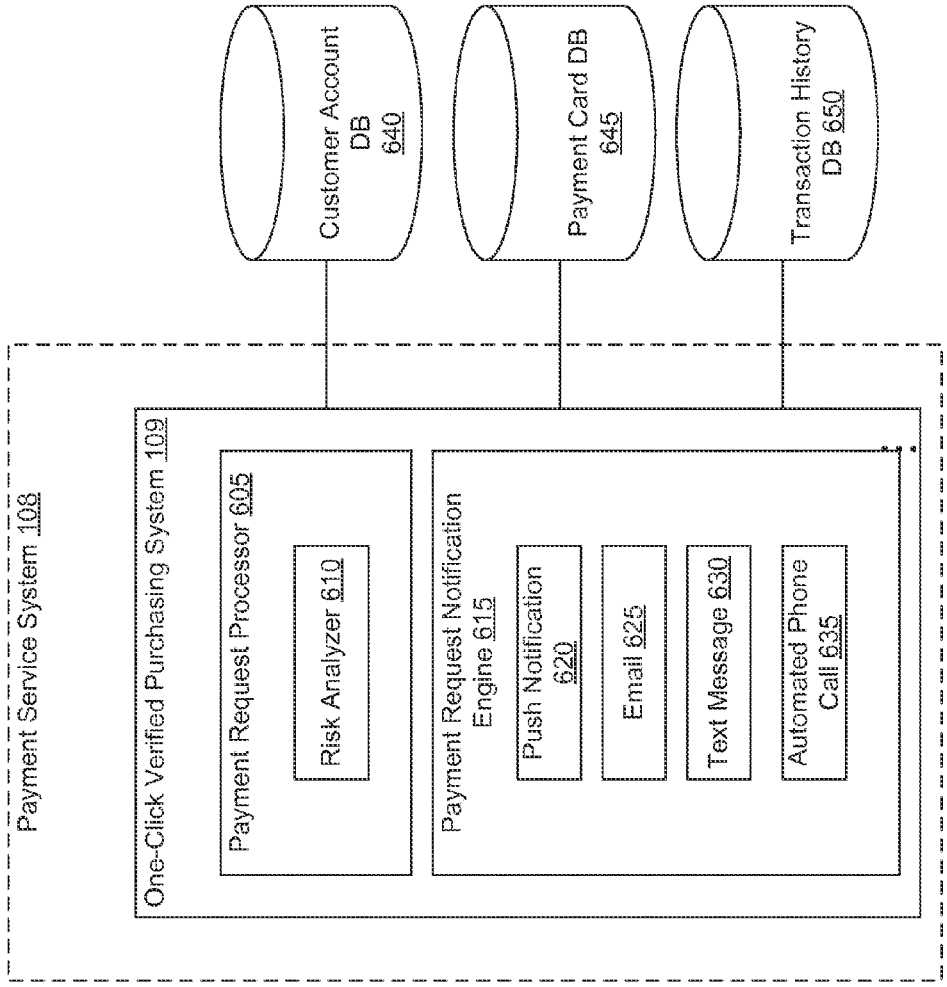

Payment Service System 108
One-Click Verified Purchasing System 109
Payment Request Processor 605
Risk Analyzer 610
Payment Request Notification Engine 615
Push Notification 620
Email 625
Text Message 630
Automated Phone Call 635
Customer Account DB 640
Payment Card DB 645
Transaction History DB 650

FIG. 6A

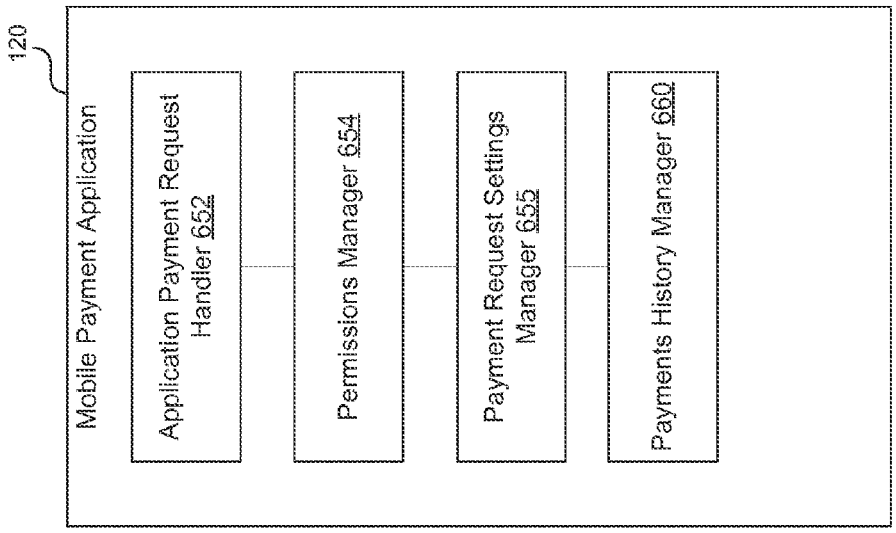

120
Mobile Payment Application
Application Payment Request Handler 652
Permissions Manager 654
Payment Request Settings Manager 655
Payments History Manager 660

FIG. 6B

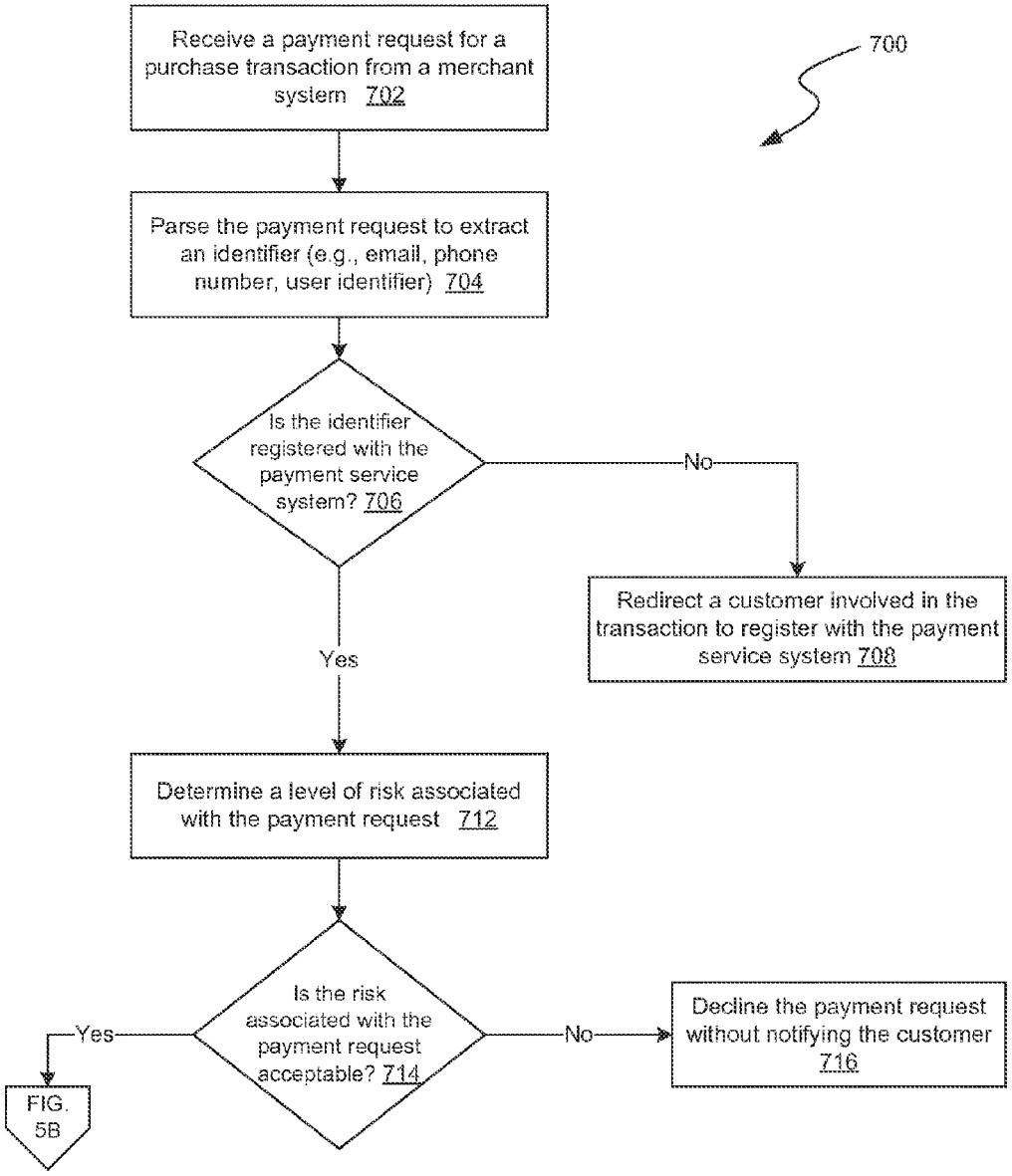

Receive a payment request for a purchase transaction from a merchant system 702
700
Parse the payment request to extract an identifier (e.g., email, phone number, user identifier) 704
Is the identifier registered with the payment service system? 706
No
Redirect a customer involved in the transaction to register with the payment service system 708
Yes
Determine a level of risk associated with the payment request 712
Is the risk associated with the payment request acceptable? 714
Yes
No
Decline the payment request without notifying the customer 716
FIG. 5B

