

8548594



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

November 26, 2024

THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE RECORDS OF THIS OFFICE OF THE FILE WRAPPER AND CONTENTS OF:

APPLICATION NUMBER: 18/197,071
FILING DATE: May 14, 2023
PATENT NUMBER: 11966920
ISSUE DATE: April 23, 2024



Certified by
Katherine Kelly Vidal

Performing the Functions and Duties of the
Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

**POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE
THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

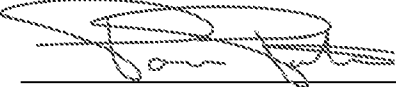
I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint the practitioners of Morgan, Lewis & Bockius LLP, Customer Number **24341** as attorneys or agents to represent the undersigned and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications and patents assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 C.F.R. § 3.73(c), said appointment to be to the exclusion of the inventor(s) and their attorney(s) in accordance with the provisions of 37 C.F.R. § 3.71, provided that, if any one of these attorneys ceases being affiliated with the law firm of Morgan, Lewis & Bockius LLP as partner, counsel, or employee, then the appointment of that attorney and all powers derived therefrom shall terminate on the date such attorney ceases being so affiliated.

Assignee Name and Address: PAYRANGE INC.
 9600 NE Cascades Pkwy, Suite 280
 Portland, OR 97220

SIGNATURE of Assignee of Record

The undersigned whose signature and title is supplied below is authorized to act on behalf of the assignee.

Signature			
Name	Paresh K. Patel, Ph.D., MBA	Date	February 9, 2018
Title	CEO, PayRange Inc.	Telephone	(855) 856-6398

A copy of this form, together with a statement under 37 C.F.R. § 3.73(c) (Form PTO/SB96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 C.F.R. § 3.73(c) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee and must identify the application in which this Power of Attorney is to be filed.

**CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION
 UNDER 37 CFR 1.102(e) (Page 1 of 1)**

First Named Inventor:	Paresh K. Patel	Nonprovisional Application Number (if known):	
Title of Invention:	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i), the prioritized examination fee set forth in 37 CFR 1.17(c), and if not already paid, the publication fee set forth in 37 CFR 1.18(d) have been filed with the request. The basic filing fee, search fee, examination fee, and any required excess claims and application size fees are filed with the request or have been already been paid.
2. The application contains or is amended to contain no more than four independent claims and no more than thirty total claims, and no multiple dependent claims.
3. The applicable box is checked below:

I. Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

- i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.
 ---OR---
 (b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.
- ii. An executed oath or declaration under 37 CFR 1.63 is filed with the application.

II. Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

- i. A request for continued examination has been filed with, or prior to, this form.
- ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
- iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
- iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
- v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /Benjamin Pezzner/	Date May 14, 2023
Name (Print/Typed) Benjamin Pezzner	Practitioner Registration Number 70711

Note: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required in accordance with 37 CFR 1.33 and 11.18. Please see 37 CFR 1.4(d) for the form of the signature. If necessary, submit multiple forms for more than one signature, see below*.

*Total of _____ forms are submitted.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS
First Named Inventor/Applicant Name:	Paresh K. Patel
Filer:	Benjamin H Pezzner
Attorney Docket Number:	104402-5075-US

Filed as Small Entity

Filing Fees for Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	64	64
UTILITY SEARCH FEE	2111	1	280	280
UTILITY EXAMINATION FEE	2311	1	320	320
REQUEST FOR PRIORITIZED EXAMINATION	2817	1	1680	1680

Pages:

Claims:

Miscellaneous-Filing:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
PROCESSING FEE, EXCEPT PROV. APPLS.	2830	1	56	56
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				2400

Electronic Acknowledgement Receipt

EFS ID:	47997575
Application Number:	18197071
International Application Number:	
Confirmation Number:	9843
Title of Invention:	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS
First Named Inventor/Applicant Name:	Paresh K. Patel
Customer Number:	24341
Filer:	Benjamin H Pezzner
Filer Authorized By:	
Attorney Docket Number:	104402-5075-US
Receipt Date:	14-MAY-2023
Filing Date:	
Time Stamp:	02:07:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$2400
RAM confirmation Number	E20235D307586800
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Petitioner Exhibit 1002-0007

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	WebADS.pdf	214104	no	8
			825b04ca4fc7d4524eea378435e15c0ce79f4876		
Warnings:					
Information:					
2		104402-5075-US_Specification.pdf	428456	yes	73
			db3b210498fbf1234a47be44ff043c5e7323a725		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	67	
	Claims		68	72	
	Abstract		73	73	
Warnings:					
Information:					
3	Drawings-only black and white line drawings	104402-5075-US_Drawings.pdf	5978985	no	45
			5adc1fd26e7922d40d33b3ed03dfc67446e021c6		
Warnings:					
Information:					
4	Oath or Declaration filed	104402-5075-US_Declaration.PDF	63528	no	1
			e26c0c0114f33144a0355b8daf93f43344e3b6179		
Warnings:					
Information:					
5	Assignee showing of ownership per 37 CFR 3.73	104402-5075-US_373c.pdf	112017	no	1
			99c16c86dd77b485bdffc9482c556d517ddf45853		

Warnings:					
Information:					
6	Power of Attorney	104402-5075-US_POA.pdf	41808 9764c2f01ba4943c05e8f6af8b2ff06f14fa8488	no	1
Warnings:					
Information:					
7	Track One Request	104402-5075-US_Track_One.pdf	140087 b6d17e59ffa9cb61cd9a04959506f97f4e691b98	no	2
Warnings:					
Information:					
8	Fee Worksheet (SB06)	fee-info.pdf	50742 91872200c40a044d321361ed51e457c00cf a1df0	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			7029727		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	104402-5075-US
		Application Number	
Title of Invention	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2:

<input type="checkbox"/>	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	---

Inventor Information:

Inventor 1					
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Paresh	K.	Patel		
Residence Information (Select One) <input checked="" type="radio"/> US Residency <input type="radio"/> Non US Residency <input type="radio"/> Active US Military Service					
City	Portland	State/Province	OR	Country of Residence ⁱ	US
Mailing Address of Inventor:					
Address 1	9600 NE Cascades Pkwy, Suite 280				
Address 2					
City	Portland	State/Province	OR		
Postal Code	97220	Country ⁱ	US		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button. <input type="button" value="Add"/>					

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).	
<input type="checkbox"/> An Address is being provided for the correspondence information of this application.	
Customer Number	24341
Email Address	<input type="button" value="Add Email"/> <input type="button" value="Remove Email"/>

Application Information:

Title of the Invention	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS		
Attorney Docket Number	104402-5075-US	Small Entity Status Claimed	<input checked="" type="checkbox"/>
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	45	Suggested Figure for Publication (if any)	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5075-US
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

Request Early Publication (Fee required at time of Request 37 CFR 1.219)

Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	<input checked="" type="radio"/> Customer Number	<input type="radio"/> US Patent Practitioner	<input type="radio"/> Limited Recognition (37 CFR 11.9)
Customer Number	24341		
Prefix	Given Name	Middle Name	Family Name
Registration Number			
Prefix	Given Name	Middle Name	Family Name
Registration Number			
Additional Representative Information blocks may be generated within this form by selecting the Add button.			

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	104402-5075-US
		Application Number	
Title of Invention	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status		Pending		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
	Continuation of	17973507	2022-10-25		
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
17973507	Continuation of	17654732	2022-03-14	11481772	2022-10-25
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
17654732	Continuation of	17147305	2021-01-12	11501296	2022-11-15
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
17147305	Continuation of	15603400	2017-05-23	10891614	2021-01-12
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15603400	Continuation of	14458199	2014-08-12	9659296	2017-05-23
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14458199	Continuation in part of	14456683	2014-08-11	9256873	2016-02-09
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14456683	Continuation of	14335762	2014-07-18	9547859	2017-01-17

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	104402-5075-US
		Application Number	
Title of Invention	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS		

Prior Application Status		Patented	<input type="button" value="Remove"/>		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14335762	Continuation of	14214644	2014-03-14	8856045	2014-10-07

Prior Application Status		Expired	<input type="button" value="Remove"/>		
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
14214644	Claims benefit of provisional	61917936	2013-12-18		

Prior Application Status		Patented	<input type="button" value="Remove"/>		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14214644	Continuation in part of	29477025	2013-12-18	D755183	2016-05-03

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
 NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5075-US
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5075-US
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

- Assignee
 Legal Representative under 35 U.S.C. 117
 Joint Inventor
 Person to whom the inventor is obligated to assign.
 Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here.

Organization Name: PAYRANGE INC.

Mailing Address Information For Applicant:

Address 1: 9600 NE Cascades Pkwy, Suite 280

Address 2:

City: Portland State/Province: OR

Countryⁱ: US Postal Code: 97220

Phone Number: Fax Number:

Email Address:

Additional Applicant Data may be generated within this form by selecting the Add button.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5075-US
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS	

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1				
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.				
If the Assignee or Non-Applicant Assignee is an Organization check here. <input type="checkbox"/>				
Prefix	Given Name	Middle Name	Family Name	Suffix
Mailing Address Information For Assignee including Non-Applicant Assignee:				
Address 1				
Address 2				
City		State/Province		
Country i	Postal Code			
Phone Number	Fax Number			
Email Address				
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.				

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5075-US
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS	

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Benjamin Pezzner/			Date (YYYY-MM-DD)	
First Name	Benjamin	Last Name	Pezzner	Registration Number	70711
Additional Signature may be generated within this form by selecting the Add button.					

**METHOD AND SYSTEM FOR PRESENTING
REPRESENTATIONS OF PAYMENT ACCEPTING UNIT
EVENTS**

PRIORITY

[0001] The present application is:

- a continuation of U.S. Patent Application No. 17/973,507, filed October 25, 2022,
- which is a continuation of U.S. Patent Application No. 17/654,732, filed March 14, 2022, and issued as U.S. Patent No. 11,481,772 on October 25, 2022,
- which is a continuation of U.S. Patent Application No. 17/147,305, filed January 12, 2021, and issued as U.S. Patent No. 11,501,296 on November 15, 2022,
- which is a continuation of U.S. Patent Application No. 15/603,400, filed May 23, 2017 and issued as U.S. Patent No. 10,891,614 on January 12, 2021,
- which is a continuation of U.S. Patent Application No. 14/458,199, filed August 12, 2014 and issued as U.S. Patent No. 9,659,296 on May 23, 2017,
- which is a continuation-in-part of U.S. Patent Application Number 14/456,683, filed August 11, 2014 and issued as U.S. Patent No. 9,256,873 on February 9, 2016,
- which is a continuation of U.S. Patent Application Number 14/335,762, filed July 18, 2014 and issued as U.S. Patent No. 9,547,859 on January 17, 2017,
- which is a continuation of U.S. Patent Application Number 14/214,644, filed March 14, 2014 and issued as U.S. Patent No. 8,856,045 on October 7, 2014,
- which claims priority to U.S. Provisional Patent Application Number 61/917,936, filed December 18, 2013.
- U.S. Patent Application Number 14/214,644, filed March 14, 2014, is also a continuation-in-part of U.S. Design Patent Application Number 29/477,025, filed December 18, 2013 and issued as U.S. Design Patent No. D755,183 on May 3, 2016.

The present application is based on and claims priority to these applications, the disclosures of which are hereby incorporated by reference in their entirety.

TECHNICAL FIELD

[0002] The present application relates to the field of payment processing systems, and in particular, to a mobile-device-to-machine payment processing system over a non-persistent network connection.

BACKGROUND

[0003] Vending machines (or “automatic retailing” machines), in the broadest sense, have been around for thousands of years. The first simple mechanical coin operated vending machines were introduced in the 1880s. Modern vending machines stock many different types of products including, but not limited to drinks (e.g., water, juice, coffee, and soda) and edible food products/items (e.g., snacks, candy, fruit, and frozen meals), as well as a wide variety of non-food items. In this fast paced world, vending machines are ubiquitous.

[0004] Vending machines are one type of “payment accepting unit” (payment accepting units are also referred to herein generically as “machines”). A payment accepting unit (or machine) is equipment that requires payment for the dispensing of products and/or services. In addition to vending machines, payment accepting units can also be other machines that require payment for the dispensing of a product and/or services including, but not limited to parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units.

[0005] In using a payment accepting unit, a user will (1) approach the payment accepting unit, (2) determine from the face of the payment accepting unit the product (or service) he/she desires, (3) insert payment (e.g., coins, bills, or payment cards), and (4) input his/her selection into the payment accepting unit using a user interface (e.g., a series of buttons, a key pad, touch screen, or other input mechanism using, for example, the column and row at which a product is located). Based on the user’s inputted selection, technology within the payment accepting unit provides the desired product (or service) to the user.

[0006] As the number of people with Internet-connected mobile devices proliferates, so does the variety of uses for such devices. Mobile payment is a logical extension. There is a large

development effort around bringing mobile payment to the retail sector in an effort to not only provide options to the user, but also increased convenience.

SUMMARY

[0007] Disclosed herein is a payment processing system or, more specifically, a mobile-device-to-machine payment processing system over a non-persistent network connection with hands-free mode and manual mode (sometimes also herein called “swipe” or “swipe-to-pay” mode).

[0008] In some implementations, a method of presenting representations of payment accepting unit events is performed at a device (e.g., the mobile device 150, Figures 5 and 21) with one or more processors, memory, one or more output devices, and two or more communication capabilities. After sending a request to a payment module (e.g., the adapter module 100, Figures 5 and 20), via a first communication capability (e.g., a short-range communication technology/protocol such as BLE), to initiate a transaction with a payment accepting unit (e.g., the payment accepting unit 120, Figures 5 and 19) (sometimes also herein called “machine 120”) associated with the payment module, the method includes obtaining a notification from the payment module via the first communication capability, where the notification indicates an event at the payment accepting unit associated with the payment module. In response to obtaining the notification, the method includes providing a representation of the notification to a user of the mobile device via the one or more output devices of the mobile device (e.g., a message displayed on a display of the mobile device, a vibration produced by a vibration mechanism of the mobile device, an aural alert produced by a speaker of the mobile device, and/or the like).

[0009] In some implementations, a method of retrofitting an offline-payment operated machine to accept electronic payments is performed at a payment module (e.g., the adapter module 100, Figures 5 and 20) with one or more processors, memory, a short-range communication capability (e.g., a short-range communication technology/protocol such as BLE), and a first interface module configured to couple the payment module with a control unit of an offline-payment operated machine (e.g., the payment accepting unit 120, Figures 5 and 19) (sometimes also herein called “machine 120”). The method includes receiving a transaction request via the short-range communication capability from a respective mobile device to perform

a transaction with the offline-payment operated machine. The method includes validating the transaction request, where validation of the transaction request indicates that the respective mobile device is authorized to initiate payment for the transaction by a remote server (e.g., the server 130, Figures 5 and 22) via the long-range communication capability (e.g., the long-range communication technology/protocol such as GSM, CDMA, or Wi-Fi). In accordance with a determination that the transaction request is valid, the method includes causing the offline-payment operated machine to perform the requested transaction by issuing a signal to perform the transaction to the control unit of the offline-payment operated machine via the first interface module.

[0010] In some implementations, a device (e.g., the machine 120, (Figures 5 and 19), the adapter module 100 (Figures 5 and 20), the mobile device 150 (Figures 5 and 21), the server 130 (Figures 5 and 22), or a combination thereof) includes one or more processors and memory storing one or more programs for execution by the one or more processors, the one or more programs include instructions for performing, or controlling performance of, the operations of any of the methods described herein. In some implementations, a non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a device (e.g., the machine 120, (Figures 5 and 19), the adapter module 100 (Figures 5 and 20), the mobile device 150 (Figures 5 and 21), the server 130 (Figures 5 and 22), or a combination thereof) with one or more processors, cause the computer system to perform, or control performance of, the operations of any of the methods described herein. In some implementations, a device (e.g., the machine 120, (Figures 5 and 19), the adapter module 100 (Figures 5 and 20), the mobile device 150 (Figures 5 and 21), the server 130 (Figures 5 and 22), or a combination thereof) includes means for performing, or controlling performance of, the operations of any of the methods described herein.

[0011] The subject matter described herein is particularly pointed out and distinctly claimed in the concluding portion of this specification. Objectives, features, combinations, and advantages described and implied herein will be more readily understood upon consideration of the following detailed description of the invention, taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Figure 1 is a schematic diagram that shows three zones: a “communication zone” (e.g., Bluetooth range), an “authorization zone,” and a “payment zone” in accordance with some implementations.

[0013] Figure 2 is a schematic diagram that shows the three zones of Figure 1 with multiple users therein in accordance with some implementations.

[0014] Figure 3 is a table that illustrates the hands-free credit or alert user principle in accordance with some implementations.

[0015] Figure 4 is a flow chart showing the logging received signal strength indicator (RSSI) information in accordance with some implementations.

[0016] Figure 5 is a block schematic that shows elements of the payment processing system including, but not limited to, the adapter module, the machine, the mobile device, and servers, as well as communications therebetween in accordance with some implementations.

[0017] Figure 6 is a block schematic that shows three areas of encryption used (each is bi-directional) between the adapter module, the machine, the mobile device, and/or servers in accordance with some implementations.

[0018] Figure 7 is a block diagram that shows communications, messaging, vending sequence, and purchase flow between the adapter module, the mobile device, and a system management server in accordance with some implementations.

[0019] Figure 8A is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) when the user enters the “communication zone” (e.g., Bluetooth range) in accordance with some implementations.

[0020] Figure 8B is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) when the user enters the “authorization zone” in accordance with some implementations.

[0021] Figure 8C is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) when the user enters the “payment zone” and, in particular, detailing a hands-free mode embodiment and a swipe mode embodiment in accordance with some implementations.

[0022] Figure 8D is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) in a vending transaction including a loop for multiple transactions in accordance with some implementations.

[0023] Figure 8E is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) in the login mode in accordance with some implementations.

[0024] Figure 8F is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) during boot-up of the adapter module in accordance with some implementations.

[0025] Figure 8G is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) during an account check/update process in accordance with some implementations.

[0026] Figures 9A-9E are flow charts that show example steps and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) in accordance with some implementations.

[0027] Figures 10A-10D show a mobile device with a graphical representation of a mobile application shown thereon, the mobile application being used as part of the mobile-device-to-machine payment processing system in accordance with some implementations.

[0028] Figure 11 is a perspective view of the in-line dongle adapter module in accordance with some implementations.

[0029] Figure 12 is a front plan view of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0030] Figure 13 is a back plan view of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0031] Figure 14 is a side view of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0032] Figure 15 is a first end view of a connector receptacle of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0033] Figure 16 is a second end view of a connector receptacle of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0034] Figure 17 is a perspective view taken from the first end of the in-line dongle adapter module of Figure 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for illustrative purposes in accordance with some implementations.

[0035] Figure 18 is a perspective view taken from the second end of the in-line dongle adapter module of Figure 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for illustrative purposes in accordance with some implementations.

[0036] Figure 19 is a perspective view of the in-line dongle adapter module of Figure 11 within a vending machine in accordance with some implementations.

[0037] Figure 20 is a block diagram of an adapter module in accordance with some implementations.

[0038] Figure 21 is a block diagram of a mobile device in accordance with some implementations.

[0039] Figure 22 is a block diagram of a server in accordance with some implementations.

[0040] Figure 23 is a schematic flow diagram of a process for authenticating a user to perform a transaction in the payment processing system in accordance with some implementations.

[0041] Figure 24A is a block diagram of a packet of information broadcast by the payment module (sometimes also herein called the “adapter module”) in accordance with some implementations.

[0042] Figure 24B is a block diagram of an authorization request in accordance with some implementations.

[0043] Figure 24C is a block diagram of an authorization grant token in accordance with some implementations.

[0044] Figure 24D is a block diagram of transaction information generated by the payment module in accordance with some implementations.

[0045] Figure 25A illustrates a schematic flow diagram of a process for providing a representation of a machine event at a mobile device in accordance with some implementations

[0046] Figure 25B is a schematic flow diagram of a process for processing acknowledgment information in the payment processing system in accordance with some implementations.

[0047] Figures 26A-26D illustrate example user interfaces for providing a representation of a machine event at a mobile device in accordance with some implementations.

[0048] Figures 27A-27B illustrate a flowchart diagram of a method of presenting representations of payment accepting unit events in accordance with some implementations.

[0049] Figure 28A illustrates a block diagram of an offline-payment operated machine in accordance with some implementations.

[0050] Figure 28B illustrates signals sampled by the payment module in accordance with some implementations.

[0051] Figures 29A-29B illustrate a flowchart diagram of a method 1600 of retrofitting an offline-payment operated machine to accept electronic payments in accordance with some implementations.

[0052] Figure 30 illustrates a flowchart diagram of a method of enabling a payment operated machine to accept electronic payments in accordance with some implementations.

[0053] Like reference numerals refer to corresponding parts throughout the several views of the drawings.

DETAILED DESCRIPTION

[0054] Disclosed herein is a payment processing system or, more specifically, a mobile-device-to-machine payment processing system for processing transactions over a non-persistent network connection. The mobile-device-to-machine payment processing system disclosed herein focuses on the unattended retail space (e.g., a payment accepting unit 120, sometimes also herein called a “machine 120”). More specifically, the mobile-device-to-machine payment processing system disclosed herein allows a user (having a mobile device 150 with a mobile application 140 thereon) to make a cashless purchase from a payment accepting unit 120 (having an adapter module 100 associated therewith).

[0055] The mobile-device-to-machine payment processing system described herein can be implemented with one or more of the following features: easy installation feature, a non-persistent network connection feature; a manual (swipe to pay) mode feature; a hands-free mode feature; and a multiple vending transactions (multi-vend) feature.

[0056] Easy Installation: Installation is very easy, requires no tools, requires no configuration, and takes as little as 30 seconds. This is accomplished by using an adapter module 100 (sometimes also herein called “payment module 100”) such as an in-line dongle (a hardware device with software thereon) design for in-line insertion within a multi-drop bus (MDB) of a payment accepting unit 120 (e.g., a vending machine) (sometimes also herein called ‘the machine 120”). Installation is as simple as “powering down” (turning off) the machine 120, identifying the “wire” that connects with a payment receiving mechanism (e.g., the coin mechanism), disconnecting the wire (so that there are two loose ends, such as a male connection end or adapter of an MDB and a female connection end or adapter of an MDB), plugging (inserting) the adapter module 100 in serial (“in-line”) with the wire (e.g., connecting the MDB female adapter to a male adapter of the adapter module 100 and connecting the MDB male adapter to a female adapter of the adapter module 100), tucking the wire and the installed adapter

module 100 back into position, and “powering up” (turning on) the machine 120. Most vending machines made since 1995 have this industry standard MDB technology that would allow this easy 30-second installation. On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g., cash).

[0057] Non-persistent Network Connection: Although payment accepting units (or “machines”) that accept only cash (e.g., paper currency and coins) may not require a connection (persistent or non-persistent) to a network, traditional payment accepting units that accept cashless payments (e.g., credit cards, debit cards, and alternative mobile device payment methods using, for example, smart phones) require a persistent connection to a network (wired or wireless) to facilitate the cashless payments. In other words, without a persistent (ongoing or accessible on demand) network connection, traditional payment accepting units cannot accept cashless payments. Most traditional payment accepting units that accept cashless payments include the technology to accomplish this persistent network connection that allows them to connect to a remote server. If the network connection to a traditional machine is temporarily interrupted, cashless payments will be temporarily unavailable. If the machine is located in a location where no network connection is available, cashless payments is not possible. In addition to using a mobile device 150 as an intermediary between the payment accepting units 120 and the server 130, the mobile-device-to-machine payment processing system described herein minimizes (i.e., the manual mode) or eliminates (i.e., the hands-free mode) user interaction with the mobile device 150. Further, in some implementations, the mobile-device-to-machine payment processing system described herein facilitates the acceptance of cashless payments without requiring any network connection near the payment accepting unit 120. In some implementations, when the mobile-device-to-machine payment processing system described herein is located in a remote location where network connection is unavailable, the mobile-device-to-machine payment processing system, therefore, can still accept cashless payments.

[0058] Manual (Swipe-to-Pay) Mode: Using a “swipe-to-pay” feature (or just “swipe”) refers to a user’s action implemented on his/her mobile device 150 where he/she quickly brushes his/her finger (or other pre-determined interaction) on the mobile device’s touch screen 152 (Figures 10A-10D) or other input devices associated with the mobile device 150. From the user’s

perspective, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g., a vending machine). The mobile application 140 might display (on the touch screen 152) a prepaid balance that the user “swipes” to transfer payment to the payment accepting unit 120. The user could observe the transferred funds on the touch screen 152 of the mobile device 150 and/or on the display 122, 124 (Figure 19) of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150 and this may be shown on the touch screen 152 of the mobile device 150.

[0059] Hands-Free Mode: A “hands-free pay” feature (or just “hands-free”) would most likely be used with “favorite” payment accepting units 120 (e.g., a frequently used vending machine at a user’s work or school). From the user’s perspective, he/she would approach the favorite payment accepting unit 120 and notice that the display 122, 124 (Figure 19) of the payment accepting unit 120 shows funds available, he/she would select the product or service using the payment accepting unit’s input mechanisms (e.g., buttons 126 or a touch screen display 124 shown in Figure 19), and he/she would retrieve dispensed services or products. It would be that simple. More specifically, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g., a vending machine). The user may leave the mobile device 150 in a pocket, purse, briefcase, backpack, or other carrier. As the user approaches the payment accepting unit 120 and is in approximately “arm’s-length” distance (e.g., 3 to 5 feet) of the payment accepting unit 120, the user could observe the transferred funds on the display 122, 124 (Figure 19) of the payment accepting unit 120. The transaction is completed just as if cash was inserted into the payment accepting unit 120 with the user inputting his/her selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150. Figure 3 details when the hands-free mode would be available.

[0060] Multiple Vending Transactions (Multi-Vend): Both the manual and hands-free modes could be used multiple times in sequence (implemented, for example, as a loop) so that a user may make multiple purchases. After making his/her first selection and receiving his product (or service), the user would observe that additional funds were available on the display 122, 124

(Figure 19) on the payment accepting unit 120. He/she could make another selection (or multiple selections) and receive additional product(s) (or service(s)). More specifically, the display 122, 124 (Figure 19) may reset as if the transaction is complete, but then, because the user is still standing in range, the mobile application 140 would send another credit to the payment accepting unit 120, allowing for a second purchase. When the user walks away, the system clears (e.g., returns unused funds to the application 140 on the mobile device 150).

[0061] The features described above, alone or in combination with other features described herein will revolutionize the hundred billion dollar automated retail industry. The hardware is very low cost and there are no reoccurring fees because no cellular connection is required on the machine 120. Using the mobile-device-to-machine payment processing system described herein, operators of machines 120 can increase frequency of visits by purchasers and items sold with each visit.

[0062] The mobile-device-to-machine payment processing system described herein may be implemented as an apparatus, system, and/or method for enabling payments to a machine 120 via a mobile device 150. The mobile-device-to-machine payment processing system may be better understood with reference to the drawings, but the shown mobile-device-to-machine payment processing system is not intended to be of a limiting nature.

DEFINITIONS

[0063] Before describing the mobile-device-to-machine payment processing system and the figures, some of the terminology should be clarified. Please note that the terms and phrases may have additional definitions and/or examples throughout the specification. Where otherwise not specifically defined, words, phrases, and acronyms are given their ordinary meaning in the art. The following paragraphs provide some of the definitions for terms and phrases used herein.

[0064] Adapter Module 100: As shown in Figures 1 and 2, the adapter module 100 (sometimes also herein called the “payment module 100”) is a physical device that is installed in a machine 120 (a payment accepting unit 120). The shown adapter module 100 is an in-line dongle (a hardware device with software thereon) device that may be inserted in-line within a multi-drop bus (MDB) of a machine 120. The adapter module 100 bridges the communication between the machine 120 and a mobile device 150. Although described as a unique component,

it should be noted that the adapter module 100 could be implemented as a plurality of devices or integrated into other devices (e.g., components of a machine 120). In its unique component form, the adapter module 100 can be easily inserted into a machine 120 so that the machine 120 is able to perform new features with the assistance of the adapter module 100. Figure 20 shows components associated with the adapter module 100. As shown in Figure 20, the communications unit 770 of the adapter module 100 includes short-range communication capability 776 (e.g., Bluetooth mechanisms). The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g., a computer or a payment accepting unit) as long as the components are associated with each other.

[0065] Mobile Device 150 and Application 140 (also referred to as a “mobile application,” “mobile app,” or “app”): In general, a mobile device 150 may be a user’s personal mobile device 150. The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. The mobile device 150 and the application 140, however, are not “trusted” in that the communications (transmissions) it passes are encrypted. Encrypted (secured) communications are undecipherable (unencryptable, unreadable, and/or unusable) by the mobile device 150. This keeps the communications passed between the adapter module 100 and the server 130 secured and safe from hacking. Mobile devices include, but are not limited to smart phones, tablet or laptop computers, or personal digital assistants (PDAs), smart cards, or other technology (e.g., a hardware-software combination) known or yet to be discovered that has structure and/or capabilities similar to the mobile devices described herein. The mobile device 150 preferably has an application (e.g., the application 140) running on it. The term “app” is used broadly to include any software program(s) capable of implementing the features described herein. Figures 10A-10D show user interfaces for the application 140 displayed by the mobile device 150. It should be noted that the phrase “mobile device” can be assumed to include the relevant app unless specifically stated otherwise. Similarly, it should be noted that an “app” can be assumed to be running on an associated mobile device unless specifically stated otherwise. Figure 21 shows components associated with the mobile device 150. The shown example may be divided into multiple distinct components that are associated with each other or the example may

be incorporated into or drawn from other technology (e.g., the cell phone itself) as long as the components are associated with each other.

[0066] Payment accepting unit 120 (or Machine 120): A payment accepting unit 120 (or the machine 120) is equipment that requires payment for the dispensing of an product and/or service. Payment accepting units 120 may be vending machines, parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units 120. Some payment accepting units 120 can accept cashless payments (payments other than cash (paper currency and coins)) by accepting payment from, for example, credit cards, debit cards, and mobile devices.

[0067] Network Connections: For purposes of this discussion, a persistent network connection is a wired or wireless communications connection that is ongoing (e.g., a dedicated connection, a dedicated online connection, and/or a hardwired connection) or accessible on demand (e.g., the ability for the machine to make a temporary connection to a server or the ability for the user to contact a server from his mobile device). Typically the persistent network connection has been conducted over “long-range communication technology” or “long-range communication protocol” (e.g., hardwired, telephone network technology, cellular technology (e.g., GSM, CDMA, or the like), Wi-Fi technology, wide area network (WAN), local area network (LAN), or any wired or wireless communication technology over the Internet that is known or yet to be discovered). Traditionally, machines that accept payment other than cash require a persistent (ongoing or accessible on demand) connection to a network to facilitate payment. This is true for machines that accept, for example, credit cards and debit cards. The payment accepting units 120 described herein do not require a traditional persistent network connection. The user’s mobile device 150 acts as a communication bridge between the adapter module 100 and the server 130. Communications between user mobile devices 150 and the servers (e.g., a system management server 130 and/or a funding source server 160) take place using long-range communication technology. Communications between user mobile devices 150 and the adapter module 100 of the payment accepting unit 120 take place using “short-range communication technology” or “short-range communication protocol” (e.g., Bluetooth (such as Bluetooth 4.0, Bluetooth Smart, Bluetooth Low Energy (BLE)), near-field communication (NFC), Ultra Wideband (UWB), radio frequency identification (RFID), infrared wireless,

induction wireless, or any wired or wireless technology that could be used to communicate a small distance (approximately a hundred feet or closer) that is known or yet to be discovered). Therefore, neither the adapter module 100 nor the payment accepting unit 120 requires a traditional persistent long-range wireless network connection. The communications technology shown in the figures may be replaced with alternative like communications technology and, therefore, specific shown communications technologies are not meant to be limiting. For example, Wi-Fi technology could be replaced with another long-range communication technology.

[0068] Server: A server is the host processing server that may be operated by the company running the payment processing system. For each user, the server 130 preferably maintains at least one “virtual wallet” having at least one “balance” (which can be \$0) of designated funds for which the server 130 keeps an accounting. The balance may represent, for example, “cash” or it may be a “promotional value” that represents funds that may be spent under certain circumstances. If these funds begin to be depleted, the user may be notified (e.g., via the application 140 on the mobile device 150) that additional funds need to be designated and/or transferred. Alternatively, funds from other sources (e.g., the funding source server 160) may be automatically transferred to restore a predetermined balance. The balance may also be increased based on a promotion (e.g., points earned or coupons). As shown in Figure 22, the server includes appropriate processors 950, memory 960 (which would keep an accounting of the user’s balance in a manner similar to a gift card), and communication systems 970. As shown in Figure 22, the communications unit 970 of the server 130 includes long-range communication capability 972 (e.g., cellular technology and/or Wi-Fi mechanisms). The server 130 also includes a security unit 955 for encrypting and decrypting messages. The server 130 receives an authorization request (sometimes also herein called an “AuthRequest”) from the adapter module 100 (via a mobile device 150) and, if funds are available, returns an authorization grant (sometimes also herein called an “AuthGrant” or an “authorization grant token”) for funds. Figure 22 shows components associated with the server 130. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g., a computer or a main frame) as long as the components are associated with each other.

[0069] Advertise Presence: Each adapter module 100 advertises its presence by broadcasting signals (advertising broadcast signals) to mobile devices in the zones 102, 104, 106. Each adapter module 100 can listen to other adapter modules' advertisements.

[0070] Received Signal Strength Indicator (RSSI): The adapter module 100 may have a self-calibrating signal strength to determine zone thresholds (e.g., a payment zone threshold and an authentication zone threshold). At the time the user selects an item (product or service) from the payment accepting unit 120, the Received Signal Strength Indicator (RSSI) is logged. At this moment, it is presumed the user is within "arm's-length" (which may be a predetermined length approximating the distance of a user standing in front of a machine for the purpose of making a purchase) from the payment accepting unit 120. A mathematical computation (i.e., In-Range Heuristics) is conducted to derive the optimal RSSI threshold at which point payment should be triggered by an application 140 on a mobile device 150. The threshold may be payment accepting unit specific and can vary over a period of time. This optimal zone threshold is preferably reported to the mobile device 150 during an initial handshake.

[0071] In-Range Heuristics: A mathematical computation that determines the RSSI threshold to determine when a user is in the authorization zone 104 and/or the payment zone 102. This computation can take into consideration numerous historical data points as well as transaction specific information such as which the mobile device 150 is being used, payment accepting unit type, among other factors. Preferably the RSSI is logged while the user is making his selection (this is the one time in the entire process that the user definitely will be "in range" (e.g., they will be arm's length from the machine 120 because they are physically interacting with the machine 120). The type of user mobile device 150, accelerometer data (e.g., is the user moving or stationary), and/or other information may also be logged while the user is making his selection. The adapter module 100 can give a reference RSSI for the payment zone 102 for the machine 120, and the application 140 can make a +/- adjustment based on the specific mobile device 150 on which it is installed. Over a period of time, the payment processing system continues to improve itself based on additional data points.

[0072] Authorization Request ("AuthRequest:): When a user enters the authorization zone 104, the mobile device 150 notifies the adapter module 100 and the adapter module 100 sends a secured authorization request (e.g., the encrypted authorization request) as a "message"

(also referred to as a communication or transmissions) to the server 130 via the mobile device 150. Encryption may be performed by a security unit 755 (Figure 20) with security technology (e.g., encryption and decryption means) that may be associated with the processing unit 750 and/or the memory 760. Significantly, the AuthRequest is a request for authorization of funds, not a request for authorization of a transaction. The purpose of the funds is irrelevant to the server 130.

[0073] Authorization Grant Token (“AuthGrant”): This is a “message” (also referred to as a communication or transmissions) encrypted by the security unit 955 (Figure 22) with security technology (e.g., encryption and decryption means) of the server 130 with the unique private key corresponding to the adapter module 100. The secured authorization grant (e.g., the encrypted authorization grant) is passed from the server 130 to the adapter module 100 via the mobile device 150 in the form of a message. The mobile device 150, however, is not able to decrypt and/or read the message. The authorization grant is in response to the authorization request. The amount of the funds granted by the AuthGrant may be determined by factors including, but not limited to, the amount of funds available (or, if funds are not available, a mini-loan could be granted), a pre-authorized amount (e.g., set by the server, set by the user during set-up, set by the funding source, or a standard amount), limited by time (e.g., only a certain amount per hour, or a predetermined amount at specific times of the day), limited to the maximum amount of an item on the machine (or enough for two or three items in the machine), or one or more of these and other factors. Significantly, the AuthGrant makes the funds available, but does not authorize a transaction. The AuthGrant may have an associated expiration period in that it may expire if it is not used in a pre-determined time period. The length of time before the AuthGrant expires may be determined by factors including, but not limited to, the trustworthiness of the user (e.g., the user has a long history with the payment processing system or some known provider (e.g., credit card provider, bank, or credit union), the user has a good credit rating, or the user has a large wallet balance), a pre-authorized time period (e.g., set by the server, set by the user during set-up, set by the funding source, or a standard time period), limited by time (e.g., predetermined time periods at specific times of the day such as longer times during breakfast, lunch, and dinner), limited by the machine or the products or services sold in the machine, limited by the number of other users near the machine (e.g., if it is a crowded machine, the AuthGrant may expire faster), or one or more of these and other factors. The AuthGrant

remains valid until it expires or some other event occurs to end its validity (e.g., the user cancels it). This means that under normal circumstances the mobile device 150 will hold the AuthGrant authorizing use of funds for a pre-determined time period that will allow the user sufficient time to make a purchase. The authorized amount may be considered to be the “wallet balance” that is held in a virtual “wallet.”

[0074] Synchronization: Time may be synchronized to the adapter module 100 from the server 130. The server 130 sends time information with encrypted messages and the adapter module 100 uses the time encoded in the messages for synchronization.

[0075] The mobile-device-to-machine payment processing system and components thereof may have associated hardware, software, and/or firmware (a variation, subset, or hybrid of hardware and/or software). The term “hardware” includes at least one “processing unit,” “processor,” “computer,” “programmable apparatus,” and/or other known or yet to be discovered technology capable of executing instructions or steps (shown as the processing unit 750 in Figure 20, the processing unit 850 in Figure 21, and the processing unit 950 in Figure 22). The term “software” includes at least one “program,” “subprogram,” “series of instructions,” or other known or yet to be discovered hardware instructions or hardware-readable program code. Software may be loaded onto hardware (or firmware) to produce a “machine,” such that the software executes on the hardware to create structures for implementing the functions described herein. Further, the software may be loaded onto the hardware (or firmware) so as to direct the mobile-device-to-machine payment processing system (and components thereof) to function in a particular manner described herein or to perform a series of operational steps as described herein. “Hardware” such as the adapter module 100, the mobile device 150, and the payment accepting unit 120 may have software (e.g., programs and apps) loaded thereon. The phrase “loaded onto the hardware” also includes being loaded into memory (shown as the memory 760 in Figure 20, the memory 860 in Figure 21, and the memory 960 in Figure 22) associated with or accessible by the hardware. The term “memory” is defined to include any type of hardware (or other technology) -readable media (also referred to as computer-readable storage medium) including, but not limited to, attached storage media (e.g., hard disk drives, network disk drives, servers), internal storage media (e.g., RAM, ROM, EPROM, FLASH-EPROM, or any other memory chip or cartridge), removable storage media (e.g., CDs, DVDs, flash drives, memory cards, floppy disks, flexible disks), firmware, and/or other known or yet to be discovered storage media.

Depending on its purpose, the memory may be transitory and/or non-transitory. Appropriate “messages,” “communications,” “signals,” and/or “transmissions” (that includes various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof) over appropriate “communication paths,” “transmission paths,” and other means for signal transmission including any type of connection between two elements on the payment processing system (e.g., the adapter module 100, the mobile device 150, the payment accepting unit 120, hardware systems and subsystems, and memory) would be used as appropriate to facilitate controls and communications.

[0076] It should be noted that the terms “programs” and “subprograms” are defined as a series of instructions that may be implemented as software (i.e. computer program instructions or computer-readable program code) that may be loaded onto a computer to produce a “machine,” such that the instructions that execute on the computer create structures for implementing the functions described herein or shown in the figures. Further, these programs and subprograms may be loaded onto a computer so that they can direct the computer to function in a particular manner, such that the instructions produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The programs and subprograms may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. The phrase “loaded onto a computer” also includes being loaded into the memory of the computer or a memory associated with or accessible by the computer. Separate, albeit interacting, programs and subprograms may be associated with the adapter modules 100, the server 130, and the mobile device 150 (including the mobile application 140) and these programs and subprograms may be divided into smaller subprograms to perform specific functions.

[0077] The terms “messages,” “communications,” “signals,” and/or “transmissions” include various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof. Appropriate technology may be used to implement the “communications,” “signals,” and/or “transmissions” including, for example,

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

[0078] When used in relation to “communications,” “signals,” and/or “transmissions,” the terms “provide” and “providing” (and variations thereof) are meant to include standard means of provision including “transmit” and “transmitting,” but can also be used for non-traditional provisions as long as the “communications,” “signals,” and/or “transmissions” are “received” (that can also mean obtained). The terms “transmit” and “transmitting” (and variations thereof) are meant to include standard means of transmission, but can also be used for non-traditional transmissions as long as the “communications,” “signals,” and/or “transmissions” are “sent.” The terms “receive” and “receiving” (and variations thereof) are meant to include

standard means of reception, but can also be used for non-traditional methods of obtaining as long as the “communications,” “signals,” and/or “transmissions” are “obtained.”

[0079] The term “associated” is defined to mean integral or original, retrofitted, attached, connected (including functionally connected), positioned near, and/or accessible by. For example, if the user interface (e.g., a traditional display 122 (Figure 19), a touch screen display 124 (Figure 19), a key pad 126 (Figure 19), buttons 126 (Figure 19, shown as part of the key pad 126), a keyboard (not shown), and/or other input or output mechanism) is associated with a payment accepting unit 120, the user interface may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120. Similarly, adapter modules 100 may be associated with payment accepting units 120 in that the adapter modules 100 may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120.

SYSTEM OVERVIEW

[0080] Figures 5, 6, and 7 together show major components of the mobile-device-to-machine payment system and the interactions there-between.

[0081] As shown, the adapter module 100 functionally connected bi-directionally to the payment accepting unit 120 via a wired serial connection such that no security is necessary. The adapter module 100 is also functionally connected bi-directionally to the mobile device 150 (and its installed mobile application 140) via short-range communication technology (e.g., a Bluetooth connection). Because the mobile device 150 is not a “trusted” link (e.g., it could be hacked by a user), only secured communications (transmissions) are passed between the adapter module 100 and the mobile device 150. This keeps communications secured and safe from hacking. The mobile device 150 (and its installed mobile application 140) is also functionally connected bi-directionally to a system management server 130 and/or a funding source server 160 via long-range communication technology (e.g., Wi-Fi or Cellular connection) that preferably has appropriate security (e.g., SSL security). Security between the mobile device 150 and the system management server 130 has the advantage of protecting communications from the mobile device 150 to the system management server 130 that may include sensitive data and may not be encrypted. The system management server 130 and the funding source server 160 may be

connected via a wired Internet connection with SSL security. The system management server 130 may be connected via a wired Internet connection with SSL security to an operators' server 170. Although not necessary to implement a purchase transaction, for other purposes (e.g., inventory), the operators' server 170 may be connected to the payment accepting unit 120 using a handheld computer sync or a cellular connection.

[0082] Also, a unique private key may be used to securely transmit encrypted messages between the adapter module 100 and the system management server 130 (although the encrypted transmissions would most likely be routed through the mobile device 150). The server 130 stores a private key for each adapter module 100, and this key is only known to the adapter module 100 and the server 130. No intermediary is privy to this key (especially not the mobile device 150). When the adapter module 100 and the server 130 communicate messages (e.g., AuthRequest and AuthGrant), the security unit 755 of the adapter module 100 encrypts the message with its private key and passes the message to the mobile device 150. The mobile device 150 (which preferably cannot decrypt the message) passes the encrypted message to the server 130. The server 130 is able to decrypt the message using the security unit 955 of the adapter module 100 and the unique private key. The security unit 955 of the server 130 uses this same unique private key to encrypt messages to the adapter module 100 and sends the message to the mobile device 150 to relay to the adapter module 100 that is able to decrypt the message using the security unit 755 of the adapter module 100 and the unique private key.

[0083] Figure 7 shows specific communications and messaging with a vending sequence (the numbers to the left of the communications and messaging) between the adapter module 100, the mobile device 150, and the system management server 130. These communications are discussed in more detail in the discussion pertaining to the schematic flow diagrams (Figures 8A-8G) and the flow charts (Figures 9A-9E).

[0084] It should be noted that Figures 5, 6, and 7 are examples, and are meant to help in the understanding of the mobile-device-to-machine payment system. For example, the shown long-range communications technology may be replaced with alternative long-range communications technology known or yet to be discovered, the shown short-range communication technology may be replaced with alternative short-range communication technology known or yet to be discovered, and the shown security may be replaced with

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

ADAPTER MODULE

[0085] Figures 11-18 show views of adapter module 100a (referred to generally as adapter module 100). Adapter module 100 is a relatively low cost hardware component that is pre-configured to work with the industry standard multi-drop bus (MDB). On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g., cash).