FIG. 7A

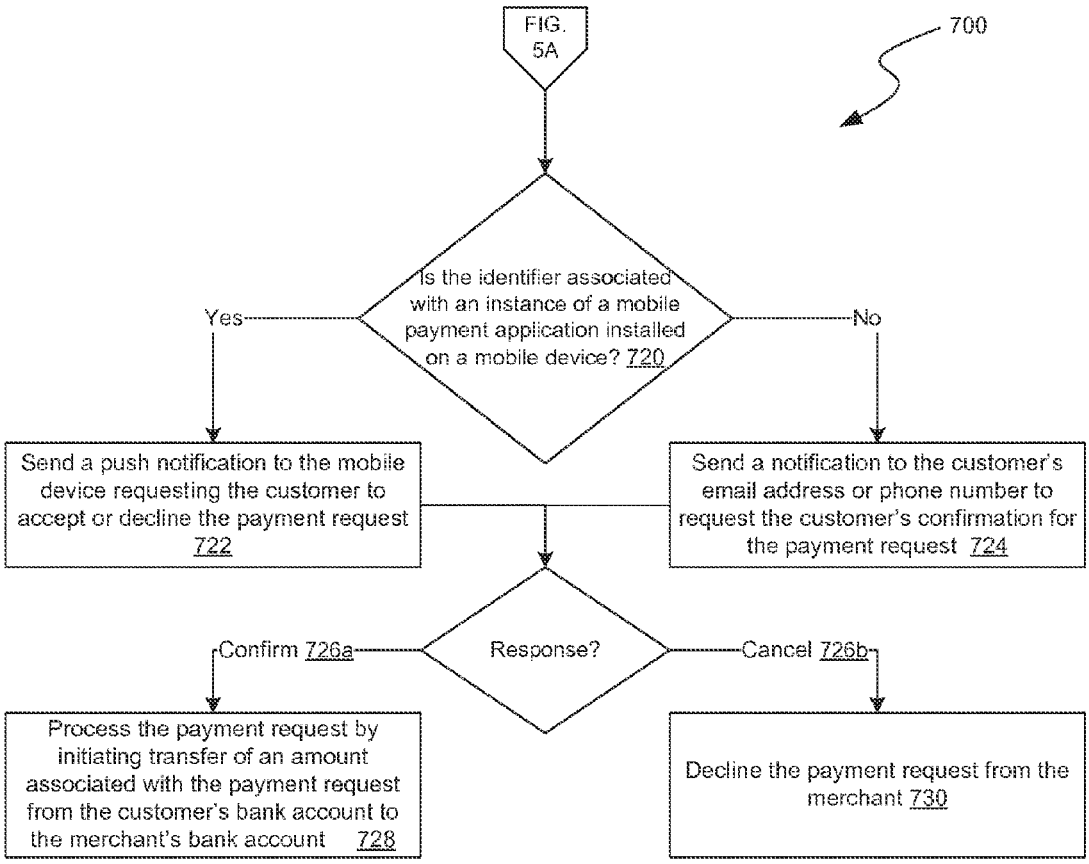


FIG. 5A
700
Is the identifier associated with an instance of a mobile payment application installed on a mobile device? 720
Yes
No
Send a push notification to the mobile device requesting the customer to accept or decline the payment request 722
Send a notification to the customer's email address or phone number to request the customer's confirmation for the payment request 724
Response?
Confirm 726a
Cancel 726b
Process the payment request by initiating transfer of an amount associated with the payment request from the customer's bank account to the merchant's bank account 728
Decline the payment request from the merchant 730

FIG. 7B

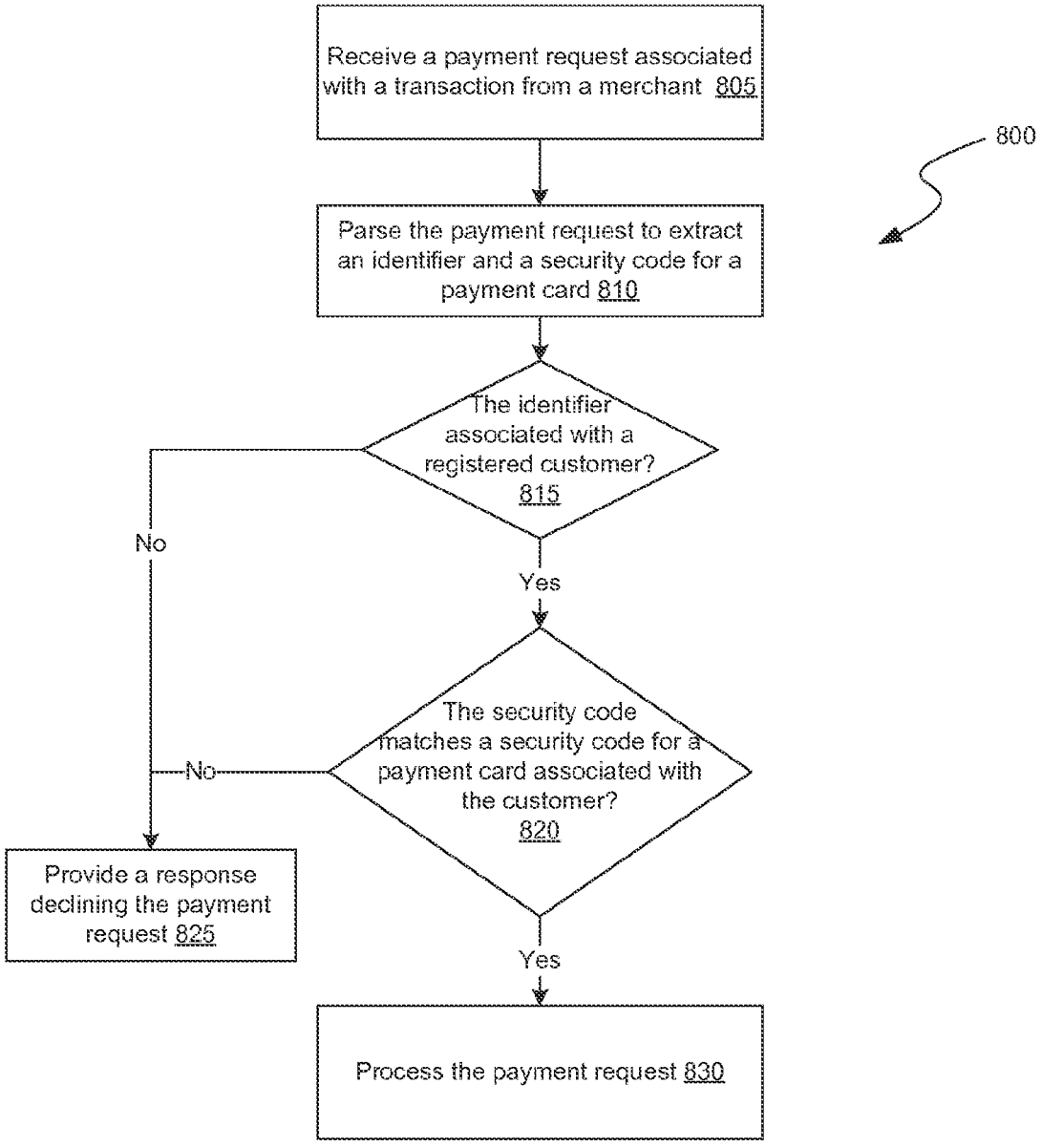

Receive a payment request associated with a transaction from a merchant 805
800
Parse the payment request to extract an identifier and a security code for a payment card 810
The identifier associated with a registered customer? 815
No
Yes
The security code matches a security code for a payment card associated with the customer? 820
No
Yes
Provide a response declining the payment request 825
Process the payment request 830