[0086] The shown adapter modules 100 are preferably designed to be used as an in-line dongle for in-line insertion within, for example, a MDB of a machine 120. The wire used in MDB technology uses male and female connection ends or adapters to allow the attachment of peripherals. In the case of a vending machine, the wire with the connection ends or adapters would be present to allow the attachment of a payment receiving mechanism (e.g., a coin mechanism). The MDB male and female adapters 700, 710 may be separated (as shown in Figures 17-18). The adapter module 100a in Figures 11 and 17-18 has a male adapter 720 and a female adapter 730. The adapter module 100a may be plugged (inserted) in serial (“in-line”) with the wire. For example, the MDB female adapter 710 may be connected to the male adapter 720 of the adapter module 100 and the MDB male adapter 700 may be connected to the female adapter 730 of the adapter module 100. The resulting in-line configuration is shown in Figure 19. It should be noted that the adapter modules 100 are designed to allow pass-through communications so that if the mobile-device-to-machine payment processing system is not enabled (e.g., for a particular purchase or simply turned off) the MDB functions as though the adapter module 100 is not there and the machine 120 can function normally.

HANDS-FREE MODE

[0087] Summarily, if it is available, a hands-free mode, from the user's perspective, would allow the user to approach a favorite payment accepting unit 120 and notice that the display (e.g., the displays 122 or 124 shown in Figure 19) associated with the payment accepting unit 120 shows funds available (e.g., the wallet balance), he would select the product or service using input mechanisms (e.g., buttons 126 or a touch screen display 124 shown in Figure 19) associated with the payment accepting unit 120, and he would retrieve his dispensed services or products.

[0088] During an initial handshake with the mobile device 150 (when the user is within range), the adapter module 100 reports to the mobile device 150 whether or not hands-free mode is available. If it is available, the installed mobile application 140 automatically connects to the payment accepting unit 120 without the user having to interact with the mobile device 150. The user observes that funds are available on the display 122, 124 of the payment accepting unit 120 and completes the purchase transaction as if cash was inserted in the machine 120 by inputting his selection on the payment accepting unit 120. The payment accepting unit 120 dispenses the product or service. After the selection is made, the change is returned to the mobile device 150.

[0089] Whether hands-free payment is available is determined by factors including, but not limited to whether if other mobile devices 150 are in range, if other adapter modules 100 are in range, if there are any alerts, if the payment trigger threshold is having wide variances and so deemed unstable, or if the payment accepting unit operator (e.g., a vending machine operator) has opted to disable hands-free mode for the payment accepting unit 120. In the latter instance, operators can disable via a maintenance mobile device 150, as well as through the operators' server 170 and/or the system management server 130.

[0090] Figure 3 is a table that shows considerations, conditions, or factors that may be used to determine whether the hands-free pay feature is available. Starting at the "Favorite?" column, this indicates whether the payment accepting unit 120 is a favorite machine. Preferably the hands-free pay feature is only available for use with "favorite" payment accepting units 120 (e.g., a vending machine at work or school). The "Alert" column has to do with whether there is some reason (e.g., there are too many users in range) that the hands-free pay feature should not work and, if there is such a reason, the user will be notified (alerted) and may be able to use the

manual mode to resolve the alert and/or complete the transaction. Figure 3 shows situations in which a user is or is not able to make hands-free purchases from a machine 120 using a mobile application 140 on his mobile device 150. It should be noted that the shown interface is an example. For example, some of the features could be automated or pre-selected. (It should be noted that the left hand column, the “Tab” column, relates to whether the selected tab on the mobile application 140 is “all” or “favorite.” Figures 10A-10D all show these tabs. Unlike the other columns in Figure 3, this column has more to do with the functionality and view of the application 140 than specifically with the hands-free feature. The tabs would allow a user to select whether he wanted to be alerted when he was in range of all payment accepting units 120 or just “favorite” payment accepting units 120 and the application 140 would show the appropriate view.)

[0091] Balance Display: An optional feature of the mobile-device-to-machine payment system that is particularly helpful in the hands-free mode (although it may be available in the manual mode and/or in a multiple-vend scenarios) is when the user’s mobile device 150 sends “credit” to the payment accepting unit 120 (either via hands-free payment or through a manual swipe), the wallet balance is sent to the payment accepting unit 120 that is then displayed to the user on a display 122, 124 of the machine 120. This is particularly beneficial during hands-free mode when the user does not retrieve the mobile device 150 and, therefore, may not know the balance. Also, in a multiple-vend scenario the user would not have to calculate a remaining balance.

[0092] An example of a hands-free, multiple-vend scenario where a balance is displayed by the payment accepting unit 120, follows: The user has \$5.00 in his/her virtual wallet as that is the amount that has been authorized (the AuthGrant being stored on the mobile device 150). The user walks up to the payment accepting unit 120 and \$5.00 is displayed on the display 122, 124 of the payment accepting unit 120 since hands-free mode was enabled and credit was sent (e.g., via the short-range communication capability) to the payment accepting unit 120. The user makes a selection of \$1.50 by interacting (e.g., pressing buttons) with the machine 120. The item (product or service) is dispensed and the “change” is “returned” (e.g., via the short-range communication capability) to the virtual wallet. But since the user is still standing in the payment zone 102, the remaining wallet balance of \$3.50 is sent to the payment accepting unit 120 and displayed so that the user can now see that he/she has a \$3.50 balance. (It should be noted that

the authorized funds may remain on the machine 120 and not be transferred back to the mobile device 150 between transactions.) The user decides to purchase a \$1.50 item, and the transaction is completed as usual (e.g., by interacting with the machine 120). Now the user is still standing in the payment zone 102 and he/she sees the wallet balance of \$2.00 on the display 122, 124 of the payment accepting unit 120. The user decides that he/she does not wish to purchase anything else and simply walks away. As he/she walks out of the payment zone 102, the credit is cleared from the machine 120, but he/she is left with the knowledge that his wallet balance is \$2.00 even though he/she never touched the mobile device 150. Communications between the payment accepting unit 120 and the adapter module 100 (via the mobile device 150) handle the accounting incidental to the transaction. The remaining balance (\$2.00) is technically stored on the server 130, and may be reflected on the application 140 on the mobile device 150.

MULTIPLE DISTINCT ZONES

[0093] As shown in Figures 1-2, the functions performed by the adapter module 100 can be divided into distinct zones: a first “communication zone” (e.g., “Bluetooth range” 106), a second “authorization zone” 104, and a third “payment zone” 102. The payment zone 102 is smaller than or equal to (overlapping completely) the authorization zone 104. Put another way, the payment zone 102 is within or coextensive with the authorization zone 104. The payment zone 102 is a subset of the authorization zone 104 with a ratio of the payment zone 102 to the authorization zone 104 ranging from 0.01:1 to 1:1. It is not necessarily a fixed ratio and can vary between different payment accepting units 120, different mobile devices 150, different users, and over time. While the zones 102, 104, 106 are depicted as having a uniform shape, the zones may not necessarily be uniform (or constant over time) in that the shape can vary. For example, the shape of the Bluetooth range 106 may vary depending on environmental conditions such as obstacles in the room and payment accepting unit 120 door/wall materials.

[0094] Bluetooth Range 106 (sometimes also herein called the “communication zone”): The outermost range is the Bluetooth range 106 (shown in Figures 1-2). This is the area in which the adapter module 100 is able to broadcast its presence. In most situations, the Bluetooth range 106 is a passive range in that no actual data is exchanged between the mobile device 150 and the adapter module 100. While in the Bluetooth range 106, the mobile device 150 monitors the RSSI (Received Signal Strength Indicator).

[0095] Authorization Zone 104: The middle region is the authorization zone 104 (shown in Figures 1-2). This is a computed area based on the RSSI. As mentioned, the mobile device 150 monitors the RSSI while it is in the Bluetooth range 106. When the RSSI reaches a certain predetermined threshold based on In-Range Heuristics, the mobile device 150 can be considered to be in the authorization zone 104. In the authorization zone 104 the mobile device 150 establishes a connection to the adapter module 100 (e.g., a Bluetooth connection (Figure 5) with SSL protection (Figure 6)) and informs the adapter module 100 of its presence. After a successful handshake with the adapter module 100, the mobile device 150 registers the adapter module 100 and the adapter module 100 requests an authorization to the server 130 via the mobile devices' network connection (e.g., a Wi-Fi or cellular connection (Figure 5) with SSL protection (Figure 6)). It is important to note the mobile device 150 and the adapter module 100 have a non-exclusive relationship at this point. The adapter module 100 may collect registrations for all mobile devices 150 that are within the authorization zone 104.

[0096] An authorization occurs in preparation for when the user enters the payment zone 102 (shown in Figures 1-2). An authorization expires in a set period of time (for example, five minutes), so if the mobile device 150 is still in the authorization zone 104 at the time of expiration, the adapter module 100 submits for and receives another authorization. This will continue for a set number of times (for example, the limit may be three times to limit cases of numerous authorizations for a mobile device that may remain in the authorization zone 104 for an extended period of time without completing a transaction). Should authorization fail (for instance if the limit had been reached) prior to the user entering the payment zone 102, the adapter module 100 will request authorization when the mobile device 150 enters the payment zone 102 (which adds a few seconds to the experience).

[0097] Payment Zone 102: As a user enters the payment zone 102, the mobile device 150 establishes exclusive control of the adapter module 100. Once established, any other user in the payment zone 102 is put into a "waiting" status.

[0098] In the payment zone 102, the payment can be triggered automatically if the payment processing system has and is in hands-free mode. In such instances, the mobile device 150 is running the application 140 in background mode and will send credit to the payment accepting unit 120 without any explicit user interaction. The user completes the transaction on

the payment accepting unit 120 in much the same manner as if cash had been inserted into the payment accepting unit 120 to establish credit. After the user completes the transaction (that may include one or more purchases), details of the transaction are preferably returned to the mobile device 150 and server 130 in separate messages. The message to the server 130 is preferably encrypted with the adapter module's 100 private key (Figure 6) to ensure data integrity. As shown in Figure 7, the "private key" coded message (Encrypted VendDetails) is preferably sent via the mobile device 150. The message to the mobile device 150 may be sent solely for the purpose of closing the transaction. The transaction history and balance are updated server-side via the encrypted message sent to the server 130.

[0099] The other mode of operation is manual mode. In manual mode, the user launches the mobile device 150 and is able to swipe to send payment to the payment accepting unit 120. The user can also swipe back to cancel the payment. Like in hands-free mode, the purchase transaction is completed on the payment accepting unit 120 in the same manner as if cash were inserted into the payment accepting unit 120. The mobile device 150 is only used to send payment. Selection is made directly on the payment accepting unit 120.

[00100] Self-Calibrating Zone Threshold: A key, but optional feature, of the payment processing system is a self-calibrating payment zone RSSI threshold. Because RSSI can vary machine to machine, environment to environment, and device to device, having a fixed threshold at which payment is triggered can be problematic. The approach suggested herein is the creation of a self-calibrating threshold. When the user is interacting with the payment accepting unit 120 (such as when he makes his selection on the payment accepting unit 120), the payment accepting unit 120 notifies the adapter module 100 and the adapter module 100 logs the conditions such as RSSI, type of user mobile device 150, accelerometer data, and other information. It is at this point that it can be ascertained safely that the user is within arm's-length from the payment accepting unit 120 (by necessity the user is arm's-length because he is making some physical interaction with the payment accepting unit 120). This is the only point in the entire transaction in which it can be certain that the user is within arm's-length from the payment accepting unit 120.

[00101] Figure 4 shows a simplified set of steps involved when users enter the payment zone 102. Specifically, Figure 4 shows that credit is established 200 (this may have been done in

the authorization zone 104, but if not it would be handled in the payment zone 102), that the user makes a selection using the machine 202, that the machine notifies the adapter module of the selection 204, that the adapter module (optionally) logs the RSSI 206, and that the purchase process(es) continues 208. Using the historically logged RSSI data, the adapter module 100 calculates one of several “average” RSSI using various mathematical models. This “average” could be a traditional average, a moving average, a weighted average, a median, or other similar summary function. The adapter module 100 could pre-process the historical data before running the function, such as to eliminate top and bottom data points, suspect data points, etc.

[00102] Optionally, during the handshake between the mobile device 150 and the adapter module 100, the information transmitted to the adapter module 100 may include, for example, the model of the mobile device 150. Using the received information pertaining to the mobile device models, the adapter module 100 can create multiple payment thresholds, one for each mobile device model. This allows for variances that may be inherent in different types of Bluetooth radios. An alternative to this method is for the adapter module 100 to broadcast a baseline payment zone threshold, and the mobile device 150 can use an offset from this baseline based on its specific model type. The payment zone thresholds (or baseline offsets) can be unique to specific types of mobile devices (e.g., by manufacturer, operating system, or component parts), models of mobile devices, or individual mobile devices (unique to each user).

[00103] In a typical scenario in which the payment zone threshold has been calibrated, the adapter module 100 advertises its presence along with the threshold at which it considers any mobile device 150 to be in the authorization zone 104. This is a one-way communication from adapter module 100 to mobile device 150. Once the mobile device 150 enters the authorization zone 104, there is a handshake that is established between the adapter module 100 and the mobile device 150. During this handshake, the mobile device 150 can share its model information with the adapter module 100, and the adapter module 100 can return the payment zone 102 threshold for that specific model.

[00104] Optionally, in addition to calibrating the payment zone threshold, the adapter module 100 can apply the self-calibrating model to the authorization zone 104 to calibrate the authorization zone threshold. As with the payment zone thresholds, the authorization zone thresholds can be unique to specific types of mobile devices, models of mobile devices, or

individual mobile devices. In this scenario, the adapter module 100 would broadcast multiple thresholds by device type and the mobile device 150 would determine which threshold to apply (or alternatively broadcast a baseline and the mobile device 150 uses an offset based on its device model). Even in this scenario, the authorization zone 104 is a one-way communication.

[00105] Optionally, along with the threshold that is calculated (in the payment and/or the authorization zone(s)), a safety margin can be added to minimize scenarios in which a user is within range, but the mobile-device-to-machine payment processing system does not recognize it because the threshold may not have been reached. For example, if the calculated RSSI for an iPhone™ 5 on machine 4567 is -68 db, the mobile-device-to-machine payment processing system may add a safety margin of -5 db, and establish the threshold at -73 db. So when a user's phone is communicating with the adapter module 100 at an RSSI of -73 db or better, the mobile-device-to-machine payment processing system will allow the mobile device 150 to credit the payment accepting unit 120. The safety margin can be set on the server 130 and downloaded to the adapter module 100, or set on the mobile device 150, or set on the adapter module 100 itself.

[00106] Optionally, in the payment zone threshold, the mobile device 150 can use other data to determine when to cancel the exclusive control of the payment accepting unit 120, to identify when the user is moving out of the payment zone 102. External data could include accelerometer data from the mobile device 150. Using that data, the mobile device 150 can determine whether the user is standing relatively still in front of the payment accepting unit 120, or if the user is in motion – effectively walking away from the payment accepting unit 120.

SIGNAL UNAVAILABILITY ADAPTATION

[00107] The mobile-device-to-machine payment processing system described herein uses a mobile device's 150 short-range communication technology (e.g., Bluetooth mechanisms) (shown as short-range communication capability 876 in Figure 21) and a mobile device's 150 long-range communications technology (e.g., cellular and/or Wi-Fi mechanisms) (shown as long-range communication capability 872 in Figure 21). The short-range communication capability 876 communicates with the adapter module's 100 short-range communication technology (e.g., Bluetooth mechanisms) (shown as short-range communication capability 776 in Figure 20). The long-range communication capability 872 communicates with the server's 130 long-range communications technology (e.g., cellular and/or Wi-Fi mechanisms) (shown as

long-range communication capability 972 in Figure 22). The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. This process is described herein and works properly if there is cellular or Wi-Fi coverage within the payment zone 102.

[00108] One option if there is no cellular or Wi-Fi coverage within the payment zone 102 is to determine whether there is cellular or Wi-Fi coverage within the authorization zone 104 or the Bluetooth range 106. If there is, then the sizes of the zones 102, 104, 106 could be adapted and the timing could be adapted. For example, if the mobile devices 150 detected problems with the cellular or Wi-Fi coverage within the payment zone 102, the user could carry his mobile device 150 into the other zones (or the mobile device 150 could use short-range communication technology to communicate with other mobile devices 150 within the authorization zone 104 or the Bluetooth range 106) to determine whether the zones have cellular or Wi-Fi coverage. If they do have coverage, communication between the mobile device 150 and the server 130 can be advanced (conducted earlier when the mobile device 150 is further from the machine 120) or delayed (conducted later when the mobile device 150 is further from the machine 120). This can be thought of as changing the size or shapes of the zones 102, 104, 106. The timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or Wi-Fi coverage again.

[00109] Another option if there is no cellular or Wi-Fi coverage within any of the zones 102, 104, 106 is for the user to obtain authorization while outside of the zones in a place with cellular or Wi-Fi coverage. This may occur, for example, if a user knows that he will be going to a place with a payment accepting unit 120 equipped with an adapter module 100 (perhaps to a favorite payment accepting unit 120) that does not have (or rarely has) cellular or Wi-Fi coverage. A user may also use the mobile application 140 to query payment accepting units 120 in a given range (e.g., within 50 miles) or at a given location (e.g., at a campground or in a particular remote city) to determine whether there is cellular or Wi-Fi coverage within the zones 102, 104, 106. The user can then obtain pre-authorization from the server 130 using the mobile application 140. Again, the timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means

that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or Wi-Fi coverage again. A mobile-device-to-machine payment system having the ability to implement this option would be able to accept cashless payments without requiring any network connection near the payment accepting unit 120. In some implementations, the mobile-device-to-machine payment processing systems described herein is located in a remote location where no signal is available, therefore, can accept cashless payments.

[00110] As an example of a situation in which there might be no cellular or Wi-Fi coverage within any of the zones 102, 104, 106 of a particular payment accepting unit 120, the user (a teenager) may be traveling to a remote location to attend summer camp where there is no cellular or Wi-Fi coverage. The camp may have several payment accepting units 120 (e.g., a machine that creates a dedicated “hot spot” that requires payment for use, vending machines, or machines for renting equipment such as bikes, kayaks, or basketballs). The camp facility might notify parents that the mobile-device-to-machine payment system is available. The parents, while at home, could obtain authorization for a particular amount (that could be doled out a certain amount per day or limited to type of machine or location) to be authorized and “loaded” into the user’s mobile device 150 and specify that the authorization will not expire for a certain period or until a certain date. Thereafter, while at camp, the user could use the mobile application 140 on his mobile device 150 in a manner similar to those discussed elsewhere herein. Short-range communications may be used for communications between the adapter modules 100 (associated with the machines 120) and users’ mobile devices 150.

[00111] One subtle but powerful component of the payment processing system described herein is that it requires a long-range communication capability (e.g., an Internet or cellular network connection) only in the authorization zone 104 and only for the time period required to send the AuthRequest and receive the AuthGrant. Once a valid AuthGrant is received by the mobile device 150, the long-range communication capability (e.g., an Internet or cellular network connection) is not required by either the mobile device 150 or the adapter module 100 in the payment zone 102 as long as the AuthGrant is valid (unexpired). This mechanism allows the system to seamlessly handle authenticated transactions in (temporary) offline mode, with the deferred acknowledgement and transaction messages performing the bookkeeping and cleanup when network connection is regained. The alternatives described above provide a unique way to

artificially extend the authorization zone to include any location where the mobile device 150 can communicate with the server 130.

MULTIPLE USER RESOLUTION

[00112] As shown in Figure 2, in one practical scenario, multiple users are in the zones 102, 104, 106. As shown in Figure 2, users 1, 2, and 3 are in the payment zone 102 near the machine 120; users 5 and 6 are shown as positioned between the authorization zone 104 and the Bluetooth range 106; users 4 and 7 are in the Bluetooth range 106, user 10 is positioned on the edge of the Bluetooth range 106; and users 8 and 9 are positioned outside of Bluetooth range 106. In some implementations, the mobile-device-to-machine payment processing system manages and resolves issues pertaining to multiple users.

[00113] Users 4 and 7 are within the Bluetooth range 106 and the user 10 is either entering or leaving the Bluetooth range 106. Within the Bluetooth range 106 the users' mobile devices 150 are able to see the adapter module's 100 advertisement. In this zone, the mobile device 150 preferably does not initiate a connection. The adapter module 100 is preferably unaware of the users in the Bluetooth range 106. All the adapter module 100 is doing is advertising its presence to any multitude of users that may be in Bluetooth range 106.

[00114] The adapter module 100 begins to log users as the users (and their respective mobile devices 150) enter the authorization zone 104 (shown in Figure 2 as users 5 and 6). At this point, there is a non-exclusive connection initiated by the mobile device 150 to the adapter module 100. It does a handshake (e.g., to exchange information needed to obtain authorization and, optionally, to log information needed for a self-calibrating authorization zone threshold) and the mobile device 150 contacts the server 130 for an authorization (e.g., sending an AuthRequest and receiving an AuthGrant). The adapter module 100 registers all mobile devices 150 that have requested and received AuthGrants. The adapter module 100 continues communicating with any other mobile device 150 that enters the authorization zone 104. After initial contact, the adapter module 100 may provide the mobile device 150 with a deferral delay of when to check back in with the adapter module 100 allowing opportunity for other mobile devices 150 to communicate with the adapter module 100.

[00115] If there is only one user in the payment zone 102, a purchase transaction may be performed. If there are multiple users in the payment zone 102, the mobile-device-to-machine payment system must handle the situation.

[00116] One optional solution for handling the situation of the multiple users in the payment zone 102 is queuing users in the payment zone 102. Once any mobile device 150 enters the payment zone 102, it establishes exclusivity to a particular mobile device 150 (e.g., in a first-come-first-serve manner). Technically, however, the adapter module 100 is not establishing an exclusive connection to the mobile device 150. The adapter module 100 can still perform a round-robin poll and communicate with and advertise to other mobile devices 150. Instead, the adapter module 100 establishes a queue prioritized by RSSI and time (e.g., who was first and whether the authorization has expired) and it notifies (e.g., alerts) other mobile devices 150 to wait. The earliest valid (unexpired) authorization takes precedence when there is any tie in the RSSI. Otherwise, for example, the strongest average RSSI takes priority. Preferably the queue is not a static measure of the RSSI but an averaged measure over the period of time in the queue. This compensates for a scenario in which a user may be walking around in the queue and then shows up at the payment accepting unit 120 just as the previous user is finishing. If another user was also in the payment zone 102 and stood there the entire time, but may have newer authorization, he could win out.

[00117] Anytime that the adapter module 100 cannot determine exactly which user is in the payment zone 102 in front of the payment accepting unit 120, the adapter module 100 will disable hands-free payment. The mobile device 150 will send an alert to the user and he can use swipe to pay (manual mode). All users in payment zone 102 will show “Connected” and the first to swipe payment to the payment accepting unit 120 then locks out other users.

MULTIPLE MODULE RESOLUTION

[00118] In the scenario where there are multiple modules present, determining which payment accepting unit 120 a user is in front of can be a challenge. In some implementations, the mobile-device-to-machine payment processing system described herein allows adapter modules 100 to communicate to other adapter modules 100 in range via Bluetooth. Each user receives authorization grants for specific payment accepting units 120. This means if there are multiple adapter modules 100 within the same authorization zone 104, there will be multiple authorization

grants for the user. When the user enters the payment zone 102, it can be difficult to differentiate which payment accepting unit 120 the user is in front of if the payment zones 102 overlap.

[00119] To solve this problem, when the user enters the payment zone 102, the adapter modules 100 communicate with each other to determine the RSSI for the particular user (based on the signal from his mobile device 150) to triangulate which adapter module 100 (and the associated payment accepting unit 120) is closer to the user. Optionally, the inter-module communications can restrict the user to establishing an exclusive connection with only one payment accepting unit 120.

[00120] Optionally, when the user connects to a payment accepting unit 120, the mobile device 150 can send a communication to the payment accepting unit 120 for momentary display to the user on the display 122, 124 of the payment accepting unit 120. For example, the mobile device 150 can send a communication (e.g., “connected” or “Fred’s Mobile Device Connected”) to the payment accepting unit’s display 122, 124 for a predetermined period of time (e.g., 1-3 seconds) so when the user is in payment zone 102, it is clear which payment accepting unit 120 the user is connected to prior to making a purchase (either in hands-free or manual mode).

[00121] In addition, when the user is in manual mode, the mobile device 150 can display (e.g., on the touch screen 152 as shown in Figures 10A-10D) a visual indication of the payment accepting unit 120 (e.g., a picture and/or a payment accepting unit ID of the payment accepting unit 120) for visual confirmation. If the user is in manual mode, the user can manually change the payment accepting unit 120.

DESCRIPTIVE SCENARIO

[00122] Figure 7, Figures 8A-8G, and 9A-9E (as well as other figures) can be used to understand a detailed scenario of the mobile-device-to-machine payment processing system described herein. A flow of communications and steps are loosely described below with reference to these (and other figures). It should be noted that alternative scenarios could include, for example, a modified order of the steps performed.

[00123] Prior to vending transactions, a user downloads a mobile application 140 onto his mobile device 150, creates an account, and configures a funding source via, for example, a funding source server 160. A funding source may be, for example, a debit card, a credit card,

campus cards, rewards points, bank accounts, payment services (e.g., PayPal™) or other payment option or combination of payment options known or yet to be discovered. The funding sources may be traditional and/or nontraditional payment sources that are integrated into the ecosystem described herein and then used indirectly as a source of funds. Funds from the funding source are preferably held on the server 130 such that when an AuthRequest is received by the server 130, the server 130 can send an AuthGrant authorizing funds for a purchase.

[00124] The user can specify one or more “favorite” adapter module(s) 100 (that has a one-to-one relationship to the payment accepting unit 120) that he may visit regularly, such as a vending machine at school or work. Favorite adapter modules 100 appear on a pre-filtered list and allow for additional rich features such as hands-free payment.

[00125] The payment accepting unit 120 may be equipped with an adapter module 100 that is constantly advertising its availability via Bluetooth (or other “signals,” “communications,” and/or “transmissions”). This ongoing advertising and scanning for adapter modules is shown in Figure 8A. As shown, the mobile device 150 is continuously scanning for any adapter module 100 within Bluetooth (or other “signal,” “communication,” and/or “transmission”) range. When the user is within range of that adapter module 100, the mobile device 150 tracks and monitors the signal strength until a predetermined “authorization zone” threshold is achieved.

[00126] Figures 8B and 9A generally show that when the authorization zone threshold is reached, the mobile device 150 enters the authorization zone (block 302) and registers the adapter module 100. The mobile device 150 connects to the server 130 (block 304). The application 140 on the mobile device 150 creates a request for authorization (AuthRequest) and passes the AuthRequest to the server 130 using appropriate communication technology (e.g., GSM, CDMA, Wi-Fi, or the like) (block 306). The server 130 responds with an authorization grant (AuthGrant) encrypted with the specific adapter module’s private key (block 306). This authorization token may minimally include the User identifier (ID), Apparatus ID (for the adapter module 100), authorization amount, and expiration time. The mobile device 150 receives the AuthGrant from the server 130, and retains it until the mobile device 150 is ready to issue payment to an adapter module 100. The mobile device 150 collects all pending AuthGrants that may be one or more depending on how many adapter modules 100 are in-range. Unused AuthGrants that expire are purged from the mobile device 150 and the server 130. It is important

to note that the mobile device 150 is unable to read the AuthGrant because it is encrypted with the adapter module's unique private key that is only known to server 130 and adapter module 100. This provides a preferred key element of security in the system as the adapter module 100 only trusts AuthGrants that are issued by the server 130, and the AuthGrants cannot be read or modified by the mobile device 150 or any other party in between the server and the adapter module 100. Additional mobile devices 150 may enter the authorization zone 104 (block 308).

[00127] As the user approaches a specific adapter module 100, the user enters the payment zone 102 and an event threshold is triggered based on heuristics performed by the mobile device 150. Blocks 310 and 312 show the loop steps of waiting for a mobile device 150 from the authorization zone 104 to enter the payment zone 102. If the user leaves the authorization zone 104 without entering the payment zone 102, the adapter module 100 returns to advertising its presence (block 300).

[00128] Figures 8C and 9B generally show the user entering the payment zone. The mobile device 150 verifies that it has an unexpired and valid AuthGrant. If the AuthGrant is not good, it may be requested again, repeating the Authorization Request process (block 315). If the AuthGrant is good, the mobile device 150 sends the valid AuthGrant (including the wallet balance (block 322)) to the adapter module 100 to initiate a transaction. The mobile device 150 may issue the AuthGrant automatically without specific user interaction if the hands-free mode is supported (and the device is a favorite (block 318), there is only one device in the payment zone 102 (block 318), and (optionally) there is only one user in the authorization zone 104 (block 320). If any of these factors are not present, the mobile device 150 will prompt and/or wait for the user to begin the transaction manually (block 324).

[00129] Figures 8D, 9C, and 9D generally show the transaction process. As shown in Figure 9C, the adapter module 100 runs through a series of questions to determine if there are any issues that would prevent vending including: has the user canceled in-app? (block 326), has the user walked away? (block 328), is the coin return pressed? (block 330), has more than a predetermined period of time elapsed? (block 332). If the answer to any of these questions is "yes," the transaction does not proceed. If the answers to all of these questions is "no," the user makes a selection (block 334) on the payment accepting unit 120 in the same or similar manner as compared to if cash or credit were presented to the payment accepting unit 120. If the machine

120 is able to vend (block 336), it attempts to release the product. If the vend fails (block 338) it is reported by the machine (block 340) and a credit is returned to the virtual wallet (block 342). If the vend is successful (block 338) it is reported by the machine (block 344). Put another way, after the transaction is complete, the adapter module 100 returns to the mobile device 150 the details of the transaction as well as an encrypted packet containing the vend details to be sent to the server 130 via the mobile device 150. Optionally, the adapter module 100 can pass additional information not directly related to the transaction such as payment accepting unit health, sales data, error codes, etc.

[00130] Figures 8D and 9E generally show the multi-vend function. If the machine has enabled multi-vend capabilities (block 350) and the multi-vend limit has not been reached, the process returns to the question of whether the user is in the payment zone (block 310 of Figure 9A). If the machine does not have enabled multi-vend capabilities (block 350) or the multi-vend limit has been reached, the wallet is decremented by the vend amount(s) and “change” is returned to the virtual wallet (block 354) and the process ends (block 356).

[00131] Figure 8E is a schematic flow diagram of an example login process. Figure 8F is a schematic flow diagram of an example boot-up process. Figure 8G is a schematic flow diagram of an example account check/update process.

[00132] Several of the figures are flow charts (e.g., Figures 9A-9E) illustrating methods and systems. It will be understood that each block of these flow charts, components of all or some of the blocks of these flow charts, and/or combinations of blocks in these flow charts, may be implemented by software (e.g., coding, software, computer program instructions, software programs, subprograms, or other series of computer-executable or processor-executable instructions), by hardware (e.g., processors, memory), by firmware, and/or a combination of these forms. As an example, in the case of software, computer program instructions (computer-readable program code) may be loaded onto a computer to produce a machine, such that the instructions that execute on the computer create structures for implementing the functions specified in the flow chart block or blocks. These computer program instructions may also be stored in a memory that can direct a computer to function in a particular manner, such that the instructions stored in the memory produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The computer

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

ADDITIONAL IMPLEMENTATIONS

[00133] Figure 23 illustrates a schematic flow diagram of a process 1000 of authenticating a user to perform a transaction in the payment processing system in accordance with some implementations. In some implementations, the payment processing system includes one or more payment modules 100 (e.g., each associated with a respective payment accepting unit 120 such as an automatic retailing machine for dispensing goods and/or services), one or more mobile devices 150 (e.g., each executing the application 140 for the payment processing system either as a foreground or background process), and the server 130. The server 130 manages the payment processing system and, in some cases, is associated with an entity that supplies, operates, and/or manufactures the one or more payment modules 100. For brevity, the process 1000 will be described with respect to a respective payment module 100 and a respective mobile device 150 in the payment processing system.

[00134] The payment module 100 broadcasts (1002), via a short-range communication capability (e.g., BLE), a packet of information (sometimes also herein called “advertised information”). The packet of information at least includes an authorization code and an identifier associated with the payment module 100 (module ID). In some implementations, the packet of information further includes a firmware version of the payment module 100 and one or more status flags corresponding to one or more states of the payment module 100 and/or the payment accepting unit 120. The information included in the packet broadcast by the payment module 100 is further discussed below with reference to Figure 24A.

[00135] In some implementations, the payment module 100 sends out a unique authorization code every X seconds (e.g., 100 ms, 200 ms, 500 ms, etc.). In some implementations, the unique authorization codes are randomly or pseudo-randomly generated numbers. In some implementations, the payment module 100 stores broadcasted authorization codes until a received authorization grant token matches one of the stored authorization codes. In some implementations, the payment module 100 stores broadcasted authorization codes for a predetermined amount of time (e.g., Y minutes) after which time an authorization code expires and is deleted. In some implementations, the authorization code is encrypted with a shared secret key known by the server 130 but unique to the payment module 100. In some implementations, the payment module 100 initializes a random number and then the authorization codes are sequential counts from this random number. In such implementations, the payment module 100 stores the earliest valid (unexpired) counter without a need to store every valid authorization code. In some implementations, the authentication code included in the broadcast packet of information is a hash value of the randomly or pseudo-randomly generated number or the sequential number.

[00136] The mobile device 150 receives the broadcasted packet of information, and the mobile device 150 sends (1004), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), an authorization request to the server 130. For example, an application 140 that is associated with the payment processing system is executing as a foreground or background process on the mobile device 150. In this example, the application 140 receives the broadcasted packet of information when the mobile device 150 is within the communication zone of the payment module 100 (i.e., BLE range) and either automatically sends the authorization request to the server 130 or sends the authorization request to the server 130 when the mobile device 150 is within the authorization zone of the payment module 100. In some implementations, the broadcasted packet of information includes a baseline authorization zone threshold (i.e., an authorization zone criterion) indicating a baseline RSSI that the mobile device 150 (or the application 140) is required to observe before being within the authorization zone of the payment module 100. In some implementations, the mobile device 150 (or the application 140) offsets the baseline authorization zone threshold based on the strength and/or reception of the short-range communication capability (e.g., BLE radio/transceiver) of the mobile device 150. In some implementations, the authorization request at least includes the authorization code which

was included in the broadcasted packet of information, an identifier associated with the user of the mobile device 150 or the user account under which the user of the mobile device 150 is logged into the application 140 (user ID), and the identifier associated with the payment module 100 (module ID). In some implementations, the authentication code included in authorization request is the hash value in cleartext. The authorization request is further discussed below with reference to Figure 24B.

[00137] After receiving the authorization request, the server 130 processes (1006) the authorization request. In some implementations, the server 130 decrypts the authorization code included in the authorization request with the shared secret key corresponding to the payment module 100. In some implementations, the server 130 determines whether the user associated with the user ID in the authorization request has sufficient funds in his/her account for the payment processing system to perform a transaction at the machine 120 that is associated with the payment module 100 corresponding to the module ID in the authorization request.

[00138] The server 130 sends (1008), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), an authorization grant token to the mobile device 150. In some implementations, the server 130 does not send the authorization grant token if the authorization code in the authorization request cannot be decrypted with the shared secret key corresponding to the payment module 100 (e.g., the authorization code is corrupted or hacked). In some implementations, the server 130 does not send the authorization grant token if the user associated with the user ID in the authorization request does not have sufficient funds in his/her account. In some implementations, in addition to the authorization grant token, the server 130 sends a message directly to the mobile device 150 which is not encrypted with the shared secret key corresponding to the payment module 100. After receiving the message, the mobile device 150 displays an appropriate message to the user such as insufficient balance or declined authorization. In some implementations, the server 130 sends an authorization grant token for an amount equal to zero; in which case, the payment module 100 interprets this as a declined or failed authorization which can result for any number of reasons including, but not limited to, insufficient balance or credit.

[00139] The mobile device 150 receives the authorization grant token, and, subsequently, the mobile device 150 detects (1010) a trigger condition. In some implementations, the mobile

device 150 (or the application 140) detects the trigger condition via the hand-free mode (e.g., upon entrance into the payment zone of the payment module 100) or manual mode (e.g., interacting with the user interface of the application 140 to initiate a transaction with the payment accepting unit associated with the payment module 100).

[00140] In some implementations, unused authorization grants (e.g., if there was no trigger condition or it expired) are canceled by the mobile device 150 by sending a cancellation message to the server 130 corresponding to the unused authorization grant. In some implementations, the server 130 denies or limits the number of authorization grants sent to the mobile device 150 until it has received transaction information or cancellation of authorization outstanding authorization grants sent to the mobile device 150.

[00141] In response to detecting the trigger condition, the mobile device 150 sends (1012), via a short-range communication capability (e.g., BLE), the authorization grant token to the payment module 100. Subsequently, the machine 120 displays credit to the user (e.g., via one of the displays 122 or 124 shown in Figure 19) and the user interacts with the input mechanisms of the machine 120 (e.g., via the buttons 126 or a touch screen display 124 shown in Figure 19) to purchase products and/or services.

[00142] Figure 24A illustrates a block diagram of a packet 1100 of information broadcast by the payment module 100 (e.g., in step 1002 of the process 1000 in Figure 23) in accordance with some implementations. In some implementations, the packet 1100 at least includes: module ID 1102 and authorization code 1104. In some implementations, the packet 110 additional includes: a firmware version 1106 and one or more status flags 1108.

[00143] In some implementations, the module ID 1102 is a unique identifier corresponding to the payment module 100 (sometimes also herein called the “adapter module 100”) that broadcast the packet 1100.

[00144] In some implementations, the authorization code 1104 is a hash value in cleartext. In some implementations, the payment module 100 randomly or pseudo-randomly generates a number or determines a sequential number (*See* step 1002 of process 1000 in Figure 23) and performs a predetermined hash function (e.g., SHA-256) on the number to produce the hash value as the authorization code 1104. In some implementations, the authorization code 1104 is a unique code that is encrypted with a secret encryption key corresponding to the payment module

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

[00145] In some implementations, the firmware version information 1106 identifies a current firmware version 1112 of the payment module 100. In some implementations, the firmware version information 1106 also includes update status information 1114 indicating one or more packets received by the payment module 100 to update the firmware or one or more packets needed by the payment module 100 to update the firmware. In some implementations, the one or more status flags 1108 indicate a state of the payment module 100 and/or the payment accepting unit 120 associated with the payment module 100. In some implementations, the one or more status flags 1108 indicate a state of the payment module 100 such upload information indicator 1116 indicating that that the payment module 100 has information to be uploaded to the server 130 (e.g., transaction information for one or more interrupted transactions). In some implementations, upload information indicator 1116 triggers the mobile device 150 to connect to payment module 100 immediately (e.g., if it has interrupted transaction information to be uploaded to the server 130). In some implementations, the one or more status flags 1108 indicate a state of the payment accepting unit 120 including one or more of an error indicator 1118 (e.g., indicating that a bill and/or coin acceptor of the payment accepting unit 120 is experiencing a jam, error code, or malfunction), a currency level indicator 1120 (e.g., indicating that the level of the bill and/or coin acceptor reservoir of the payment accepting unit 120 is full or empty), and/or inventory level(s) indicator 1122 (e.g., indicating that one or more products of the payment accepting unit 120. In some implementations, the one or more status flags 1108 are error codes issued by payment accepting unit 120 over the MDB.

[00146] In some implementations, the zone criteria information 1110 specifies an authorization zone criterion 1124 (e.g., a baseline authorization zone threshold indicating a baseline RSSI that the mobile device 150 (or the application 140) is required to observe before being within the authorization zone of the payment module 100) and/or a payment zone criterion 1126 (e.g., a baseline payment zone threshold indicating a baseline RSSI that the mobile device 150 (or the application 140) is required to observe before being within the payment zone of the payment module 100). In some implementations, the baseline authorization zone threshold and

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

[00147] Figure 24B is a block diagram of an authorization request 1130 sent by the mobile device 150 to the server 130 (e.g., in step 1004 of the process 1000 in Figure 23) in accordance with some implementations. In some implementations, the authorization request 1130 at least includes: a module ID 1102, a user ID 1134, and an authorization code 1104.

[00148] In some implementations, the module ID 1102 is a unique identifier corresponding to the payment module 100 that broadcast the 1100 that included the authorization code 1104.

[00149] In some implementations, the user ID 1134 is an identifier associated with the user of the mobile device 150 sending the authorization request 1130 to the server 130. In some implementations, the user ID 1134 is associated with the user account under which the user of the mobile device 150 is logged into the application 140.

[00150] In some implementations, the authorization code 1130 includes the authorization code 1104 included in the packet 1100 of information that was broadcast by the payment module 100.

[00151] Figure 24C is a block diagram of an authorization grant token 1140 sent by the server 130 to the mobile device 150 (e.g., in step 1008 of the process 1000 in Figure 23) in accordance with some implementations. In some implementations, in accordance with a determination that the authorization code 1136 included in the authorization request 1130 from the mobile device 150 is valid and that the user associated with the mobile device 150 has sufficient funds in his/her account for the payment processing system, the server 130 generates the authorization grant token 1140. In some implementations, the authorization grant token 1140 at least includes: a module ID 1102, a user ID 1134, an authorized amount 1146, (optionally) an expiration period offset 1148, and (optionally) the authorization code 1104.

[00152] In some implementations, the module ID 1102 is a unique identifier corresponding to the payment module 100 that broadcast the packet 1100 that included the authorization code 1104.

[00153] In some implementations, the user ID 1134 is an identifier associated with the user of the mobile device 150 that sent the authorization request 1130 to the server 130.

[00154] In some implementations, the authorized amount 1146 indicates a maximum amount for which the user of the mobile device 150 is authorized for a transaction using the authorization grant token 1140. For example, the authorized amount 1146 is predefined by the user of the mobile device 150 or by the server 130 based on a daily limit or based on the user's total account balance or based on a risk profile of the user correspond to the user ID 1134.

[00155] In some implementations, the expiration period 1148 offset indicates an offset to the amount of time that the payment module 100 holds the authorization grant token 1140 valid for initiation of a transaction with the machine 120 associated with the payment module 100. For example, the expiration period offset 1148 depends on the history and credit of the user of mobile device 150 or a period predefined by the user of mobile device 150.

[00156] In some implementations, the authorization grant token 1140 further includes the authorization code 1104 that was included in the authorization request 1130. In some implementations, when the authorization code 1104 is the hash value, the server 130 encrypts the authorization grant token 1140 including the hashed value with the shared secret encryption key associated with payment module 100. Subsequently, when mobile device 150 sends the authorization grant token 1140 to payment module 100 after detecting a trigger condition, the

payment module 100 decrypts the authorization grant token 1140 using the secret key known only to server 130 and payment module 100 (which authenticates the message and the authorization grant), and then matches the hash value included in the decrypted authorization grant token 1140 to previously broadcast valid (unexpired) hash values (i.e., auth codes) to determine validity of the (which was known only by payment module 100).

[00157] Figure 24D illustrates a block diagram of transaction information 1150 generated by the payment module 100 (e.g., in step 1254 of the process 1250 in Figure 25B) in accordance with some implementations. In some implementations, the transaction information 1150 includes: a transaction ID 1152 for the respective transaction, a module ID 1154, a user ID 1156, (optionally) the authorization code 1158, transaction status information 1160, the transaction amount 1162, and other information 1164.

[00158] In some implementations, the transaction ID 1152 is a unique identifier corresponding to the respective transaction. In some implementations, the transaction ID 1152 is encoded based on or associated with the time and/or date on which and the location at which the respective transaction took place.

[00159] In some implementations, the module ID 1154 is a unique identifier corresponding to the payment module 100 that performed the respective transaction.

[00160] In some implementations, the user ID 1156 is an identifier associated with the user of the mobile device 150 that initiated the respective transaction.

[00161] In some implementations, the authorization code 1158 corresponds to the original authorization code (e.g., auth code 1104, Figures 24 A-24C) and/or authorization grant token (e.g., auth grant token 1140, Figure 24C) that was used to initiate the respective transaction. In some implementations, the authorization code 1156 is encrypted with a unique encryption key corresponding to the payment module 100.

[00162] In some implementations, the transaction status information 1160 includes an indication whether the respective transaction was completed, not-completed, or aborted. For example, the respective transaction is incomplete if a jam occurred at the payment accepting unit 120 and the user did not receive the product associated with the respective transaction. For example, if the user walks away from the payment accepting unit 120 after money was credited

for the respective transaction, the respective transaction is aborted. In another example, if respective transaction times out after a predetermined time period because the user failed to select a product at the payment accepting unit 120, the respective transaction is aborted. In another example, if the user actuates a bill or coin return mechanism of the payment accepting unit 120, the respective transaction is aborted.

[00163] In some implementations, the transaction amount 1162 indicates the amount of the respective transaction or the amount of each of multiple transactions (e.g., in a multi-vend scenario). In some implementations, the transaction amount 1162 is encrypted with a unique encryption key corresponding to the payment module 100.

[00164] In some implementations, the other information 1164 includes other information related to the respective transaction such as the items dispensed by the payment accepting unit 120 and the type of transaction (e.g., coins, bills, credit card, manual mode, hands-free mode, etc.). In some implementations, the other information 1164 includes other information related to the payment module 100 and/or the payment accepting unit 120 associated with the payment module 100. For example, the other information 1164 includes a verification request to the server 130 in order to implement new firmware. In another example, the other information 1164 includes transaction information from one or more previous interrupted transactions. In another example, the other information 1164 includes transaction information for one or more transactions paid via bills and/or coins. In another example, the other information 1164 includes inventory information as to one or more products of the payment accepting unit 120.

[00165] Figure 25A illustrates a schematic flow diagram of a process 1200 for providing a representation of a machine event at a mobile device in accordance with some implementations. In some implementations, the payment processing system includes one or more payment modules 100 (e.g., each associated with a respective payment accepting unit 120 such as an automatic retailing machine for dispensing goods and/or services), one or more mobile devices 150 (e.g., each executing the application 140 for the payment processing system either as a foreground or background process), and the server 130. The server 130 manages the payment processing system and, in some cases, supplies, operates, and/or manufactures the one or more payment modules 100. For brevity, the process 1200 will be described with respect to a respective payment module 100 associated with a respective payment accepting unit 120

(sometimes also herein called the “machine 120”) and a respective mobile device 150 in the payment processing system.

[00166] In some implementations, the process 1200 occurs after the mobile device 150 sends the AuthGrant in Figure 8C. In some implementations, the process 1200 occurs after the mobile device 150 sends the authorization grant to the payment module 100 in operation 1012 of process 1000 in Figure 23.

[00167] The payment module 100 obtains (1202) an indication corresponding to an event at the machine 120. For example, after the process 1000 in Figure 23, the user of the mobile device 150 selects a product to purchase from the machine 120 by interacting with one or more input mechanisms of the machine 120 (e.g., buttons 126 or a touch screen display 124 shown in Figure 19), and the machine 120 dispenses the selected product. Continuing with this example, after the product is dispensed, the transaction is complete and the payment module 100 obtains an indication from the machine of the completed transaction. In some implementations, the indication includes the amount of the transaction and (optionally) machine status information associated with the machine 120 such as inventory information as to one or more products of the payment accepting unit 120 and/or the like. In some implementations, the indication includes status information indicating that the transaction was aborted (e.g., via actuation of a coin return mechanism at the machine 120) or that there was an error with the transaction (e.g., a vending jam or other malfunction with the machine 120).

[00168] After obtaining the indication corresponding to completion of the first transaction, the payment module 100 generates (1204) a notification corresponding to the event at the machine 120.

[00169] The payment module 100 sends (1206), via a short-range communication capability (e.g., BLE), the notification to the mobile device 150. In some embodiments, in addition to the notification corresponding to the event at machine 120, the payment module 100 sends a promotion or advertisement to the mobile device 150 that is targeted to the user of the mobile device 150 based on the transaction or the user ID included in the AuthGrant or authorization grant token that initiated the transaction. In some embodiments, in addition to the notification corresponding to the event at machine 120, the payment module 100 sends a pseudo randomly selected promotion or advertisement to the mobile device 150 that is selected from a

set of promotions or advertisements stored by the payment module 100. For example, the promotion is a coupon for a free soda following the purchase of ten sodas from the machine 120 by the user of the mobile device 150. For example, the promotion is a random 50% off coupon or free soda coupon. For example, the transaction corresponds to a vended soda and the advertisement corresponds to a new soda from the same company that produces the vended soda.

[00170] The mobile device 150 provides (1208) a representation of the notification. For example, in Figure 26A, the mobile device 150 displays user interface 1302 on touch screen 152 with a message 1306 that indicates that the first transaction is complete. For example, in Figure 26C, the mobile device 150 displays user interface 1320 on touch screen 152 with a message 1322 that indicates that the transaction was aborted. For example, in Figure 26D, the mobile device 150 displays user interface 1330 on touch screen 152 with a message 1332 that indicates that there was an error with the transaction. For example, the mobile device 150 also displays a representation of the promotion of advertisement on the user interface for the application 140.

[00171] Figure 25B illustrates a schematic flow diagram of a process 1250 for processing acknowledgement information in accordance with some implementations. In some implementations, the payment processing system includes one or more payment modules 100 (e.g., each associated with a respective payment accepting unit 120 such as an automatic retailing machine for dispensing goods and/or services), one or more mobile devices 150 (e.g., each executing the application 140 for the payment processing system either as a foreground or background process), and the server 130. The server 130 manages the payment processing system and, in some cases, supplies, operates, and/or manufactures the one or more payment modules 100. For brevity, the process 1250 will be described with respect to a respective payment module 100 associated with a respective payment accepting unit 120 (machine 120) and a respective mobile device 150 in the payment processing system.

[00172] In some implementations, the process 1250 occurs after the mobile device 150 sends the AuthGrant in Figure 8C. In some implementations, the process 1250 occurs after the mobile device 150 sends the authorization grant to the payment module 100 in operation 1012 of process 1000 in Figure 23.

[00173] The payment module 100 obtains (1252) an indication corresponding to completion of a first transaction from the machine 120. For example, after the process 1000 in

Figure 23, the user of the mobile device 150 selects a product to purchase from the machine 120 by interacting with one or more input mechanisms of the machine 120 (e.g., buttons 126 or a touch screen display 124 shown in Figure 19), and the machine 120 dispenses the selected product. Continuing with this example, after the product is dispensed, the transaction is complete and the payment module 100 obtains an indication from the machine of the completed transaction. In some implementations, the indication includes the amount of the transaction and (optionally) machine status information associated with the machine 120 such as inventory information as to one or more products of the payment accepting unit 120 and/or the like.

[00174] After obtaining the indication corresponding to completion of the first transaction, the payment module 100 generates (1254) a first notification with first transaction information based on the indication, and the payment module 100 stores the first transaction information. In some implementations, the first transaction information includes a transaction ID for the first transaction, a module ID corresponding to payment module 100, a user ID corresponding to the mobile device 150, transaction status information indicating that the first transaction is complete, and the transaction amount indicated by the indication. In some implementations, the payment module 100 retains the authorization code included in the original broadcasted packet and/or the authorization grant token and includes the authorization code in the first transaction information. In some implementations, the authorization code is encrypted with a secret key corresponding to the payment module 100, which is shared with the server 130 but not the mobile device 150. In some implementations, the first transaction information further includes other information such as the machine status information included in the first notification or transaction information corresponding to previous interrupted transaction(s). See Figure 24D and the accompanying text for further discussion regarding transaction information 1150.

[00175] The payment module 100 sends (1256), via a short-range communication capability (e.g., BLE), the first notification with first transaction information to the mobile device 150. In some embodiments, in addition to first transaction information corresponding to completion of the first transaction at machine 120, the first notification includes a promotion or advertisement to the mobile device 150 that is targeted to the user of the mobile device 150 based on the transaction or the user ID included in the AuthGrant or authorization grant token that initiated the transaction. In some embodiments, in addition to first transaction information corresponding to completion of the first transaction at machine 120, the first notification includes

a pseudo randomly selected promotion or advertisement to the mobile device 150 that is selected from a set of promotions or advertisements stored by the payment module 100. For example, the promotion is a coupon for a free soda following the purchase of ten sodas from the machine 120 by the user of the mobile device 150. For example, the promotion is a random 50% off coupon or free soda coupon. For example, the transaction corresponds to a vended soda and the advertisement corresponds to a new soda from the same company that produces the vended soda.

[00176] The mobile device 150 provides (1258) a representation of the first notification. For example, in Figure 26A, the mobile device 150 displays user interface 1302 on touch screen 152 with a message 1306 that indicates that the first transaction is complete. For example, the mobile device 150 also displays a representation of the promotion of advertisement on the user interface for the application 140.

[00177] The mobile device 150 sends (1260), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), the first transaction information to the server 130.

[00178] The server 130 processes (1262) the first transaction information. For example, the server 130 debits the account of the user associated with the user ID in the first transaction information in the amount indicated by the first transaction information.

[00179] The server 130 sends (1264), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), first acknowledgment information to the mobile device 150. In some implementations, the first acknowledgment information acknowledges that the server 130 received the first transaction information. In some implementations, the first acknowledgment information includes the user ID, the module ID, the transaction ID, and (optionally) the authorization grant included in the transaction information (e.g., auth grant 1158, Figure 24D).

[00180] After receiving the first acknowledgement information, the mobile device 150 sends (1266), via a short-range communication capability (e.g., BLE), the first acknowledgment information to the payment module 100.

[00181] After receiving the first acknowledgment information, the payment module 100 deletes (1268) the stored first transaction information.

[00182] Attention is now directed towards implementations of user interfaces and associated processes that may be implemented on the mobile device 150 with zero or more speakers, zero or more microphones, and a display. For example, the display is a touch screen (sometimes also herein called a “touch screen display”) enabled to receive one or more contacts and display information (e.g., media content, websites and web pages thereof, user interface for the application 140, and/or user interfaces for applications). Figures 26A-26D illustrate example user interfaces for providing a representation of a machine event at a mobile device in accordance with some implementations.

[00183] Figures 26A-26D show user interfaces displayed on mobile device 150 (e.g., a mobile phone); however, one skilled in the art will appreciate that the user interfaces shown in Figures 26A-26D may be implemented on other similar computing devices. The user interfaces in Figures 26A-26D are used to illustrate the processes described herein, including the process described with respect to Figures 25A-25B and 27A-27B.

[00184] For example, a user of the mobile device 150 approaches a machine 120 (e.g., vending machine 78x928 as shown in Figures 10A-10D) and executes application 140 on the mobile device 150 so as to perform an electronic transaction with the machine 120. For example, with reference to Figures 10C-10D, the user of the mobile device 150 initiates a transaction with the machine 120 (e.g., vending machine 78x928) by performing a swipe gesture at a location corresponding to the representation of the dollar bill (e.g., a substantially vertical swipe gesture from a location corresponding to the representation of the dollar bill to the top edge of the mobile device 150).

[00185] Figure 26A illustrates the mobile device 150 displaying a user interface 1302 of the application 140 on touch screen 152 after the user of the mobile device 150 initiates and performs a transaction with the machine 120. In Figure 26A, the user interface 1302 includes prepaid balance 1304 which indicates that \$1.00 has been deducted from the prepaid balance after performing a transaction with the machine 120 as compared to the prepaid balance in Figure 10C-10D (i.e., \$9.00 in Figures 10C-10D and \$8.00 in Figure 26A). In Figure 26A, the user interface 1302 also includes a message 1306 indicating that the transaction with the machine 120 is complete.

[00186] Figure 26B illustrates the mobile device 150 displaying a user interface 1310 of the application 140 on touch screen 152 after the user of the mobile device 150 initiates a transaction with the machine 120 and an error with the transaction occurs or the transaction is aborted. In Figure 26B, the user interface 1310 shows the representation of the dollar bill sliding onto the touch screen 152 (e.g., in a substantially top to bottom manner). In Figure 26B, the interface 1310 includes prepaid balance 1312 which indicates that no money has been deducted from the prepaid balance after performing a transaction with the machine 120 as compared to the prepaid balance in Figure 10C-10D (i.e., \$9.00 in Figures 10C-10D and \$9.00 in Figure 26B).

[00187] Figure 26C illustrates the mobile device 150 displaying a user interface 1320 of the application 140 on touch screen 152 after the representation of the dollar bill slides onto the touch screen 152 in Figure 26B due to the transaction being aborted. For example, the user aborts the transaction by actuating a coin return mechanism of the machine 120. In another example, the user aborts the transaction by selection an abort affordance on the interface of the application 140 (not shown). In Figure 26C, the user interface 1320 includes a message 1322 indicating that the transaction with the machine 120 was aborted and that the user's account was not debited for the aborted transaction.

[00188] Figure 26D illustrates the mobile device 150 displaying a user interface 1330 of the application 140 on touch screen 152 after the representation of the dollar bill slides onto the touch screen 152 in Figure 26B due to the occurrence of an error with the transaction. For example, a malfunction with the machine 120 (e.g., a vending jam or stuck item) causes the error to occur. In Figure 26D, the user interface 1330 is associated with the application 140 executed on the mobile device 150. In Figure 26D, the user interface 1330 includes a message 1332 indicating that an error occurred during the transaction with the machine 120 and that the user's account was not debited for the transaction.

[00189] Figures 27A-27B illustrate a flowchart diagram of a method 1400 of presenting representations of payment accepting unit events in accordance with some implementations. In some implementations, the method 1400 is performed by a device with one or more processors, memory, one or more output devices, and two or more communication capabilities. For example, in some implementations, the method 1400 is performed by the mobile device 150 (Figures 5 and 21) or a component thereof (e.g., the application 140). In some implementations, the method

1400 is governed by instructions that are stored in a non-transitory computer readable storage medium (e.g., the memory 860, Figure 21) and the instructions are executed by one or more processors (e.g., the processing unit 850, Figure 21) of the device. Optional operations are indicated by dashed lines (e.g., boxes with dashed-line borders).

[00190] After sending a request to a payment module via a first communication capability transaction to initiate a transaction with a payment accepting unit (e.g., an offline-payment operated machine such as a vending machine or kiosk) associated with the payment module, the mobile device obtains (1402) a notification from the payment module via the first communication capability, where the notification indicates an event at the payment accepting unit associated with the payment module. In some implementations, method 1400 occurs after the mobile device 150 sends the AuthGrant in Figure 8C. In some implementations, method 1400 occurs after the mobile device 150 sends the authorization grant to the payment module 100 in operation 1012 of process 1000 in Figure 23. Operation 1206 of Figure 25A, for example, shows the mobile device 150 receiving a notification sent by the payment module 100 (e.g., the adapter module 100, Figures 5 and 20) sent via the first communication capability (e.g., a short-range communication technology/protocol such as BLE). The notification indicates an event at the payment accepting unit (e.g., the payment accepting unit 120, Figures 5 and 19) (sometimes also herein called “machine 120”) associated with the payment module 100.

[00191] In some implementations, the first communication capability corresponds (1404) to a short-range communication protocol. As described above, the short-range communication protocols include BLE, NFC, and/or other protocols utilizing non-persistent communication channels.

[00192] In response to obtaining the notification, the mobile device provides (1406) a representation of the notification to a user of the mobile device via the one or more output devices of the mobile device. For example, in Figure 26A, the mobile device 150 displays user interface 1302 on touch screen 152 with a message 1306 that indicates that the first transaction is complete. For example, in Figure 26C, the mobile device 150 displays user interface 1320 on touch screen 152 with a message 1322 that indicates that the transaction was aborted. For example, in Figure 26D, the mobile device 150 displays user interface 1330 on touch screen 152 with a message 1332 that indicates that there was an error with the transaction.

[00193] In some implementations, the one or more output devices of the mobile device include (1408) at least one of: a display, one or more speakers, one or more LEDs, and a vibration mechanism. For example, the mobile device 150 includes one or more of a display (e.g., the touch screen 152, Figures 10A-10D), one or more speakers, one or more LEDs, and a vibration mechanism.

[00194] In some implementations, the representation of the notification is at least one of (1410): a message displayed on the display of the mobile device; a banner notification displayed on a display of the mobile device; a vibration alert from the vibration mechanism of the mobile device; an aural alert from the one or more speakers of the mobile device; and a visual alert from the one or more LEDs of the mobile device. For example, in Figures 26B-26D, the representation of the notification includes messages 1306, 1322, and 1332 displayed on the touch screen 152 of the mobile device 150. In another example, the representation of the notification is a predefined sequence of vibrations provided by the vibration mechanism of the mobile device 150. In another example, the representation of the notification is a predefined sequence of tones provided by the one or more speakers of the mobile device 150. In another example, the representation of the notification is a predefined sequence of blinking LEDs of the mobile device 150.

[00195] In some implementations, the notification indicates (1412) abortion of a transaction initiated by the user of the mobile device. In Figure 26C, for example, the user interface 1320 includes the message 1322 indicating that the transaction has been aborted. For example, the user aborts the transaction by actuating a coin return mechanism of the machine 120. In another example, the user aborts the transaction by selection an abort affordance on the interface of the application 140 (not shown).

[00196] In some implementations, the notification indicates (1414) completion of a transaction between the user of the mobile device and the payment accepting unit. In Figure 26A, for example, the user interface 1302 includes the message 1306 indicating that completion of the transaction with the machine 120 initiated by the user of the mobile device 150.

[00197] In some implementations, the notification indicating completion of the transaction at least includes (1416) an amount of the completed transaction. In Figure 26A, for example, the user interface 1302 includes prepaid balance 1304 which indicates that \$1.00 has been deducted

from the prepaid balance after performing a transaction with the machine 120 as compared to the prepaid balance in Figure 10C-10D (i.e., \$9.00 in Figures 10C-10D and \$8.00 in Figure 26A).

[00198] In some implementations, the mobile device sends (1418) at least a portion of the notification to a server via a second communication capability distinct from the first communication capability. Operation 1260 of Figure 25B, for example, shows the mobile device 150 sending first transaction information to the server 130 for a completed transaction via the second communication capability (e.g., a long-range communication protocols such as Wi-Fi, CDMA, GSM, and/or the like). For example, the first transaction information at least includes the amount of the first completed transaction.

[00199] In some implementations, the first communication capability corresponds (1420) to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol. For example, the first communication capability of the mobile device 150 is a radio/transceiver means for communicating via one or more short-range communication protocols such as BLE, NFC, and/or the like (i.e., a non-persistent communication channel). For example, the second communication capability of the mobile device 150 is a radio/transceiver means for communicating via one or more long-range communication protocols such as Wi-Fi, CDMA, GSM, and/or the like.

[00200] In some implementations, the notification indicates (1422) failure of a transaction initiated by the user of the mobile device or a malfunction associated with the payment accepting unit. In Figure 26D, for example, the user interface 1330 includes the message 1332 indicating that there was an error with the transaction. For example, the transaction fails due to a vending jam or other malfunction. In another example, the payment accepting unit experiences a malfunction due to an open door or the like. In some implementations, at least a portion of the failure/malfunction notification is sent to the sever 130 and an alert is subsequently sent to the operator of the payment accepting unit (e.g., the machine 120) by the server 130.

[00201] It should be understood that the particular order in which the operations in Figures 27A-27B have been described is merely for example purposes and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to

other methods described herein are also applicable in an analogous manner to the method 1400 described above with respect to Figures 27A-27B.

[00202] Figure 28A illustrates a block diagram of an offline-payment operated machine 1500 in accordance with some implementations. For example, the offline-payment operated machine 1500 (e.g., a form of the machine 120) is an electro-mechanical machine capable of accepting currency (e.g., coins), which is not connected to any networks (e.g., telephone, cellular, or Wi-Fi). For example, the offline-payment operated machine 1500 is a washer or dryer at a laundromat, a parking meter, a car wash payment kiosk, or other offline-payment operated machine that dispenses goods and/or services.

[00203] In Figure 28A, the offline-payment operated machine 1500 includes a microswitch 1502, a control unit 1506, a power supply 1508, a transistor 1510, and an operation unit 1512. The components of the offline-payment operated machine 1500 in Figure 28A are examples and one of skill in the art will appreciate that various other components may be included in or excluded from the offline-payment operated machine 1500.

[00204] In Figure 28A, the microswitch 1502 is a leveraged microswitch with lever 1504. For example, the microswitch 1502 is a CHERRY BRAND™ microswitch with a normally open terminal (“NO”), a normally closed terminal (“NC”), and a common terminal. For example, the lever 1504 is incorporated into a coin slot of the offline-payment operated machine 1500 and is depressed whenever a coin slides down the coin slot into a coin reservoir of the offline-payment operated machine 1500 (not shown). For example, when the lever 1504 is depressed and the microswitch 1502 is wired in the NO configuration as shown in Figure 28A, the switch is closed. Continuing with this example, when the switch is closed, control unit 1506 receives a pulse (i.e., a payment acceptance signal) from the common terminal of the microswitch 1502 indicating depression of the lever 1504 from the reception of a US quarter (i.e., \$0.25) or coin of another value.

[00205] In some implementations, when the control unit 1506 receives a preset sequence of payment acceptance signals indicative of a preset number of coins being received by the microswitch 1502, the control unit 1506 initiates the operation of the offline-payment operated machine 1500. For example, after receiving the preset sequence of payment acceptance signals (e.g., three pulses indicating reception of three US quarters), the control unit 1506 initiates

operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512. For example, the operation unit 1512 is a motor of a dryer which begins spinning once current flows from the power supply 1508.

[00206] In Figure 28A, payment module 1520 (e.g., a form of the adapter module 100, Figures 5 and 20) is configured to be installed in the offline-payment operated machine 1500 so as to retrofit the offline-payment operated machine 1500 to be able to accept electronic payments. In some implementations, the payment module 1520 includes all or some of the components included adapter module 100 in Figure 20 such as processing unit 750, memory 760, a security unit 755, and a communications unit 770. In some implementations, the payment module 1520 also includes a first interface module 1522, a second interface module 1524, and a lead 1536 for drawing power from power supply 1508 of the offline-payment operated machine 1500.

[00207] In Figure 28A, the first interface module 1522 is configured to sample payment acceptance signals from the microswitch 1502 (e.g., a coin receiving switch) via lead 1532 of the offline-payment operated machine 1500. For example, the payment acceptance signals are indicative of a coin being received by the microswitch 1502 which depress lever 1504. In Figure 28A, the second interface module 1524 is configured to sample control signals from the control unit 1506 of the offline-payment operated machine 1500 via lead 1534 that initiate an operation of the offline-payment operated machine (e.g., the application of current to the gate of the transistor 1510) in response to receiving a preset sequence of payment acceptance signals from the microswitch 1502 (e.g., the coin receiving switch) indicative of the preset number of coins.

[00208] Figure 28B illustrates signals sampled by the payment module 1520 in accordance with some implementations. In Figure 28B, sample 1550 represents a preset sequence of payment acceptance signals sampled by the first interface module 1522 via lead 1532 that are sent from the microswitch 1502 to the control unit 1506. For example, the preset sequence of payment acceptance signals indicative of the preset number of coins include pulses (i.e., payment acceptance signals) 1552, 1554, 1556, and 1558. For example, the leading edges of pulses 1552, 1554, 1556, and 1558 at times 1582, 1584, 1586, and 1588 indicate reception of a coin by microswitch 1502 which causes the switch to close when wired in the NO configuration as

shown in Figure 28A. In Figure 28B, sample 1570 represents a control signal sampled by the second interface module 1524 via lead 1534 that is sent from the control unit 1506 to transistor 1510. In Figure 28B, the sample 1570 includes a pulse 1572 that is sent from the control unit 1506 to transistor 1510 at time 1590 after receiving the preset sequence of payment acceptance signals from the microswitch 1502 (i.e., pulses 1552, 1554, 1556, and 1558).

[00209] Figures 29A-29B illustrate a flowchart diagram of a method of retrofitting an offline-payment operated machine to accept electronic payments in accordance with some implementations. In some implementations, the method 1600 is performed by a payment module with one or more processors and memory. In some implementations, the payment module also includes a short-range communication capability corresponding to a short-range communication protocol (e.g., a non-persistent communication channel such as BLE, NFC, and/or the like), where the short-range communication capability is configured to communicate with one or more mobile devices, where each of the one or more mobile devices is configured with a complimentary short-range communication capability and a long-range communication capability corresponding to a long-range communication protocol (e.g., Wi-Fi, CDMA, GSM, and/or the like).

[00210] In some implementations, the payment module is coupled with an offline-payment operated machine (e.g., the payment accepting unit 120, Figures 5 and 19 (sometimes also herein called “machine 120”), or the offline-payment operated machine 1500, Figure 28A) such as dryer or washer in a laundromat, a parking meter, a car wash payment kiosk, or the like. In some implementations, the offline-payment operated machine includes a coin receiving switch (e.g., the microswitch 1502, Figure 28A) and a control unit (e.g., the control unit 1506, Figure 28A). In some implementations, the payment module further includes: (A) a first interface module (e.g., the first interface module 1522, Figure 28A) configured to sample payment acceptance signals from the coin receiving switch of the offline-payment operated machine, where the signals are indicative of a coin being received by the coin receiving switch; and (B) a second interface module (e.g., the second interface module 1524, Figure 28A) configured to sample control signals from the control unit of the offline-payment operated machine that initiate an operation of the offline-payment operated machine in response to receiving a preset sequence of payment acceptance signals from the coin receiving switch indicative of the preset number of coins. By sampling and storing these signals, the payment module 1520 is able to simulate

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

[00211] For example, in some implementations, the method 1600 is performed by the adapter module 100 (Figures 5 and 20) or payment module 1520 (Figure 28A). In some implementations, the method 1600 is governed by instructions that are stored in a non-transitory computer readable storage medium (e.g., the memory 760, Figure 20) and the instructions are executed by one or more processors (e.g., the processing unit 750, Figure 20) of the payment module. Optional operations are indicated by dashed lines (e.g., boxes with dashed-line borders).

[00212] In some implementations, the payment module detects (1602), via the first interface module, a preset sequence of payment acceptance signals from the coin receiving switch that causes the control unit to initiate the operation of the offline-payment operated machine, where the preset sequence of payment acceptance signals are indicative of a preset number of coins received by the coin receiving switch. For example, with reference to Figures 28A-28B, the first interface module 1522 of the payment module 1520 samples payment acceptance signals via lead 1532 from the microswitch 1502 to the control unit 1506. For example, each of the payment acceptance signals is indicative of reception of a coin by the microswitch 1502. Continuing with this example, the second interface module 1524 of the payment module 1520 samples control signals via lead 1534 from the control unit 1506 to the transistor 1510. The payment module 1520 detects a preset sequence of payment acceptance signals from the microswitch 1502 that causes the control unit 1506 to apply a current to the gate of the transistor 1510 (e.g., the control signals). For example, the preset sequence of payment acceptance signals is indicative of a preset number of coins received by the microswitch 1502 to cause operation of the offline-payment operated machine 1500. For example, the application of current to the gate of the transistor 1510 allows current to flow from the power supply 1508 to the operation unit 1512 so that the operation. For example, the operation unit 1512 is a motor of a dryer which begins spinning once current flows from the power supply 1508.

[00213] In some implementations, the payment module determines (1604) the predefined signal sequence to emulate the preset sequence of payment acceptance signals from the coin receiving switch. In some implementations, after detecting the preset sequence of payment

acceptance signals that causes the control unit 1506 to initiate the operation of the offline-payment operated machine 1500, the payment module 1520 determines a predefined signal sequence to emulate the preset sequence of payment acceptance signals. In some implementations, the money value associated with each pulse in the preset sequence of payment acceptance signals from the microswitch 1502, indicative of the preset number of coins to initiate the operation of the offline-payment operated machine 1500, is a default currency (e.g., USD) and amount (e.g., \$0.25) set in the firmware of the payment module 1520. In some implementations, the money value associated with the each pulse in the preset sequence of payment acceptance signals from the microswitch 1502, indicative of the preset number of coins to initiate the operation of the offline-payment operated machine 1500, is set by the server 130 and can be changed remotely by using the mobile device 150 as a communications bridge to send information indicating the value of a pulse from the server 130 to the mobile device 150 via the second communication capability (e.g., GSM, CDMA, or Wi-Fi) and forwarding the information from the mobile device to the payment module 1520 via the first communication capability (e.g., BLE). For instance, in most cases, each pulse is US \$0.25.

[00214] In some implementations, determining the predefined signal sequence includes (1606) at least one of: identifying a count of pulses in the present sequence of payment acceptance signals; identifying amplitude of pulses in the present sequence of payment acceptance signals; identifying shape of pulses in the present sequence of payment acceptance signals; and identifying an interval between pulses. In some implementations, after detecting the preset sequence of payment acceptance signals (e.g., the sample 1550, Figure 28B), the payment module 1520 determines a predefined signal sequence to emulate the preset sequence of payment acceptance signals by identifying a count of pulses in the preset sequence of payment acceptance signals, an interval between pulses in the preset sequence of payment acceptance signals, the shape of pulses in the preset sequence of payment acceptance signals, and an amplitude of pulses in the preset sequence of payment acceptance signals.

[00215] The payment module receives (1608) a request via the short-range communication capability from a respective mobile device to perform an operation of the offline-payment operated machine. For example, with reference to Figure 8C, the payment module 1520 (Figure 28A) receives the AuthGrant from the mobile device 150 via the short-range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the

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

[00216] The payment module validates (1610) the request. Validation of the request indicates (1612) that the respective mobile device is authorized to initiate payment for the operation by a remote server via the long-range communication capability. In some implementations, the payment module 1520 validates the request from the mobile device 150 by determining whether the AuthGrant or the authorization grant token includes a valid authorization code.

[00217] In accordance with a determination that the request is valid, the payment module causes (1614) the payment operated machine to perform the operation by issuing a predefined signal sequence to the control unit, where the predefined signal sequence emulates a signal sequence that would be issued by the coin receiving switch in response to receiving a preset number of coins. For example, with reference to Figure 28B, the payment module 1520 issues a predefined signal sequence with first interface module 1522 to the control unit 1506 that emulates sample 1550 in Figure 28B. Continuing with this example, in response to receiving the predefined signal sequence from the payment module 1520 control unit 1506 causes initiation of the operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512. In some implementations, the control unit 1506 causes initiation of the operation by setting a timer to an amount of time corresponding to the preset number of coins whereby current flows to the gate of the transistor 1510 for the set amount of time. For example, the preset number of coins is a number of a coins required to run the offline-payment operated machine 1500 by for a default amount of time and subsequent coins may be added to extend the amount of time that the offline-payment operated machine 1500 by will run. In some implementations, the preset number of coins is a number of a coins required to cause the offline-payment operated machine 1500 to dispense a purchased item, such as laundry detergent.

[00218] Alternatively, in some implementations, in accordance with a determination that the request is valid, the offline-payment operated machine 1500 displays credit to the user (e.g., via one of the displays 122 or 124 shown in Figure 19) and the user interacts with the input mechanisms of the offline-payment operated machine 1500 120 (e.g., via the buttons 126 or a touch screen display 124 shown in Figure 19) to perform the operation of the machine. For example, if the offline-payment operated machine 1500 is a dryer, the user of the mobile device 150 selects the appropriate spin cycle via input mechanisms of the dryer, and when the user of the mobile device 150 selects a start/run input mechanism of the dryer, control unit 1506 of the dryer causes initiation of the operation of the dryer (e.g., starting a motor that corresponds to operation unit 1512 in Figure 28A).

[00219] In some implementations, prior to sending the operation information and after causing the offline-payment operated machine to perform the operation by issuing the predefined signal sequence to the control unit, the payment module obtains (1616) a notification from the offline-payment operated machine indicating initiation of the operation of the offline-payment operated machine and the preset number of coins. For example, after issuing the preset signal sequence to control unit 1506, the payment module 1520 (Figure 28A) obtains a notification indicating that the control unit 1506 sent control signals to initiate operation of the offline-payment operated machine 1500 in response to receiving the predefined signal sequence. For example, the notification is obtained by the second interface module 1524 (e.g., the sample 1570, Figure 28B) sampling controls signals sent by control unit 1506 (e.g., application of current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512).

[00220] In response to receiving the notification, the payment module (1618): generates the operation information based at least in part on the notification; and stores the generated operation information in the memory. For example, after obtaining the notification, the payment module 1520 (Figure 28A) generates operation information corresponding to performance of the operation and the preset number of coins associated with the predefined signal sequence (e.g., the amount required to initiate operation of the offline-payment operated machine 1500) and stores the operation information in memory local to the payment module 1520 (e.g., the memory 760, Figure 20).

[00221] In some implementations, the payment module sends (1620) operation information corresponding to the operation to the respective mobile device via the short-range communication capability. For example, after operation 1618, the payment module 1520 (Figure 28A) sends the operation information to the mobile device 150 via the first communication capability of the mobile device 150 such as a radio/transceiver means for communicating via one or more short-range communication protocols such as BLE, NFC, and/or the like (i.e., a non-persistent communication channel)

[00222] It should be understood that the particular order in which the operations in Figures 29A-29B have been described is merely for example purposes and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to other methods described herein (e.g., the method 1700 in Figure 30) are also applicable in an analogous manner to the method 1600 described above with respect to Figures 29A-29B.

[00223] Figure 30 illustrates a flowchart diagram of a method 1700 of enabling a payment operated machine to accept electronic payments in accordance with some implementations. In some implementations, the method 1700 is performed by an offline-payment operated machine (e.g., the payment accepting unit 120, Figures 5 and 19 (sometimes also herein called “machine 120”), or the offline-payment operated machine 1500, Figure 28A) such as dryer or washer in a laundromat, a parking meter, a car wash payment kiosk, or the like.

[00224] In some implementations, the offline-payment operated machine includes a control unit (e.g., the control unit 1506, Figure 28A), memory, and a coin receiving switch (e.g., the microswitch 1502, Figure 28A). In some implementations, the offline-payment operated machine also includes a short-range communication capability corresponding to a short-range communication protocol (e.g., a non-persistent communication channel such as BLE, NFC, and/or the like), where the short-range communication capability is configured to communicate with one or more mobile devices, where each of the one or more mobile devices is configured with a complimentary short-range communication capability and a long-range communication capability corresponding to a long-range communication protocol (e.g., Wi-Fi, CDMA, GSM, and/or the like). For example, in some implementations, the method 1700 is performed by the

machine 120, (Figures 5 and 19). In some implementations, the method 1700 is governed by instructions that are stored in a non-transitory computer readable storage medium and the instructions are executed by the control unit of the offline-payment operated machine.

[00225] The offline-payment operated machine receives (1702) a request via a short-range communication capability from a respective mobile device to perform an operation of the offline-payment operated machine. For example, with reference to Figure 8C, the payment module 1520 (Figure 28A) receives the AuthGrant from the mobile device 150 via the short-range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A). For example with reference to operation 1012 in Figure 23, the payment module 1520 (Figure 28A) receives an authorization grant token from the mobile device 150 via the short-range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A).

[00226] The offline-payment operated machine validates (1704) the request. Validation of the request indicates (1706) that the respective mobile device is authorized to initiate payment for the operation by a remote server via the long-range communication capability. In some implementations, the payment module 1520 validates the request from the mobile device 150 by determining whether the AuthGrant or the authorization grant token includes a valid authorization code.

[00227] In accordance with a determination that the request is valid, the offline-payment operated machine performs (1708) the operation by issuing a predefined signal sequence to the control unit, where the predefined signal sequence emulates a preset number of coins received by the coin receiving switch. For example, in accordance with a determination that the request is valid, the offline-payment operated machine or a component thereof issues a predefined signal sequence to the control unit 1506 that emulates sample 1550 in Figure 28B. Continuing with this example, in response to receiving the predefined signal sequence from the payment module 1520, control unit 1506 causes initiation of the operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512. In another example, in accordance with a determination that the request is valid, the control unit 1506 causes initiation of the operation of

the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512.

[00228] It should be understood that the particular order in which the operations in Figure 30 have been described is merely for example purposes and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to other methods described herein (e.g., the method 1600 in Figures 29A-29B) are also applicable in an analogous manner to the method 1700 described above with respect to Figure 30.

MISCELLANEOUS

[00229] It should be noted that relative terms are meant to help in the understanding of the technology and are not meant to limit the scope of the invention. Similarly, unless specifically stated otherwise, the terms used for labels (e.g., “first,” “second,” and “third”) are meant solely for purposes of designation and not for order or limitation. The term “short” in the phrase “short-range” (in addition to having technology specific meanings) is relative to the term “long” in the phrase “long-range.”

[00230] The terms “may,” “might,” “can,” and “could” are used to indicate alternatives and optional features and only should be construed as a limitation if specifically included in the claims.

[00231] It should be noted that, unless otherwise specified, the term “or” is used in its nonexclusive form (e.g., “A or B” includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, “and/or” is used similarly (e.g., “A and/or B” includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, the terms “includes” and “has” mean “comprises” (e.g., a device that includes, has, or comprises A and B contains A and B, but optionally may contain C or additional components other than A and B). It should be noted that, unless otherwise specified, the singular forms “a,” “an,” and “the” refer to one or more than one, unless the context clearly dictates otherwise.

[00232] It is to be understood that the inventions, examples, and implementations described herein are not limited to particularly exemplified materials, methods, and/or structures. It is to be understood that the inventions, examples, and implementations described herein are to be considered preferred inventions, examples, and implementations whether specifically identified as such or not.

[00233] The terms and expressions that have been employed in the foregoing specification are used as terms of description and not of limitation, and are not intended to exclude equivalents of the features shown and described. While the above is a complete description of selected implementations of the present invention, it is possible to practice the invention using various alternatives, modifications, adaptations, variations, and/or combinations and their equivalents. It will be appreciated by those of ordinary skill in the art that any arrangement that is calculated to achieve the same purpose may be substituted for the specific embodiment shown. It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described and all statements of the scope of the invention that, as a matter of language, might be said to fall therebetween.

CLAIMS

1. A method of presenting representations of payment accepting unit events, comprising:
at a mobile device with one or more processors, memory, one or more output devices including a display, and one or more radio transceivers:

identifying one or more payment accepting units that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier or location corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input selecting an available payment accepting unit of the one or more payment accepting units;

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete a transaction with the available payment accepting unit, wherein the user interface includes a visual representation of the available payment accepting unit, an indication of a balance, and an affordance that, in response to a user input, indicates completion of the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

2. The method of claim 1, wherein the updated user interface of the mobile payment application includes at least one of:

a message displayed on the display of the mobile device;

a banner notification displayed on a display of the mobile device; and/or

a visual alert from one or more LEDs of the mobile device.

3. The method of claim 1, wherein the information indicates completion of the transaction between the user of the mobile device and the available payment accepting unit.
4. The method of claim 3, wherein the mobile device includes a long-range transceiver and the information at least includes an amount of the completed transaction, and the method further comprises:
 - sending at least the amount of the completed transaction to a server via the long-range transceiver.
5. The method of claim 1, wherein the information indicates abortion of the transaction initiated by the user of the mobile device.
6. The method of claim 1, wherein the information indicates failure of the transaction initiated by the user of the mobile device or a malfunction associated with the available payment accepting unit.
7. The method of claim 1, wherein the mobile device includes an accelerometer and the method further comprises:
 - based on data from the accelerometer, determining whether the user is walking away from the available payment accepting unit; and
 - in accordance with a determination that the user is walking away from the available payment accepting unit, canceling the wireless communication path.
8. The method of claim 1, wherein the information reflects availability of the available payment accepting unit to conduct a transaction.
9. The method of claim 1, further comprising:
 - in addition to exchanging the information, receiving, via the one or more radio transceivers, a coupon that is targeted to the user of the mobile device based on the transaction.
10. The method of claim 1, wherein the user interface of the mobile payment application, after establishing the wireless communication path, indicates that the wireless communication path has been established with the available payment accepting unit.

11. The method of claim 1, wherein the user input is a swipe that causes the affordance to be slid.

12. The method of claim 1, wherein the payment operated machines include a payment activated washer, a payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

13. A mobile device, comprising:

one or more radio transceivers;

one or more output devices including a display;

one or more processors; and

memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for:

identifying one or more payment accepting units that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier or location corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input selecting an available payment accepting unit of the one or more payment accepting units;

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete a transaction with the available payment accepting unit, wherein the user interface includes a visual representation of the available payment accepting unit, an indication of a balance, and an affordance that, in response to a user input, indicates completion of the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

14. The mobile device of claim 13, wherein identifying the one or more payment accepting units includes identifying a payment activated washer, a payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

15. A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a mobile device with one or more processors, one or more output devices including a display, and one or more radio transceivers, cause the mobile device to perform operations comprising:

identifying one or more payment accepting units that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier or location corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input selecting an available payment accepting unit of the one or more payment accepting units;

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete a transaction with the available payment accepting unit, wherein the user interface includes a visual representation of the available payment accepting unit, an indication of a balance, and an affordance that, in response to a user input, indicates completion of the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

16. The non-transitory computer readable storage medium of claim 15, wherein the updated user interface of the mobile payment application includes at least one of:

- a message displayed on the display of the mobile device;
- a banner notification displayed on a display of the mobile device; and/or
- a visual alert from one or more LEDs of the mobile device.

17. The non-transitory computer readable storage medium of claim 15, wherein:
the information indicates completion of the transaction between the user of the mobile device and the available payment accepting unit;

- the information at least includes an amount of the completed transaction; and
- the instructions further cause the mobile device to send at least the amount of the completed transaction to a server.

18. The non-transitory computer readable storage medium of claim 15, wherein the information indicates abortion of the transaction initiated by the user of the mobile device.

19. The non-transitory computer readable storage medium of claim 15, wherein the information indicates failure of the transaction initiated by the user of the mobile device or a malfunction associated with the available payment accepting unit.

20. The non-transitory computer readable storage medium of claim 15, wherein identifying the one or more payment accepting units includes identifying a payment activated washer, a payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

ABSTRACT

A mobile device presents representations of payment accepting unit events on a display, by identifying a payment accepting unit that is available to accept payment, displaying a visual indication of the payment accepting unit, and accepting user input to receive selection of the payment accepting unit and trigger payment, establishing a wireless communication path including the mobile device and the payment accepting unit, enabling user interaction with the user interface to complete the transaction, exchanging information with the available payment accepting unit via the one or more radio transceivers in conjunction with the transaction, and displaying an updated user interface of the mobile payment application.