FIG. 8

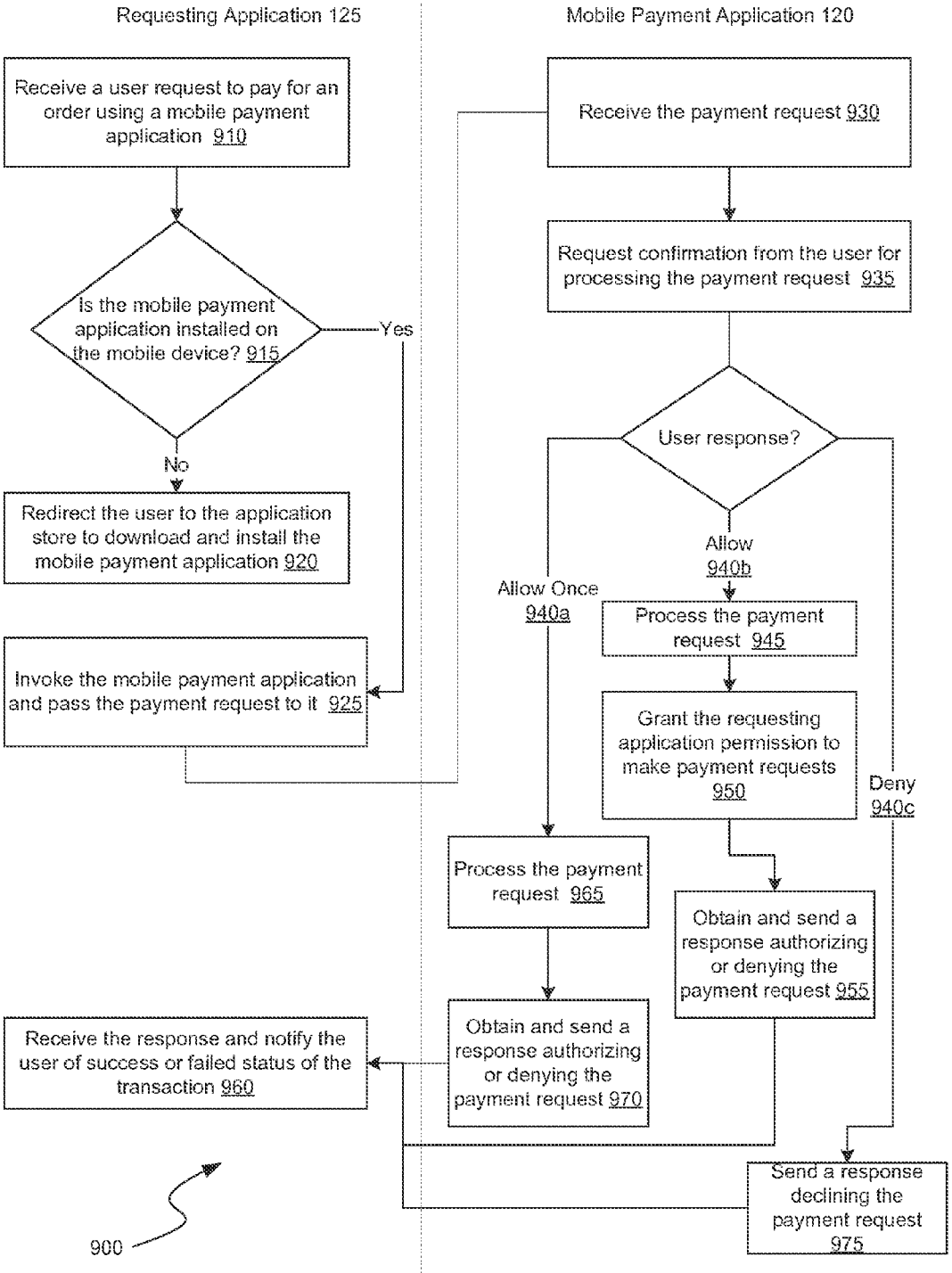

Requesting Application 125
Mobile Payment Application 120
Receive a user request to pay for an order using a mobile payment application 910
Is the mobile payment application installed on the mobile device? 915
Yes
No
Redirect the user to the application store to download and install the mobile payment application 920
Invoke the mobile payment application and pass the payment request to it 925
Receive the payment request 930
Request confirmation from the user for processing the payment request 935
User response?
Allow Once 940a
Allow 940b
Deny 940c
Process the payment request 945
Grant the requesting application permission to make payment requests 950
Process the payment request 965
Obtain and send a response authorizing or denying the payment request 955
Obtain and send a response authorizing or denying the payment request 970
Receive the response and notify the user of success or failed status of the transaction 960
Send a response declining the payment request 975
900

FIG. 9

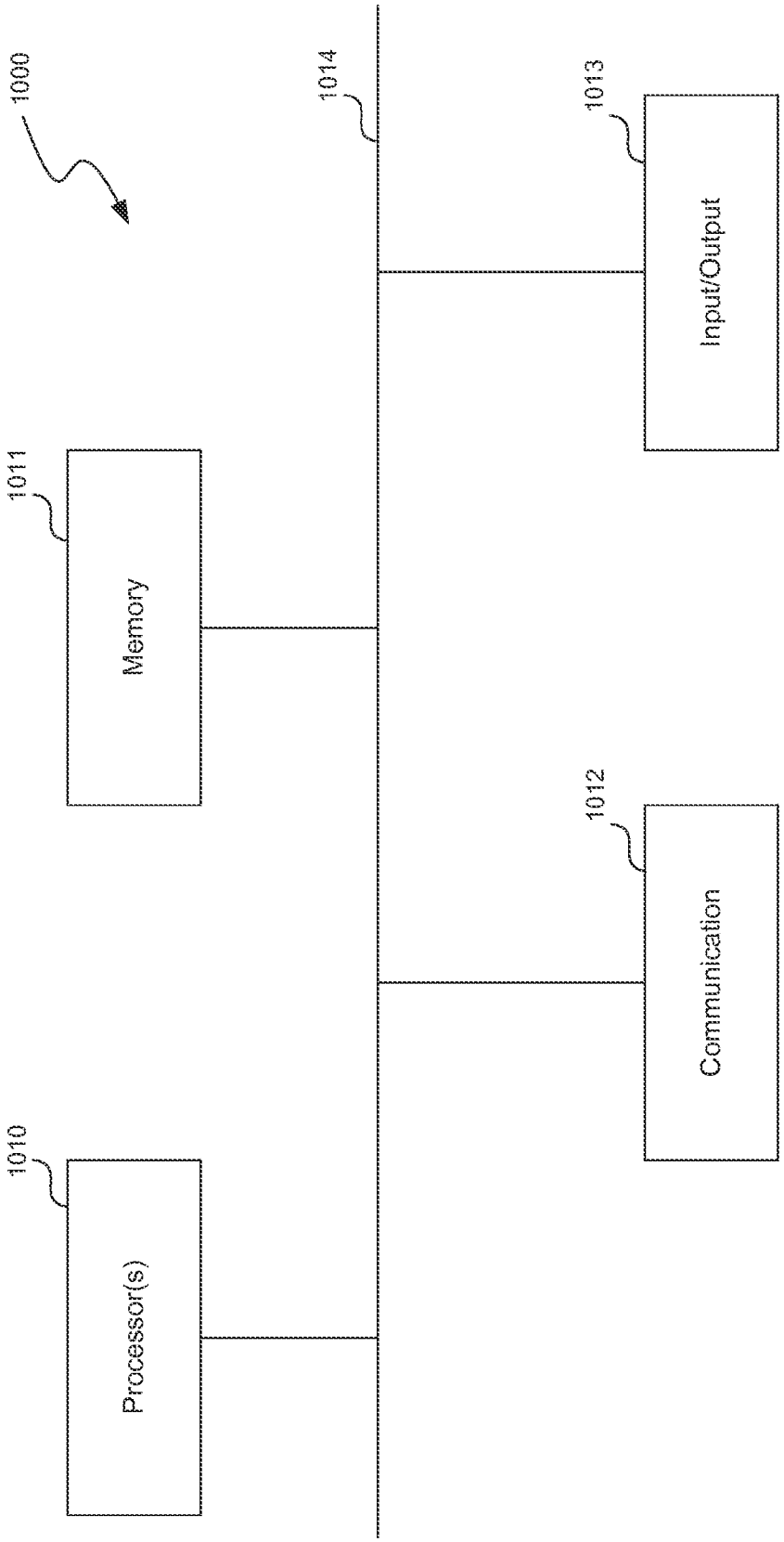

1000
1014
1013
Input/Output
1011
Memory
1012
Communication
1010
Processor(s)

FIG. 10

VERIFIED PURCHASING BY PUSH NOTIFICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is related to U.S. patent application Ser. No. _____ titled "Verified Purchasing" (Attorney Docket No. 078494-8063.US02) filed concurrently herewith and U.S. patent application Ser. No. _____ titled "Verified Purchasing By Email" (Attorney Docket No. 078494-8063.US03) also filed concurrently herewith. The entire content of the aforementioned applications are expressly incorporated by reference herein.