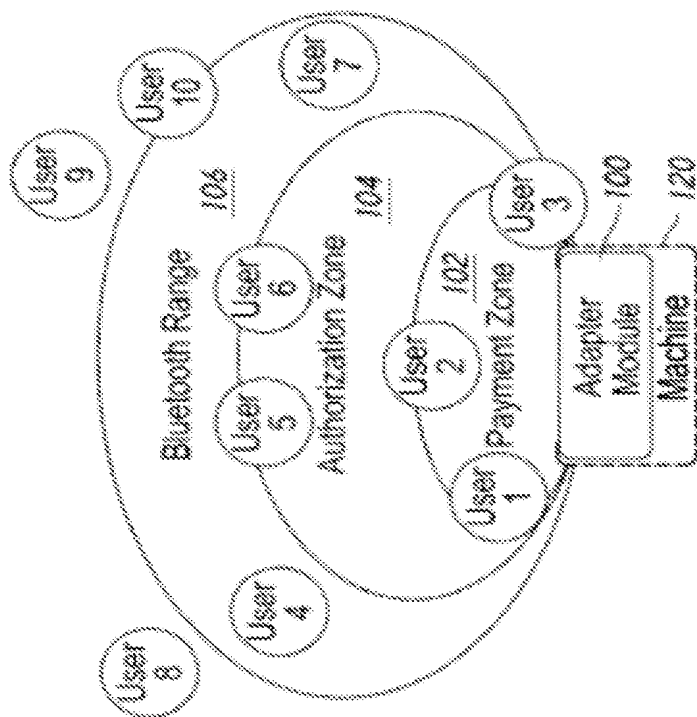


Figure 2

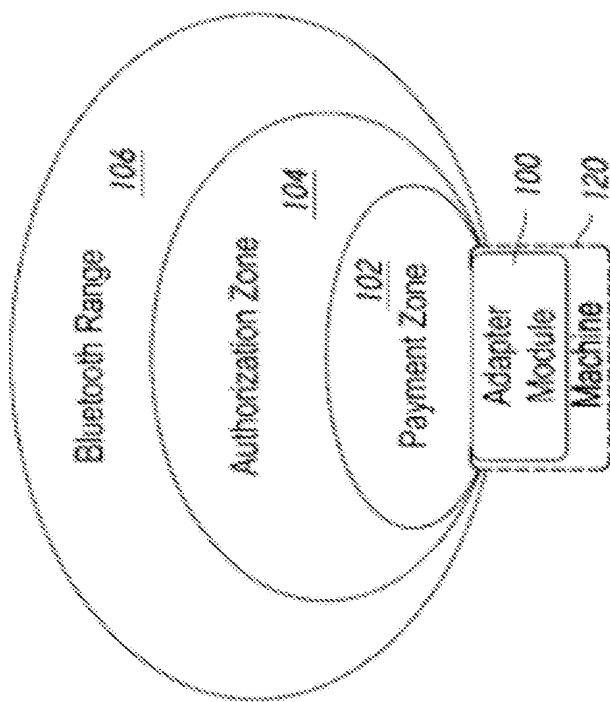


Figure 1

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

Figure 3

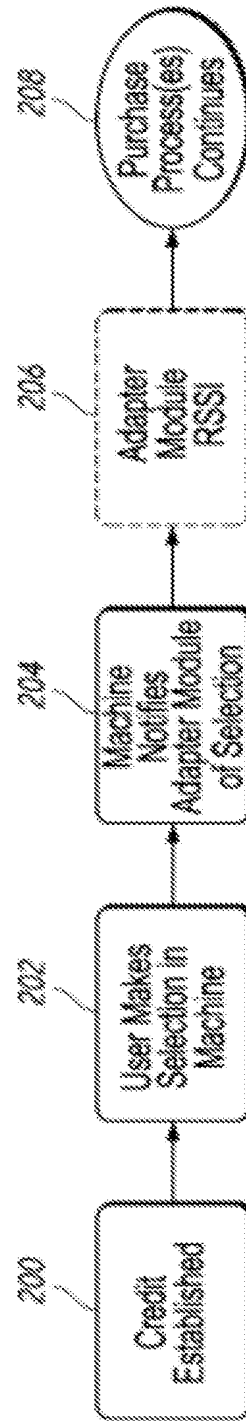


Figure 4

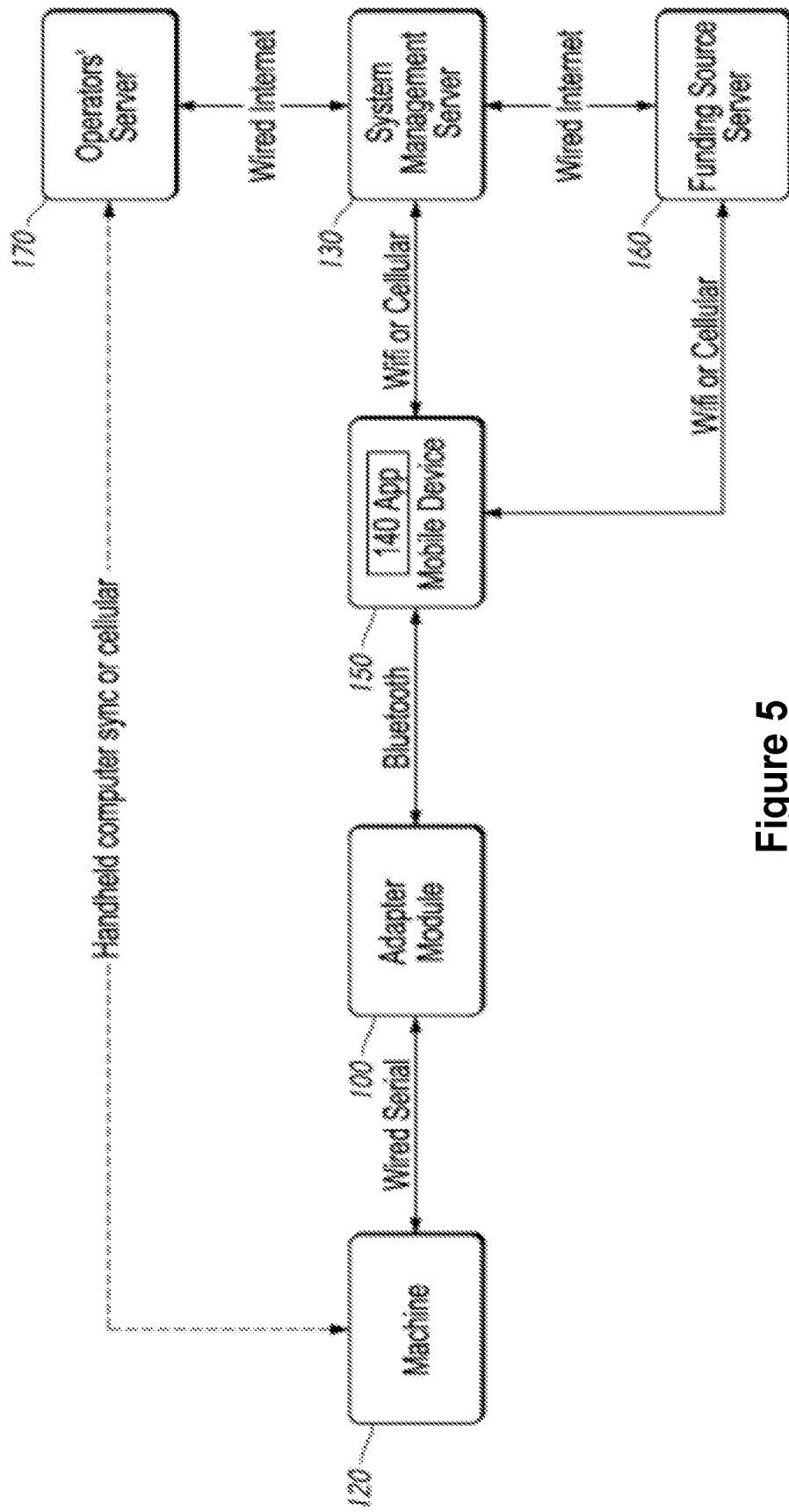


Figure 5

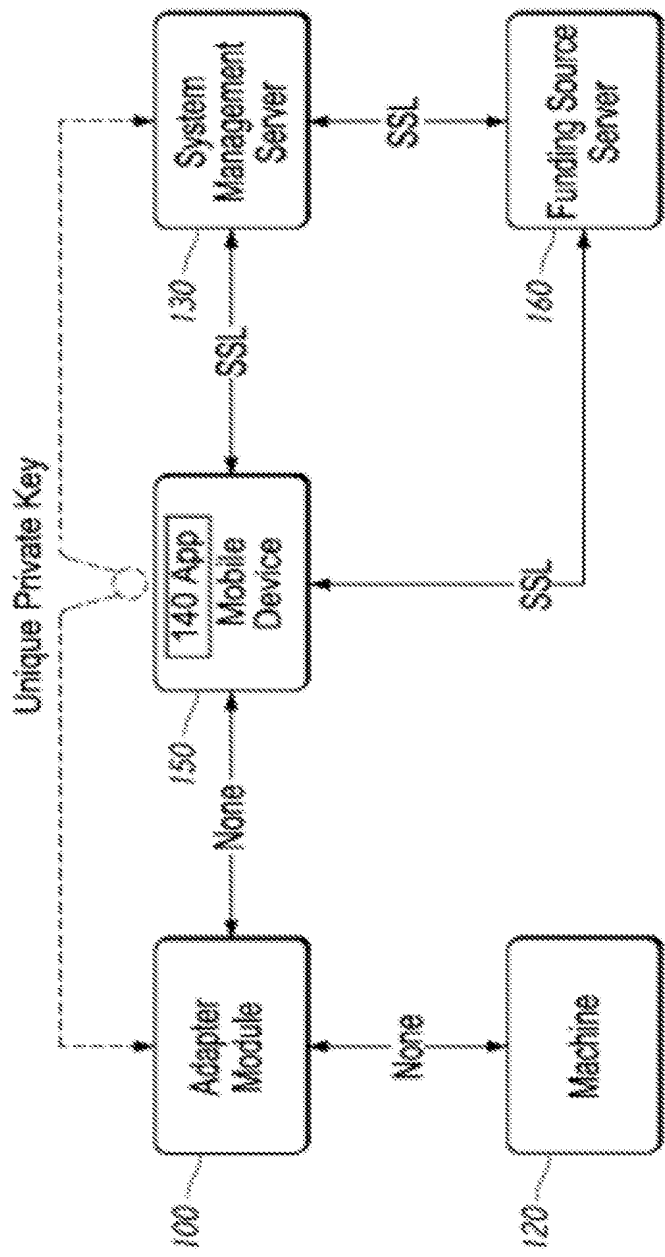


Figure 6

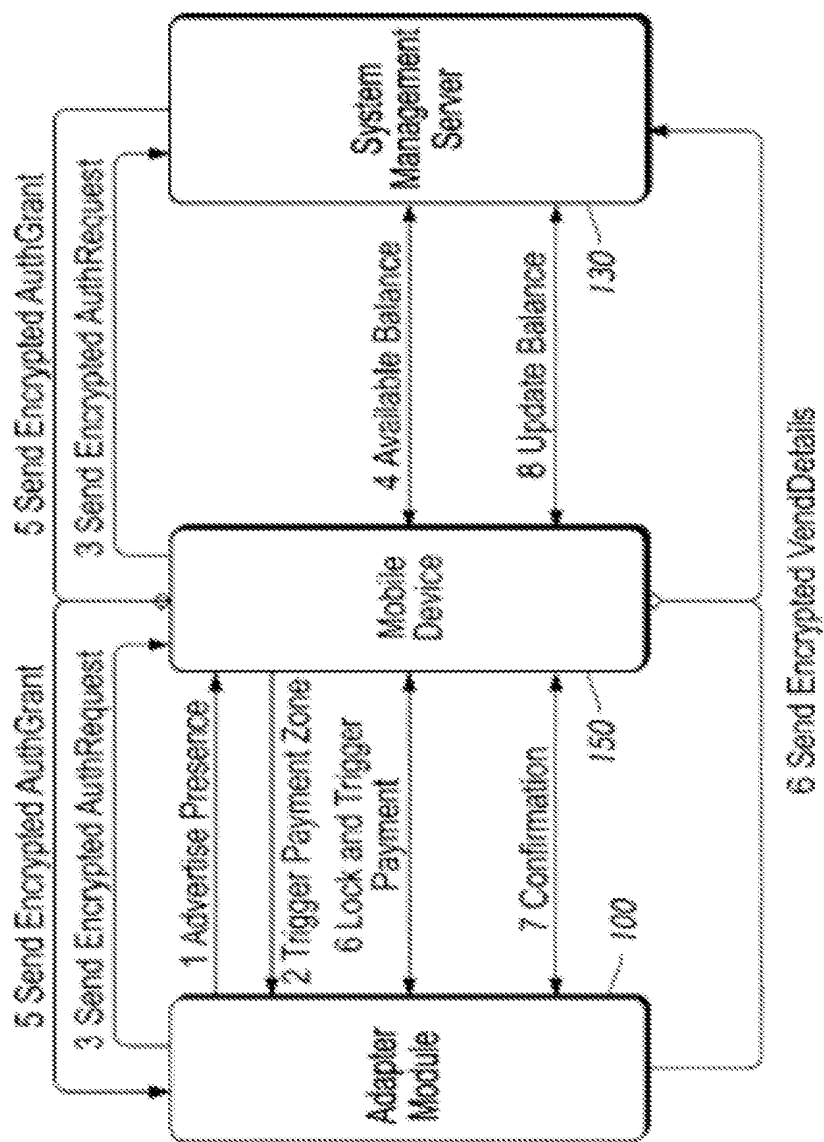


Figure 7

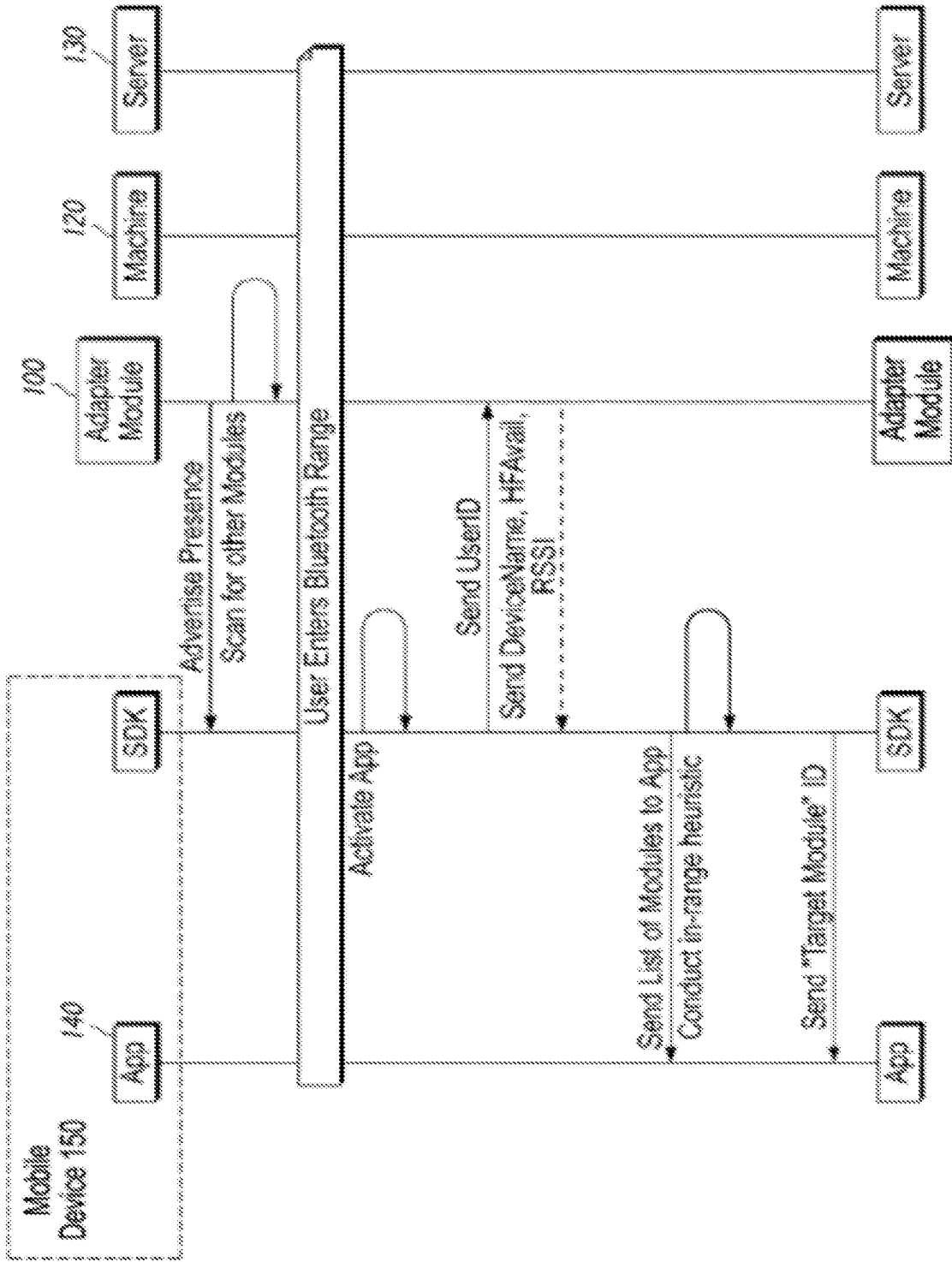


Figure 8A

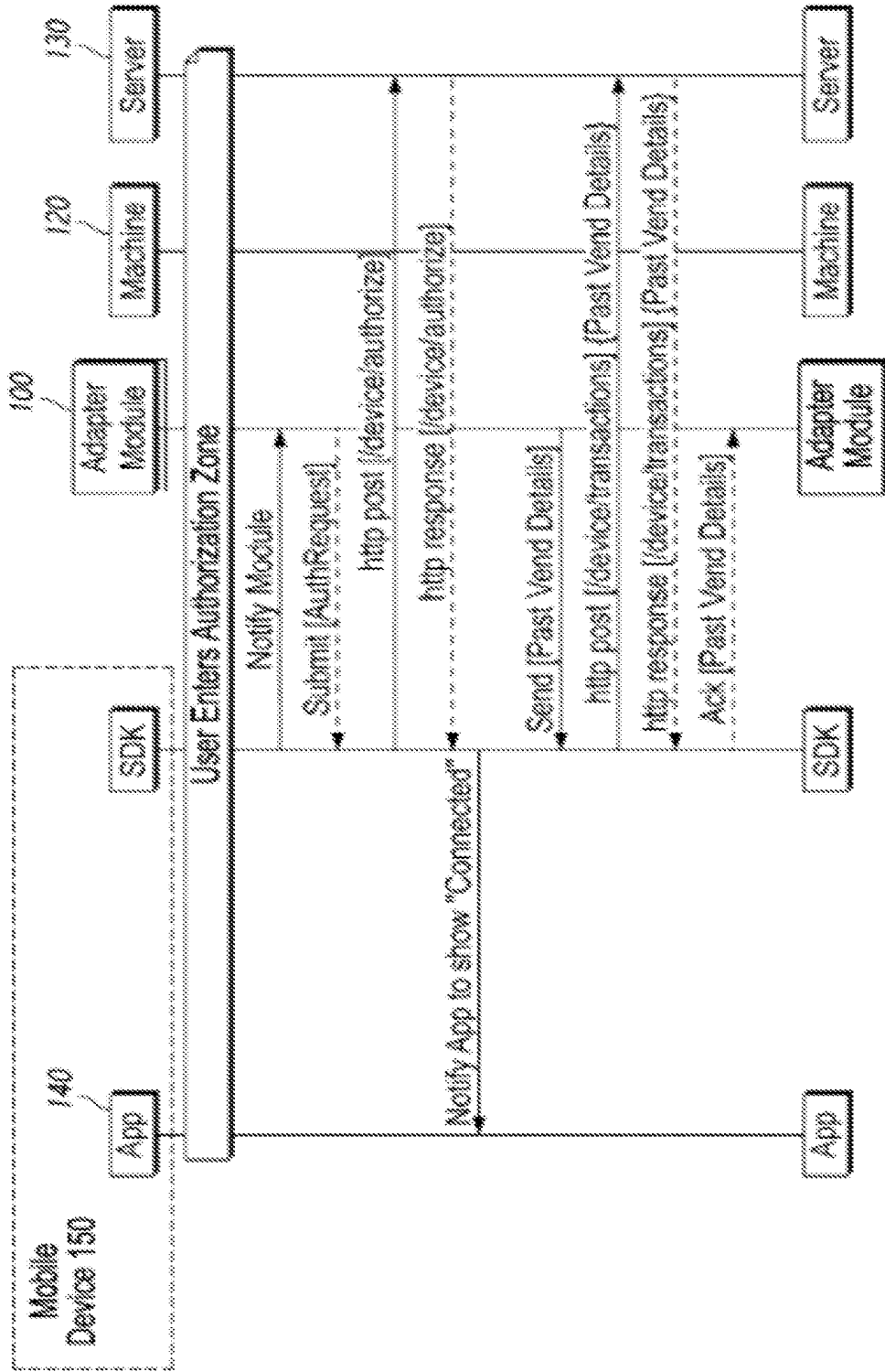


Figure 8B

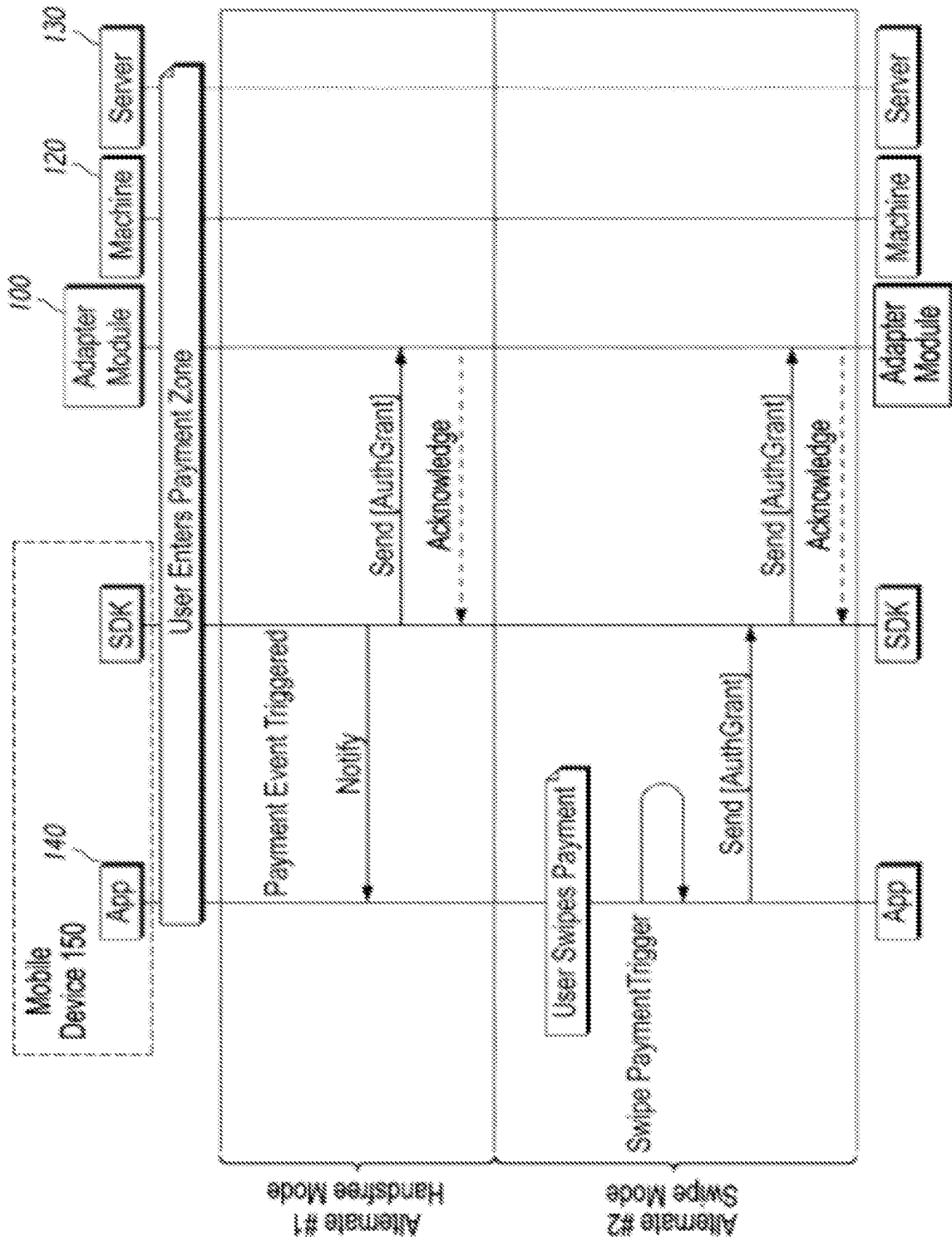


Figure 8C

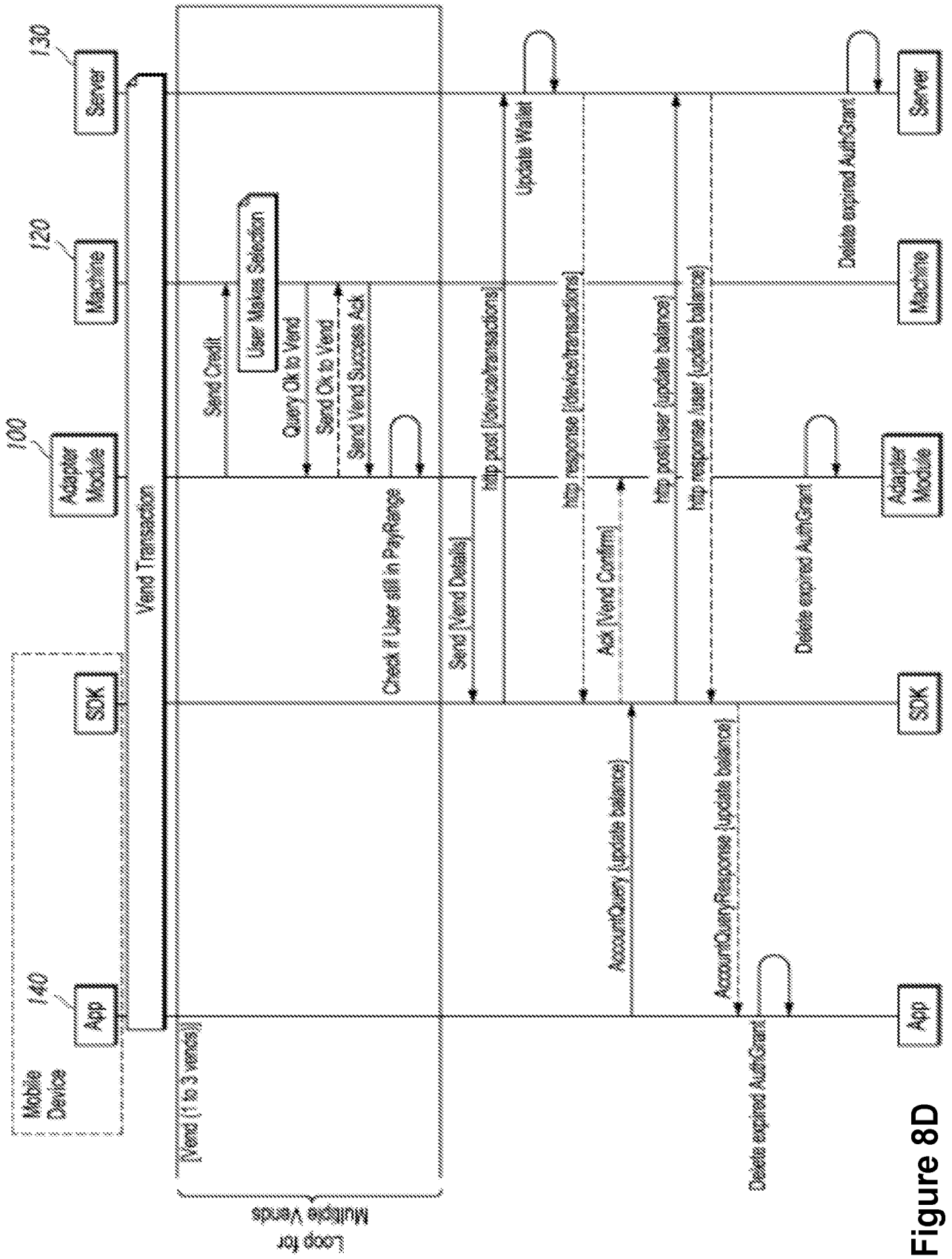


Figure 8D

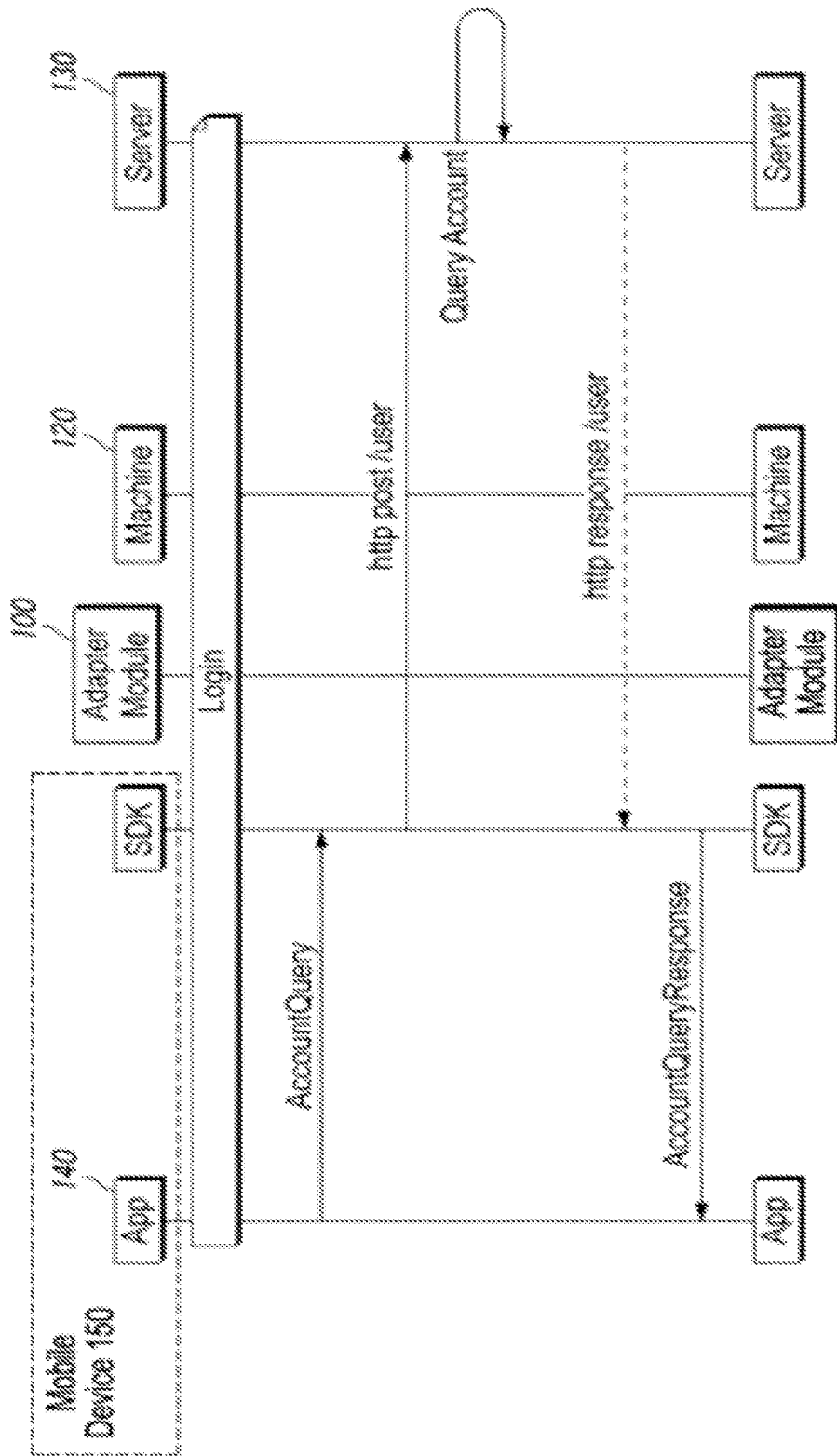


Figure 8E

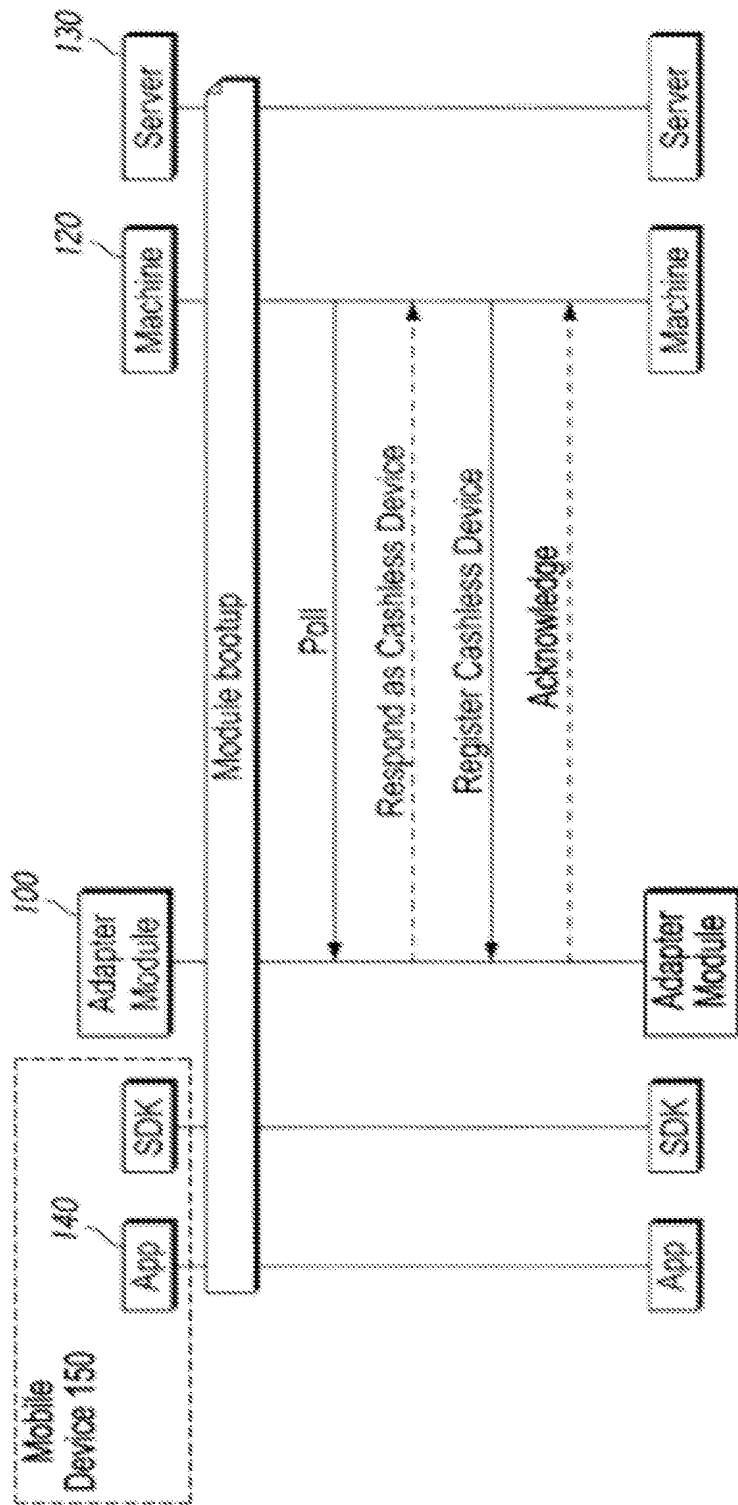


Figure 8F

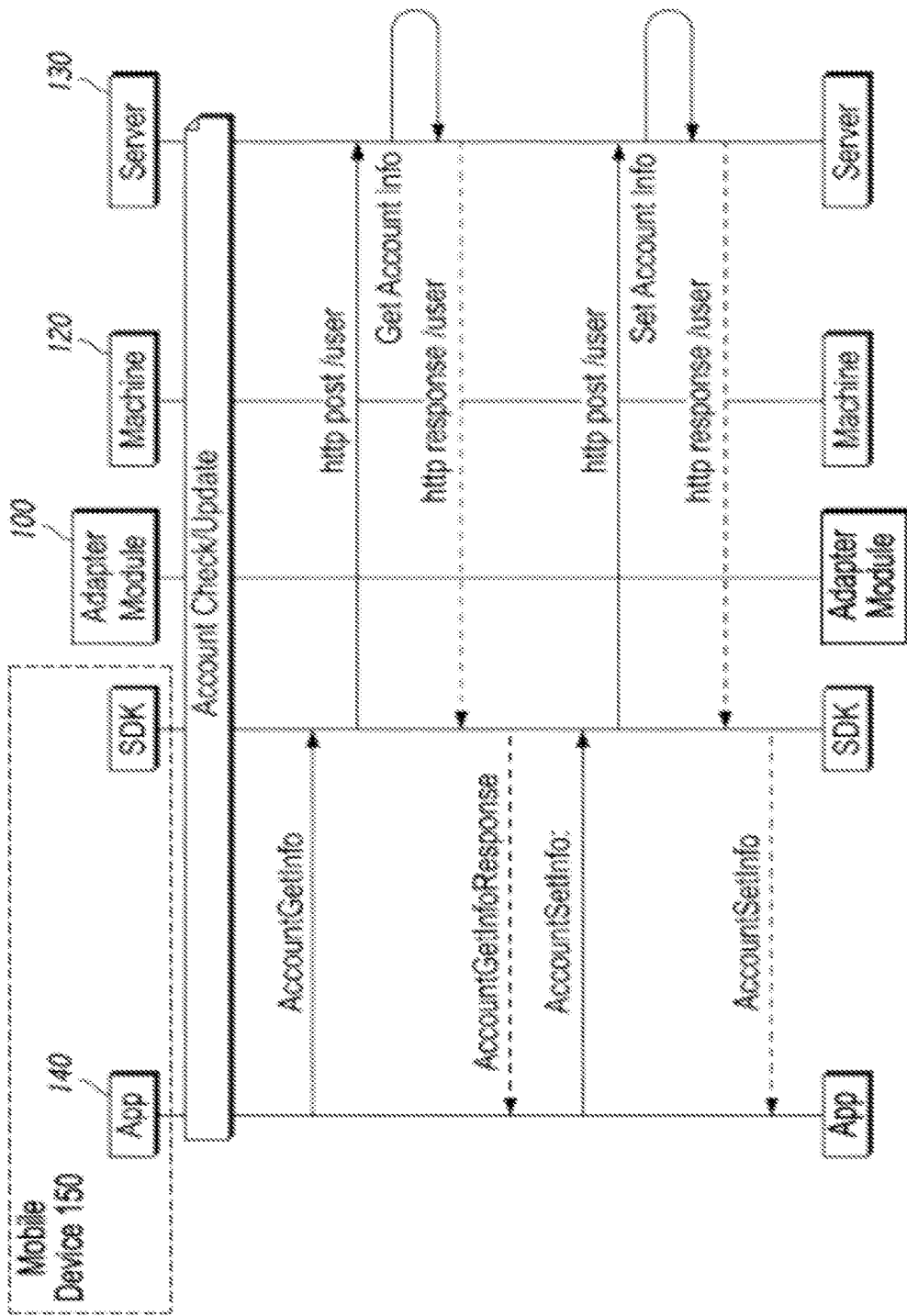


Figure 8G

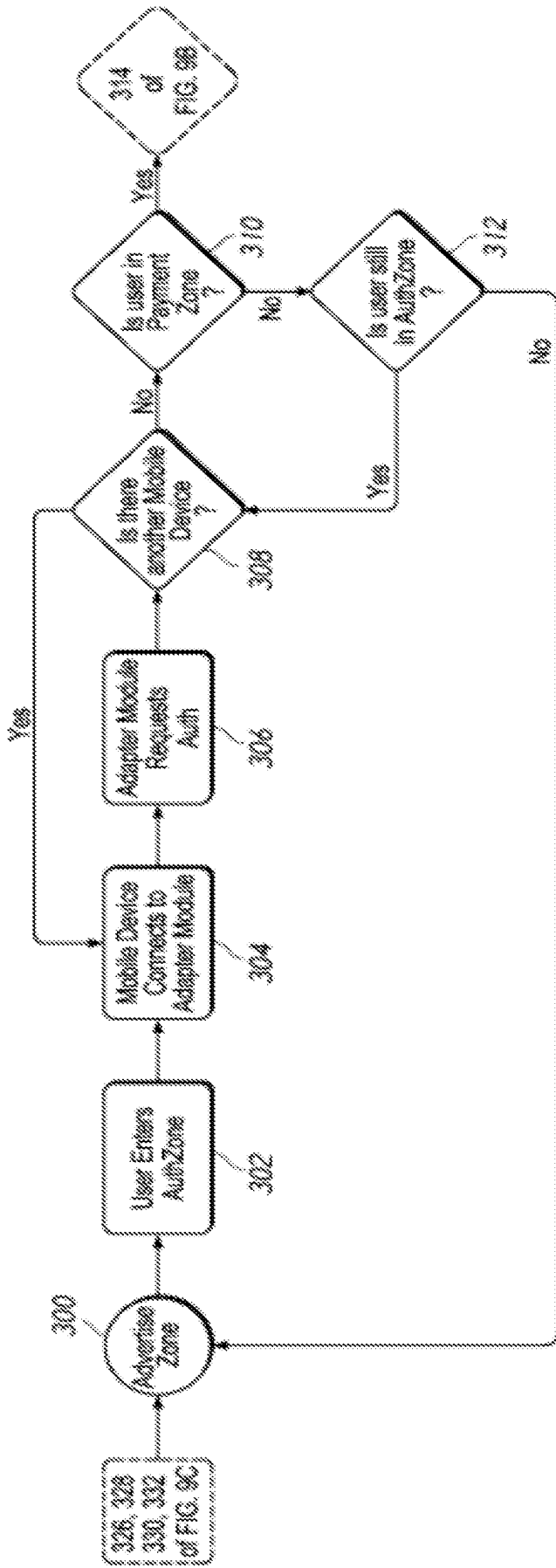


Figure 9A

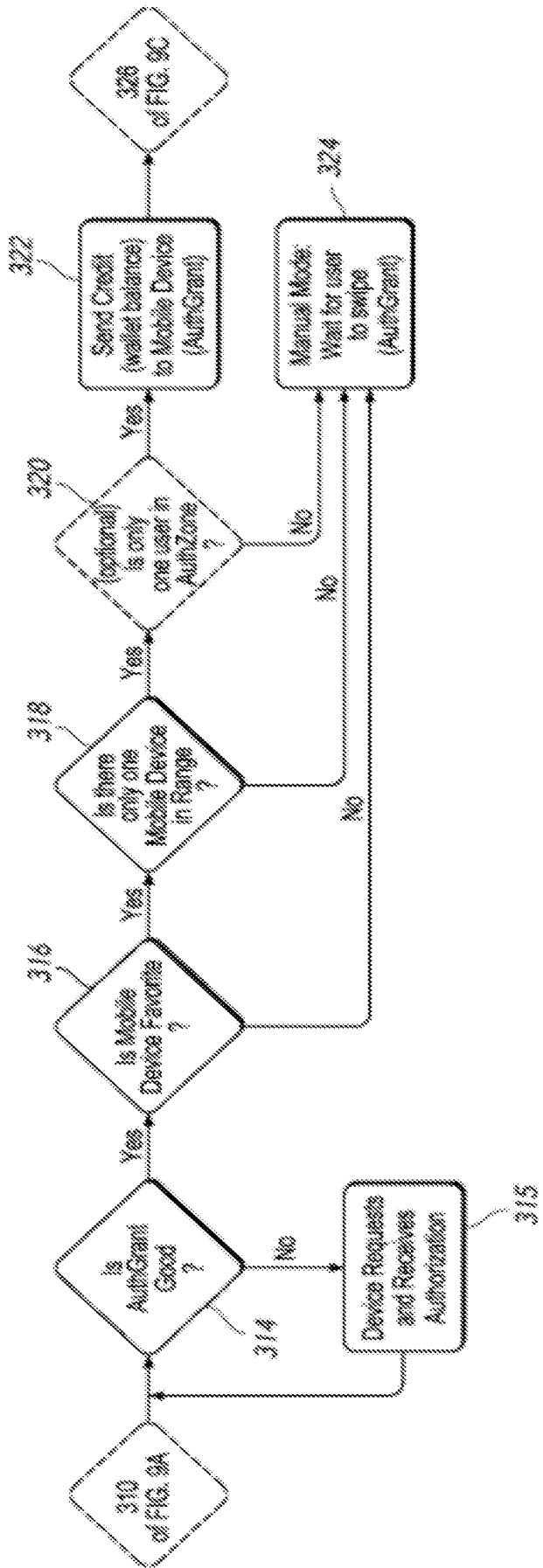
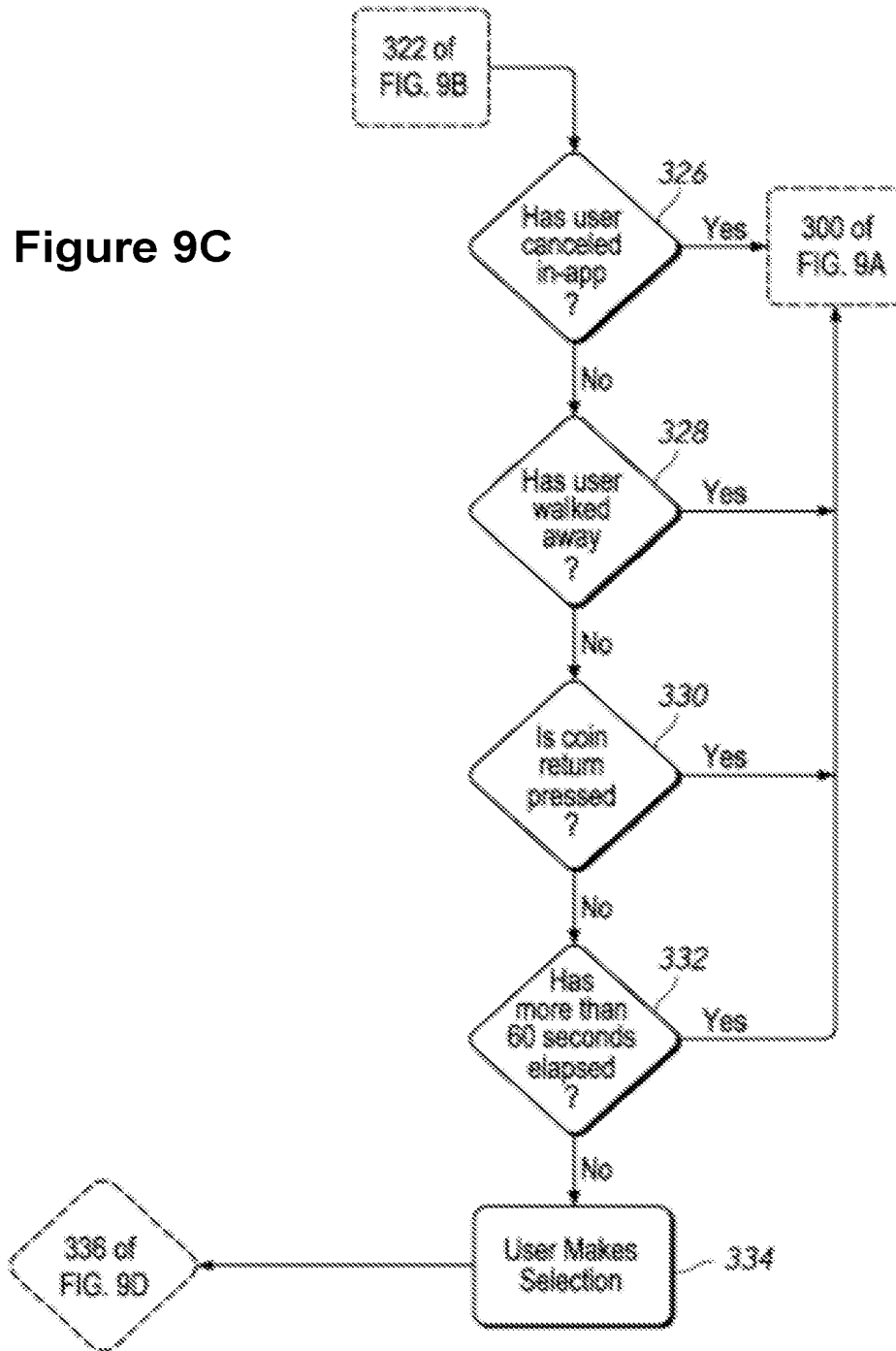