BACKGROUND

[0002] Online merchants provide a variety of checkout options for customers. A typical checkout experience for a new customer shopping on a website includes signing up for an account by setting up a username and password, providing payment information relating to a debit or credit card and billing and shipping information and then placing an order. The payment information is typically saved under the account to allow returning customers to sign in and place an order using the payment information stored under the account. These checkout experiences for new and returning customers require customers to go through multiple steps and can thus discourage customers from completing a purchase transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] One or more embodiments of the present disclosure are illustrated, by way of example and not limitation, in the figures of the accompanying drawings in which like references indicate similar elements.

[0004] FIG. **1** illustrates an environment in which a one-click verified purchasing technology can be implemented.

[0005] FIG. **2** illustrates an example purchase flow in accordance with a first embodiment of the one-click verified purchasing technology.

[0006] FIG. **3** illustrates an example purchase flow in accordance with a second embodiment of the one-click verified purchasing technology.

[0007] FIG. **4** illustrates an example purchase flow in accordance with a third embodiment of the one-click verified purchasing technology.

[0008] FIG. **5** illustrates an example purchase flow in accordance with a fourth embodiment of the one-click verified purchasing technology.

[0009] FIG. **6**A illustrates an example of components of the one-click verified purchasing system in accordance with some embodiments of the one-click verified purchasing technology

[0010] FIG. **6**B illustrates an example of components of a mobile payment application on a mobile device in accordance with some embodiments of the one-click verified purchasing technology.

[0011] FIGS. **7**A-**7**B illustrate an example method of processing a payment request in accordance with a first embodiment of the one-click verified purchasing technology.

[0012] FIG. **8** illustrates an example method of processing a payment request in accordance with a second embodiment of the one-click verified purchasing technology.

[0013] FIG. **9** illustrates an example method of processing a payment request in accordance with a third embodiment of the one-click verified purchasing technology.

[0014] FIG. **10** is a high-level block diagram showing a computer system in which at least some operations related to the disclosed technology can be implemented.

DETAILED DESCRIPTION

[0015] The present disclosure is related to a system and methods for purchasing items online by taking a single verification action (hereinafter "one-click verified purchasing technology"). In some embodiments, the single verification action can be a submission of a security code associated with a payment card or payment account when placing an online order. In other embodiments, the single verification action can be responding to a confirmation request (e.g., a push notification, an email message, a text message, etc.) or a permission request. The disclosed technology employs one or more of these verification actions to identify and block fraudulent transactions and provide customers engaging in legitimate transactions a faster and efficient checkout experience that does not involve signing in or registering for an account.

[0016] The one-click verified purchasing technology, in some embodiments, enables a customer to place an online order for items from a merchant website or a web application ("merchant system"), without creating an account or signing in to an account. Instead, the one-click verified purchasing technology enables a customer to use a communication identifier linked to a payment card stored on file with a one-click verified purchasing system to complete the checkout process. When the customer submits the order, the one-click verified purchasing system implementing the disclosed technology receives a payment request to initiate a payment transaction. The payment request can include the customer's communication identifier (or in some instances a user identifier) and details of the order from the merchant system. If the customer has a mobile application installed on his or her mobile device, the one-click verified purchasing system can send a push notification to the customer's mobile device requesting the customer to confirm or cancel the online order. If the customer confirms the order, the one-click verified purchasing system processes the payment request from the merchant system by initiating a transfer of an amount of funds corresponding to the payment request from a bank account associated with the payment card to a bank account associated with the merchant system.

[0017] In some embodiments, the one-click verified purchasing technology allows a customer to place an order for items with a merchant system using a communication identifier linked to a payment card on file with the one-click verified purchasing system and a security code (e.g., a card verification value) associated with the payment card. When the customer places an order with the merchant system in the disclosed manner, the one-click verified purchasing system receives a payment request including these two pieces of information and details of the order (e.g., order identifier, order amount, pre-tax amount, sales tax amount, shipping cost, description and quantity of items ordered, etc.) from the merchant system. The one-click verified purchasing system then checks that the communication identifier is mapped to a valid payment card and the security code included in the payment request matches the corresponding security code on the payment card. If so, the one-click verified purchasing

system processes the payment request from the merchant system by initiating a transfer of an amount of funds corresponding to the payment request from a bank account associated with the payment card to a bank account associated with the merchant system.

[0018] In some embodiments, the one-click verified purchasing technology enables a customer to order items from a mobile application ("requesting application") on a mobile device by using a mobile payment application installed on the same mobile device as a payment method or checkout option. The mobile payment application appears as a payment option on the checkout user interface of the requesting application. When the mobile payment application is selected as the payment method, the mobile payment application comes to the foreground of the mobile device, while the requesting application goes into the background. The customer can then permission the requesting application to use the mobile payment application as a payment method in the current transaction or in the current and future transactions. In some embodiments, the mobile payment application can provide one or more user interfaces for managing settings and permissions associated with various requesting applications, tracking payment requests initiated from the requesting applications, or the like.

[0019] In some embodiments, the one-click verified purchasing technology enables use of a mobile payment application that generates an email-based payment request as a payment method to submit an order. When the customer selects the mobile payment application as a payment method on the checkout user interface of a requesting application, the mobile payment application comes to the foreground of the mobile device. The mobile payment application can then pre-fill a payment amount and compose an email-based payment request by filling out the "To" and "Cc" fields. The "To" field includes the email address of the party receiving the payment (i.e., the merchant) and the "Cc" field includes the email address of the party providing the payment service (i.e., the one-click verified purchasing system). Other details relating to the order associated with the payment request can also be auto-filled by the mobile payment application. The customer can then send the e-mail to initiate the payment transaction.

[0020] As described above, the disclosed technology enhances the checkout experience for customers by removing account registration and sign in barriers. Because the disclosed technology uses mapping or association between a communication identifier and one or more payment cards to process payment requests from merchant systems, customers can provide minimal information to complete the checkout process. Moreover, the disclosed technology enables the checkout process to be completed in a shorter amount of amount and using a single verification action.

[0021] Various embodiments and implementations of the disclosed one-click verified purchasing technology will now be described. The following description provides specific details for a thorough understanding and an enabling description of these implementations. One skilled in the art will understand, however, that the disclosed system and methods may be practiced without many of these details. Additionally, some well-known structures or functions may not be shown or described in detail, so as to avoid unnecessarily obscuring the relevant description of the various implementations. The terminology used in the description presented below is intended to be interpreted in its broadest reasonable manner, even though it is being used in conjunction with a detailed description of certain specific implementations of the disclosed system and methods.

[0022] FIG. **1** illustrates an environment **100** in which the one-click verified purchasing technology can be implemented. The environment includes a merchant system **122** (e.g., e-commerce websites or web applications hosted on a web server(s) or application server(s)). The merchant system **122** can be accessed by a customer using a client device **104** (e.g., a desktop computer, a laptop computer, a mobile device, a tablet or any other processing device) or a mobile device **102** of a customer. The mobile device **102** can be, for example, a smart phone, a tablet computer, a phablet, a notebook computer, or any other form of mobile processing device. In some embodiments, a mobile payment application **120** runs on the customer's mobile device **102**. The mobile device **102** can also include other e-commerce applications ("requesting applications") that are associated with one or more merchant systems and can be used by the customer to purchase products or services.

[0023] The environment **100** can also include a computer system of the merchant's acquirer (hereinafter "acquirer **114**"), a computer system of an issuing bank (hereinafter "issuer **118**"), a computer system of a card payment network (hereinafter "card payment network **116**"), and a computer system of a payment service (hereinafter "payment service system **108**") implementing the one-click verified purchasing system **109**. Each of the aforementioned computer systems can include one or more distinct physical computers and/or other processing devices which, in the case of multiple devices, can be connected to each other through one or more wired and/or wireless networks. All of the aforementioned devices are coupled to each other through a network **106**, which can be, or include, the Internet and one or more wireless networks (e.g., a Wi-Fi network and/or a cellular telecommunications network).

[0024] The environment **100**, illustrated in FIG. **1**, can accommodate transactions involving payment cards such as debit cards, credit cards, pre-paid cards, bank accounts, mobile payment applications and the like. The mobile payment application **120** can include an electronic wallet application, money transfer application (e.g., application for sending and receiving money via email or phone), or any other application having an account that is linked to one or more payment cards and/or bank accounts and can be used by the owner of the mobile device to initiate transactions. Such transactions can include traditional purchase transactions between customers and merchants or service providers, person to person transactions and the like.

[0025] In a traditional online purchase transaction using a payment card (e.g., debit or credit card), the merchant system receives details of the payment card including the cardholder's name, payment card number, expiration date, card verification value (CVV)), billing address, etc., and provides such information to the payment service system **108**. The payment service system, in turn, processes the transaction by routing the authorization request to the acquirer **114**. The acquirer **114** sends this data to the card payment network **116** (e.g., Visa, MasterCard), which forwards the data to the issuer **118** for authorization. If the transaction is approved or authorized by the issuer **118**, a payment authorization message is sent from the issuer **118** to the merchant system **122** via a path opposite of that described above. Once the transaction is authorized, settlement and clearing occurs. During settlement

and clearing, the issuer **118** sends the funds associated with the authorized transaction through the card payment network **116** to the acquirer **114** to be deposited in the merchant's account with the acquirer **114**.

[0026] FIG. **2** illustrates an example purchase flow **200** in accordance with a first embodiment of the one-click verified purchasing technology. The purchase flow **200** begins on a merchant's website or web application **205**. When a customer is ready to purchase an item, the customer selects a "payment service" **210** as a payment method. The merchant's website **205** may include additional checkout options **220** such as a payment card (e.g., a debit or credit card such as VISA, AMERICAN EXPRESS). When the payment service **210** is selected as the payment method, the customer is requested to enter a communication identifier **215** such as an email address or a phone number and submit the order by selecting the "Place Order" button **225**. In this example purchase flow, the customer can place the order using the payment service option **210** without signing in or registering for an account with the merchant.

[0027] The details of the order submitted by the customer is received by the merchant system **122** which then sends a payment request to the payment service system **108** to initiate a payment transaction. The one-click verified purchasing system **109** of the payment service system receives the payment request including the communication identifier and order information (e.g., order identifier, product description and quantity, etc.). The one-click verified purchasing system **109** uses the communication identifier to look up or identify an associated payment card. The one-click verified purchasing system **109** can also use the communication identifier to determine whether the customer associated with the payment card has a mobile payment application installed on his or her mobile device **102**. For example, if storage of a device identifier or a mobile application identifier in association with the communication identifier in one or more database tables can be an indication that the customer's has installed the mobile payment application on his or her mobile device. The mobile device identifier and/or the application identifier can be used by the one-click verified purchasing system **109** to send a push notification **235** to the customer's mobile device **102**.

[0028] The push notification **235** can include information about the order and can request the customer confirm the order by selecting the confirm button **240** or cancel the order by selecting the cancel button **245**. If the customer confirms the order, the payment service system processes the payment request from the merchant system **122** by sending an authorization request to the issuer **118** of the payment card via the acquirer **114** and the card payment network **116**. If the authorization request is approved, the one-click verified purchasing system sends a success response to the merchant system **122** which then notifies the customer on its website **205** accordingly. In some embodiments, the one-click verified purchasing system **109** can also provide additional information such as a shipping address for the customer when sending the response to the merchant system **122** to facilitate physical delivery of purchased items to the customer. In the event that the customer cancels the payment request by selecting the cancel button **245** on the push notification user interface **235**, the one-click verified purchasing system **109** provides a failed response to the merchant system **122**, which then cancels the order and notifies the customer of the cancellation.

[0029] In some embodiments, the disclosed technology provides additional security in processing purchase transactions by implementing a two-factor verification method. For example, the website **205** can be accessed using a client device (e.g., client **104**) that is separate from the mobile device **102**. The confirmation on the mobile device **102** can thus act as a second verification factor, while the email address of the customer acts as a first verification factor. In other embodiments, the website **205** can be accessed on a mobile web browser of the same mobile device **102** to which the push notification is delivered.

[0030] FIG. **3** illustrates an example purchase flow **300** in accordance with a second embodiment of the one-click verified purchasing technology. The purchase flow **300** begins on a website or a web application **305** (e.g., display component for displaying information identifying one or more items). In this example purchase flow, the customer can submit the order without registering for or signing in to an account (e.g., with the merchant system or any other service that processes payments for the merchant system) and thereby avoid a need to use an authentication procedure associated with accessing the account to complete the purchase transaction. For example, when a customer is ready to checkout, he or she can select the payment service **310** as the payment method. When the customer selects the payment service payment method, the customer is requested to enter a communication identifier **315** such as an email address or a phone number and a card verification value **320** associated with a payment card linked to the communication identifier into the user interface elements. The customer can then submit the order by selecting the "Place Order" button **325**. In response to the customer selecting the button **325** using a single action (e.g., a single tap, a single click, a single gesture), a purchase order submission component can gather at least some of the information identifying the items in the order (e.g., item ID or stock keeping unit), the communication identifier and the card verification value to generate a request and transmits the request to the merchant system. In some embodiments, other information associated with the payment card such as a portion of the payment card number (e.g., primary account number or PAN) can be requested instead of or in addition to the card verification value.

[0031] The order submitted by the customer is received at the merchant system **122**, which then sends a payment request to the payment service system **108** to request payment for the transaction initiated by the customer. The one-click verified purchasing system **109** receives the payment request and uses the communication identifier and the card verification value included in the payment request to identify a payment card that is to be used to pay for the transaction. The payment service system **108** then sends an authorization request to the issuer **118** of the payment card via the acquirer **114** and the card payment network **116**. If the authorization request is approved, the one-click verified purchasing system **109** sends a success response to the merchant system **122** which then notifies the customer on its website **330** accordingly.

[0032] FIG. **4** illustrates an example purchase flow **400** in accordance with a third embodiment of the one-click verified purchasing technology. The purchase flow **400** begins on the requesting mobile application **125** on the mobile device **102**. The requesting application **125** can be a browser application that can be used to access a website or a web application or a mobile e-commerce application installed on the mobile device. When a customer is ready to checkout, the customer selects one of the payment methods, e.g., **410** or **420**, displayed on a user interface **405** of the requesting mobile appli-

cation **125**. When the customer selects the payment method **420** to pay for the transaction using the mobile payment application, the requesting mobile application **125** invokes the mobile payment application **120**. The user interface **425** of the mobile payment application **120** displays a request from the requesting application **125** for permission to use a payment card linked to the mobile payment application **120**. The customer can select option **430** to grant the requesting application **125** a one-time permission to use the mobile payment application **120** to make a request for payment. The option **435** can be selected to grant the requesting application a permission (e.g., perpetual or long term) to make payment requests to the mobile payment application **120**. The "Deny" option **440** can be selected to deny the requesting application from using the mobile payment application to request payments.

[0033] In the purchase flow **400**, when the customer grants the requesting application **125** permission to make payment requests to the mobile application **120** by selecting option **430** or **435**, the mobile payment application **120** sends a payment request to the payment service system **108** on behalf of the requesting application **125** to initiate the payment transaction. The payment request can include a communication identifier which can be an email address, a phone number, an identifier corresponding to the mobile payment application, an identifier corresponding to the mobile device or a combination thereof, which can be used by the payment service system to identify the payment card that is to be used to pay for the transaction. In some embodiments, the payment request can be a HyperText Transfer Protocol (HTTP) request. In other embodiments, as described with respect to FIG. **5**, the payment request can be an email message.