Figure 9B

Figure 9C



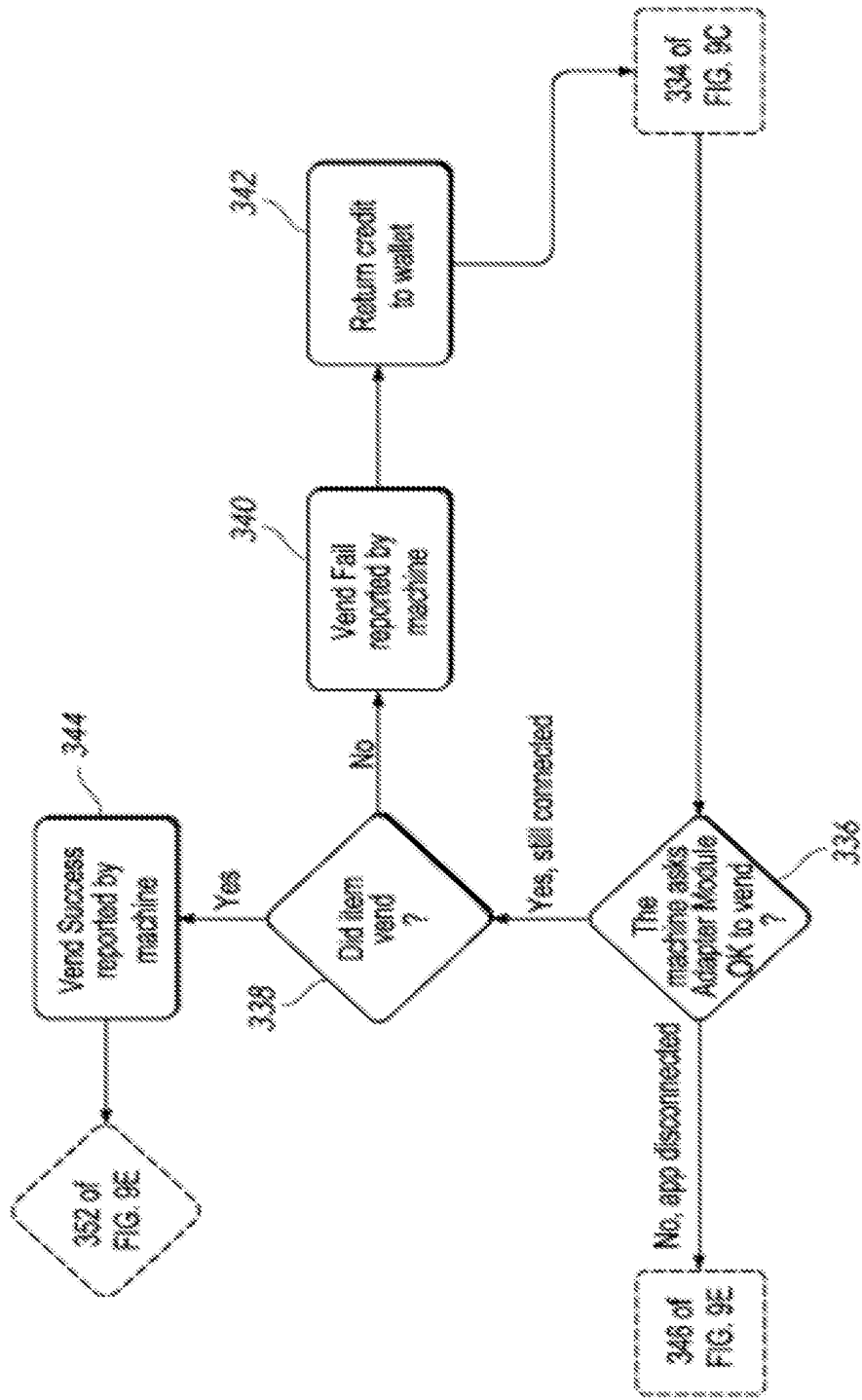


Figure 9D

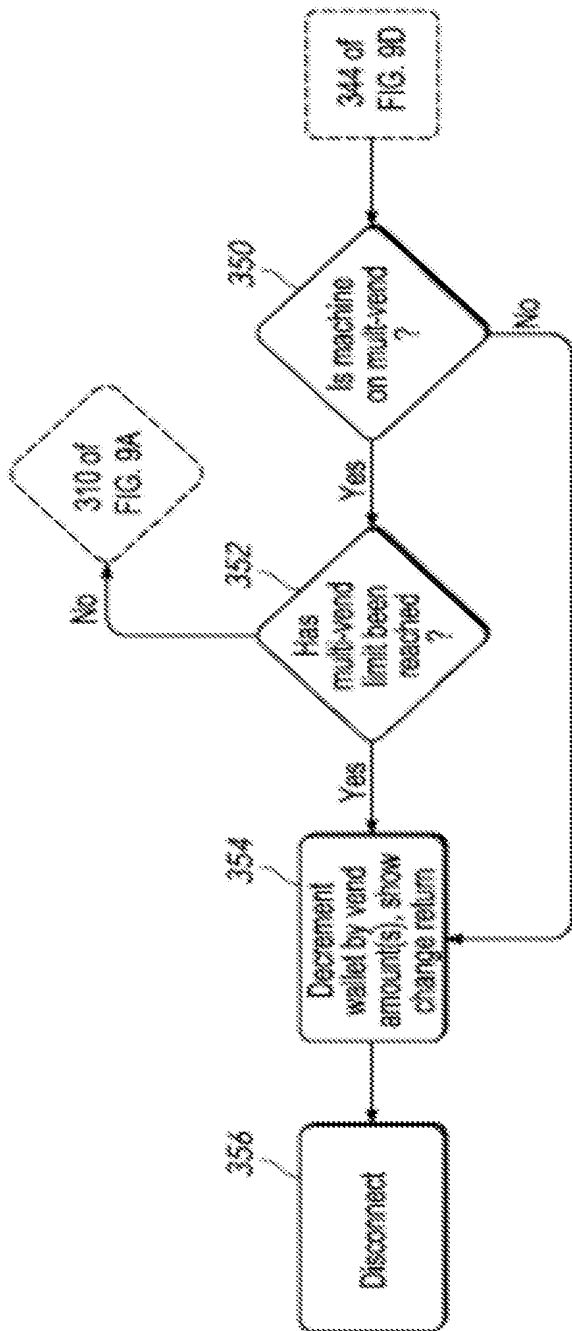


Figure 9E

150

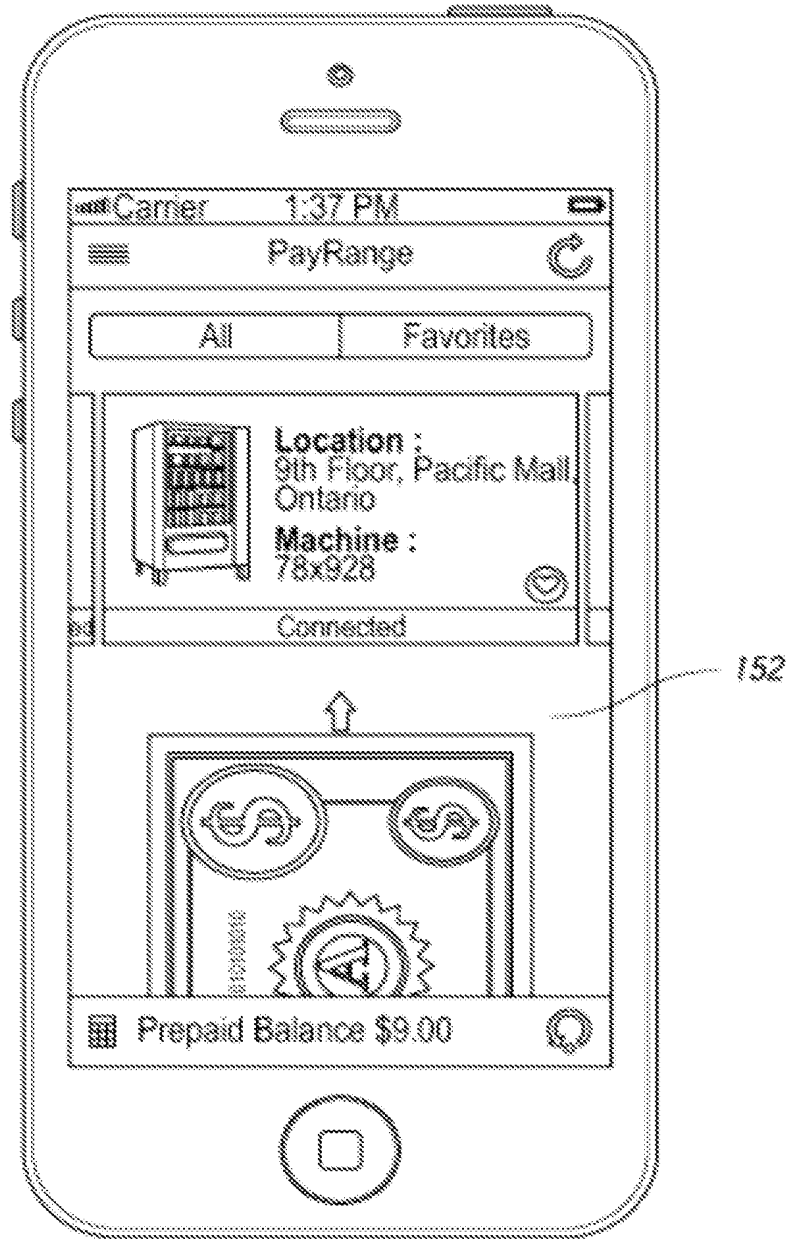


Figure 10A

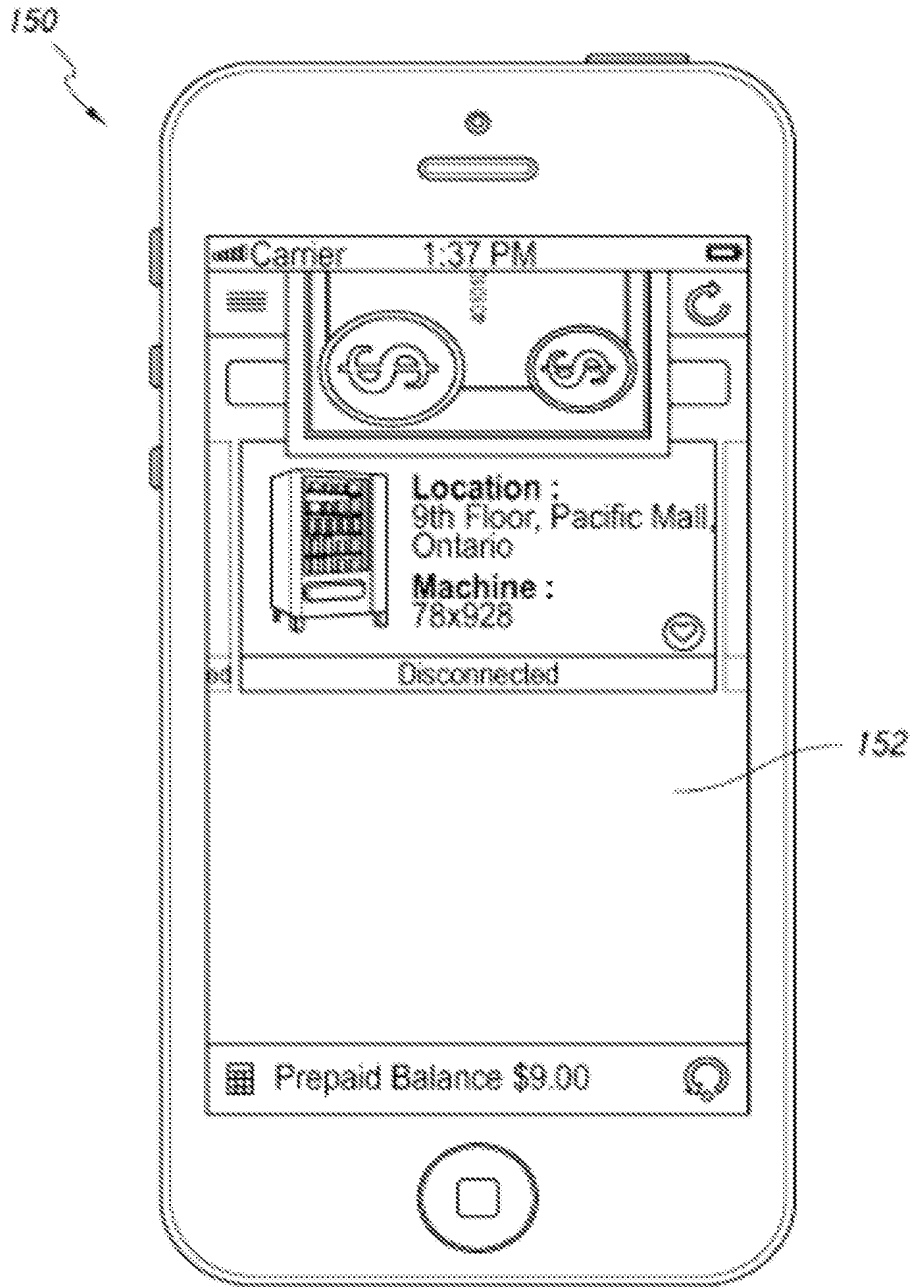


Figure 10B

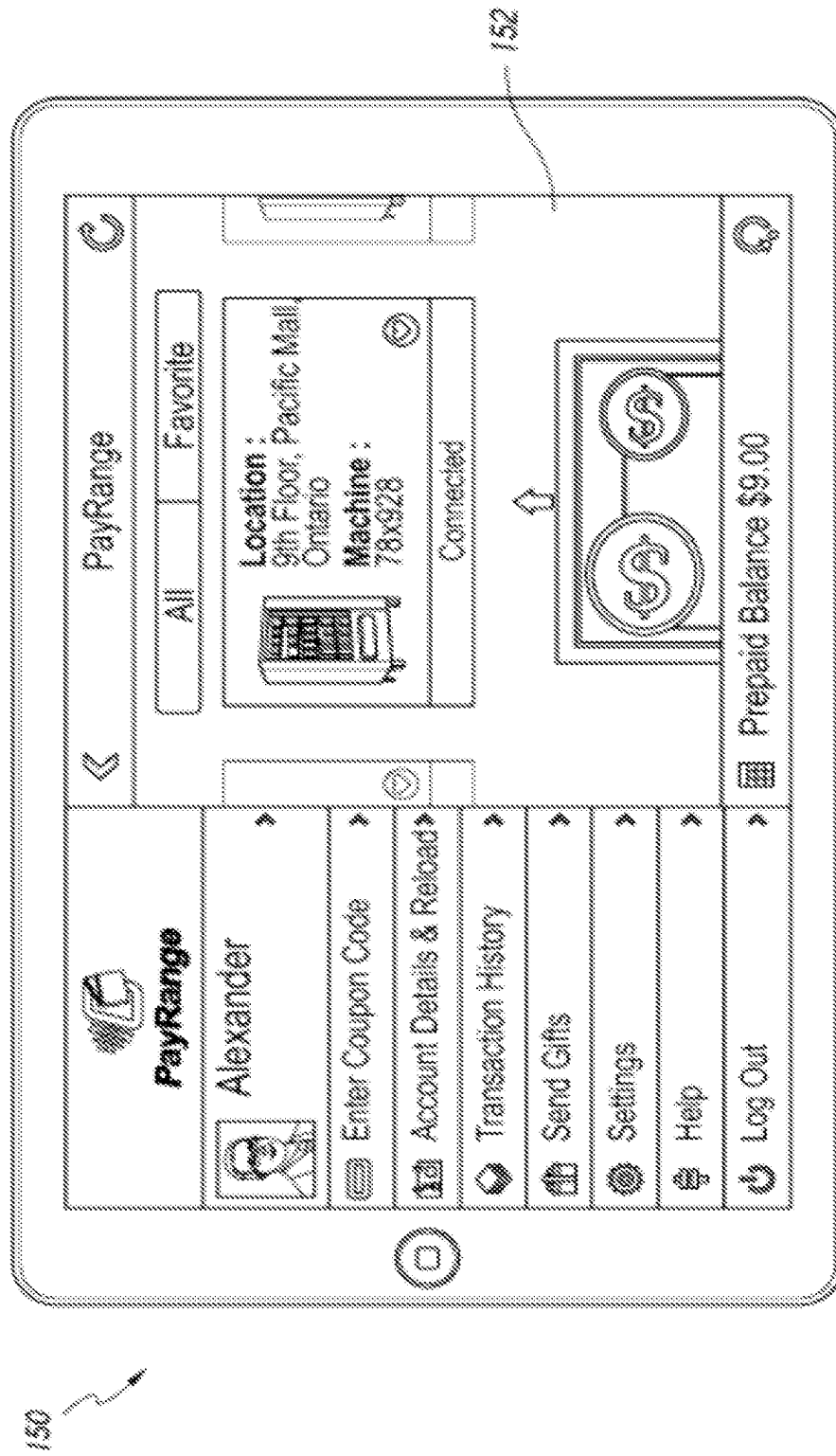


Figure 10C

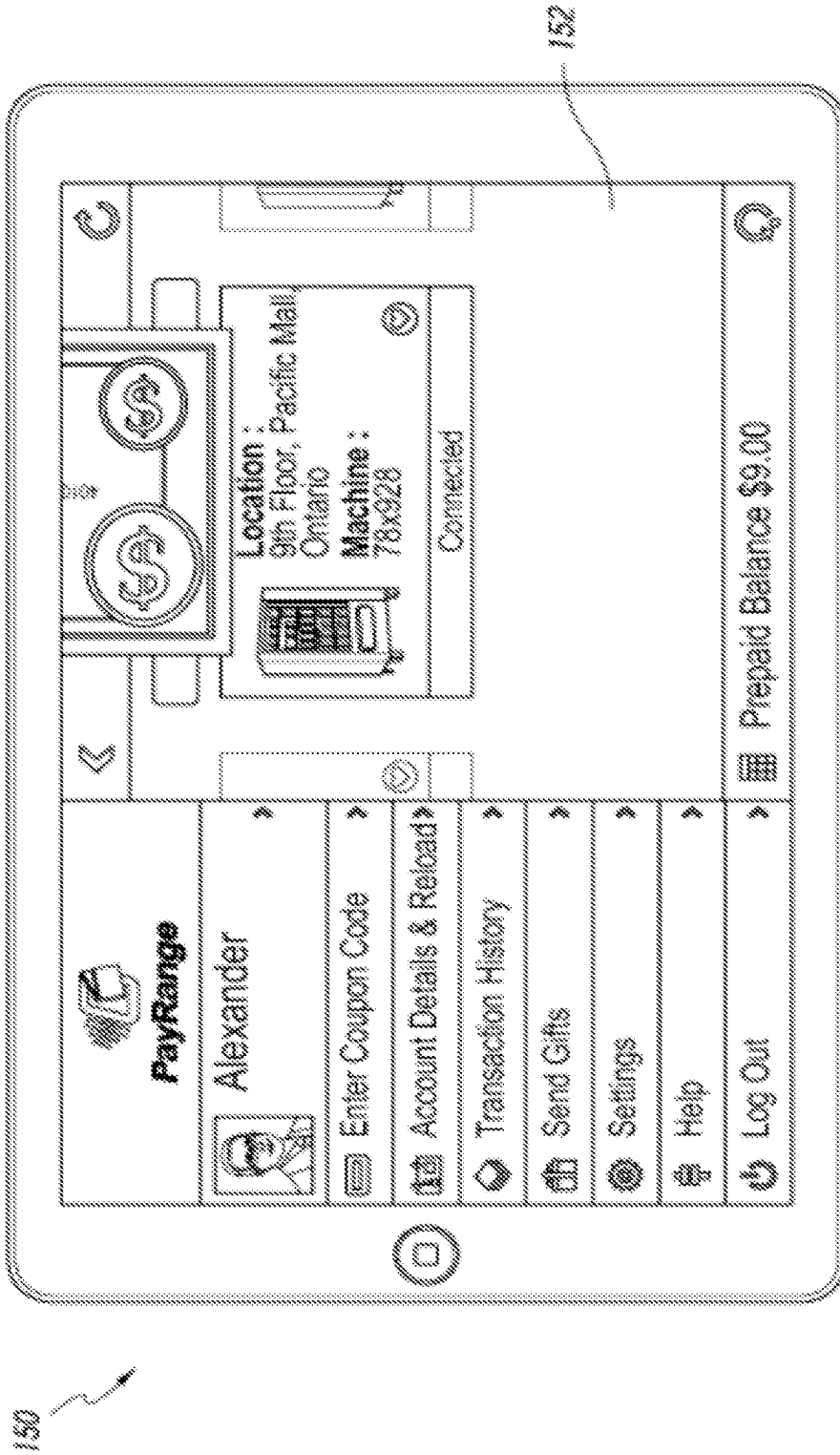


Figure 10D

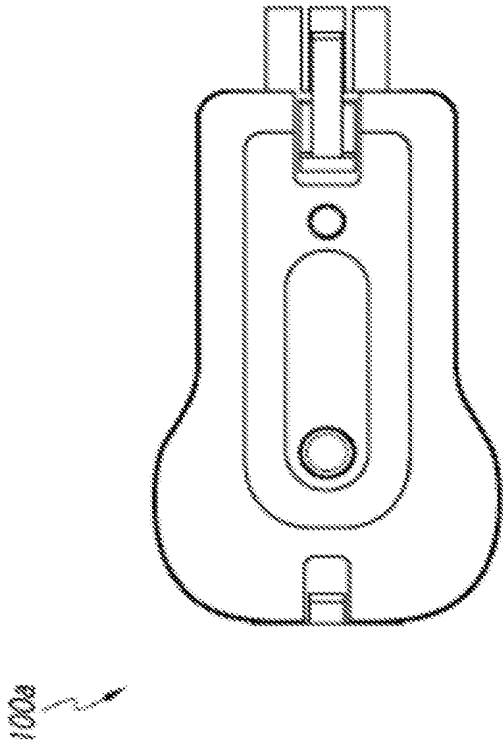


Figure 12

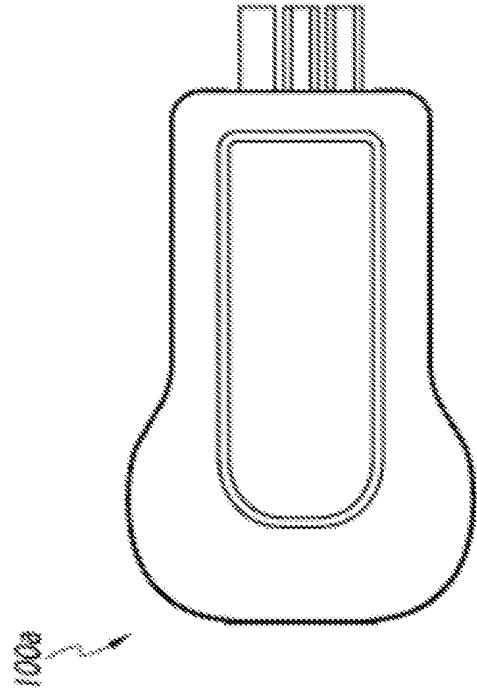


Figure 13

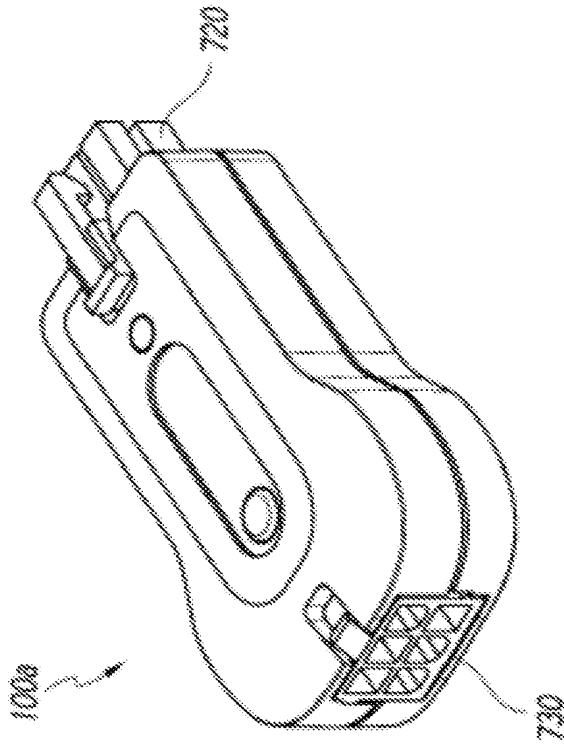


Figure 11

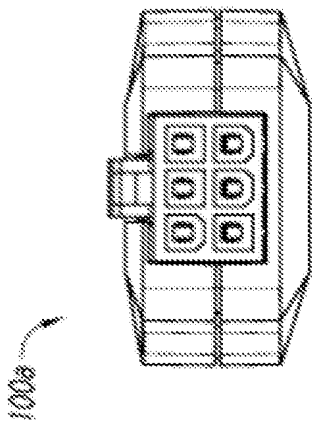


Figure 14

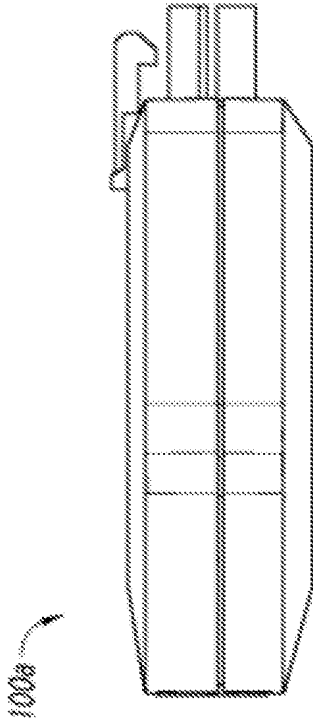


Figure 15

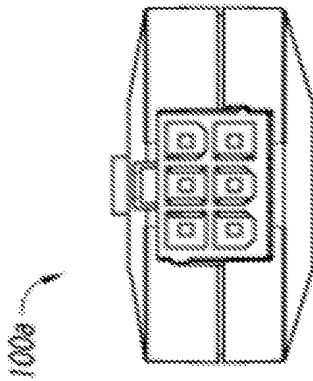


Figure 16

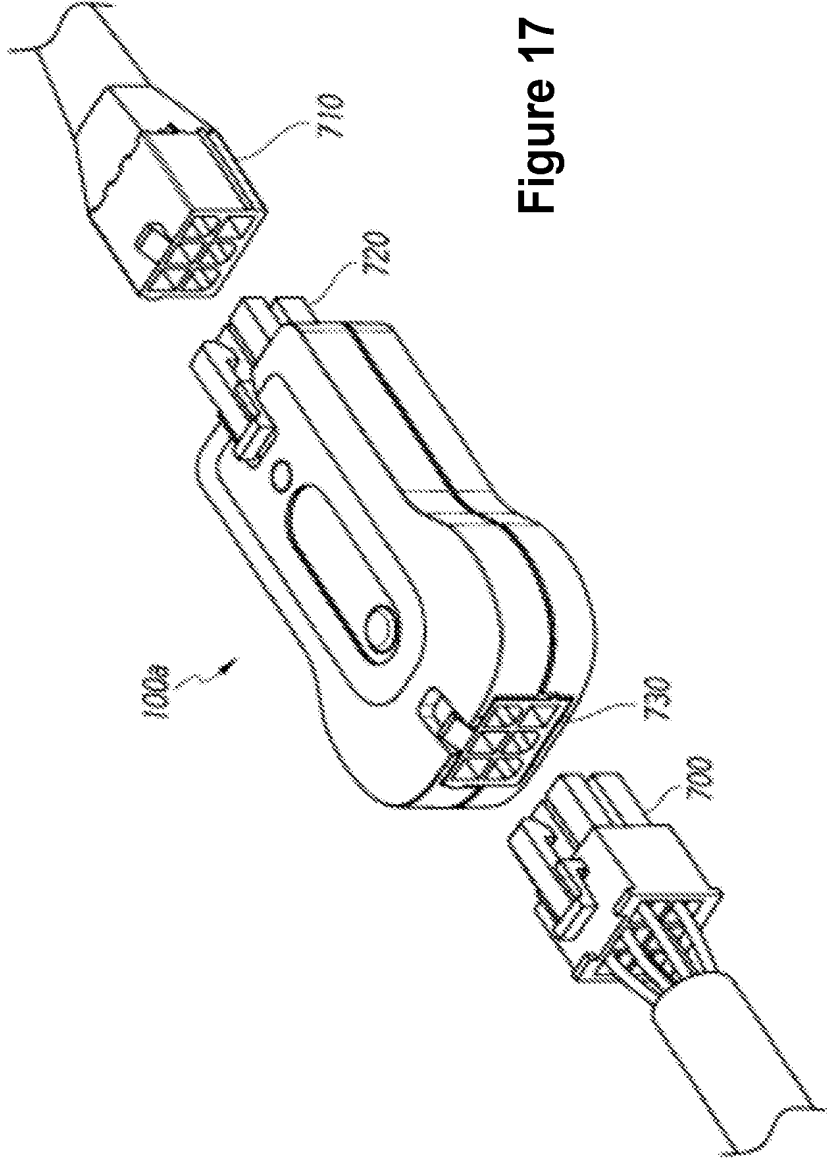


Figure 17

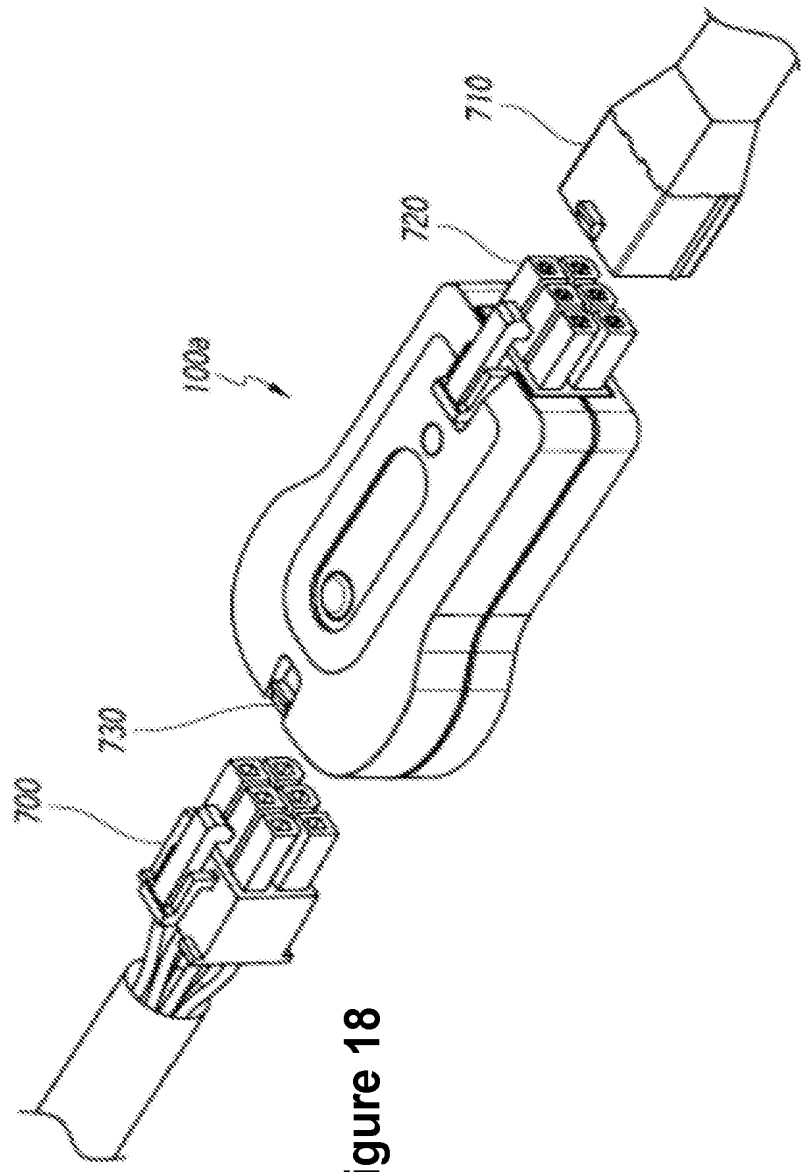


Figure 18

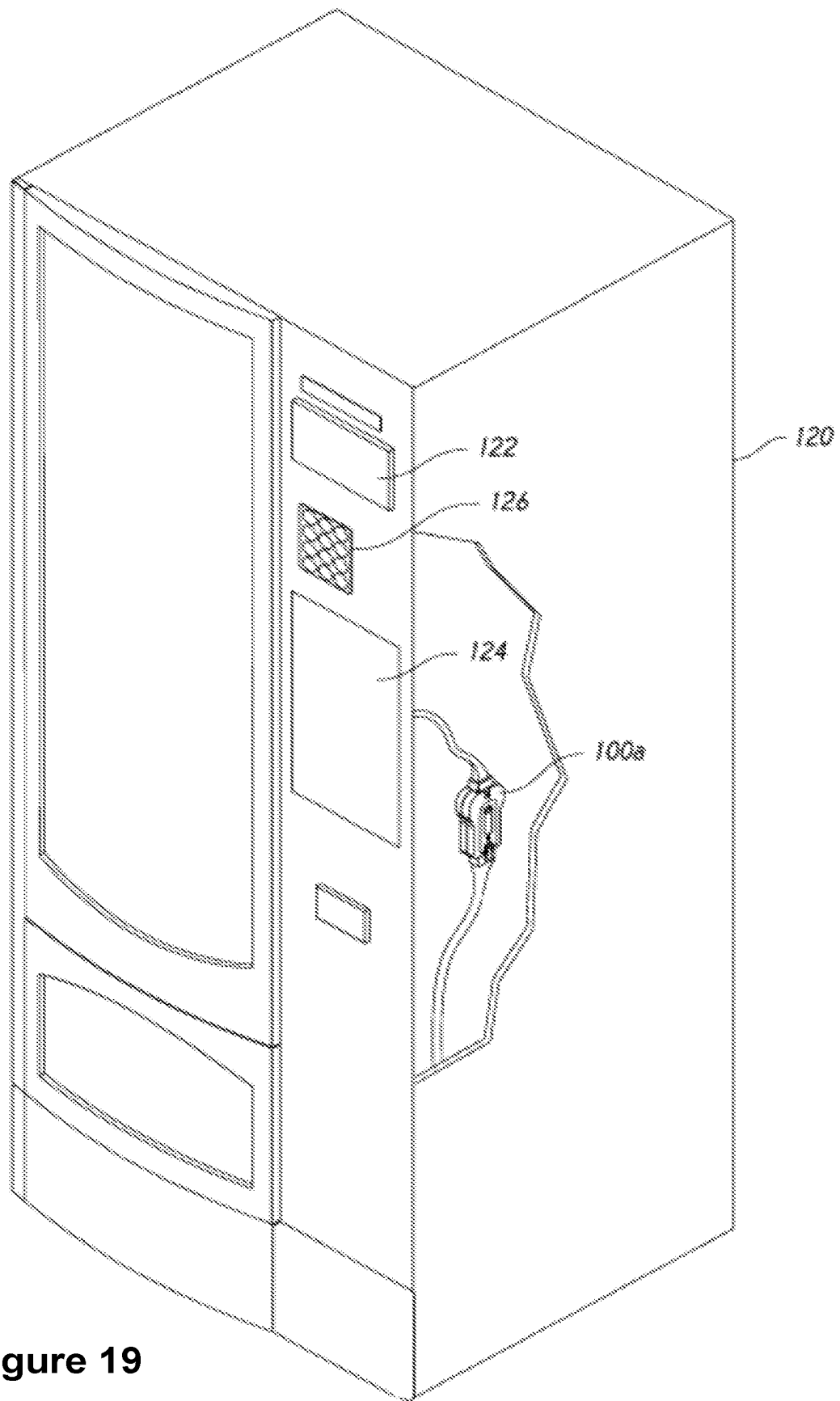


Figure 19

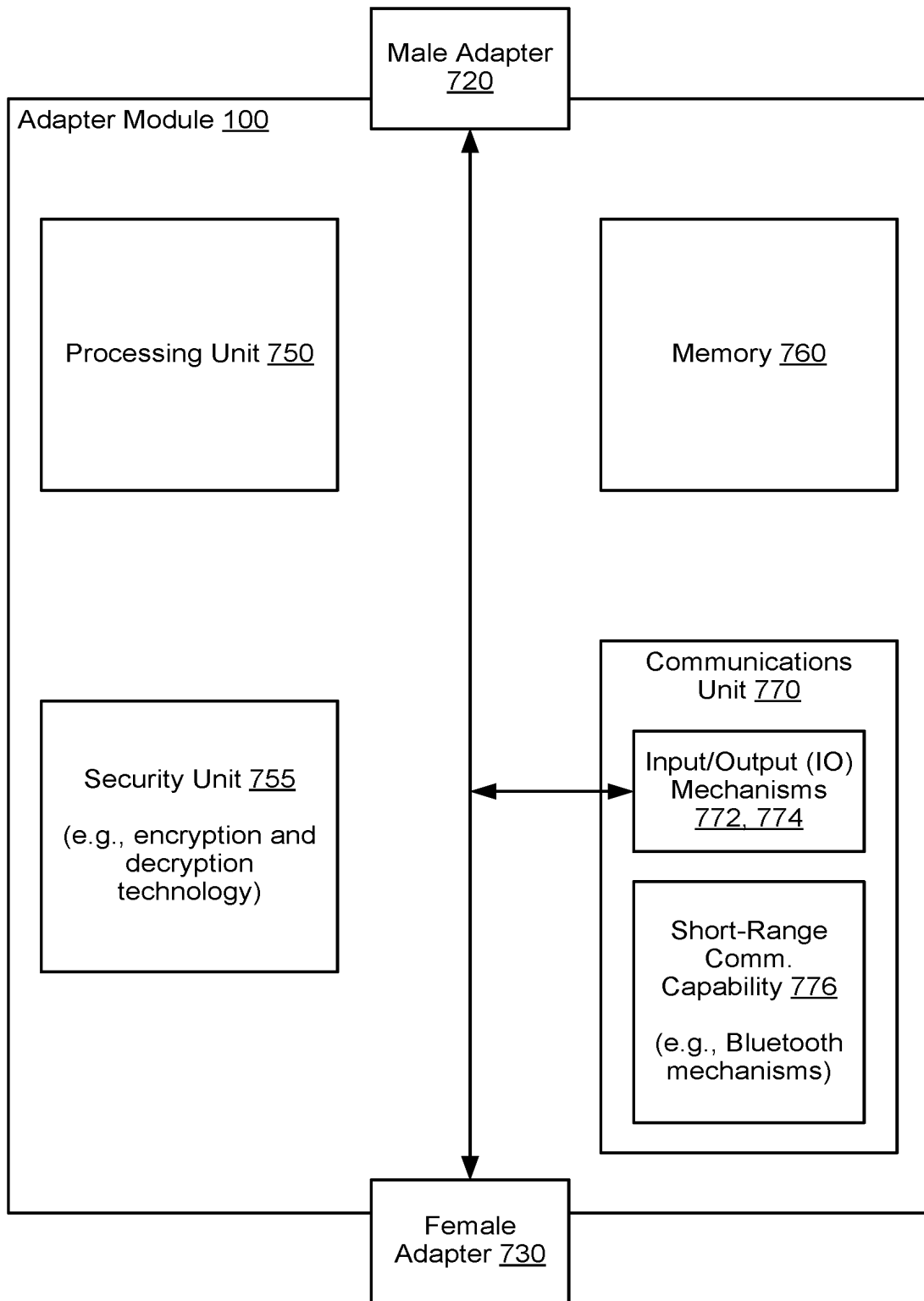


Figure 20

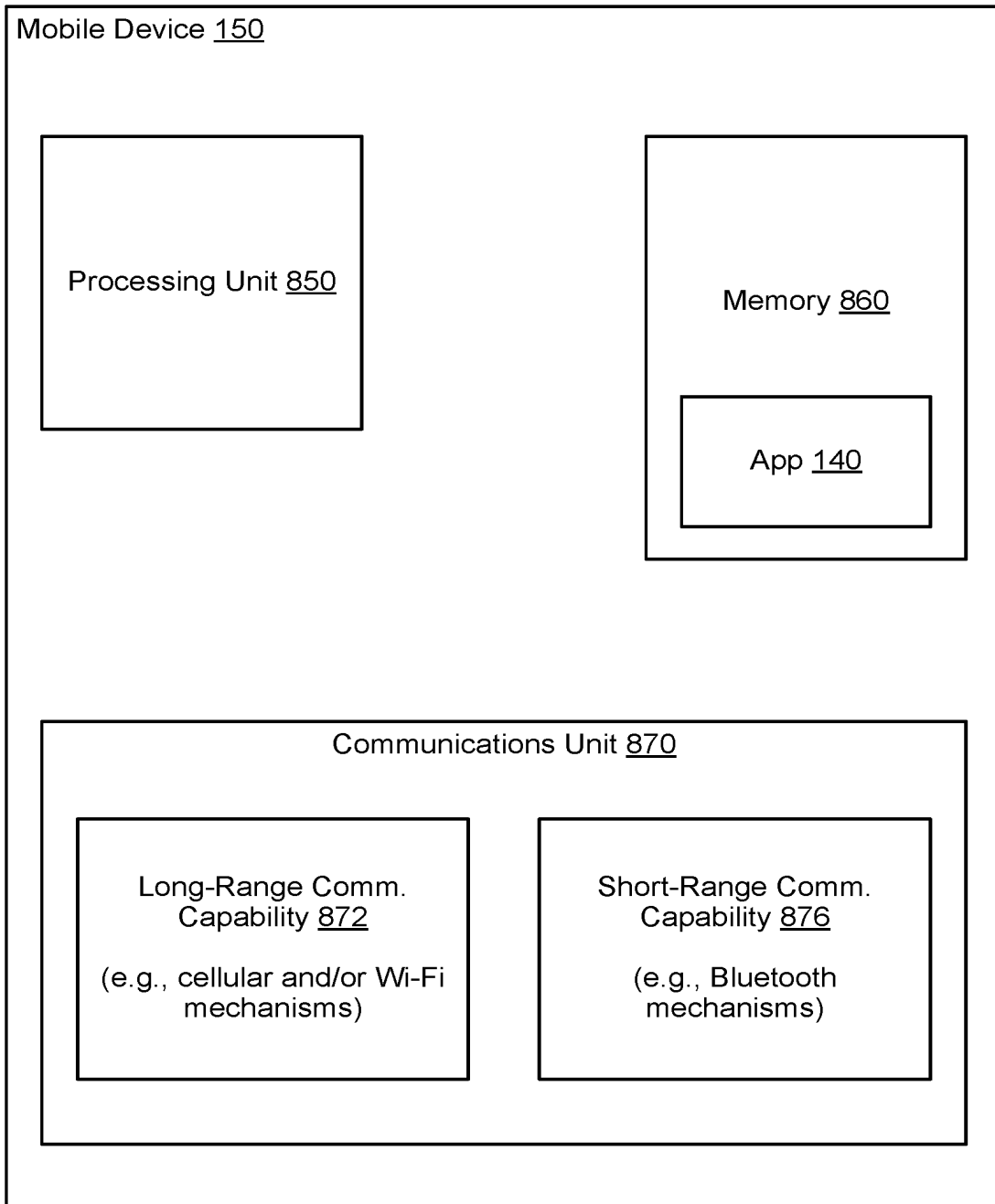


Figure 21

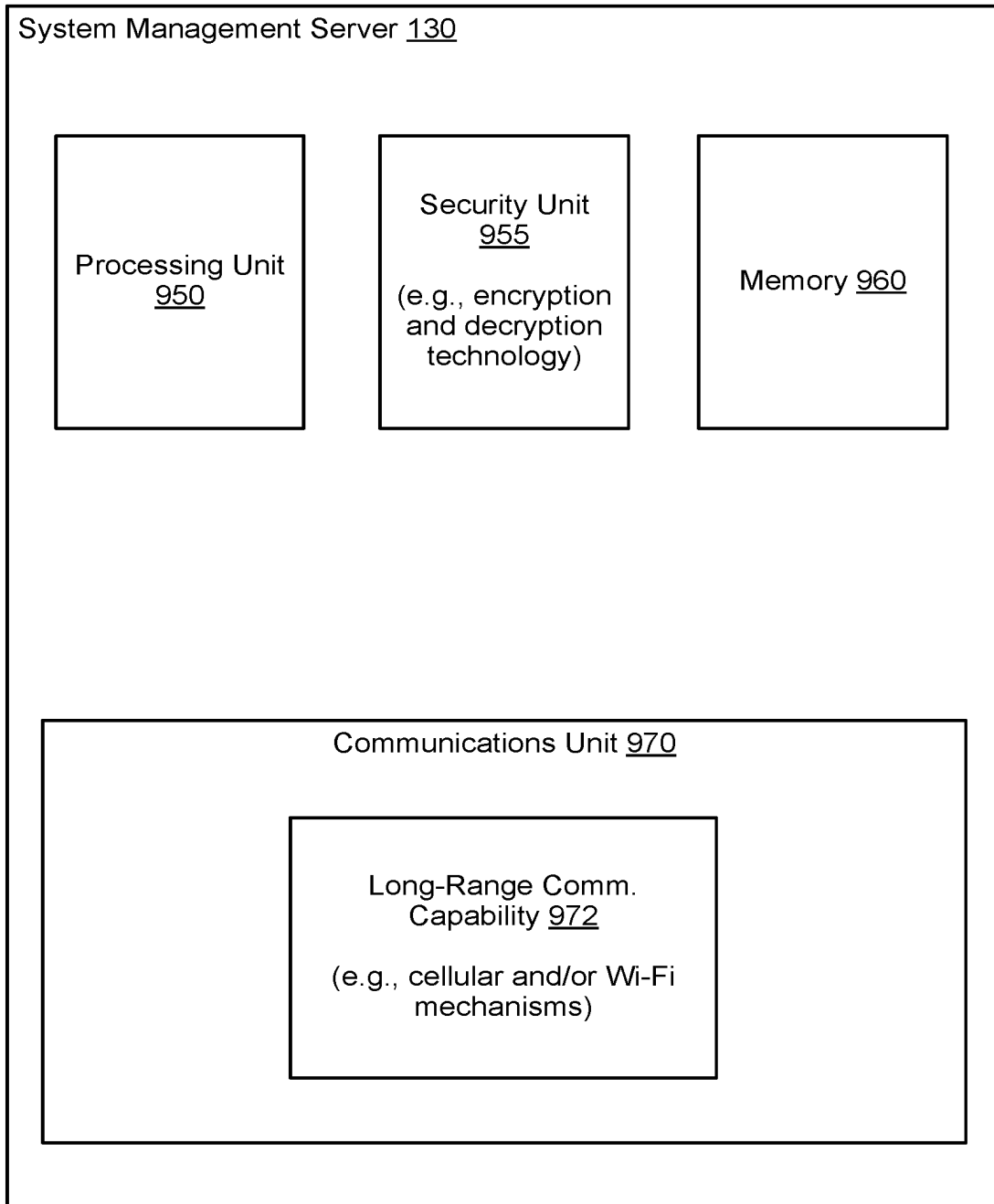


Figure 22

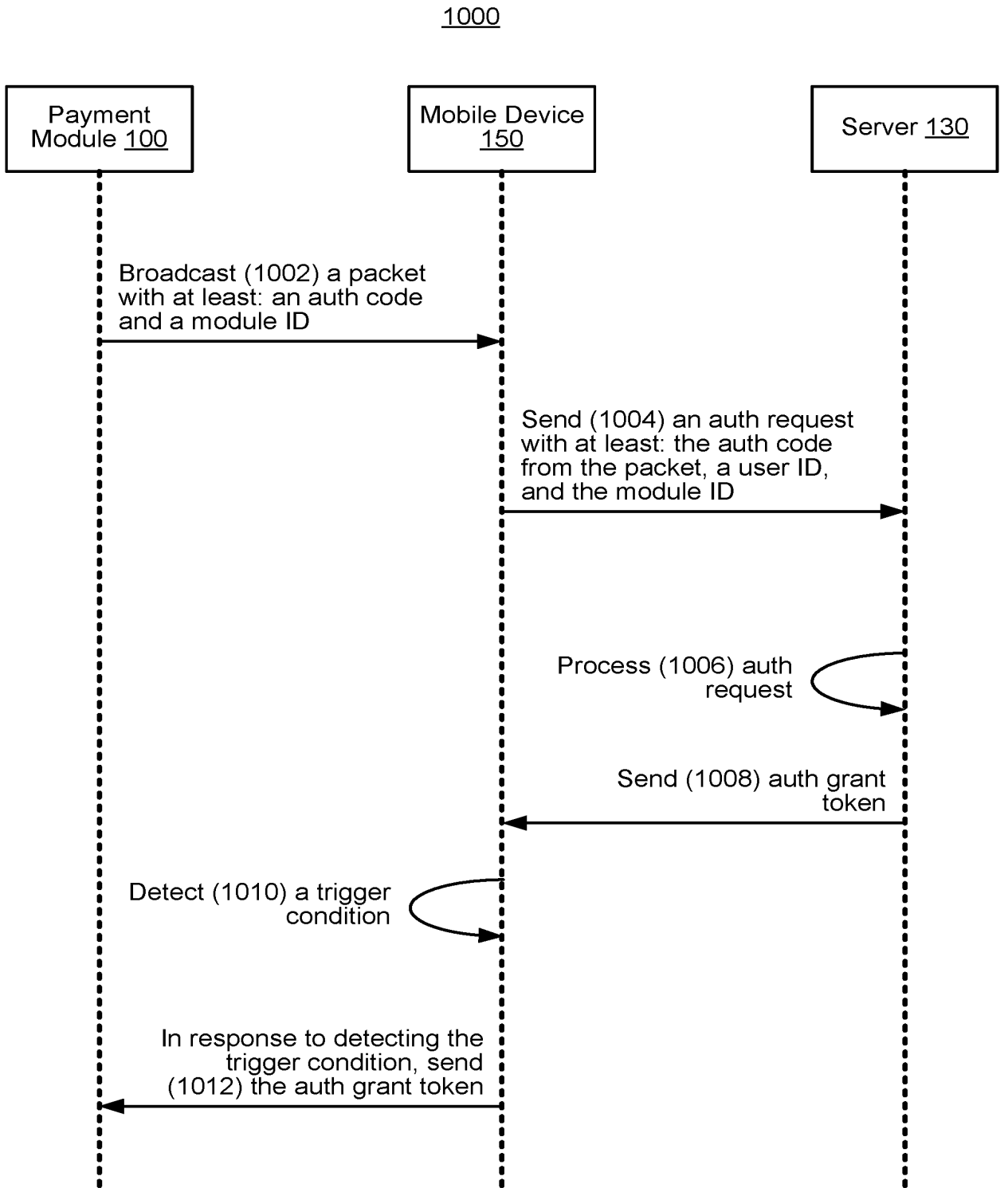


Figure 23

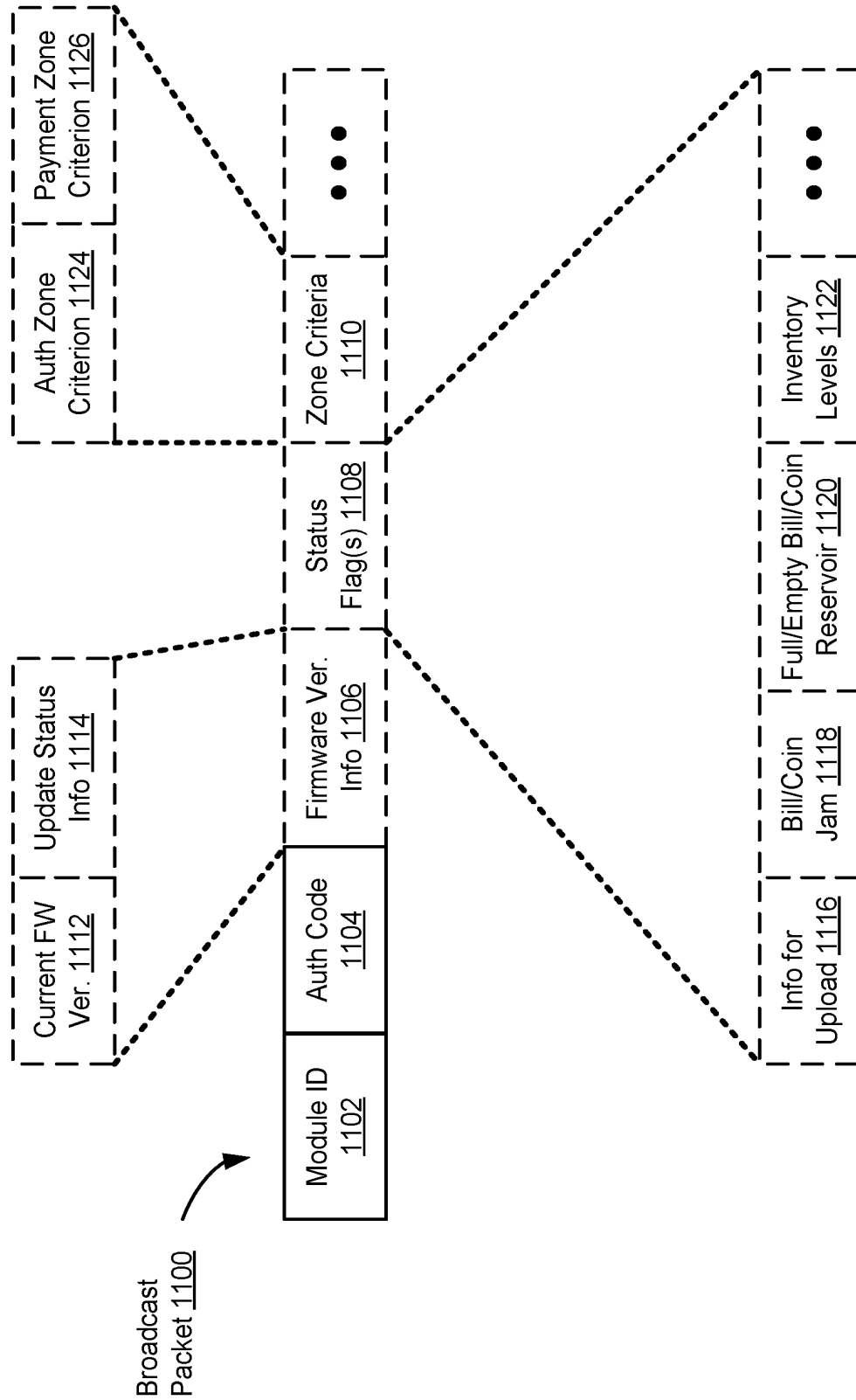


Figure 24A

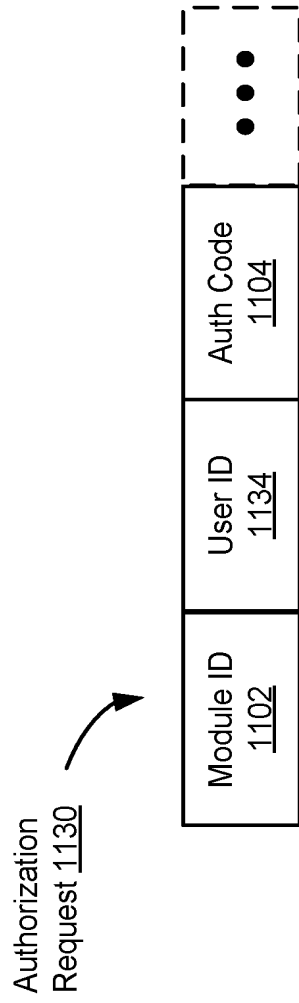


Figure 24B

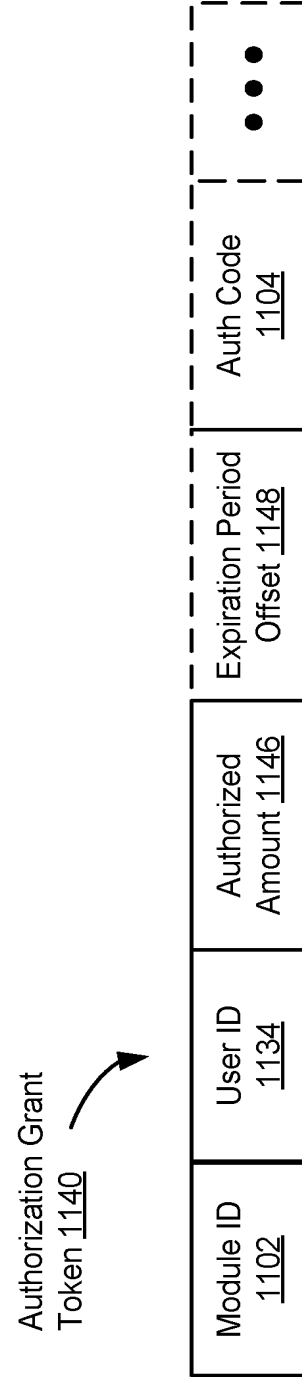


Figure 24C

Transaction Info
1150

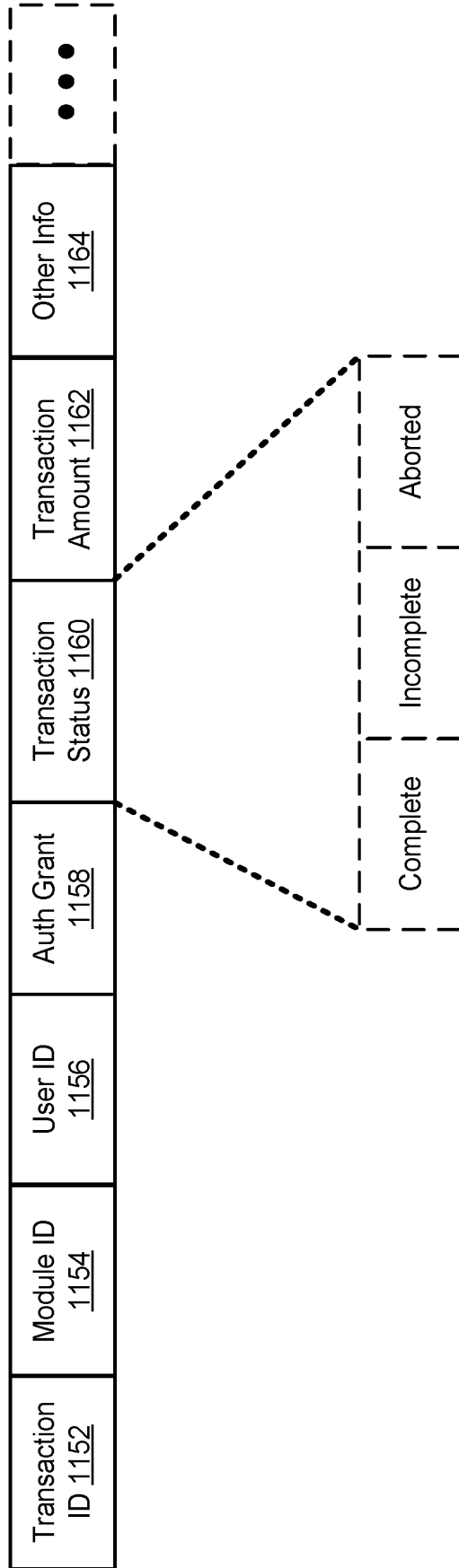


Figure 24D

1200

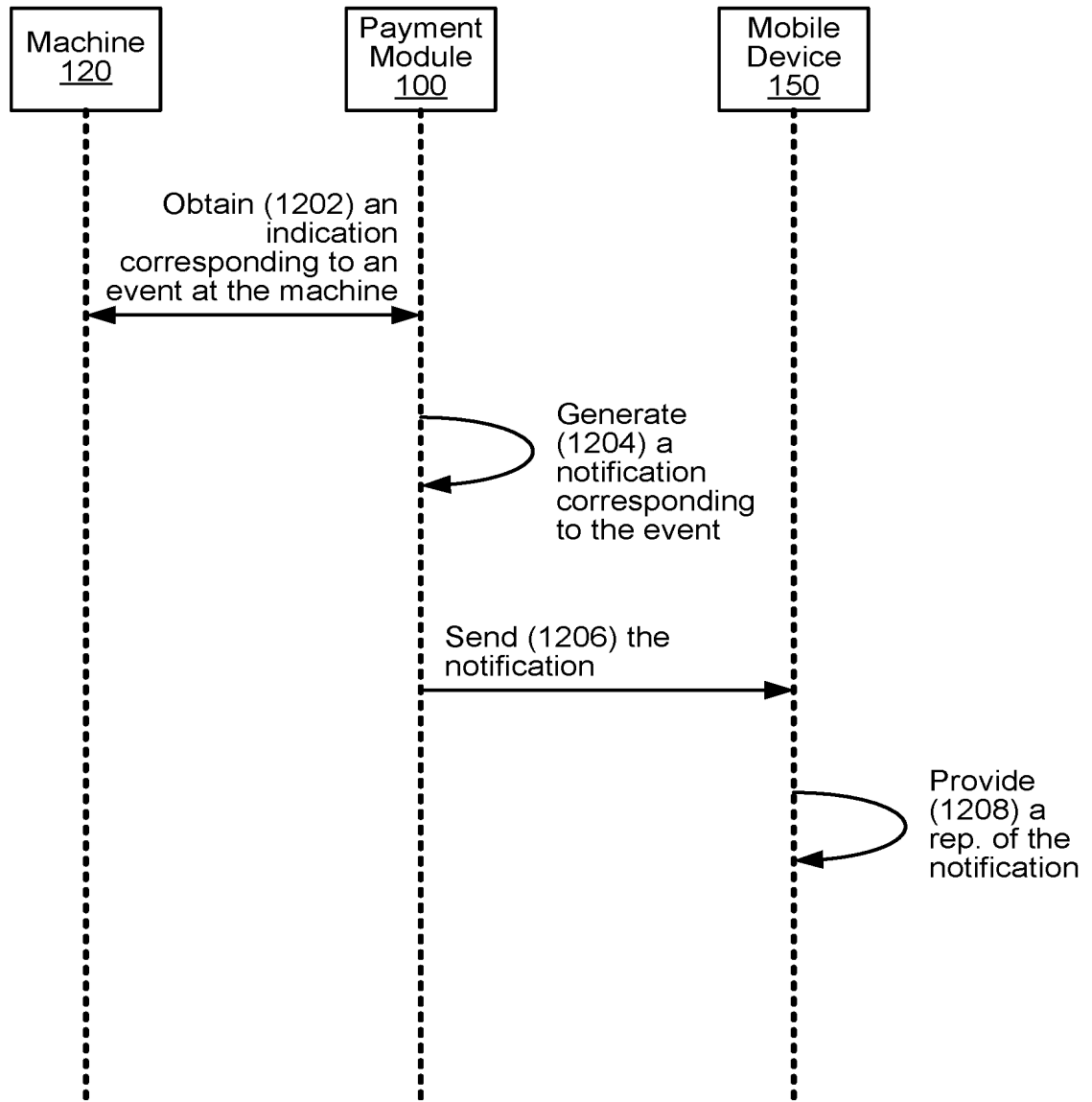


Figure 25A

1250

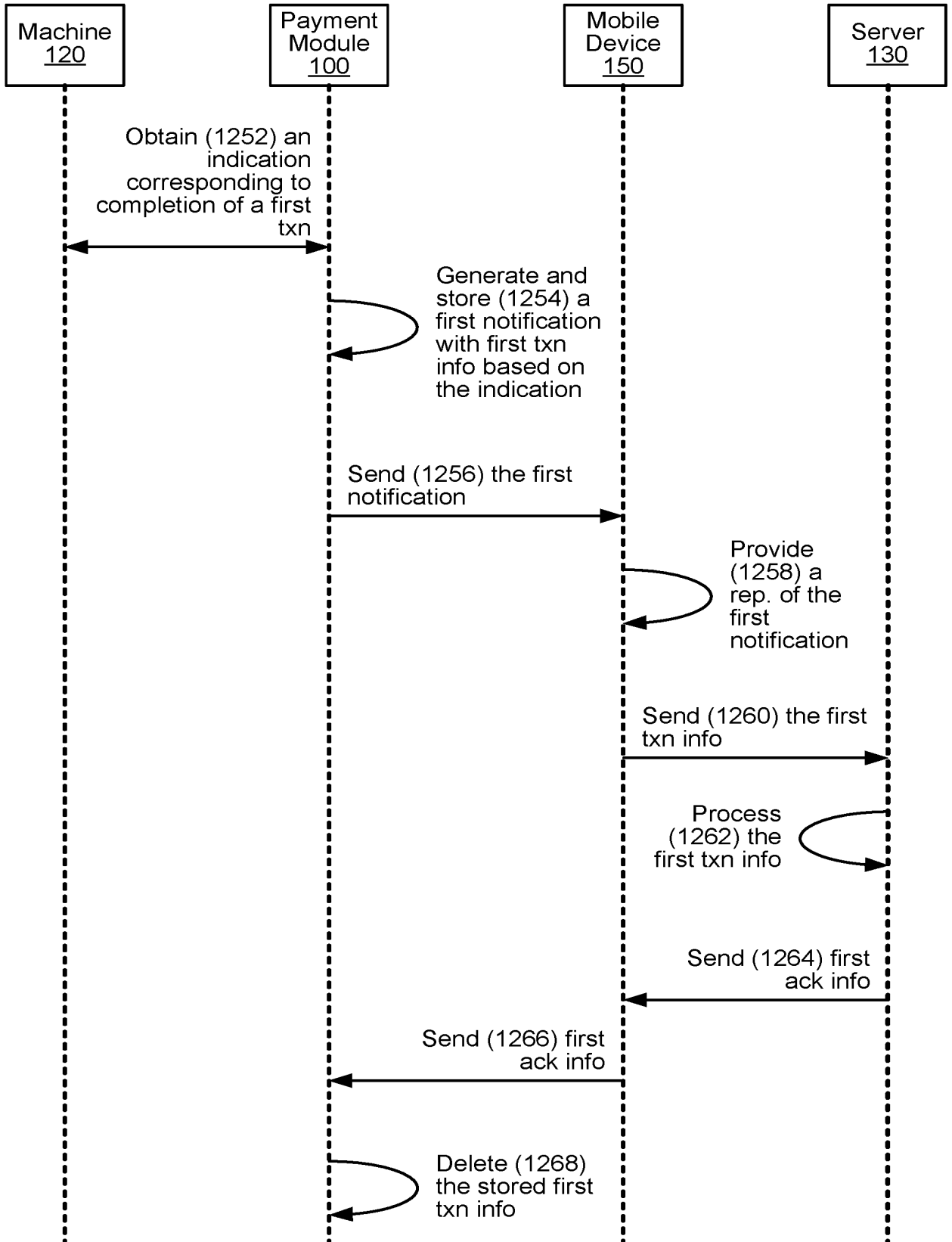


Figure 25B

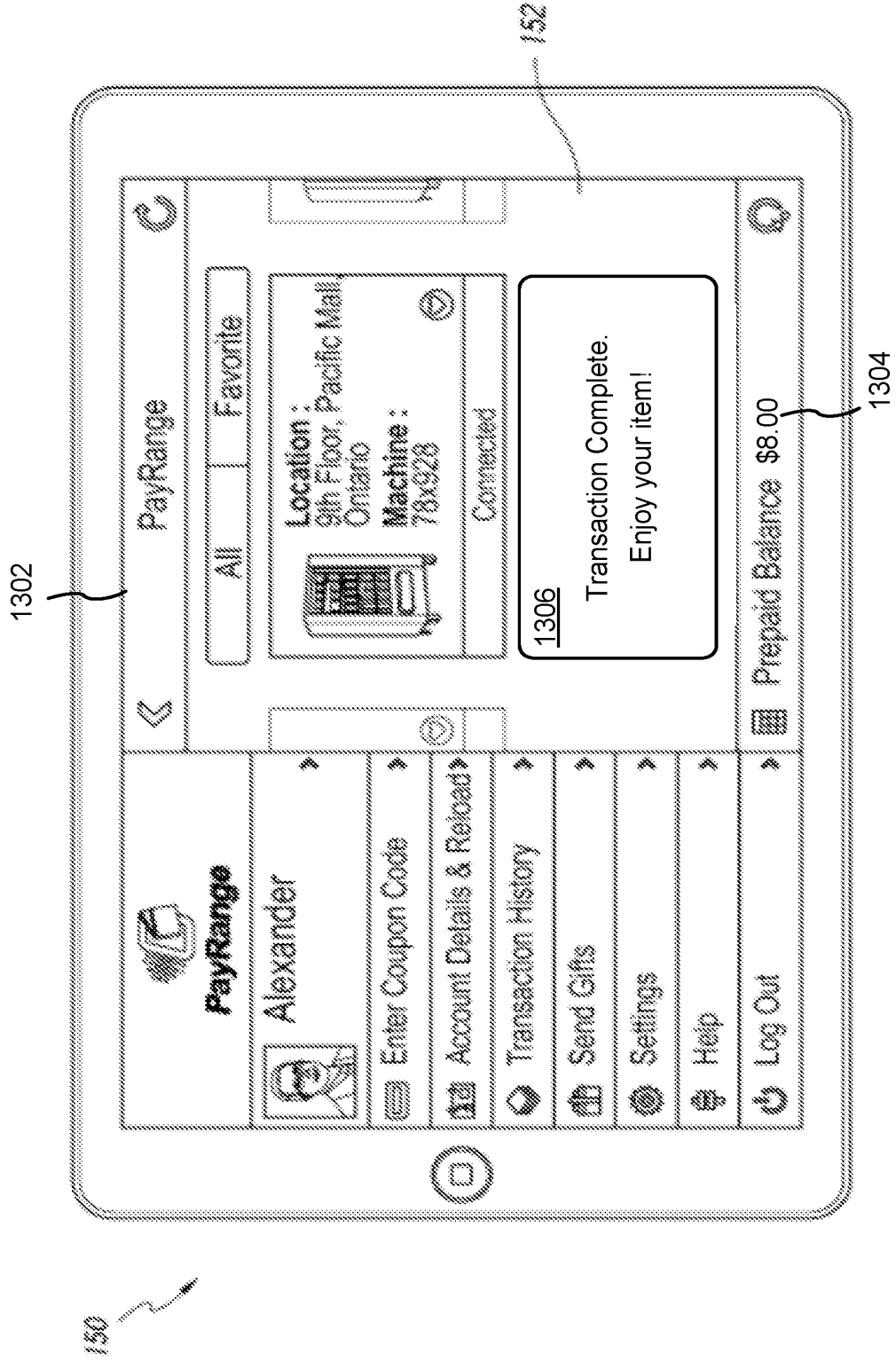


Figure 26A

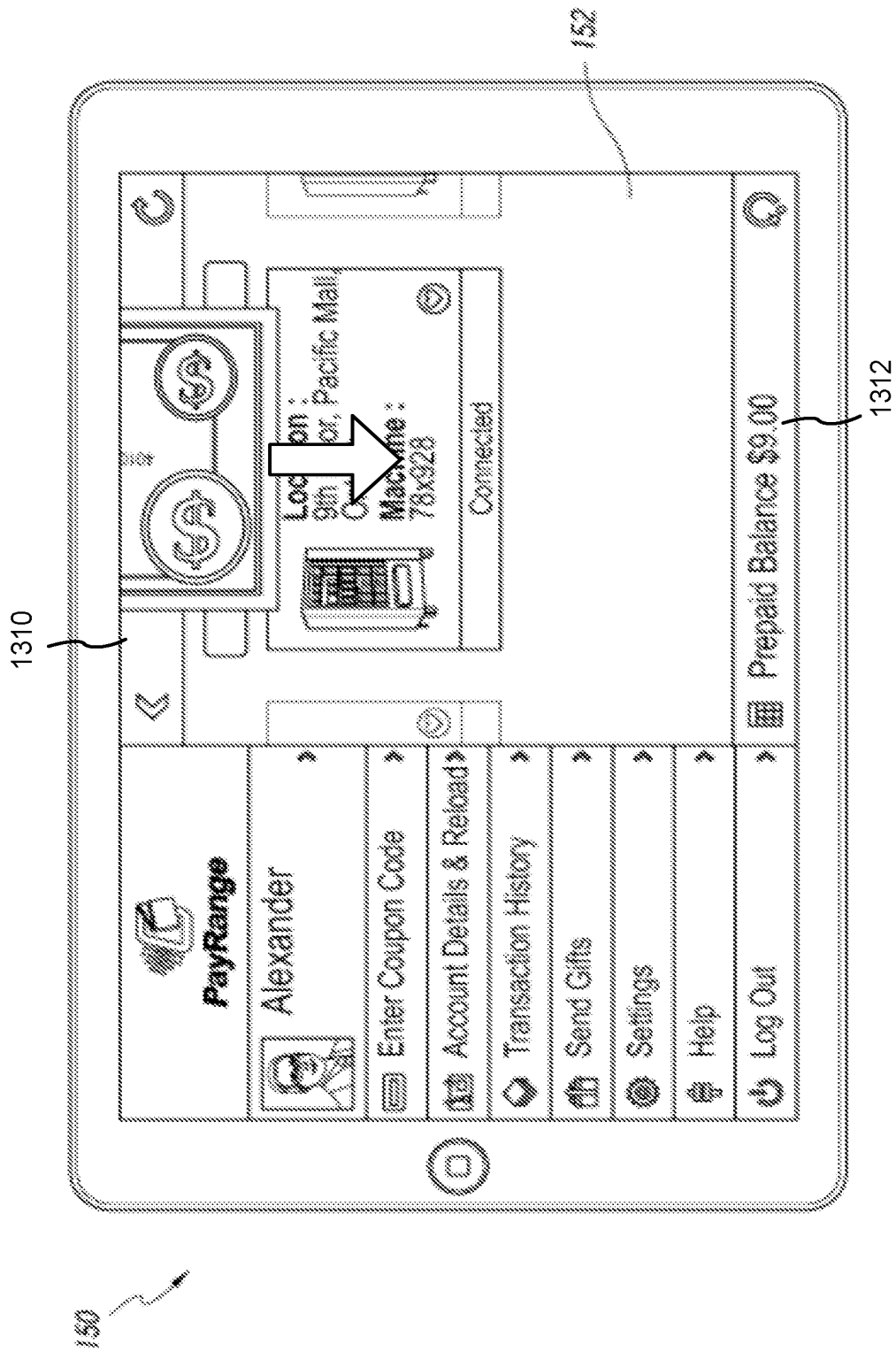


Figure 26B

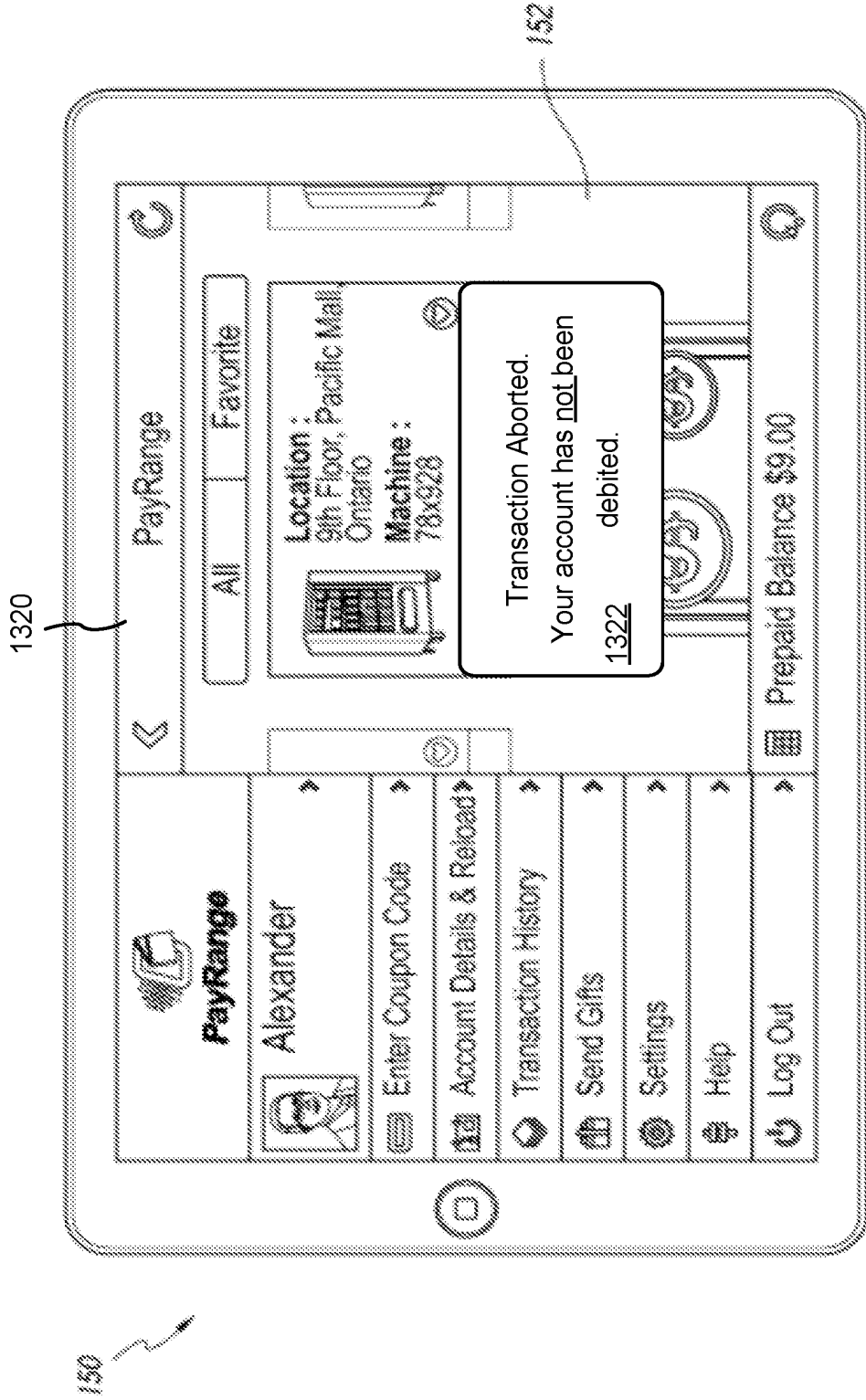


Figure 26C

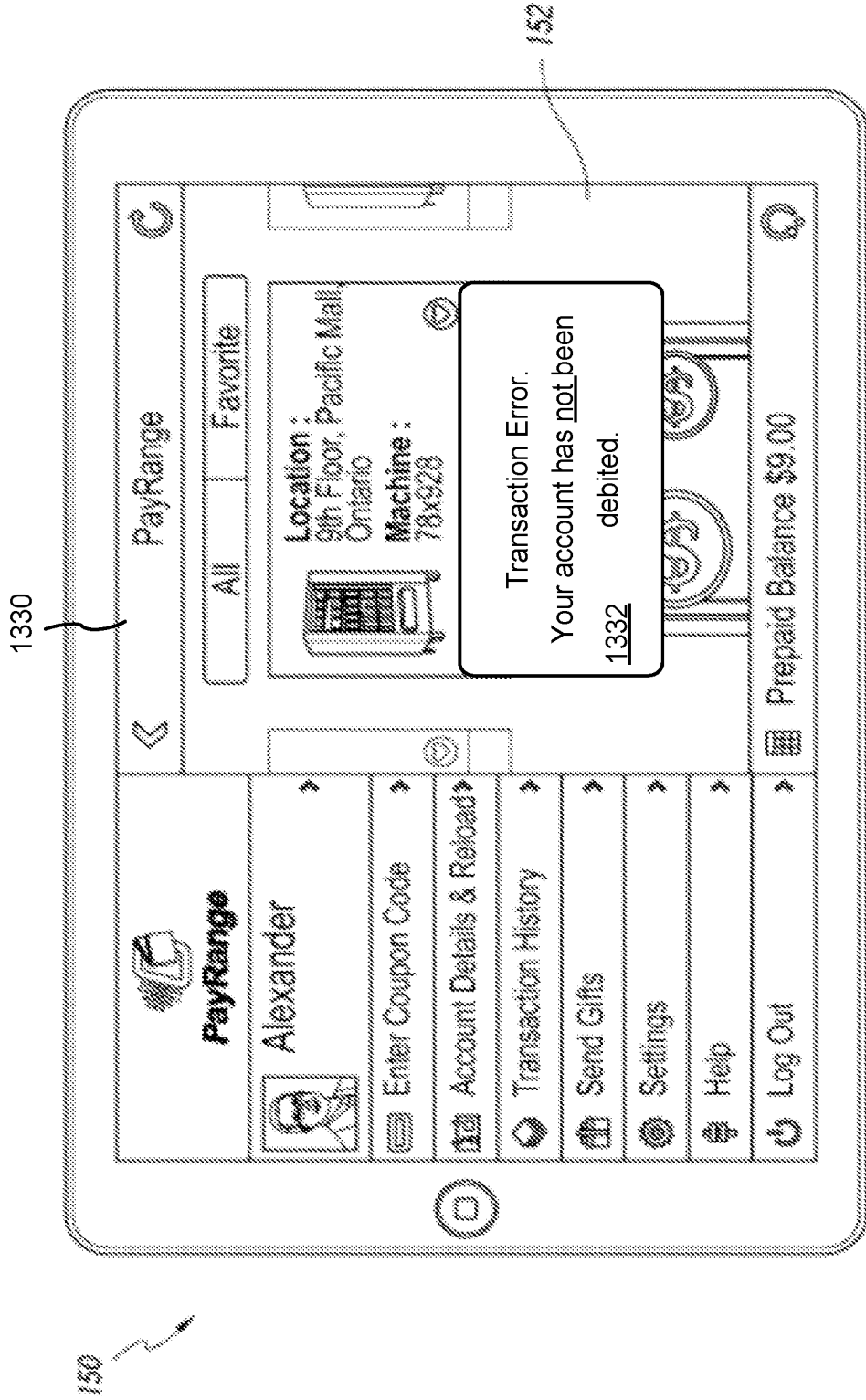


Figure 26D

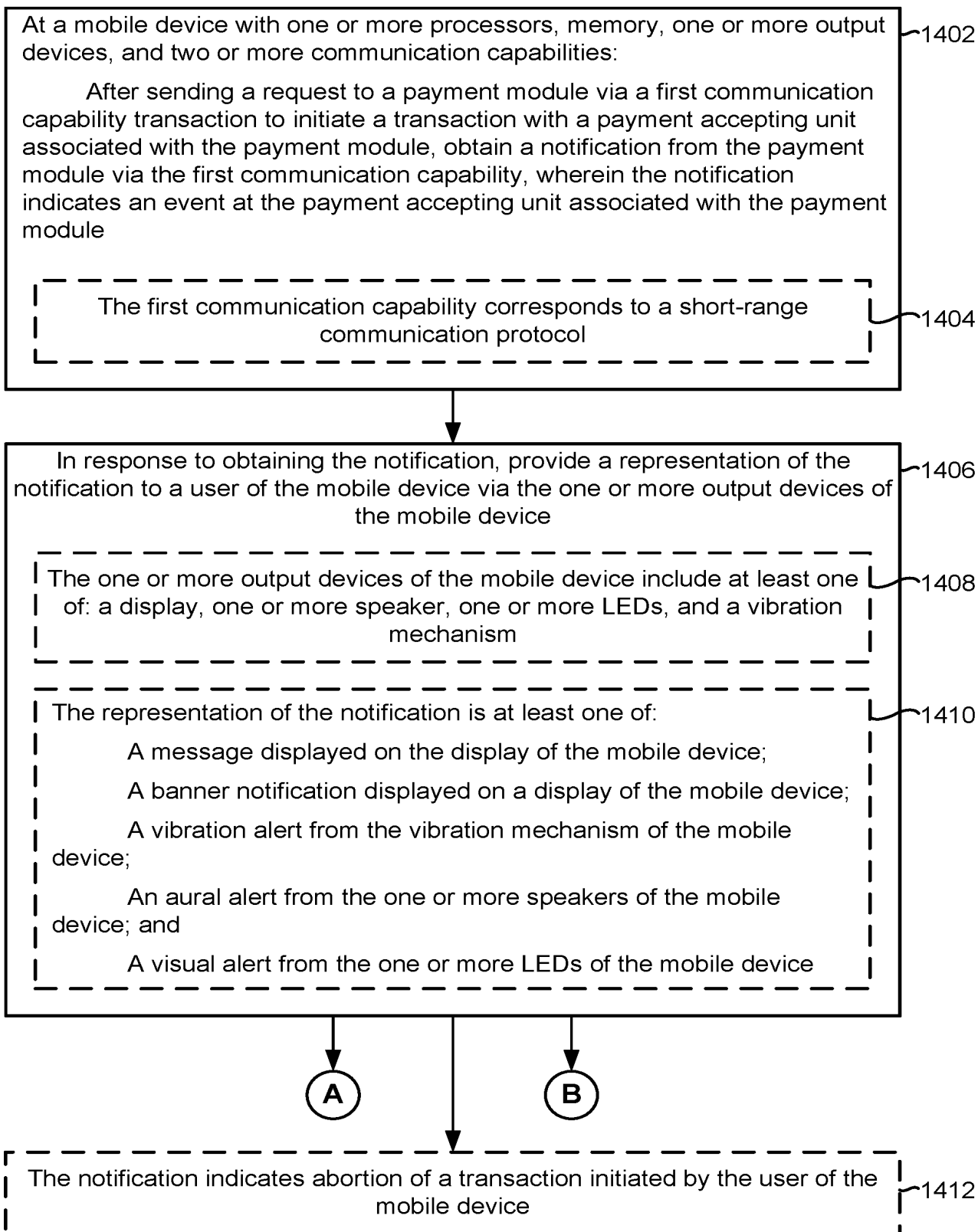


Figure 27A

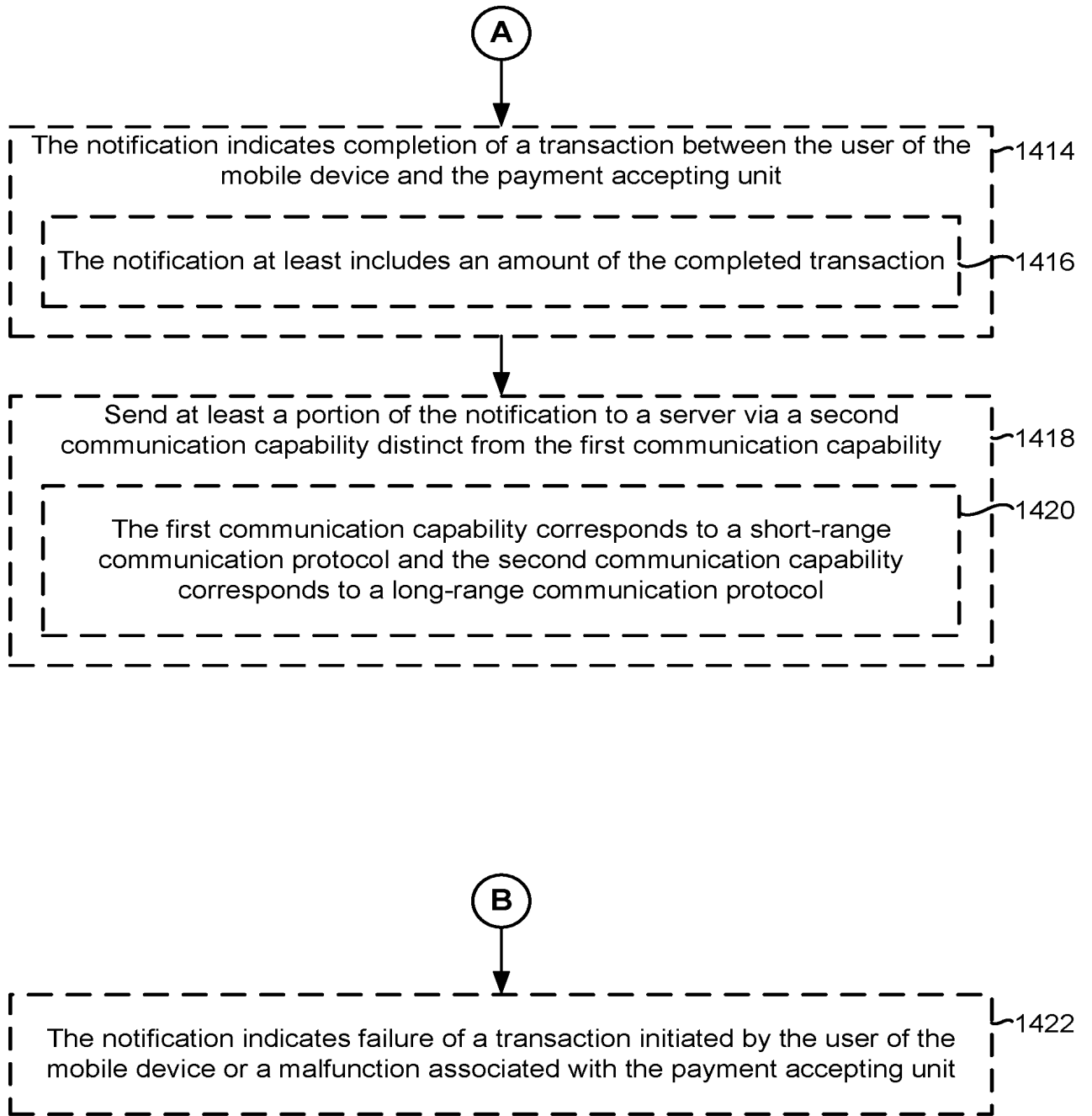


Figure 27B

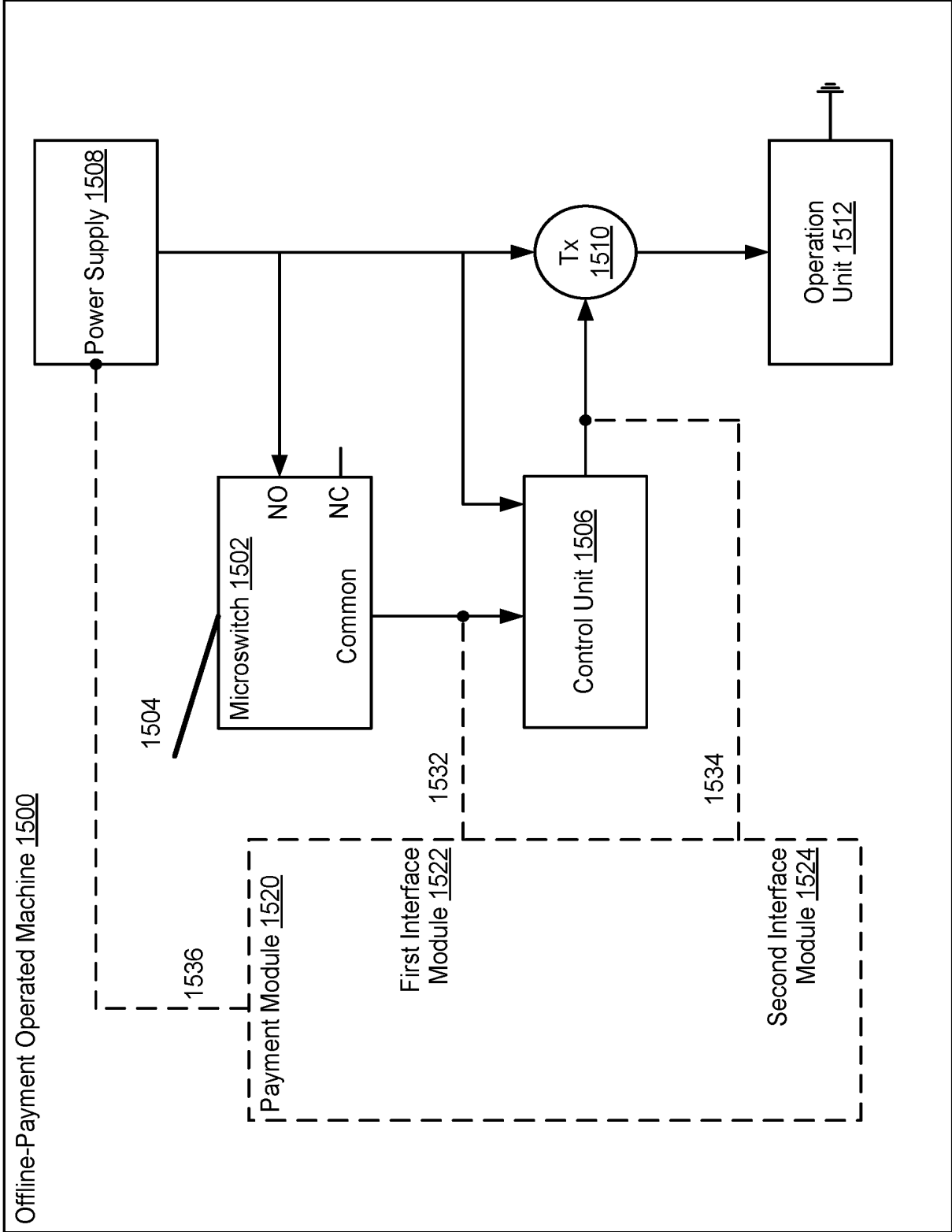


Figure 28A

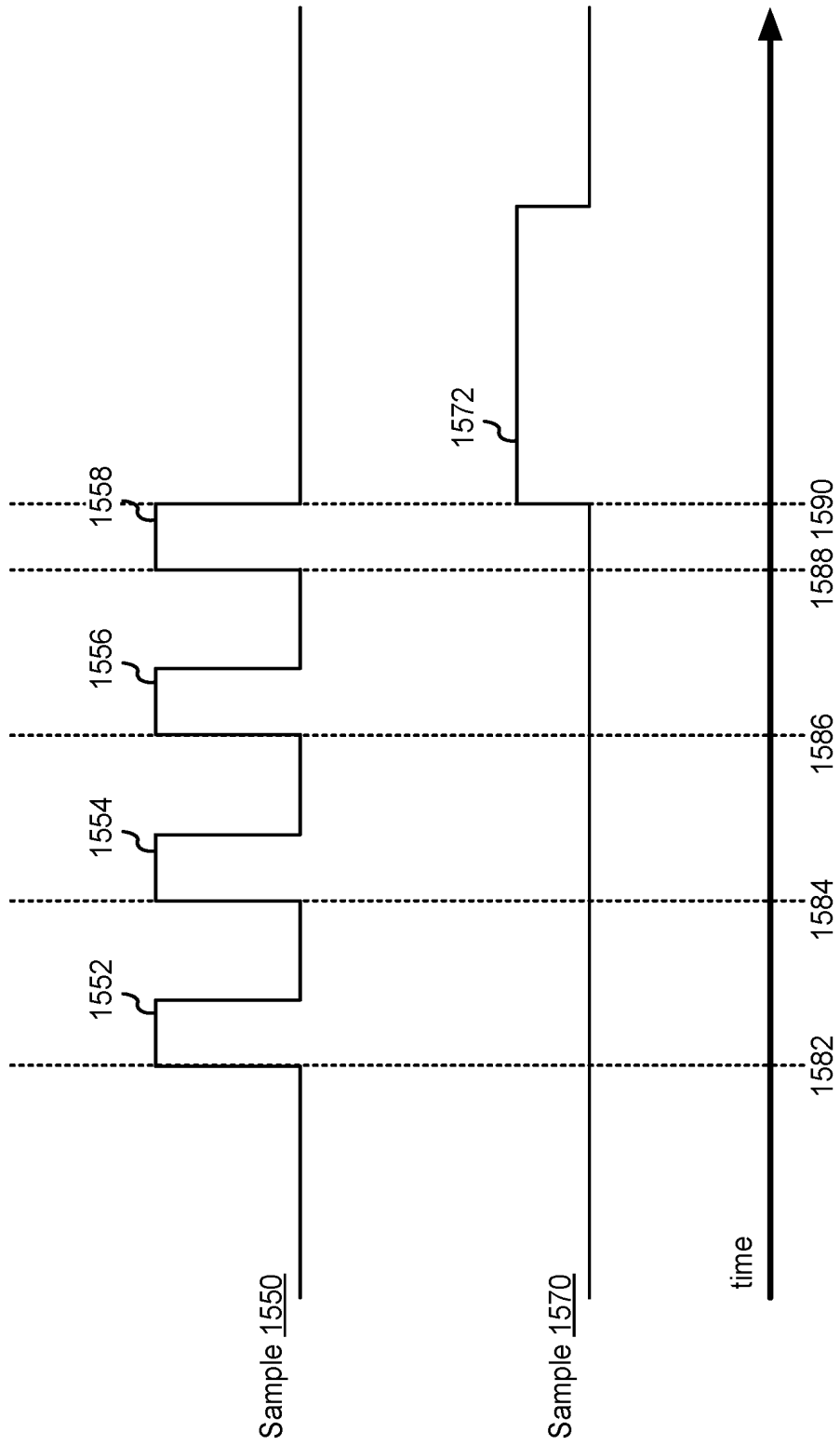


Figure 28B

1600

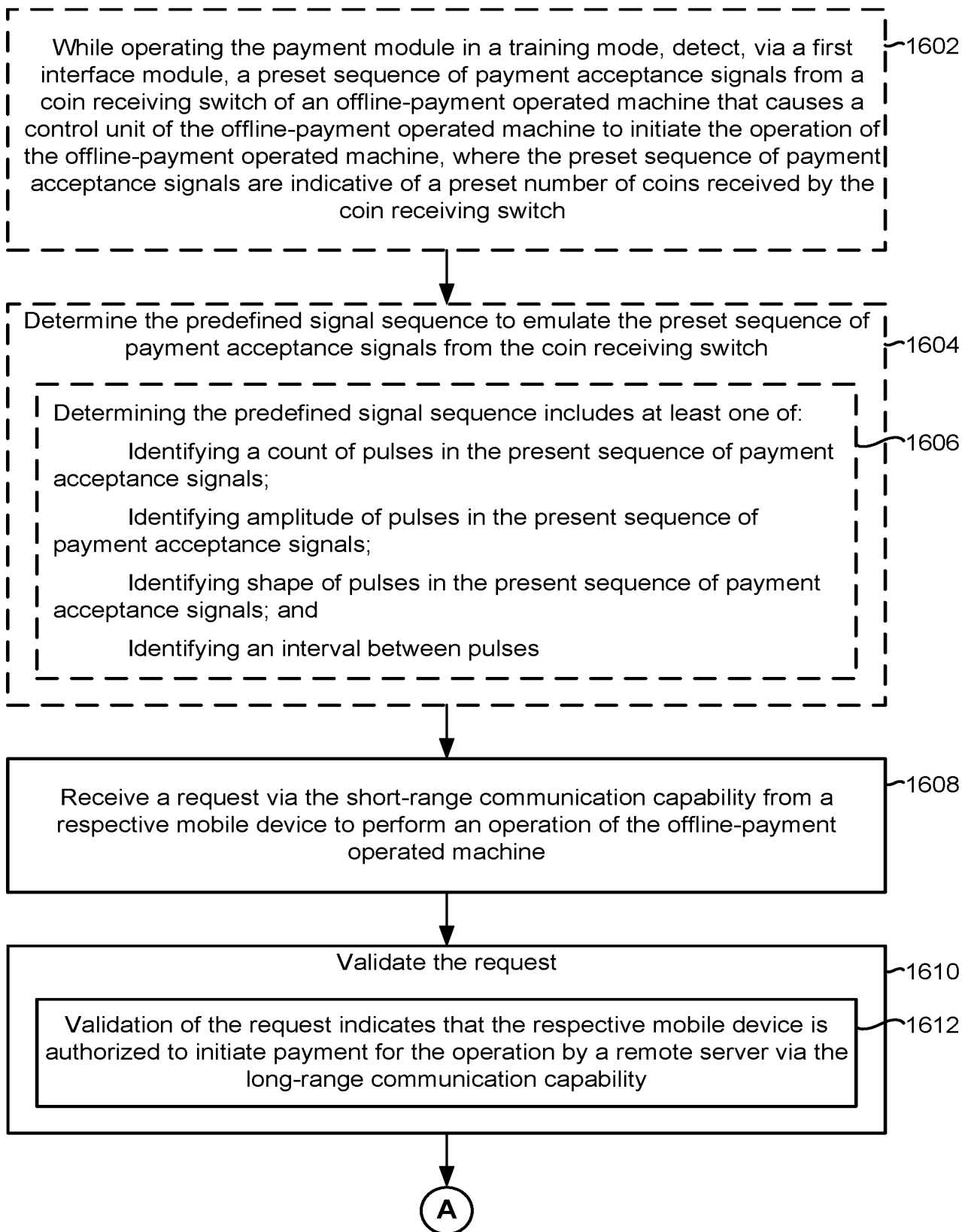


Figure 29A

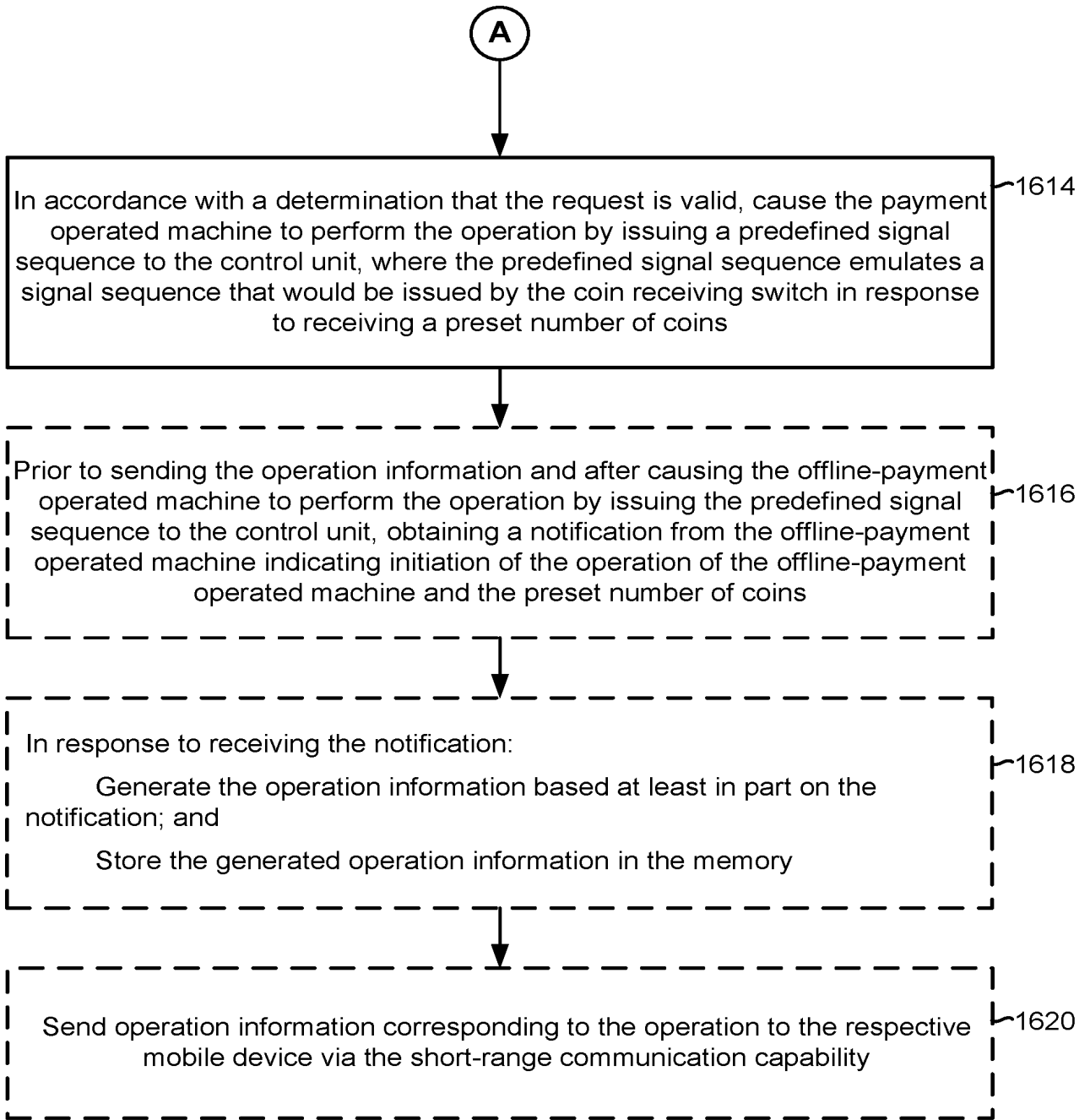


Figure 29B

1700

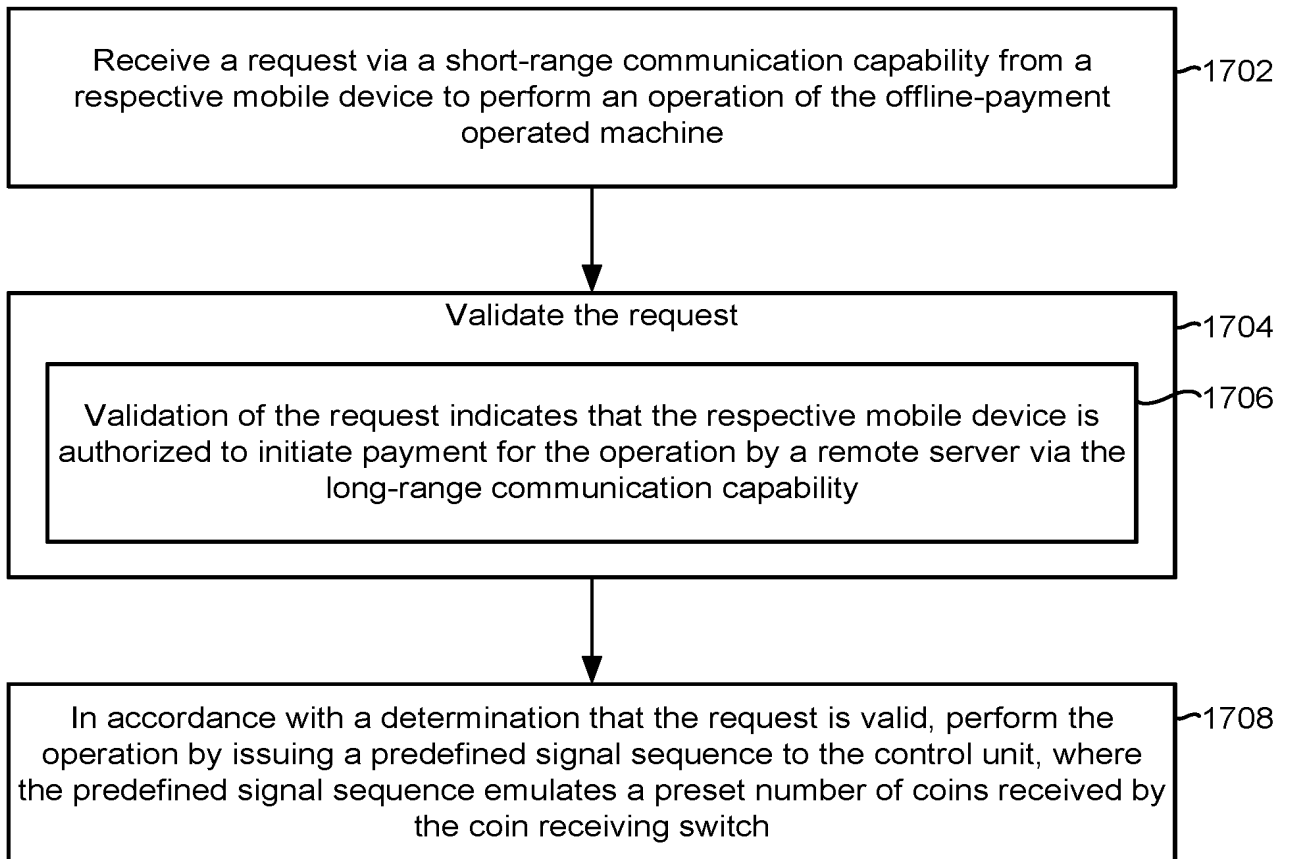


Figure 30

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS
--------------------	--

As the below named inventor, I hereby declare that:

This declaration is directed to: The attached application, or United States application or PCT international application number 14/458,199 filed on August 12, 2014

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims.

I acknowledge the duty to disclose information known to me to be material to patentability as defined by 37 CFR 1.56.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Dr. Paresh K. Patel Date: 10/16/2014

Signature: 

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Paresh K. Patel	Confirmation No.:	To be assigned
Serial No.:	To be assigned	Art Unit	To be assigned
Filed:	Filed Herewith	Examiner:	To be assigned
Title:	<i>METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS</i>	Attorney Docket No.:	104402-5075-US

STATEMENT UNDER 37 C.F.R. § 3.73(c)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

PAYRANGE INC., a corporation, states that it is the assignee of the entire right, title and interest in the patent application/patent identified above by virtue of an assignment from the inventor(s) of the patent application/patent identified above.

The assignment was recorded in the United States Patent and Trademark Office on _____ at Reel _____, Frame _____, or for which a copy thereof is attached.

The undersigned is authorized to act on behalf of the assignee.

Date: May 13, 2023

/Benjamin Pezzner/	70,711
Benjamin Pezzner	(Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP	
1400 Page Mill Road	
Palo Alto, CA 94304	
(650) 843-4000	



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 6 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, TOT CLAIMS, IND CLAIMS. Values: 18/197,071, 05/14/2023, 664, 104402-5075-US, 20, 3

CONFIRMATION NO. 9843

24341
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

FILING RECEIPT



Date Mailed: 06/02/2023

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Paresh K. Patel, Portland, OR;

Applicant(s)

PAYRANGE INC., Portland, OR;

Power of Attorney: The patent practitioners associated with Customer Number 24341

Domestic Priority data as claimed by applicant

This application is a CON of 17/973,507 10/25/2022
which is a CON of 17/654,732 03/14/2022 PAT 11,481,772
which is a CON of 17/147,305 01/12/2021 PAT 11,501,296
which is a CON of 15/603,400 05/23/2017 PAT 10,891,614
which is a CON of 14/458,199 08/12/2014 PAT 9,659,296
which is a CIP of 14/456,683 08/11/2014 PAT 9,256,873
which is a CON of 14/335,762 07/18/2014 PAT 9,547,859
which is a CON of 14/214,644 03/14/2014 PAT 8,856,045
which claims benefit of 61/917,936 12/18/2013
and is a CIP of 29/477,025 12/18/2013 PAT D755183

Foreign Applications for which priority is claimed (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 05/31/2023

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 18/197,071**

Projected Publication Date: 09/07/2023

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING
UNIT EVENTS

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor

community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number
18/197,071

APPLICATION AS FILED - PART I

(Column 1)		(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	64		N/A	
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	280		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	320		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 = *	0	x =	0	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 = *		x =	0			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	664		TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT A	(Column 1)	(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
Total (37 CFR 1.16(i))	*	Minus **	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus ***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))						OR		
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR		
				TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
AMENDMENT B	(Column 1)	(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
Total (37 CFR 1.16(i))	*	Minus **	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus ***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))						OR		
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR		
				TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

TO: padocketingdepartment@morganlewis.com,donald.mixon@morganlewis.com
FROM: noreply@uspto.gov
CC: patentcenter_eofficeaction@uspto.gov
SUBJECT: USPTO: Patent Electronic System - Correspondence Notification for Customer Number 24341

Fri Jun 02 05:02:21 EDT 2023

Dear Patent Center Customer:

Correspondence Address:

Morgan, Lewis &Bockius LLP (PA)
1400 Page Mill Road
Palo Alto,CALIFORNIA,94304-1124
UNITED STATES

This is a courtesy notification regarding the following USPTO patent application(s) associated with your Customer Number, 24341, that have new outgoing correspondence. This correspondence is now available for viewing in Patent Center.

The official date of notification of the outgoing correspondence will be indicated on the form (e.g., PTOL-90) accompanying the correspondence.

Disclaimer:

The list of documents shown below are provided as a courtesy and is not part of the official file wrapper. The content of the images shown in the Image File Wrapper is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
18197071	APP.FILE.REC	06/02/2023	104402-5075-US

To view your correspondence online, please sign in to [Patent Center](#) and then select Workbench/View correspondence. To update your email address(es), select Manage/Manage customer numbers.

If you have any questions, please contact the [Patent Electronic Business Center](#) (EBC) at ebc@uspto.gov or 866-217-9197 Monday – Friday, 6 a.m. to midnight ET.

Please do not reply to this email as it was sent from an unmonitored mailbox.

Sincerely,

The Patent Center Team



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes application details for 18/197,071 and 24341 7590, inventor Paresh K. Patel, and examiner information.

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

donald.mixon@morganlewis.com
padocketingdepartment@morganlewis.com

<i>Decision Granting Request for Prioritized Examination (Track I)</i>	Application No. 18/197,071	Applicant(s) Patel, Paresh K.	
	Examiner FIKIRTE A GEREMEW	Art Unit OMBL	AIA (FITF) Status Yes

1. THE REQUEST FILED 14 May 2023 IS **GRANTED** .

The above-identified application has met the requirements for prioritized examination

- A. for an original nonprovisional application (Track I).
- B. for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination.** The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

- A. filing a **petition for extension of time** to extend the time period for filing a reply;
- B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims**, or a multiple dependent claim;
- C. filing a **request for continued examination** ;
- D. filing a notice of appeal;
- E. filing a request for suspension of action;
- F. mailing of a notice of allowance;
- G. mailing of a final Office action;
- H. completion of examination as defined in 37 CFR 41.102; or
- I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to FIKIRTE GEREMEW at (703) 756-1930. In his/her absence, calls may be directed to Petition Help Desk at (571) 272-3282.

/FIKIRTE A GEREMEW/
PROGRAM SUPPORT ASSISTANT, OMBL

TO: padocketingdepartment@morganlewis.com,donald.mixon@morganlewis.com
FROM: noreply@uspto.gov
CC: patentcenter_eofficeaction@uspto.gov
SUBJECT: USPTO: Patent Electronic System - Correspondence Notification for Customer Number 24341

Wed Jun 28 08:32:21 EDT 2023

Dear Patent Center Customer:

Correspondence Address:

Morgan, Lewis &Bockius LLP (PA)
1400 Page Mill Road
Palo Alto,CALIFORNIA,94304-1124
UNITED STATES

This is a courtesy notification regarding the following USPTO patent application(s) associated with your Customer Number, 24341, that have new outgoing correspondence. This correspondence is now available for viewing in Patent Center.

The official date of notification of the outgoing correspondence will be indicated on the form (e.g., PTOL-90) accompanying the correspondence.

Disclaimer:

The list of documents shown below are provided as a courtesy and is not part of the official file wrapper. The content of the images shown in the Image File Wrapper is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
18197071	TRACK1.GRANT	06/27/2023	104402-5075-US

To view your correspondence online, please sign in to [Patent Center](#) and then select Workbench/View correspondence. To update your email address(es), select Manage/Manage customer numbers.

If you have any questions, please contact the [Patent Electronic Business Center](#) (EBC) at ebc@uspto.gov or 866-217-9197 Monday – Friday, 6 a.m. to midnight ET.

Please do not reply to this email as it was sent from an unmonitored mailbox.

Sincerely,

The Patent Center Team



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes application details for 18/197,071 and 24341 7590, inventor Paresh K. Patel, attorney 104402-5075-US, examiner POINVIL, FRANTZY, art unit 3698, notification date 08/16/2023, and delivery mode ELECTRONIC.

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

donald.mixon@morganlewis.com
padocketingdepartment@morganlewis.com

Office Action Summary

Application No.

18/197,071

Applicant(s)

Patel, Paresh K.

Examiner

FRANTZY POINVIL

Art Unit

3698

AIA (FITF) Status

Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 5/14/2023.
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
- 2a) This action is **FINAL**.
- 2b) This action is non-final.
- 3) An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
- 4) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

- 5) Claim(s) 1-20 is/are pending in the application.
5a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 6) Claim(s) 1,3-15 and 17-20 is/are allowed.
- 7) Claim(s) 2 and 16 is/are rejected.
- 8) Claim(s) _____ is/are objected to.
- 9) Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

- 10) The specification is objected to by the Examiner.
- 11) The drawing(s) filed on 5/14/2023 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- a) All b) Some** c) None of the:
 - 1. Certified copies of the priority documents have been received.