[0034] In some embodiments, the mobile payment application can request the customer to provide a card verification value of the payment card for an extra layer of security. In some embodiments, the customer can configure preference settings **450** for each requesting application to define the conditions or rules under which payment requests from the requesting application can be processed. For example, by setting an amount threshold, the customer can authorize the mobile payment application to process payment requests from the requesting application that are in the amount $150.00 or less, without prompting the customer for confirmation. For payment requests higher than the threshold amount, the mobile payment application can request a verification action (e.g., entry of a card verification value) from the customer or a confirmation that the customer wishes to proceed with the transaction. The preference settings **450** may also include an option to turn on/off notifications when a payment request is processed. In some embodiments, a default setting can be specified by the mobile payment application for processing payment requests. For example, by default in the absence of preference settings, all payment requests can cause the mobile payment application to notify the customer to obtain confirmation from the customer to proceed with the transaction. In some embodiments the user interface **445** can include a payment history panel **455** which displays a list of payment requests processed by the mobile payment application on behalf of the requesting application These setting options are exemplary and several other setting options may be available for each requesting application that uses the mobile payment application as a payment method.

[0035] FIG. **5** illustrates an example purchase flow **500** in a fourth embodiment of the one-click verified purchasing system. The purchase flow **500** begins on the user interface **505** of a requesting application (e.g., **125**) which displays multiple payment methods, e.g., **510** and **520**. When the customer selects the "Checkout with Mobile Payment Application" option **520**, the requesting application invokes the mobile payment application **120** if it is installed on the mobile device. The customer can enter an amount **530** corresponding to the purchase on the user interface **155**, or alternately, the payment amount can be auto-populated based on order information received from the requesting application. The customer can select the "attach to email" option **535** to generate an email **540**, with the merchant's email address in the "To" field **545** and the payment service system's email address in the "Cc" field **550**. The subject and message body can also be auto-populated using order information from the requesting application. Alternatively, the email **540** can be automatically generated and populated with the recipient email address and the payment amount. The customer can send the email (e.g., by selecting the send button) to initiate transfer of the payment amount from a payment account associated with the customer to a financial account associated with the requesting application. In some embodiments, when the requesting application invokes the mobile payment application to request the payment amount, the mobile payment application can display a notification message to the customer to obtain a confirmation from the customer to proceed with the transaction. Upon receiving confirmation from the customer, the mobile payment application can generate an email message that includes the email address of the requesting application, the email address of the payment service system and an email address of the customer in a header portion and at least the payment amount in the header portion or a body portion of the email message via a background process that is transparent to the customer (i.e., the email message is generated and sent in a manner that is generally undetectable or invisible to the customer). In some instances when the customer has more than one payment card stored with the payment service system, the notification message can include an option for the customer to select a payment card that is to be used for payment.

[0036] FIG. **6**A illustrates an example of components of the one-click verified purchasing system in accordance with some embodiments of the one-click verified purchasing technology. The one-click verified purchasing system **109** can be a component or a sub-system of the payment service system **108**. Alternately, the one-click verified purchasing system **109** can be implemented on a separate computing system (e.g., on a separate server or server(s)). The one-click verified purchasing system **109** can include a payment request processor **605** and a payment request notification engine **615**, among others, in some embodiments. The one-click verified purchasing system **109** can access one or more database tables such as the customer account database table **640**, payment card database table **645** and/or transaction history database table **650** to retrieve and/or store data. The customer account database table **640** can store various fields of information such as a customer identifier, name, email address, phone number, device identifier, mobile application identifier, billing address, shipping address, and/or the like. The payment card database table **645** can include various fields of information such as a customer identifier, payment card/account number (e.g., primary account number or PAN), expiration date, card/account type, and/or the like. The transaction history database table **650** can include various fields of information such as a transaction identifier, customer identifier,

date, merchant name, amount, product/service item names/codes, and/or the like. Various other database tables may also be accessed by the one-click verified purchasing system **109**.

[0037] The payment request processor **605** can process payment requests from merchant systems as described in detail with respect to FIGS. **2-5**. For example, the payment request processor **605** can receive payment requests from merchant systems, parse the payment requests to extract details such as the communication identifier, the security code for a payment card, order information, or the like. The payment request processor **605** can check whether a communication identifier is associated with one or more payment cards and can process payment requests when triggered by a verification action by initiating a transfer of an amount associated with the payment request from a bank account funding one of the payment cards to a financial account associated with the merchant system.

[0038] In some embodiments, the risk analyzer **610** can examine incoming payment requests for any indications for fraud and evaluate a level of risk associated with processing the payment requests. Based on the level of risk, the payment request processor **605** can determine whether to block the payment request or to allow the payment request to be processed. The risk analyzer can determine or assess a level of risk associated with a payment request by analyzing attributes of the payment request and historical data (e.g., past transactions associated with the a customer) to identify one or more risk factors. The historical data associated with past transactions can be stored in a database table **650**. Examples of risk factors can include, but are not limited to: pattern of purchase behavior, transaction amount, volume, frequency and/or timing of payment requests, identity of the merchant, and/or the like. Each of the risk factors can be scored and/or weighted to determine an aggregate risk score that provides an assessment of the level of risk associated with a payment request. When the aggregate risk score is higher than a threshold, indicating a higher likelihood of fraud, the risk analyzer can, for example, notify the trigger payment request processor **605** and/or the payment request notification engine **615** so that the payment request can be blocked from reaching the customer and can be canceled.

[0039] In some embodiments, customers can have mobile payment applications installed on their mobile devices. Payment requests associated with those customers can cause the payment request notification engine **615** to generate and send push notifications using the push notification module **620**. In general, a push notification for a payment request is generated based on information included in the payment request, and can prompt the customer to confirm or cancel the payment request. Based on the customer's response, the payment service system can process the payment request by initiating transfer of an amount of funds corresponding to the payment request from a bank account associated with the payment card to a financial account associated with the merchant system. In some embodiments, when a payment request is determined to have a level of risk higher than a threshold, the payment request notification engine **615** can block a push notification for the payment request from being sent to the customer's mobile device.

[0040] Some customers may not have the mobile payment application installed on their mobile devices. The payment request notification engine **615**, in this instance, can send a notification in the form of an email **625**, text message **630** and/or an automated phone call **635** to request a customer to confirm or cancel a payment request. For example, the customer can confirm the payment request by providing a card verification value associated with a payment card or send another confirmatory response. In some embodiments, the notification engine **615** can select a notification method for requesting verification or confirmation from a customer based on the level of risk associated with the payment request. For example, if the level of risk is high, the notification engine **615** can use the automated phone call option. Similarly, if the level of risk is low, the notification engine can use the push notification option.

[0041] FIG. **6**B illustrates an example of components of the mobile payment application **120** on a mobile device in some embodiments of the one-click verified purchasing technology. The mobile payment application **120** can include an application payment request handler **652**, a permissions manager **654**, a payment request settings manager **655** and a payments history manager **660**, among others in some embodiments.

[0042] The application payment request handler **652** can receive payment requests from requesting applications on the mobile device and process the payment requests based on permissions managed by the permissions manager **654**. The permissions manager **654** can track permissions granted by a customer to various requesting applications to make payment requests via the mobile payment application. Those requesting applications that have been permissioned by the customer to request payment via the mobile payment application can send payment requests to the mobile payment application in the background. For example, when the application payment request handler **652** receives an incoming payment request from a requesting application, the payment request handler checks with the permissions manager **654** to determine whether the requesting application is allowed to make the payment request. If the requesting application has a valid permission, then the application payment request handler **652** handles the payment request by sending it on to the payment service system. If, for example, the requesting application does not have a valid permission, the application payment request handler **652** can decline to process the payment request or notify the customer for confirmation.

[0043] The payment request settings manager **655**, in some embodiments, can receive and store preference settings specified by the customer for handling payment requests by the application payment request handler **652**. For example, the application payment request handler **652** can check with the settings manager to determine whether a payment request from a requesting application meets all the rules set up by the customer (e.g., payment amount threshold) and process the payment request when the payment request meets the conditions associated with the rules. The payment history manager **660**, in some embodiments, can track and store a history of payment requests from each requesting application handled by the mobile payment application.

[0044] FIGS. **7**A-**7**B illustrate an example method of processing a payment request in accordance with a first embodiment of the one-click verified purchasing technology. In this embodiment, the disclosed technology receives a payment request including an identifier from a merchant system, analyzes the payment request to assess a level of risk associated with it and based on the level of risk, determines whether to send a push notification to a mobile device associated with the identifier to request confirmation on the payment request.