 - 2. Certified copies of the priority documents have been received in Application No. _____.
 - 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date _____.
- 3) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
- 4) Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Claim Rejections - 35 USC § 112

2. Claims 2 and 16 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor (or for applications subject to pre-AIA 35 U.S.C. 112, the applicant), regards as the invention.

As per claims 2 and 16, acronyms are not permitted in the claims. They should be clearly expressed.

As per claim 2, line 5, the acronym "LED's" should be changed to - -light emitted diodes (LED's) - -.

Also, as per claim 16, line 5, the acronym "LED's" should be changed to - -light emitted diodes (LED's) - -.

Double Patenting

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-20 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-23 of U.S. Patent No. 9,659,296. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-20 of the instant application are directed to a similar subject matter contained in claims 1-23 of the '296 patent. The only difference between the instant application and the '296 patent is merely a labeling difference. It is noted that all the features of claims 1-20 are contained in claims 1-23 of the '296 patent.

Claims 1-20 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-25 of U.S. Patent No. 10,891,614. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-20 of the instant application are directed to a similar subject matter contained in claims 1-25 of the '614 patent. The only difference between the instant application and the '614 patent is merely a labeling difference. It is noted that all the features of claims 1-20 are contained in claims 1-25 of the '614 patent.

Claims 1-20 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-28 of U.S. Patent No. 11,501,296. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-20 of the instant application are directed to a similar subject matter contained in claims 1-28 of the '296 patent. The only difference between the instant application and the '296 patent is merely a labeling difference. It is noted that all the features of claims 1-20 are contained in claims 1-28 of the '296 patent.

Claims 1-20 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 11,481,772. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-20 of the instant application are directed to a similar subject matter contained in claims 1-25 of the '772 patent. The only difference between the instant application and the '772 patent is merely a labeling difference. It is noted that all the features of claims 1-20 are contained in claims 1-20 of the '772 patent.

Claims 1-20 are provisionally rejected under the Judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-20 of copending Application No. 17,973,507. Although the conflicting claims are not patentably distinct from each other because claims 1-20 of the instant application are directed to a similar subject matter contained in claims 1-20 of the '507 application. Both inventions are obvious variations of each other achieving the same end result. It would have been obvious to one of

ordinary skill in the art to note that the features of claims 1-20 of the instant application are contained in claims 1-20 of the '507 application.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

4. The prior art taken alone or in combination failed to teach or disclose the limitations of claims 1, 13 and 15. Particularly, the prior art failed to teach or suggest: “after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete a transaction with the available payment accepting unit, wherein the user interface includes a visual representation of the available payment accepting unit, an indication of a balance, and an affordance that, in response to a user input, indicates completion of the transaction, exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction, and after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device” as recited in independent claims 1, 13 and 15.

Wheeler (US Pub. No. 20180374076) discloses a system and method for performing automated operations to identify one or more computing devices associated with potential payees that are within a defined proximity of a user mobile device. A processor-based computing system retrieves stored photographic and biographic information regarding the identified potential payees, and displays the retrieved photographic and biographic information for possible selection by a user of the mobile device. One or more payments from the user of the mobile device may be specified and initiated via the processor-based computing system to potential

payees selected by the user, including for partial or full payment of a customer order of the user with a merchant associated with an identified point-of-sale computing system.

Murray (US Pub. No. 20210056552 A1) a method and apparatus for allowing a customer or payor to select from a plurality of nearby vendors or payees when a computing device of the payor is physically close to electronic devices of the payees. Payee devices and locations of those payee devices may be identified and displayed on a display of a payee device. Once displayed, a specific payee device may be selected by the customer and an order for a product or service may be sent to the selected payee device from the payor device. After the product or service has been provided to the customer, information that confirms that purchase may be sent to any of the selected payee device.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to FRANTZY POINVIL whose telephone number is (571)272-6797. The examiner can normally be reached M-Th 7:00AM to 5:30PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Michael Anderson** can be reached on 571-270-0508. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit:

<https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/fp/

/FRANTZY POINVIL/
Primary Examiner, Art Unit 3698

August 1, 2023

Notice of References Cited

Application/Control No. 18/197,071	Applicant(s)/Patent Under Reexamination Patel, Paresh K.	
Examiner FRANTZY POINVIL	Art Unit 3698	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20220405733-A1	12-2022	Yao; Zhendong	G06Q20/4015	1/1
*	B	US-20210056552-A1	02-2021	Murray; Patrick L.	G06Q20/3276	1/1
*	C	US-20210012318-A1	01-2021	Ducoulombier; Sergio Nicolas	G06Q20/3278	1/1
*	D	US-20180374076-A1	12-2018	Wheeler; Therman	G06Q20/3224	1/1
*	E	US-20140052607-A1	02-2014	Park; Gui Sug	G06Q20/322	705/38
*	F	US-20080010190-A1	01-2008	Rackley III; Brady Lee	G06Q20/3223	705/39
	G					
	H					
	I					
	J					
	K					
	L					
	M					


FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes 	Application/Control No. 18/197,071	Applicant(s)/Patent Under Reexamination Patel, Paresh K.
	Examiner FRANTZY POINVIL	Art Unit 3698

CPC - Searched*		
Symbol	Date	Examiner
G06Q20/40; G06Q20/18; G06Q20/322; G06Q20/3226; G06Q20/327; G06Q20/3278; G07F7/0893; G07F9/023	08/01/2023	FP

CPC Combination Sets - Searched*		
Symbol	Date	Examiner


US Classification - Searched*			
Class	Subclass	Date	Examiner
705	3-44	08/01/2023	FP

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
See the attached DAV and Proquest searches.	08/01/2023	FP

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
705	44	08/01/2023	FP

/FRANTZY POINVIL/ Primary Examiner, Art Unit 3698	
--	--

<i>Index of Claims</i> 	Application/Control No. 18/197,071	Applicant(s)/Patent Under Reexamination Patel, Paresh K.
	Examiner FRANTZY POINVIL	Art Unit 3698

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS									
<input type="checkbox"/> Claims renumbered in the same order as presented by applicant <input type="checkbox"/> CPA <input type="checkbox"/> T.D. <input type="checkbox"/> R.1.47									
CLAIM			DATE						
Final	Original	08/01/2023							
	1	=							
	2	✓							
	3	=							
	4	=							
	5	=							
	6	=							
	7	=							
	8	=							
	9	=							
	10	=							
	11	=							
	12	=							
	13	=							
	14	=							
	15	=							
	16	✓							
	17	=							
	18	=							
	19	=							
	20	=							



Search Strategy from Dialog

August 01 2023 15:11

Search Strategy

Databases: ABI/INFORM® Professional Advanced, Abstracts in New Technology & Engineering, AdisInsight: Drugs, AdisInsight: Trials, Adis Pharmacoconomics & Outcomes News, AGRICOLA, AGRIS, Allied & Complementary Medicine™, Analytical Abstracts, APA PsycInfo®, Aqualine, Aquatic Science & Fisheries Abstracts (ASFA), Australian Education Index, BIOSIS® Toxicology, BIOSIS Previews®, British Library Inside Conferences, British Nursing Index, Business & Industry, CAB ABSTRACTS, Chemical Business Newsbase, Chemical Engineering & Biotechnology Abstracts, Chemical Safety Newsbase, Civil Engineering Abstracts, ClinicalTrials.gov, Current Contents® Search, Derwent Drug File, Derwent Drug Registry, DH-DATA: Health Administration, Medical Toxicology & Environmental Health, DIOGENES® FDA Regulatory Updates, Drug Information Fulltext, Earthquake Engineering Abstracts, EconLit, Ei Compendex®, Ei EnCompassLIT, Embase®, Embase® French Local Literature, EMCare®, ERIC, ESPICOM Pharmaceutical & Medical Device News, FDAnews, FLUIDEX (Fluid Engineering Abstracts), Foodline®: MARKET, Foodline®: PRODUCT, Foodline®: SCIENCE, FSTA®, Gale Group Computer Database™, Gale Group Health Periodicals Database, Gale Group New Product Announcements / Plus®, Gale Group Newsletter Database™, Gale Group PharmaBiomed Business Journals, Gale Group PROMT®, Gale Group Trade & Industry Database™, GEOBASE, GeoRef, Global Health, HSELINE: Health and Safety, ICONDA - International Construction Database, IMS Company Profiles, IMS New Product Focus, IMS Pharma Trademarks, IMS R&D Focus, IMS R&D Focus Drug News, Inspec®, International Pharmaceutical Abstracts, Jane's Defense & Aerospace News, King's Fund, KOSMET: Cosmetic Science, Lancet Titles, Mechanical & Transportation Engineering Abstracts, MEDLINE®, Meteorological & Geostrophysical Abstracts, Morressier Life Science Conference Abstracts and Posters, New England Journal of Medicine, Northern Light Life Sciences Conference Abstracts, NTIS: National Technical Information Service, Oceanic Abstracts, PAIS International, Paperbase, PAPERCHEM, ProQuest Advanced Tech & Aerospace Professional, ProQuest Biological & Health Science Professional, ProQuest Dissertations and Theses Professional, ProQuest Environmental Science Professional, ProQuest Materials Research Professional, ProQuest Newsstand Professional, ProQuest Technology Research Professional, Proux Science Daily Essentials, Proux Science Drug Data Report, Proux Science Drugs Of The Future™, Publicly Available Content, Registry of Toxic Effects of Chemical Substances (RTECS®), SciSearch®: a Cited Reference Science Database, Social SciSearch®, ToxFile®, Transport Research International Documentation, TULSA™ (Petroleum Abstracts), UBM Computer Full Text, Weldasearch®, Zoological Record

Set#	Searched for	Results
S1	((vending pre/5 machine[*1]) or kiosk[*1]) pre/15 (mobile* or phone[*1] or transceiv*)	46237
S2	S1 and ((payment[*1] or paying) pre/8 (trigg* or transaction[*1]))	2131
S3	((((Select* or chos* or choos* or accept*) or pre/15 or (payee* or seller[*1]))) or pre/15 or (terminal[*1] or computer[*1] or mobile or phone or device[*1]))	278807480
S4	S2 and S3	2131
S5	S4 and mobile and accelerat*	794
S6	S1 and S3	46177
S7	S5 and S6	749°
S8	s7 and ((dispens* or eject*) pre/10 (product[*1] or good[*1] or item[*1] or service*!))	44°

° Duplicates are removed from the search and from the result count.

Contact ProQuest

Copyright © 2023 ProQuest LLC. All rights reserved. - **Terms and Conditions**

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	411	(payee\$ OR seller\$1) adj10 (terminal\$1 OR computer\$1 OR device\$1) adj10 (payment\$ OR card\$1 OR mobile) adj10 (bluetooth OR wireless\$)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 06:56 AM
L2	1971	(payee\$ OR seller\$1) adj15 (terminal\$1 OR computer\$1 OR mobile OR phone OR device\$1) adj15 (id\$1 OR identif\$) adj15 pay\$	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 06:58 AM
L3	1189	(Select\$ OR chos\$or choos\$ OR accept\$) adj15(payee\$ OR seller\$1) adj15 (terminal\$1 OR computer\$1 OR mobile OR phone OR device\$1) adj15 (pay\$ OR card\$1)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 07:09 AM
L4	54413	((vending adj5 machine\$1) OR kiosk\$1) adj15 (mobile\$ OR phone\$1 OR transceiv\$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 07:19 AM
L5	411	L2 AND I3	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 07:20 AM
L6	9	L5 AND L4	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 07:23 AM
L7	54	L5 AND L1	(US-PGPUB; USPAT; USOCR; FIT (AP, AT,	OR	ON	ON	2022/05/16 07:23 AM

L8	0	(mobile OR wireless OR gps) adj15 accelerometer\$1 adj15 (walk\$ OR distance\$) adj15 (transaction\$)	AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 07:47 AM
L9	17	(mobile OR wireless OR gps) SAME accelerometer\$1 adj15 (walk\$ OR distance\$) SAME (transaction\$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 07:48 AM
L10	1	"10891614".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/16 11:32 AM
L11	419	(payee\$ OR seller\$1) adj10 (terminal\$1 OR computer\$1 OR device\$1) adj10 (payment\$ OR card\$1 OR mobile) adj10 (bluetooth OR wireless\$)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/08/30 04:57 PM
L12	2006	(payee\$ OR seller\$1) adj15 (terminal\$1 OR computer\$1 OR mobile OR phone OR device\$1) adj15 (id\$1 OR identif\$) adj15 pay\$	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/08/30 04:57 PM
L13	1205	(Select\$ OR chos\$or choos\$ OR accept\$) adj15(payee\$ OR seller\$1) adj15 (terminal\$1 OR computer\$1 OR mobile OR phone OR device\$1) adj15 (pay\$ OR card\$1)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/08/30 04:57 PM
L14	55797	((vending adj5 machine\$1) OR kiosk\$1) adj15 (mobile\$ OR phone\$1 OR transceiv\$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2022/08/30 04:57 PM

L15	414	L2 AND I3	IBM_TDB) (US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/08/30 04:57 PM
L16	9	L5 AND L4	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/08/30 04:57 PM
L17	54	L5 AND L1	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/08/30 04:57 PM
L18	0	(mobile OR wireless OR gps) adj15 accelerometer\$1 adj15 (walk\$ OR distance\$) adj15 (transaction\$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/08/30 04:57 PM
L19	18	(mobile OR wireless OR gps) SAME accelerometer\$1 adj15 (walk\$ OR distance\$) SAME (transaction\$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/08/30 04:57 PM
L20	1	"10891614".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/08/30 04:57 PM
L21	440	(payee\$ OR seller\$1) adj10 (terminal\$1 OR computer\$1 OR device\$1) adj10 (payment\$ OR card\$1 OR mobile) adj10 (bluetooth OR wireless\$)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L22	2145	(payee\$ OR seller\$1) adj15 (terminal\$1 OR computer\$1 OR mobile OR phone OR	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR,	OR	ON	ON	2023/08/01 12:02 PM

L23	1298	device\$1) adj15 (id\$1 OR identif\$) adj15 pay\$ (Select\$ OR chos\$or choos\$ OR accept\$) adj15(payee\$ OR seller\$1) adj15 (terminal\$1 OR computer\$1 OR mobile OR phone OR device\$1) adj15 (pay\$ OR card\$1)	GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L24	60284	((vending adj5 machine\$1) OR kiosk\$1) adj15 (mobile\$ OR phone\$1 OR transceiv\$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L25	449	L2 AND I3	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L26	12	L5 AND L4	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L27	54	L5 AND L1	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L28	0	(mobile OR wireless OR gps) adj15 accelerometer\$1 adj15 (walk\$ OR distance\$) adj15 (transaction\$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L29	21	(mobile OR wireless OR gps) SAME accelerometer\$1 adj15	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD,	OR	ON	ON	2023/08/01 12:02 PM

L30	1	(walk\$ OR distance\$) SAME (transaction\$) "10891614".pn.	DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB) (US-PGPUB; USPAT)	OR	ON	ON	2023/08/01 12:02 PM
L31	440	(payee\$ OR seller\$1) adj10 (terminal\$1 OR computer\$1 OR device\$1) adj10 (payment\$ OR card\$1 OR mobile) adj10 (bluetooth OR wireless\$)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L32	2145	(payee\$ OR seller\$1) adj15 (terminal\$1 OR computer\$1 OR mobile OR phone OR device\$1) adj15 (id\$1 OR identif\$) adj15 pay\$	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L33	1298	(Select\$ OR chos\$or choos\$ OR accept\$) adj15(payee\$ OR seller\$1) adj15 (terminal\$1 OR computer\$1 OR mobile OR phone OR device\$1) adj15 (pay\$ OR card\$1)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L34	60284	((vending adj5 machine\$1) OR kiosk\$1) adj15 (mobile\$ OR phone\$1 OR transceiv\$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L35	449	L2 AND I3	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L36	12	L5 AND L4	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM

L37	54	L5 AND L1	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L38	0	(mobile OR wireless OR gps) adj15 accelerometer\$1 adj15 (walk\$ OR distance\$) adj15 (transaction\$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L39	21	(mobile OR wireless OR gps) SAME accelerometer\$1 adj15 (walk\$ OR distance\$) SAME (transaction\$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:02 PM
L40	1	"10891614".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2023/08/01 12:02 PM
L41	284	L35 AND mobile AND payment\$1 AND ((machine\$ OR vending OR device\$1) SAME (good\$1 OR product\$1 OR item\$))	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:13 PM
L42	146521	(G06Q20/40 OR G06Q20/18 OR G06Q20/322 OR G06Q20/3226 OR G06Q20/327 OR G06Q20/3278 OR G07F7/0893 OR G07F9/023).cpc.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:16 PM
L43	137	L41 AND I42	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/08/01 12:17 PM
L44	41	((("PAYRANGE") near3 ("INC"))).AS,AANM.	(USPAT)	OR	ON	ON	2023/08/01 12:28 PM
L45	133	((("PATEL") near3 ("Paresh"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/08/01 12:29 PM

L46	83	L44 AND I45	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2023/08/01 12:32 PM
-----	----	-------------	---	----	----	----	------------------------

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

TO: padocketingdepartment@morganlewis.com,donald.mixon@morganlewis.com
FROM: noreply@uspto.gov
CC: patentcenter_eofficeaction@uspto.gov
SUBJECT: USPTO: Patent Electronic System - Correspondence Notification for Customer Number 24341

Wed Aug 16 05:04:26 EDT 2023

Dear Patent Center Customer:

Correspondence Address:

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CALIFORNIA, 94304-1124
UNITED STATES

This is a courtesy notification regarding the following USPTO patent application(s) associated with your Customer Number, 24341, that have new outgoing correspondence. This correspondence is now available for viewing in Patent Center.

The official date of notification of the outgoing correspondence will be indicated on the form (e.g., PTOL-90) accompanying the correspondence.

Disclaimer:

The list of documents shown below are provided as a courtesy and is not part of the official file wrapper. The content of the images shown in the Image File Wrapper is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
18197071	CTNF	08/16/2023	104402-5075-US
18197071	892	08/16/2023	104402-5075-US

To view your correspondence online, please sign in to [Patent Center](#) and then select Workbench/View correspondence. To update your email address(es), select Manage/Manage customer numbers.

If you have any questions, please contact the [Patent Electronic Business Center \(EBC\)](#) at ebc@uspto.gov or 866-217-9197 Monday – Friday, 6 a.m. to midnight ET.

Please do not reply to this email as it was sent from an unmonitored mailbox.

Sincerely,

The Patent Center Team



**UNITED STATES
PATENT AND TRADEMARK OFFICE**

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

APPROVAL LETTER

APPLICATION #
18/197,071


FILING DATE
05/14/2023

APPLICANT/PATENT UNDER REEXAMINATION
Paresh Patel

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Electronic terminal disclaimer filed on 08/16/2023

 Approved

This patent is subject to a Terminal Disclaimer

Approved / Disapproved by: Electronic Terminal Disclaimer automatically approved



ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #
18/197,071

RECEIPT DATE / TIME
08/16/2023 07:58:36 PM ET

ATTORNEY DOCKET #
104402-5075-US

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	9843	FILED BY	Benjamin Pezzner
PATENT CENTER #	62629566	FILING DATE	05/14/2023
CUSTOMER #	24341	FIRST NAMED INVENTOR	Paresh K. Patel
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
petition-request.pdf	3	Terminal Disclaimer-Filed (Electronic)	50 KB
grantLetter.pdf	1	Terminal Disclaimer-Electronic-Approved	19 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
petition-request.pdf	5AAAC969C12D2D5CCE49DBE699BA56BA300D672081834A8B CB668FABC3B09AC883D7E09BDC1F698C44FD8D46A8A6C346

Petitioner Exhibit 1002-0171

61DC4FB13EE9758C4E0AF5996BE8C908

grantLetter.pdf

692ED596AA469B5C9CE1481200B932960353FAD2CFE36B331
56D4A9390E73E2A62334B043EE52A16FDF557C3F705CC1364
E292B80FB01B3A964DF6312964227C

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



ELECTRONIC PAYMENT RECEIPT

APPLICATION #
18/197,071

RECEIPT DATE / TIME
08/16/2023 07:58:36 PM ET

ATTORNEY DOCKET #
104402-5075-US

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	9843	FILED BY	Benjamin Pezzner
PATENT CENTER #	62629566	AUTHORIZED BY	-
CUSTOMER #	24341	FILING DATE	05/14/2023
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Paresh K. Patel

Payment Information

PAYMENT METHOD CARD / 8177	PAYMENT TRANSACTION ID E20238FK08245408	PAYMENT AUTHORIZED BY Benjamin Pezzner
--------------------------------------	---	--

FEE CODE	DESCRIPTION	ITEM PRICE(\$)	QUANTITY	ITEM TOTAL(\$)
2814	STATUTORY DISCLAIMER, INCLUDING TERMINAL DISCLAIMER	170.00	1	170.00
			TOTAL AMOUNT:	\$170.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

**TERMINAL DISCLAIMER TO OBTAIN A PROVISIONAL DOUBLE PATENTING REJECTION OVER
A PENDING "REFERENCE" APPLICATION**

APPLICATION #
18197071

FILING DATE
05/14/2023

FIRST NAMED INVENTOR
Paresh Patel

ATTORNEY DOCKET #
104402-5075-US

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT
EVENTS



Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action



This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent interest
PYRANGE INC.	100%
Total	100%

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

Application #	Filing Date
17973507	10/25/2022

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so

granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

Patent #

9659296

10891614

11501296

11481772

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.



Terminal disclaimer fee under 37 CFR 1.20(d) included with Electronic Terminal Disclaimer request.

Applicant claims the following entity status:

Small

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I certify, in accordance with 37 CFR 1.4(d)(4) that I am: An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Signature	Name	Registration #
/Benjamin Pezzner/	Benjamin Pezzner	70711

* Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this certification. See MPEP 324.



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 4 columns: APPLICATION NUMBER (18/197,071), FILING OR 371(C) DATE (05/14/2023), FIRST NAMED APPLICANT (Paresh K. Patel), ATTY. DOCKET NO./TITLE (104402-5075-US)

CONFIRMATION NO. 9843

24341
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

PUBLICATION NOTICE



OC00000061560249

Date Mailed: 09/07/2023

Title:METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Publication No.US-2023-0281623-A1

Publication Date:09/07/2023

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

TO: padocketingdepartment@morganlewis.com,donald.mixon@morganlewis.com
FROM: noreply@uspto.gov
CC: patentcenter_eofficeaction@uspto.gov
SUBJECT: USPTO: Patent Electronic System - Correspondence Notification for Customer Number 24341

Thu Sep 07 05:08:41 EDT 2023

Dear Patent Center Customer:

Correspondence Address:

Morgan, Lewis &Bockius LLP (PA)
1400 Page Mill Road
Palo Alto,CALIFORNIA,94304-1124
UNITED STATES

This is a courtesy notification regarding the following USPTO patent application(s) associated with your Customer Number, 24341, that have new outgoing correspondence. This correspondence is now available for viewing in Patent Center.