[0045] Referring to FIG. **7**A, at block **702**, the one-click verified purchasing system receives a payment request associated with a purchase transaction from a merchant system. The one-click verified purchasing system parses the payment request at block **704** to extract an identifier which is typically an email address or a phone number, but can be any other identifier such as a user identifier, a TWITTER handle, etc. The extracted information can also include details of the transaction. At decision block **706**, the one-click verified purchasing system determines if the identifier is associated with a payment card in the payment service system. If the identifier is not associated with a payment card, the one-click verified purchasing system can send a notification (e.g., an email or a text message) to register with the payment service system by associating a payment card to the identifier at block **708**.

[0046] In some embodiments, if the identifier is associated with a payment card, the one-click verified purchasing system can examine the customer's transaction history and attributes of the payment request to determine a level of risk (or a risk score) associated with the payment request at block **712**. For example, if the customer's transaction history indicates a history of purchase of clothing for male and the order is associated with a clothing for female, the change in purchase behavior can be an indication of fraud, which is considered in assessing the level of risk. Similarly, a payment request for an amount much larger than in the past can be another indication of fraud that can be considered in determining the level of risk. At decision block **714**, if the level of risk associated with the payment request is acceptable or under a pre-defined threshold, the payment request is highly likely to be fraudulent and so in that instance, the one-click verified purchasing system can decline the payment request without notifying the customer at block **716**.

[0047] Referring to FIG. **7**B, if the level of risk associated with the payment request is determined to be acceptable or above a predefined threshold, the one-click verified purchasing system can determine if the identifier included in the payment request is associated with an instance of a mobile payment application installed on a mobile device at decision block **720**. If so, the one-click verified purchasing system can retrieve a device identifier associated with the mobile device and send a push notification to the mobile device to request the customer to confirm or cancel the payment request. If the identifier is not associated with an instance of the mobile payment application, the one-click verified purchasing system can send a notification to the customer's email address or phone number to request the customer to confirm or cancel the payment request at block **724**. If a "confirm" response **726***a* is received from the customer, the one-click verified purchasing system processes the payment request at block **728**. If a "cancel" response **726***b* is received from the customer, the one-click verified purchasing system declines the payment request from the merchant system at block **730**.

[0048] FIG. **8** illustrates an example method of processing a payment request in accordance with a second embodiment of the one-click verified purchasing technology. In this embodiment, the disclosed technology receives a payment request for a purchase transaction from a merchant system and uses an identifier and a security code submitted by a customer at a merchant system as part of the purchase transaction to approve or deny the payment request.

[0049] The method **800** begins at block **805** when the one-click verified purchasing system receives a payment request associated with a purchase transaction from a merchant system. The one-click verified purchasing system parses the payment request to extract an identifier and a security code associated with a payment card at block **810**. At decision block **815**, the one-click verified purchasing system determines if the identifier is associated with one or more payment cards and if so, at decision block **820**, the one-click verified purchasing system determines if the security code in the payment request matches the security code on one of the payment cards. If so, the one-click verified purchasing system processes the payment request at block **830** by transferring a payment amount included in the payment request from an account associated with the payment card with the matching security code to a financial account associated with the merchant system. Alternatively, if the identifier is not associated with a payment card or the security code does not match, the one-click verified purchasing system provides a response declining the payment request at block **825**.

[0050] FIG. **9** illustrates an example method of processing a payment request in accordance with a third embodiment of the one-click verified purchasing technology. In this embodiment, a mobile payment application **120** on a mobile device processes a payment request initiated by a requesting application **125** on the same mobile device.

[0051] The method **900** begins at block **910**, when the requesting application receives a user request to pay for an order using the mobile payment application. If the mobile payment application is not installed on the mobile device as determined at decision block **915**, the user can be redirected to an application store on the mobile device to download and install the mobile payment application at block **920**. If, on the other hand, the mobile payment application is installed on the mobile device, the requesting application can invoke or call the mobile payment application and pass a payment request to it at block **925**. The payment request can include details of the order. At block **930**, the mobile payment application (or a background service listening to a call or Intent) can answer the call from the requesting application to handle the payment request. At block **935**, the mobile payment application can request confirmation from the user for processing the payment request. If the user response is "allow once" **940***a*, the mobile payment application processes the payment request at block **965** as a one-time request by sending the payment request to the one-click verified purchasing system over a network. The payment request can include a device identifier, a mobile application instance identifier, communication identifier or the like appended to it, which can be used by the one-click verified purchasing system to identify a payment account to be used to pay for the order. At block **970**, the mobile payment application obtains a response authorizing or denying the payment request **970** from the one-click verified purchasing system and sends the response to the requesting application. The requesting application receives the response and notifies the user accordingly at block **960**. For example, if the authorization failed, the requesting application can notify the user of the failed transaction status.

[0052] If the user selects "allow" **940***b* as the response, the mobile payment application processes the payment request at block **945** and grants the requesting application permission to make subsequent payment requests to the mobile payment application at block **950**. In other words, the next time the user selects the mobile payment application as a checkout option from the checkout user interface of the requesting application, the payment request from the requesting application is

processed by the mobile payment application in the background without the user having to leave the requesting application. Since the user does not leave the requesting application and the payment requests are processed in the background, this method provides a seamless purchase experience for the user without sharing the user's payment card data to the requesting application. In some embodiments, the mobile payment application can generate and send the requesting application a token using which the requesting application can directly communicate with the one-click verified purchasing system to request payments. The token can be uniquely associated with a user and the requesting mobile application, and can be invalidated at any time (e.g., by the user revoking or changing the permission, after a period of time, etc.) In the instance that the user response is a "deny" response **940***c*, the mobile payment application can send a response to the requesting application declining the payment request at block **975**.

[0053] FIG. **10** is a high-level block diagram showing an example of a processing device **1000** that can represent any of the devices described above, such as the mobile device **102**, client device **104**, merchant system **122**, payment processor system **114**, **116** or **118**, the payment service system **108** and the one-click verified purchasing system **109**. As noted above, any of these systems may include two or more processing devices such as represented in FIG. **10**, which may be coupled to each other via a network or multiple networks.

[0054] In the illustrated embodiment, the processing system **1000** includes one or more processors **1010**, memory **1011**, a communication device **1012**, and one or more input/output (I/O) devices **1013**, all coupled to each other through an interconnect **1014**. The interconnect **1014** may be or include one or more conductive traces, buses, point-to-point connections, controllers, adapters and/or other conventional connection devices.

[0055] The processor(s) **1010** may be or include, for example, one or more general-purpose programmable microprocessors, microcontrollers, application specific integrated circuits (ASICs), programmable gate arrays, or the like, or a combination of such devices. The processor(s) **1010** control the overall operation of the processing device **800**.

[0056] Memory **1011** may be or include one or more physical storage devices, which may be in the form of random access memory (RAM), read-only memory (ROM) (which may be erasable and programmable), flash memory, miniature hard disk drive, or other suitable type of storage device, or a combination of such devices. Memory **1011** may store data and instructions that configure the processor(s) **1010** to execute operations in accordance with the techniques described above.

[0057] The communication device **1012** may be or include, for example, an Ethernet adapter, cable modem, Wi-Fi adapter, cellular transceiver, Bluetooth transceiver, or the like, or a combination thereof. Depending on the specific nature and purpose of the processing device **1000**, the I/O devices **1013** can include devices such as a display (which may be a touch screen display), audio speaker, keyboard, mouse or other pointing device, microphone, camera, etc.

[0058] Unless contrary to physical possibility, it is envisioned that (i) the methods/steps described above may be performed in any sequence and/or in any combination, and that (ii) the components of respective embodiments may be combined in any manner.

[0059] The techniques introduced above can be implemented by programmable circuitry programmed/configured by software and/or firmware, or entirely by special-purpose circuitry, or by a combination of such forms. Such special-purpose circuitry (if any) can be in the form of, for example, one or more application-specific integrated circuits (ASICs), programmable logic devices (PLDs), field-programmable gate arrays (FPGAs), etc.

[0060] Software or firmware to implement the techniques introduced here may be stored on a machine-readable storage medium and may be executed by one or more general-purpose or special-purpose programmable microprocessors. A "machine-readable medium", as the term is used herein, includes any mechanism that can store information in a form accessible by a machine (a machine may be, for example, a computer, network device, cellular phone, personal digital assistant (PDA), manufacturing tool, any device with one or more processors, etc.). For example, a machine-accessible medium includes recordable/non-recordable media (e.g., read-only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; etc.).

[0061] Note that any and all of the embodiments described above can be combined with each other, except to the extent that it may be stated otherwise above or to the extent that any such embodiments might be mutually exclusive in function and/or structure.

[0062] Although the present invention has been described with reference to specific exemplary embodiments, it will be recognized that the invention is not limited to the embodiments described, but can be practiced with modification and alteration within the spirit and scope of the appended claims. Accordingly, the specification and drawings are to be regarded in an illustrative sense rather than a restrictive sense.

1. A method performed by a payment service system for processing an online purchase transaction between a user and a third-party merchant system, comprising:

receiving, by the payment service system, a payment request from the third-party merchant system, the payment request including a communication identifier, wherein the communication identifier is submitted, in lieu of login credentials or payment information, by the user, using a computing device associated with the user, to the third-party merchant system to complete a checkout process for the online purchase transaction via the computing device;

determining, by the payment service system, whether the communication identifier is associated with a payment card by accessing a datastore coupled to the payment service system;

after a determination that the communication identifier is not associated with the payment card, transmitting, by the payment service system, a first notification to a mobile device associated with the user using the communication identifier, the first notification configured to prompt the user to associate the payment card with the communication identifier to process the payment request; and

after a determination that the communication identifier is associated with the payment card,

identifying, by the payment service system, a verification device associated with the communication iden-

tifier, wherein the verification device is separate from the computing device at which the communication identifier is submitted;

transmitting, by the payment service system, a second notification to the verification device associated with the communication identifier to request the user to confirm or cancel the online purchase transaction, the second notification including information relating to the online purchase transaction;

receiving, by the payment service system, a response from the verification device, the response confirming the online purchase transaction; and

based on the response, processing the payment request from the third-party merchant system by transferring a payment amount associated with the online purchase transaction from a financial account associated with the payment card to a financial account associated with the third-party merchant system.

2. The method of claim **1**, wherein the communication identifier is submitted by the user via a user interface of the third-party merchant system, the user interface accessible via the computing device.

3. The method of claim **1**, wherein the communication identifier is submitted by the user via a user interface of the third-party merchant system, the user interface accessible via an application installed on the verification device.

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

prior to transmitting the second notification to the verification device, assessing whether a level of risk associated with the payment request is lower than a predefined threshold, wherein the second notification is transmitted to the verification device in an event that the level of risk is lower than the predefined threshold, the level of risk being lower than the predefined threshold indicating that the online purchase transaction is a legitimate purchase transaction.

5. The method of claim **4**, wherein assessing the level of risk associated with the payment request includes assessing at least one risk factor including a purchase pattern associated with the user, the payment amount, a frequency of payment requests in a given duration, a timing of the payment request or an identity of the third-party merchant system.

6. The method of claim **1**, wherein the communication identifier includes at least one of an email address or a phone number.

7. The method of claim **1**, wherein the verification device is identified based on a mobile application installed on the verification device, wherein the mobile application is associated with the payment service, wherein the second notification is transmitted to the verification device using a push notification service associated with the mobile application.

8. The method of claim **1**, wherein the second notification is transmitted to the verification device using the communication identifier that includes at least one of an email address or a phone number.

9. (canceled)

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

providing by the payment service system an address associated with the user to the third-party merchant system when the online purchase transaction involves a physical delivery of a product.

11. A method performed by a payment service system for processing an online purchase transaction between a user and a merchant system, comprising:

receiving, from the merchant system, an email address and a payment request specifying a payment amount corresponding to the online purchase transaction, wherein the email address, instead of payment information or login credentials, is submitted to the merchant system via a computing device to complete a checkout process with the merchant system;

maintaining, in a storage area associated with the payment service system, information associated with user accounts, including email addresses, mobile device identifiers and information associated with payment cards;

based on the email address received from the merchant system,

retrieving, from the storage area, a mobile identifier associated with the email address;

identifying a mobile device of the user based on the mobile identifier, wherein the mobile device is separate from the computing device at which the email address is submitted; and

retrieving, from the storage area, information associated with a payment card for accessing a financial account associated with the user;

transmitting a message to the identified mobile device to request the user to confirm the online purchase transaction;

receiving a response to the message from the user via the mobile device, the response including a security code;

verifying that the security code in the response matches a card verification value associated with the payment card; and

in response to the verifying of the security code received via the mobile device, causing a transfer of the specified payment amount from the financial account associated with the payment card to a financial account associated with the merchant system to pay for the online purchase transaction completed at the computing device.

12. The method of claim **11**, wherein the email address is submitted by the user via a user interface of the merchant system, the user interface accessible by the user via the computing device.

13. The method of claim **11**, wherein the email address is submitted by the user via a user interface of the merchant system, the user interface accessible via an application on the mobile device.

14. The method of claim **11**, wherein the request is transmitted to the mobile device using a push notification service associated with an application installed on the mobile device, the application associated with the payment service.

15. The method of claim **11**, further comprising:

determining a risk score associated with the online purchase transaction; and

based on the risk score relative to a predefined threshold, determining an action for processing the online purchase transaction;

wherein the action includes transmitting the request to the mobile device to obtain a confirmation of the online purchase transaction when the risk score indicates that the online purchase transaction is unlikely to be a fraudulent transaction.

16. The method of claim **15**, wherein the risk score is determined based on at least two of: the specified payment amount, a number of online purchase transactions occurring

in a given duration, a timing of the online purchase transaction or an identity of a merchant associated with the merchant system.

17. The method of claim **15**, wherein the action includes blocking the request to the mobile device when the risk score is higher than the predefined threshold indicating that the online purchase transaction is likely to be a fraudulent transaction.

18. A payment service system for processing a purchase transaction between a user and a merchant system distinct from the payment service system, comprising:

a memory;

a processor configured to execute instructions stored in the memory to:

receive a payment request from the merchant system over a communication network, the payment request being generated by the merchant system in response to receiving a communication identifier submitted by the user to the merchant system to complete a checkout process for the purchase transaction, wherein the checkout process is completed at the merchant system without login credentials or payment information submitted to the merchant system;

identify an account associated with the communication identifier, the account including information associated with a payment card for accessing a financial account associated with the user and information identifying a mobile device;

examine transaction history associated with the account and a payment amount specified in the payment request to determine whether a level of risk associated with the payment request is higher than a predefined threshold;

in an event that the level of risk is higher than the predefined threshold, automatically block the payment request without notifying the user, the level of risk being higher than the predefined threshold indicating that the purchase transaction is potentially fraudulent;

in an event that the level of risk is not higher than the predefined threshold:

send a push notification to the mobile device associated with the communication identifier;

receive a confirmation of the purchase transaction from the user; and

in response to receiving the confirmation from the user, cause a transfer of the payment amount specified in the payment request from the financial account associated with the user to a financial account associated with the merchant system to complete the purchase transaction.

19. The system of claim **18**, wherein the purchase transaction is initiated using a computing device that is separate from the mobile device.

20. (canceled)

21. The system of claim **18**, further wherein the processor is further configured to examine a number of payment requests in a given duration, a timing of the payment request or an identity of the merchant system to determine the level of risk associated with the payment request.

22. The system of claim **18**, wherein the communication identifier includes at least one of an email address or a phone number.

23. A method of purchasing an item, comprising:

receiving, at a merchant system, a communication identifier to complete a checkout process for purchasing the item, the checkout process initiated at a computing device, the submission of the communication identifier being a substitute for entry of payment information or login credentials;

transmitting, by the merchant system, a payment request to the payment service system, wherein the payment request includes the communication identifier and a payment amount corresponding to the item being purchased;

receiving, by the merchant system, a response to the payment request from the payment service system, wherein the response is based on an identification of a payment card of a user associated with the communication identifier, and further based on a user confirmation or rejection obtained through an exchange of messages between a mobile device of the user and the payment service system, wherein the mobile device is identified by the payment service system based on the communication identifier, the mobile device being separate from the computing device at which the checkout process is initiated;

wherein when the response is a success response, the payment amount specified in the payment request is deposited in a financial account associated with the merchant system by the payment service system; and

wherein when the response is a failed response, canceling, by the merchant system based on the failed response, the purchase of the item and notifying the user of the cancellation.

24. The method of claim **23**, wherein the communication identifier is any one of an email address or a phone number.

25. The method of claim **1**, wherein the verification device is the mobile device or a different device.

* * * * *