The official date of notification of the outgoing correspondence will be indicated on the form (e.g., PTOL-90) accompanying the correspondence.

Disclaimer:

The list of documents shown below are provided as a courtesy and is not part of the official file wrapper. The content of the images shown in the Image File Wrapper is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
18197071	NTC.PUB	09/07/2023	104402-5075-US

To view your correspondence online, please sign in to [Patent Center](#) and then select Workbench/View correspondence. To update your email address(es), select Manage/Manage customer numbers.

If you have any questions, please contact the [Patent Electronic Business Center](#) (EBC) at ebc@uspto.gov or 866-217-9197 Monday – Friday, 6 a.m. to midnight ET.

Please do not reply to this email as it was sent from an unmonitored mailbox.

Sincerely,

The Patent Center Team



**UNITED STATES
PATENT AND TRADEMARK OFFICE**

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

**TERMINAL DISCLAIMER TO OBIVATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER
A PENDING "REFERENCE" APPLICATION**

**APPLICATION #
18197071**

**FILING DATE
05/14/2023**

**FIRST NAMED INVENTOR
Paresh Patel**

**ATTORNEY DOCKET #
104402-5075-US**

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT
EVENTS



Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action



This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent interest
PYRANGE INC.	100%
Total	100%

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

Application #	Filing Date
17973507	10/25/2022

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so

granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

Patent #

9659296

10891614

11501296

11481772

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.



Terminal disclaimer fee under 37 CFR 1.20(d) included with Electronic Terminal Disclaimer request.

Applicant claims the following entity status:

Small

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I certify, in accordance with 37 CFR 1.4(d)(4) that I am: An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Signature	Name	Registration #
/Benjamin Pezzner/	Benjamin Pezzner	70711

* Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this certification. See MPEP 324.



ELECTRONIC PAYMENT RECEIPT

APPLICATION #
18/197,071

RECEIPT DATE / TIME
11/15/2023 03:24:56 AM Z ET

ATTORNEY DOCKET #
104402-5075-US

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	9843	FILED BY	Benjamin Pezzner
PATENT CENTER #	63251511	AUTHORIZED BY	-
CUSTOMER #	24341	FILING DATE	05/14/2023
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Paresh K. Patel

Payment Information

PAYMENT METHOD CARD / 8177	PAYMENT TRANSACTION ID E2023AE425108602	PAYMENT AUTHORIZED BY Benjamin Pezzner
--------------------------------------	---	--

FEE CODE	DESCRIPTION	ITEM PRICE(\$)	QUANTITY	ITEM TOTAL(\$)
2814	STATUTORY DISCLAIMER, INCLUDING TERMINAL DISCLAIMER	170.00	1	170.00
			TOTAL AMOUNT:	\$170.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

APPROVAL LETTER

APPLICATION #
18/197,071

FILING DATE
05/14/2023

APPLICANT/PATENT UNDER REEXAMINATION
Paresh Patel

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Electronic terminal disclaimer filed on 11/15/2023

 Approved

This patent is subject to a Terminal Disclaimer

Approved / Disapproved by: Electronic Terminal Disclaimer automatically approved



ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #
18/197,071

RECEIPT DATE / TIME
11/15/2023 03:24:56 AM Z ET

ATTORNEY DOCKET #
104402-5075-US

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	9843	FILED BY	Benjamin Pezzner
PATENT CENTER #	63251511	FILING DATE	05/14/2023
CUSTOMER #	24341	FIRST NAMED INVENTOR	Paresh K. Patel
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
petition-request.pdf	3	Terminal Disclaimer-Filed (Electronic)	50 KB
grantLetter.pdf	1	Terminal Disclaimer-Electronic-Approved	19 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
petition-request.pdf	B9E BC3F460B3DCE2957864154EDD6A68758AD66108A23060D65215A503F4D8F1A74D9B102C10F1A997DBEF04D4967EB9C4

Petitioner Exhibit 1002-0186

803BD646CA4BA4C74B1C4B6EE523B6

grantLetter.pdf

C66A8A324C054C9F0D43830160B55AF5158E009213E502E294
EF8518CCEBEDCC08DC6D49F8456639B028D210EFD6FF60A7
9E11E652629D472F78E047C6786721

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application #	Confirmation #	Attorney Docket #	Filing Date
18/197,071	9843	104402-5075-US	05/14/2023
Title		Inventors	Examiner
Method And System For Presenting Representations Of Payment Accepting Unit Events		Paresh K. Patel	Frantzy Poinvil AU 3698

RESPONSE TO NON-FINAL OFFICE ACTION DATED 8/16/2023

Contents of Submission

Claims, pages 2-6

Remarks, pages 7-8

Extension of Time

No extensions are necessary for this filing.

Fee Authorization

The Director is authorized to charge any required fees to Deposit Account 50-0310.

CLAIMS

Rewrite the pending claims as follows:

1. (Original) A method of presenting representations of payment accepting unit events, comprising:

at a mobile device with one or more processors, memory, one or more output devices including a display, and one or more radio transceivers:

identifying one or more payment accepting units that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier or location corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input selecting an available payment accepting unit of the one or more payment accepting units;

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete a transaction with the available payment accepting unit, wherein the user interface includes a visual representation of the available payment accepting unit, an indication of a balance, and an affordance that, in response to a user input, indicates completion of the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

2. (Currently Amended) The method of claim 1, wherein the updated user interface of the mobile payment application includes at least one of:

a message displayed on the display of the mobile device;

a banner notification displayed on a display of the mobile device; and/or
a visual alert from one or more light-emitting diodes (LEDs) of the mobile device.

3. (Original) The method of claim 1, wherein the information indicates completion of the transaction between the user of the mobile device and the available payment accepting unit.

4. (Original) The method of claim 3, wherein the mobile device includes a long-range transceiver and the information at least includes an amount of the completed transaction, and the method further comprises:

 sending at least the amount of the completed transaction to a server via the long-range transceiver.

5. (Original) The method of claim 1, wherein the information indicates abortion of the transaction initiated by the user of the mobile device.

6. (Original) The method of claim 1, wherein the information indicates failure of the transaction initiated by the user of the mobile device or a malfunction associated with the available payment accepting unit.

7. (Original) The method of claim 1, wherein the mobile device includes an accelerometer and the method further comprises:

 based on data from the accelerometer, determining whether the user is walking away from the available payment accepting unit; and

 in accordance with a determination that the user is walking away from the available payment accepting unit, canceling the wireless communication path.

8. (Original) The method of claim 1, wherein the information reflects availability of the available payment accepting unit to conduct a transaction.

9. (Original) The method of claim 1, further comprising:

 in addition to exchanging the information, receiving, via the one or more radio transceivers, a coupon that is targeted to the user of the mobile device based on the transaction.

10. (Original) The method of claim 1, wherein the user interface of the mobile payment application, after establishing the wireless communication path, indicates that the wireless communication path has been established with the available payment accepting unit.

11. (Original) The method of claim 1, wherein the user input is a swipe that causes the affordance to be slid.

12. (Original) The method of claim 1, wherein the payment operated machines include a payment activated washer, a payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

13. (Original) A mobile device, comprising:
one or more radio transceivers;
one or more output devices including a display;
one or more processors; and
memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for:

identifying one or more payment accepting units that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier or location corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input selecting an available payment accepting unit of the one or more payment accepting units;

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete a transaction with the available payment accepting unit, wherein the user interface includes a visual representation of the

available payment accepting unit, an indication of a balance, and an affordance that, in response to a user input, indicates completion of the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

14. (Original) The mobile device of claim 13, wherein identifying the one or more payment accepting units includes identifying a payment activated washer, a payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

15. (Original) A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a mobile device with one or more processors, one or more output devices including a display, and one or more radio transceivers, cause the mobile device to perform operations comprising:

identifying one or more payment accepting units that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier or location corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input selecting an available payment accepting unit of the one or more payment accepting units;

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete a transaction with the available payment accepting unit, wherein the user interface includes a visual representation of the

available payment accepting unit, an indication of a balance, and an affordance that, in response to a user input, indicates completion of the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

16. (Currently Amended) The non-transitory computer readable storage medium of claim 15, wherein the updated user interface of the mobile payment application includes at least one of:

a message displayed on the display of the mobile device;

a banner notification displayed on a display of the mobile device; and/or

a visual alert from one or more light-emitting diodes (LEDs) of the mobile device.

17. (Original) The non-transitory computer readable storage medium of claim 15, wherein: the information indicates completion of the transaction between the user of the mobile device and the available payment accepting unit;

the information at least includes an amount of the completed transaction; and

the instructions further cause the mobile device to send at least the amount of the completed transaction to a server.

18. (Original) The non-transitory computer readable storage medium of claim 15, wherein the information indicates abortion of the transaction initiated by the user of the mobile device.

19. (Original) The non-transitory computer readable storage medium of claim 15, wherein the information indicates failure of the transaction initiated by the user of the mobile device or a malfunction associated with the available payment accepting unit.

20. (Original) The non-transitory computer readable storage medium of claim 15, wherein identifying the one or more payment accepting units includes identifying a payment activated washer, a payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

REMARKS

This communication is in response to the Non-Final Office Action dated August 16, 2023. In the Office Action:

- claims 2 and 16 were rejected under 112(b),
- claims 1-20 were rejected under obviousness-type double patenting, and
- claims 1, 3-16, and 17-20 were found to be allowable.

In this response, claims 2 and 16 have been amended. Support for the amendments can be found in the original disclosure; no new matter has been added. Upon entry of this response, claims 1-20 are pending.

112(b) Rejection

Claims 2 and 16 have been amended to clarify the acronyms.

Double Patenting

A terminal disclaimer is being filed concurrently with this response to address this non-statutory double patenting rejection.

Allowable Subject Matter

The Applicant acknowledges the allowability of claims 1, 3-15, and 17-20.

Upon entry of this response, claims 1-20 are pending.

McKesson Statement

In view of *McKesson Information Solutions v. Bridge Medical* (Fed. Cir. 2007), the Applicant wishes to inform the Examiner that the prosecution history of the following US Patent Applications may contain information relevant to the pending application:

14/214644*, 14/320534, 14/335762, 14/611065, 14/641236, 14/321717, 14/321724, 14/321733, 14/456683, 14/968703*, 14/614336, 14/458192, 14/458199*, 15/893514, 15/435228, 15/878352*, 15/603400*, 15/406492*, 16/029483, 15/956741, 16/681673, 16/748727, 16/750477, 16/934933*, 17/529111, 17/147305, 16/934392, 17/216399, 17/973506, 17/968672, 17/973505, 17/443802, 17/983311, 17/985832, 17/654732*, 17/978894, 17/963170, 17/973507, 18/197070, 18/197071

The Examiner is encouraged to review the art made of record, office actions, and notices of allowance, if any, in the above-mentioned applications.

In addition, applications marked with an asterisk (*) have been or are currently being challenged at the PTAB. The Examiner is encouraged to review the record of each of these proceedings in the Patent Trial and Appeal Case Tracking System (P-TACTS).

Concluding Remarks

By responding in the foregoing remarks only to particular positions asserted by the examiner, the Applicant does not necessarily acquiesce in other positions that have not been explicitly addressed. In addition, the Applicant's arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist.

In light of the above amendments and remarks, the Applicant respectfully requests that the Examiner reconsider this application with a view towards allowance. The Examiner is invited to call the undersigned attorney at (650) 843-4000, if a telephone call could help resolve any remaining items.

Respectfully submitted,

Date: November 15, 2023

/Douglas J. Crisman/

39,951

Douglas J. Crisman

(Reg. No.)

MORGAN, LEWIS & BOCKIUS LLP

1400 Page Mill Road

Palo Alto, CA 94304

Phone: (650) 843-4000



ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #
18/197,071

RECEIPT DATE / TIME
11/15/2023 07:19:12 PM Z ET

ATTORNEY DOCKET #
104402-5075-US

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	9843	FILED BY	Benjamin Pezzner
PATENT CENTER #	63251523	FILING DATE	05/14/2023
CUSTOMER #	24341	FIRST NAMED INVENTOR	Paresh K. Patel
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 3

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
104402-5075-US Response to OA.pdf	8	-	166 KB
104402-5075-US Response to OA-A....pdf	(1-1) 1	Amendment/Request for Reconsideration-After Non-Final Rejection	90 KB
104402-5075-US Response to OA-CLM.pdf	(2-6) 5	Claims	122 KB
104402-5075-US Response to OA-REM.pdf	(7-8) 2	Applicant Arguments/Remarks Made in an Amendment	141 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
104402-5075-US Response to OA.pdf	C3CB7ED139168CA6A671A71B21215699E6EBAE850317B3AB084FFEA8037AD1F8E6B978307613662871DAE24DEC0902B0F759F343A7071475B26AA936A600D6EC
104402-5075-US Response to OA-A....pdf	0276E5573C7F2D12268C9FA140049D924FF13F47F8E60C60889AFA70AF35EEE7854B42A1CED29F8421D450102B166803333A51E5C4A24B7D59B421418BED16AD
104402-5075-US Response to OA-CLM.pdf	01E26E80FB0C3A9051EC67523E19E5D0CB31875B57D75CE470D3049AD3876A0B280D7C1AFB1945B15EAB70B05D09BC04482626FC572F09E4FF84DECE7589FEC0
104402-5075-US Response to OA-REM.pdf	9FF50FF357AE50EF159201EB3D58A46C71573F8AA39006C0D17BD2213EFAEF756D041800E11278783BB1BE8070C8D676D71CD27698E12146580F8FAA5F58A058

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 18/197,071	Filing Date 05/14/2023	<input type="checkbox"/> To be Mailed
---	--	---------------------------	---------------------------------------

ENTITY: LARGE SMALL MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 = *		x \$40 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 = *		x \$ 192 =	
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT	11/15/2023	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	x \$ 40 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	x \$ 192 =	0
<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))							
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
						TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)	RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		
	Total (37 CFR 1.16(i))	*	Minus	**	=	x \$ 0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x \$ 0 =	
<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))							
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. LIE

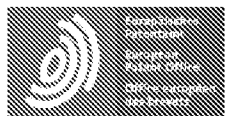
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". /ANDREA V FREEMAN/

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Espacenet

Bibliographic data: CN106803175 (A) — 2017-06-06

Snap mobile payment apparatuses, methods and systems

Inventor(s): HAMMAD AYMAN; KARPENKO IGOR; GAVRILOV MIROSLAV;
SHRIVASTAVA ABHINAV; CARLSON MARK; HARIRAMANI
PRAKASH ± (A·哈曼德, ; I·卡彭科, ; M·加夫利洛夫, ; A·施里瓦司塔瓦,
; M·卡尔森, ; P·哈里拉马尼)

Applicant(s): VISA INT SERVICE ASS ± (维萨国际服务协会)

Classification: - international: G06Q20/36
- cooperative: G06Q20/20 (EP, US); G06Q20/204 (EP, US);
G06Q20/326 (EP); G06Q20/3276 (EP, US);
G06Q20/36 (CN); G06Q20/3674 (EP, US);
G06Q20/384 (EP); G06Q30/06 (EP, US)

Application number: CN20171037081 20120216 [Global Dossier](#)

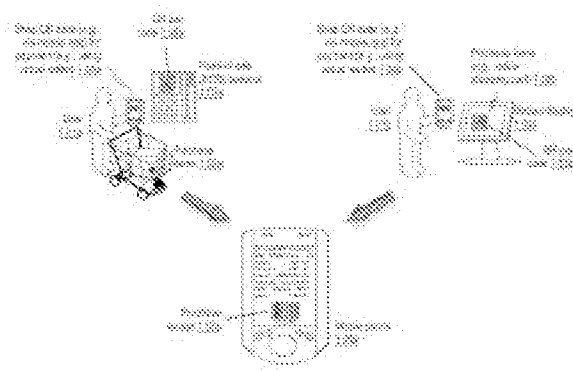
Priority number(s): US201161443624P 20110216 ; US201161512248P 20110727 ;
US201161522213P 20110810 ; US201161527576P 20110825 ;
CN20128018719 20120216

Also published as: CN106803175 (B) AU2012217606 (A1) AU2016204018 (A1)
AU2018204759 (A1) AU2018204759 (B2) BR112013021059 (A2)
CN103765453 (A) CN103765453 (B) CN109118199 (A)
SG193481 (A1) US11288661 (B2) US2012209749 (A1)
US2014197234 (A1) US2019034921 (A1) US2022253832 (A1)
WO2012112822 (A2) WO2012112822 (A3) [less](#)

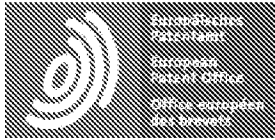
Abstract of CN106803175 (A)

The snap mobile payment apparatuses, methods and systems (SNAP) transform real-time-generated merchant-product Quick Response codes via SNAP components into virtual wallet card-based transaction purchase notifications. In one embodiment, the SNAP obtains a snapshot of a QR code presented on a display screen of a point-of-sale device from a mobile device. The SNAP decodes the QR code to obtain product information included in a checkout request of the user, and merchant information for processing a user purchase transaction with a merchant providing the QR code. The SNAP accesses a user virtual wallet to obtain user account information to process the user purchase transaction with the merchant. Using the product information, merchant information and user account information, the SNAP generates a card authorization

request, and which the SNAP provides to a payment network for transaction processing. Also, the SNAP obtains a purchase receipt confirming processing of the user purchase transaction.



ESPACENET PUBLIC DOMAIN



Patent Translate

Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION CN106803175A

10 Snapshot mobile payment device, method and system

[0001]

14 This application is a divisional application based on the patent application with the application number 201280018719.7, the application date is February 16, 2012, and the invention title is "Quick shot mobile payment device, method and system".

[0002]

20 This patent application publication document (hereinafter referred to as "the specification") describes the inventive aspects leading to each new innovation (hereinafter referred to as the new invention technology and/or new method) and contains the subject matter of copyright, mask work and/or other knowledge Property Rights Protected Materials.

24 The respective owners of this intellectual property have no objection to the facsimile reproduction by anyone of the patent disclosure document as it appears in published patent office files/records, but otherwise reserve all rights.

[0003]

30 priority statement

[0004]

34 This application claims priority under 35 USC §119: Serial No. 61/443,624 filed February 16, 2011, entitled "Mobile Capture Checkout Apparatus, Method, and System," Attorney No. P-42032PRV|20270 - U.S. Provisional Patent Application for 127PV; Serial No. 61/512,248 filed July 27, 2011, entitled "Quickshot Mobile Payment Apparatus, Method, and System," Attorney No. 10US01|20270-175PV for U.S. Provisional

Patent Application ; U.S. Provisional Patent Application Serial No. 61/522,213 filed August 10, 2011, entitled "Universal Mobile Payment Platform, Apparatus, Method, and System," Attorney No. 10US03|20270-175PV2; and August 2011 The serial number of the application on the 25th is 61/527,576, the title is "Quipai mobile payment device, method and system", and the US provisional patent application number is 10US02|20270-175PV1.

⁴³ The entire teaching of the aforementioned application is hereby incorporated by reference.

[0005]

⁴⁷ technical field

[0006]

⁵¹ The present invention relates generally to devices, methods and systems for electronic purchase transactions, and in particular, to Snapshot mobile payment devices, methods and systems ("SNAP").

[0007]

⁵⁶ Background technique

[0008]

⁶⁰ A customer transaction typically requires the customer to select a product from a display shelf or a website and then check out at a checkout counter or on a web page.

⁶² Product information is usually selected from web catalogs or entered into point-of-sale terminals.

⁶³ In a physical retail environment, product information is automatically entered by scanning item barcodes at point-of-sale registers with integrated barcode scanners, and customers are typically provided with multiple payment options, such as cash, check, credit card or debit card.

⁶⁶ Once payment is made and approved, the point-of-sale recorder stores the transaction in the merchant's computer system and generates a receipt indicating that the transaction has been satisfactorily concluded.

[0009]

⁷¹ Description of drawings

[0010]

⁷⁵ According to the inventive aspects of the present invention, the appendix and/or accompanying drawings illustrate non-limiting examples according to various examples of the present invention, aspects of the invention:

[0011]

81 1A-F show block diagrams illustrating example aspects of snap mobile payment based purchase transactions in some embodiments of SNAP;

[0012]

86 2A-F show application user interface diagrams illustrating example features of the Snap Mobile Payment application that facilitates Snap Mobile Payments, in some embodiments of the SNAP;

[0013]

91 3A-E show application user interface diagrams illustrating example features of the Snap mobile payment application for capturing product barcodes, protecting user data, and preventing fraud, in some embodiments of the SNAP;

[0014]

97 Figures 4A-D show data flow diagrams illustrating an example snap mobile payment process in some embodiments of the SNAP;

[0015]

102 5A-E show logic flow diagrams illustrating example aspects of implementing Snap Mobile Payments, such as Snap Mobile Payment Execution (“SMPE”) component 500, in some embodiments of the SNAP;

[0016]

107 6A-B show logic flow diagrams illustrating example aspects of processing quick response codes, such as Quick Response Code Processing (“QRCP”) component 600, in some embodiments of the SNAP;

[0017]

112 Figure 7 shows a user interface diagram illustrating an overview of example features of a virtual wallet application in some embodiments of the SNAP;

[0018]

117 8A-G show user interface diagrams illustrating example features of a virtual wallet application in shopping mode, in some embodiments of the SNAP;

[0019]

122 9A-F show user interface diagrams illustrating example features of a virtual wallet application in payment mode, in some embodiments of the SNAP;

[0020]

127 Figure 10 shows a user interface diagram illustrating example features of a virtual wallet application in history mode, in some embodiments of the SNAP;

[0021]

132 11A-F show user interface diagrams illustrating example features of a virtual wallet application in snap mode, in some embodiments of the SNAP;

[0022]

137 Figure 12 shows a user interface diagram illustrating example features of a virtual wallet application in offer mode, in some embodiments of the SNAP;

[0023]

142 13A-B show user interface diagrams illustrating example features of a virtual wallet application in security and privacy mode, in some embodiments of the SNAP;

[0024]

147 Figure 14 shows a block diagram illustrating an embodiment of a SNAP controller.

[0025]

151 The number preceding each reference number within the figure indicates the figure in which the reference number is introduced and/or elaborated upon.

153 Accordingly, a detailed discussion of reference numeral 101 will appear and/or be referenced in FIG. 1 , reference numeral 201 is introduced in FIG. 2 , and so on.

[0026]

158 Detailed ways

[0027]

162 Snapshot Mobile Payment (SNAP)

[0028]

- 166 The snapshot mobile payment device, method and system (hereinafter "SNAP") converts the quick response codes of merchant products generated in real time into transaction purchase notifications of card-based virtual wallets through SNAP components.
- 169 1A-F show block diagrams illustrating example aspects of snap mobile payment based purchase transactions in some embodiments of SNAP.
- 171 Referring to FIG. 1A, in some implementations, a user such as 101a-b may wish to purchase a product at a merchant store such as 103a or at a merchant website such as 103b.
- 173 For example, at a merchant store, a user may scan the barcodes of multiple products (eg, 102a) on a point-of-sale ("POS") terminal in the store, eg, 103a, and then indicate which scanned items the user wishes to checkout.
- 176 In some implementations, the POS terminal generates, via a payment network, a quick response ("QR") code, such as 105a, including information related to the scanned product item, and merchant information for processing the purchase transaction.
- 179 A user using a user device such as a smartphone may capture an image of the QR code generated by the POS terminal.
- 181 For example, the user equipment may have an application for quickly obtaining a QR code of the merchant's product.
- 183 The user device may use the information extracted from the QR code, along with information about a virtual wallet bound to the user device, to initiate a purchase transaction.
- 185 For example, the user device may use the product and merchant information extracted from the QR code and financial payment information from the virtual wallet to create a purchase transaction request and submit the request to a payment network (e.g., credit card processing network).

[0029]

- 191 In some implementations, the user device may use an alternative method of capturing a QR code to obtain information from the POS terminal.
- 193 For example, the POS terminal may communicate to the user device via Bluetooth, Wi-Fi, SMS, text messaging, email, and/or other communication methods the information required to submit a purchase transaction request to the payment network.

[0030]

- 199 In some implementations, the user 101b may wish to checkout items stored in a virtual shopping cart on an online store website, such as 102b.
- 201 For example, a user may browse the website using a secure display (eg, part of the user's trusted computing device).
- 203 When indicating that the user wishes to checkout items in the virtual shopping cart, the website may provide a QR code including information about the products and merchant information in the virtual shopping cart.
- 205 For example, in cases where the user uses a secure display, a QR code may be displayed at a random location

within the secure display for security purposes.

207 The user may take a snapshot of the displayed QR code and use payment information from a virtual wallet associated with the user device to create a purchase transaction request for processing by the payment network.

210 When the purchase transaction is complete, the payment network provides a purchase receipt, e.g. 107, directly to the user device 106, the POS terminal in the store, and/or the secure display (for a secure online shopping situation) as confirmation that the transaction processing is complete .

213 Accordingly, in some implementations the merchant can be shielded from obtaining the user's personal and/or private information while processing the purchase transaction, while securing the user's virtual wallet using a secure display presenting the merchant's product QR code. integrity.

[0031]

219 In various implementations, such payment processing can be used for a wide variety of transactions.

220 For example, a user dining at a restaurant may obtain a bill that includes a QR payment code that includes details about the cost of the meal included in the bill, as well as the restaurant's merchant ID.

222 Without disclosing any financial or personal information about the user to the restaurant, the user can use the user's smartphone to take a snapshot of the restaurant bill, and use the user's virtual wallet to pay the restaurant bill.

[0032]

228 Referring to FIG. 1B , in some implementations, eg 110 , a user 111 may wish to use the reverse snapshot mobile payment process to checkout items stored in a (virtual) shopping cart in an (online) store, eg 112 .

230 For example, a user may use a secure display, such as 113, that is part of the user's trusted computing device, or browse a website via a POS terminal in a brick and mortar store.

232 When indicating that the user wishes to checkout the items in the virtual shopping cart, the user may generate (e.g., 114) via a mobile application on the user's mobile device connected to the user's virtual wallet, a payment method, offer, reward, etc. for the user. , and/or QR code 115b for other information.

235 The user may provide the QR code displayed on the user's mobile device to a webcam (or other QR code capture device and/or mechanism) installed on the trusted computing device (or POS terminal).

237 The user's trusted computing device or POS terminal can take a snapshot, e.g., 116, of the QR code generated by the user's mobile device and create a purchase transaction request using the payment information from the user-generated QR code for the payment network to process.

240 When the purchase transaction is complete, the payment network may provide a purchase receipt directly to the user's mobile device, POS terminal in the store, and/or a secure display (for secure online shopping situations) as confirmation that transaction processing is complete.

243 Thus, in some implementations, the user will be able to use the QR code generated by the user's mobile device as a replacement for a plastic payment card (e.g., credit, debit, prepaid card), or as an alternative such as near field communication, , etc. and other financial information transmission mechanisms.

248 In some implementations, the QR code can be representative of a one-time anonymous credit card number (see, eg, description associated with FIG. 3B).

[0033]

253 In some implementations, the first user 121b may wish to pay the second user 121a some amount (or equivalent, such as virtual currency, alternative currency, rewards, miles, points, etc.), such as P2P Snapshot mobile payment 120.

256 The second user 121a may generate a time-limited validity QR code, such as 122, including information about the amount to be transferred and a privacy token/alias linked to the second user's financial account.

258 The second user may display the generated QR code to the first user (e.g., display the QR code to the first user by holding the second user's mobile phone; send the QR code via email, social networking message, twitter, etc.). The first user takes a snapshot of the QR code, e.g. 123, using the first user's mobile phone, and uses the amount, the second user's privacy token/alias linked to the financial account, and the QR code linked to the first user's mobile phone A first user's virtual wallet to generate a purchase transaction request for processing by the payment network. When the transaction is complete, the payment network may provide a transaction notification receipt to the user who is a party to the transaction. In an alternative implementation, the two users may share data encoded in the QR code via alternate methods of the QR code, including but not limited to: Near Field Communication (NFC), Wi-Fi, Bluetooth, Cellular Web, SMS, email, text messaging and/or other communication protocols.

[0034]

271 In general, it should be understood that such tokens, aliases and/or treatments may be used to advantage in various implementations of Stories mobile payment.

273 For example, a user wishing to participate in a reverse snapshot mobile payment process (see, e.g., FIG. 1B, element 110) may generate a QR containing information about a handle to financial payment information stored on a server of the payment network system code. For example, some implementations of QuickPay mobile payments may generate and/or process handles using a payment token process similar to that described in U.S. Application Serial No. 13/153,301, entitled "Payment Token Apparatus Method and System" Similarly, the entire content is hereby expressly incorporated by reference. Additionally, in some implementations, the handle may encode information in accordance with a compact messaging protocol, such as in Serial No. 6,837,425, entitled "Concise Protocol and Method for Solving Substantially Offline Messaging Between Portable Consumer Devices and Base Devices" described in U.S. Patents, the entire contents of which are expressly incorporated herein by reference. In some Reverse Snap mobile implementations, the user may provide the QR code containing the handle and displayed on the user's mobile device to a webcam (or other QR code) installed on a trusted computing device (or POS terminal) capture device and/or mechanism). A computing device or POS terminal trusted by the user may obtain a snapshot, e.g., 116, of the QR code generated by the user's mobile device and provide a handle extracted from the QR code to the merchant server for a purchase transaction request processed by the payment network. To process the purchase transaction using the handle, the merchant server may generate a card authorization request (such as further described in the discussion below with reference to FIG. 4A) and

provide the card authorization request to the payment network. When the purchase transaction is completed, the payment network may provide a purchase receipt directly to the user mobile device, the POS terminal in the store, and/or the secure display (e.g., for a secure online shopping situation) as a transaction using the handle Acknowledgment that processing is complete.

[0035]

297 In some implementations, a user warning mechanism can be built into the Kuaipai mobile payment purchase transaction processing flow.

299 For example, in some implementations, the merchant server may embed a URL specific to the transaction into the card authorization request. For example, in some implementations, the POS terminal, remote device, and/or desktop computer may embed the URL in optional layer 3 data in the card authorization request. The URL may point to a web page stored on a merchant server dedicated to the transaction that is the subject of the card authorization request. For example, the web page pointed to by the URL may include details about the purchase transaction, such as products purchased, cost of restocking, time expiration, status of order processing, and the like. Thus, by passing the URL of the webpage to the payment network, the merchant server can provide the payment network with details of the transaction. In some implementations, the payment network may provide notifications to the user, such as payment receipts, transaction authorization confirmation messages, shipping notifications, and the like. In such a message, the payment network may provide the URL to the user device. The user can navigate to the URL on the user's device to obtain alerts about the user's purchases, as well as other information, such as offers, coupons, related products, reward notifications, and the like.

[0036]

315 In some implementations, multiple users may participate in a group payment via Snap Mobile Payment to split a tender, eg, 130 .

317 In some implementations, one of the users 131a may obtain a snapshot (eg, 132) of a QR payment code (eg, 134) generated at a POS terminal, eg, 133 (or, eg, presented on paper such as a meal bill). The user may in turn generate a QR split payment code containing information about the amounts into which the payment has been split. The user 131a can present the decomposed payoff QR code 135 to other users 131b-c, and the user 131b-c can obtain a snapshot, e.g., 136, of the decomposed payoff QR code. In some implementations, the user 131b-c may reimburse user 131a via the payment network for payment of the original QR code, or the user 131b-c may make direct payment to the merchant via the decomposed reimbursement QR code (e.g., When the user 131a takes a snapshot of the merchant's QR code, no payment processing occurs immediately). In some implementations, the merchant may provide the split-pay QR code directly to the users 131a-c.

[0037]

330 In some implementations, group mobile payments may be enabled by using an alternative communication mechanism, rather than using QR codes.

332 For example, in some implementations, the POS terminal 133 may communicate with the users 131a-c using a communication protocol such as Bluetooth . The POS terminal can establish an independent communication session with each user serially or in parallel. Through these separate communication sessions, the POS terminal may transmit the product and/or merchant data required by the user's device to generate individual purchase transaction processing requests. Thus, through these separate communication sessions, the POS terminal can break down group reimbursements associated with users 131a-c into individual payment amounts.

[0038]

342 Referring to Figure 1C, in some implementations, for authentication/verification purposes, as well as to provide digital permission to disclose personal and/or private information, Snap Mobile Billing can be used.

344 For example, a user 142 visiting his/her doctor 143 may be required to provide formal permission to disclose personal information (eg, medical records) to the doctor. The doctor's terminal (eg, 144) may generate a QR code containing the doctor's digital credential and information about the type/content of the requested user's medical record. The user can take a snapshot of the QR code through the user's mobile device. The user's mobile device can generate a request for record release from the QR code and serve as verification that the request was obtained from a personally trusted device, such as the user's mobile device. In an alternative implementation, the user can select the personal information that the user would like to disclose to the medical provider, and the user's mobile device can generate a QR code for the doctor's terminal to take a snapshot to retrieve the user's medical information. In some implementations, the QR code can also include payment information (eg, the user's payment account information, or the doctor's acquirer information) and information about the controlled release of personal information.

[0039]

358 In some implementations, SNAP can facilitate P2P transactions by pre-populating a changeable QR payment code, such as 150.

360 For example, a first user with a public profile page (eg, 151) can place an image of a QR code in the public profile, eg, 152 . For example, the QR code may include a predetermined payment amount for a purchase transaction initiated by taking a snapshot of the QR code. In some implementations, the predetermined amount can be \$0 (eg, \$0 QR payment code). The second user can use the mobile device to capture a snapshot of the QR payment code, and can set the amount the second user wants to pay the first user through the second user's mobile device. The second user's mobile device can provide the payment network for transaction processing with the information encoded within the QR code and the payment amount selected by the second user.

[0040]

371 It should be understood that the various aspects of Snap Mobile Payment described herein may be used for any controlled exchange of information and/or payment.

373 For example, referring to FIG. 1D , in some implementations, a user may obtain a pay-per-view program,

such as 160 , through QuickPai mobile payment. For example, a television display may provide an advertisement including program information (eg, 162) and a QR payment code for obtaining the program content, eg, 161 . The QR code includes information identifying the program information, as well as information identifying the television subscriber account information, television address, and the like. The user can take a snapshot of the QR code and provide the information embedded in the QR code along with the user's mobile device information (eg, subscriber account number linked to the user's virtual wallet, payment account information, etc.). When the payment information is processed by the payment network, the payment network can provide an indication that the payment is complete to the television programming provider, and the television programming provider can stream the programming content to the user's television. As another example, a similar flow can be used for in-flight entertainment, such as 170, where an on-board screen can provide program information 172 and a QR payment code 171 for the user to snap for in-flight entertainment initiation. As another example, billboards, wall hangings, posters, in-store advertisements, temporary fences, etc., such as 180, may include offers for products/services, as well as QR codes including merchant information and product information identifying purchase quantities, etc. The user can snap a snapshot of the QR code with the user's mobile device linked to the user's virtual wallet to purchase the product and/or service, and, if appropriate, the product can be exchanged directly with the payment network as The purchase information specified as part of the purchase request sent by the user's mobile device is shipped to the user's address. As another example, a newspaper, such as 185, may include offers, advertisements, job postings, etc., containing QR codes, such as 186, containing information necessary for a user to initiate a purchase transaction using a payment network. It should be understood that any aspect of implementing the Snapshot mobile payment discussed in the implementations herein, and/or their equivalents, may be used in any other implementations discussed herein and/or their equivalents.

[0041]

³⁹⁹ Referring to Figures 1E-F, in some implementations, the data required to process a purchase transaction can be provided by methods that replace QR codes, including but not limited to: Near Field Communication (NFC), Wi-Fi , Bluetooth , Cellular Web, SMS, email, text messaging and/or other communication protocols.

⁴⁰³ For example, in some implementations, a user shopping online through a web browser executing on a client device, such as 190, may wish to pay for the purchase of items from an online store website (eg, 191). The website may include user interface elements that a user can activate to initiate shopping checkout and payment. When the user activates the user element, the client displaying the online shopping site may provide a message to the merchant's server to initiate a secure purchase transaction. A merchant server running the online shopping site may establish a secure connection (eg, a secure socket layer connection) to a payment network server of a payment network (eg, 192). And, the payment network server can establish a secure connection to the client. For example, the client may include a secure I/O chip that only allows a secure connection to be established between the client and the payment network server of the payment network. Through a secure connection, the payment network server may provide instructions to the client to request the user to launch the virtual wallet mobile application on the user's user device, see eg FIG. 1F, 196 . The client may thus provide a request to the user to launch the virtual wallet mobile application on the user's user device (eg 193). When the user launches the virtual wallet mobile application on the user device, the user

device and the client can establish a secure connection with each other (eg, via Bluetooth , Wi-Fi, cellular, etc.). In some implementations, the client and user equipment can be preconfigured to rapidly establish the secure communication channel with each other. Through the secure communication channel, the client can provide data to the user's mobile device, or vice versa, to facilitate initiation of the purchase transaction. The virtual wallet application on the user's mobile device (or client) can then generate a purchase transaction initiation message and provide this message to the payment network server for processing the purchase transaction. When the transaction processing is completed, the payment network server may provide a payment completion notification to the client, such as 197 in FIG. 1F, or to the user equipment.

[0042]

⁴²⁷ 2A-F illustrate application user interface diagrams showing example features of the Snap Mobile Payment application that facilitate Snap Mobile Payments, in some embodiments of the SNAP.

⁴²⁹ Referring to FIG. 2A , in some implementations, a user may wish to checkout one or more items stored in a virtual shopping cart on an online merchant website. For example, a user may use a browser application, eg, 201, to visualize a checkout page, eg, 202, of the merchant website. The checkout web page can describe the details of the checkout order, such as 203, and can provide the user with one or more options to provide payment for the purchase of stored items. In some implementations, the checkout web page can include an option to pay for the purchase using the Snap Mobile Payment process, eg, 204 .

[0043]

⁴³⁸ Referring to FIG. 2B , in some implementations, when the option to use the snapshot mobile payment process is selected, the merchant checkout webpage, such as 206, may provide a QR code, such as 209, through the browser application 205, which includes information about the virtual information about the items in the shopping cart and merchant information for the payment network to process the purchase (eg, a private token/alias linked to the merchant's acquirer financial account).

⁴⁴³ In some implementations, the web page can be displayed by a secure display of the user's trusted computing device. For example, as a security measure, the position of the QR code frame within the display, such as 207, can be randomly changed to prevent snapshots of the QR code from being obtained by fraudulent means (eg, tampering with the trusted computing device). In some implementations, a security image pre-selected by the user, such as 208, can be displayed on the screen so that the user can verify that it is accurate. In some implementations, the image can be encrypted by SNAP before the image is provided to the trusted computing device. In some implementations, the trusted computing device may be the only device holding the decryption key needed to decrypt and successfully display the image to the user on the secure display.

[0044]

⁴⁵⁴ Referring to Figure 2C, in some implementations, such merchant product information including QR codes may be used by point-of-sale ("POS") terminals, such as 210a-b.

⁴⁵⁶ For example, in a brick-and-mortar store, when the user indicates that they wish to check out for items in the user's physical shopping cart, the POS terminal may display a QR code, such as 211a-b, which includes the

payment amount for the purchase, such as 212a-b. For example, the QR code may include data formatted according to Extensible Markup Language ("XML"), such as the following example data structure:

[0046]

⁴⁶³ Referring to Figure 2D, in some implementations, a user can use a smartphone (eg, 213) to obtain a snapshot of the QR code displayed on a secure display or screen of the POS terminal.

⁴⁶⁵ For example, the user's smartphone can run an application to detect and capture an application, e.g., 214, of the QR code (e.g., 216a).

⁴⁶⁷ For example, the user can use a registration feature, such as 215, to register the QR code within the smartphone's display. In some implementations, the application can provide the user with the ability to zoom in (eg, 217) or zoom out (eg, 218) the QR code to ensure that the image of the QR code fits the size of the smartphone's screen. The user will be able to use a user interface element such as 219 to obtain a snapshot of the QR code when it is QR coded within the smartphone's display. The user can cancel the snap mobile payment process using the user interface element 220 on the display of the smartphone.

[0047]

⁴⁷⁶ Referring to Figure 2E, in some implementations, when a snapshot of the merchant's product QR code is obtained, the user's smartphone can extract the product and merchant data stored within the QR code and use the account number of the user's virtual wallet to generate a purchase transaction request for processing by the payment network.

⁴⁸⁰ Upon completion of processing the payment transaction by the payment network using information provided by the user's smartphone, merchant website 222 (via the browser application 221) may provide the user with a purchase receipt 225 . Referring to FIG. 2F , in an implementation in which the user uses the snapshot mobile payment process in a physical store, the POS terminal can display a purchase receipt for the user. In some implementations, the payment network can provide the buyer's receipt directly to the user's smartphone.

[0048]

⁴⁸⁹ 3A-E show application user interface diagrams illustrating example components of the Snap mobile payment application for capturing product barcodes, securing user data, and preventing fraud, in some embodiments of the SNAP.

⁴⁹² Referring to FIG. 3A , in some implementations, an application executing on a user's device may include an application interface that provides the user with various features. In some implementations, the application can be configured to recognize a product identifier (eg, barcode, QR code, etc.), such as 301 . For example, the application can be configured to capture merchant product QR codes for Snapshot mobile payment processing, as discussed above with reference to Figures 2A-F. In some implementations, the user may be required to log in to the application to activate its features. Once activated, the camera can provide the user with an in-person one-tap-to-buy feature. For example, the client device may have a camera through which the application can acquire images, video data, stream live video, etc., eg 303 . The application may be

configured to analyze input data and retrieve (eg 301) product identifiers, eg 304 , such as QR codes 209 , 211a - b , 216a and 227 . In some implementations, the application can overlay crosshairs, target boxes, and/or similar alignment reference marks, such as 305, so that the user can use the reference marks to align the product identifier, thereby aiding in the identification and identification of the product identifier. explain. In some implementations, the application may include an interface element to allow the user to toggle back and forth between the product identification mode and the product offer interface display screen (see, e.g., 306) so that the user can research exactly what is available to the user before capturing the product identifier. transaction. In some implementations, the application can provide the user with the ability to browse previous product identifier captures (see, eg, 307) so that the user will be able to better decide which product identifier the user wishes to capture. In some implementations, the user may wish to cancel the product purchase; the application may provide the user with a user interface element (eg, 308) to cancel the product identifier identification process and return to the previous interface screen the user was originally using. In some implementations, the user may be provided with information about products, user settings, merchants, offers, etc., such as in a list form (see, eg, 309) , so that the user can better understand the user's purchase options. Various other features may be provided in application (see eg 310).

[0049]

518 Referring to FIG. 3B , in some implementations, the application may include an indication of the user's location (eg, name of the merchant store, geographic location, information related to aisles within the merchant store, etc.), such as 311 .

521 The application may provide an indication, eg 312, of the amount due for the product purchase. In some implementations, the application can provide the user with various options to pay for the purchase of the product. For example, the app may use GPS coordinates to determine the merchant's store where the user is located and direct the user to the merchant's website. In some implementations, SNAP may provide APIs to directly engage merchants to assist in transaction processing. In some implementations, a tagged merchant's SNAP application can be developed with SNAP functionality that can directly connect the user to the merchant's transaction processing system. For example, a user may select from a plurality of cards (eg, credit cards, debit cards, prepaid cards, etc.) from various card providers (eg, 313). In some implementations, the application may provide the user with an option to pay for the purchase amount using funds contained in the user's bank account, such as checking, deposit, money market, current account, etc. (eg, 314). In some implementations, the user can set default options through the application to set which card, bank account, etc. to use for the purchase transaction. In some implementations, the setting of such default options may allow the user to initiate the purchase transaction via a single click, tap, swipe, and/or other corrected user input action, such as 315a. In some implementations, when the user uses this option, the application can use the user's default settings to initiate the purchase transaction. In some implementations, the application allows the user to use other accounts (eg, Google checkout, Paypal account, etc.) to pay for the purchase, eg, 316 . In some implementations, the app allows the user to pay for the purchase using reward points, airline miles, hotel points, electronic coupons, printed coupons (e.g., by capturing printed coupons in a similar manner to product identifiers), etc. Transactions, eg 317-318. In some implementations, the application provides an option to provide quick authorization, eg, 319, before initiating the purchase transaction. In some implementations, the application can provide a progress indicator to provide an indication of the

progress of the transaction after the user has selected an option to initiate the purchase transaction, eg, 320 . In some implementations, the app can provide the user with historical information, eg, 321, about the user's previous purchases made through the app. In some implementations, the app can provide the user with options to share information about the purchase with other users (e.g., via email, SMS, wall post on , tweet on Twitter , etc.) and/or Controlling information shared with merchants, acquirers, payment networks, etc., to process the purchase transaction, e.g., 322.

549 In some implementations, the application may provide the user with an option to display product identification information captured by the client device (eg, to display the product information to a customer service representative upon leaving the store), such as 324. In some implementations, the user, application, device, and/or SNAP may encounter errors in processing. In this case, the user will be able to chat with a customer service representative (eg VerifyChat323) to resolve difficulties during the purchase transaction.

[0050]

557 In some implementations, the user may choose to use a one-time anonymous credit card number for the transaction, see eg 315b.

559 For example SNAP may use a set of pre-specified anonymous card details (see eg "AnonCard1", "AnonCard2"). As another example, a SNAP might generate a set of one-time bearer card details, eg in real time, to securely complete a purchase transaction (eg Anon It 1X). In such an implementation, the application may automatically set the user profile settings so that any personally identifying information of the user will not be provided to merchants and/or other entities. In some implementations, the user is required to enter a username and password to activate the bearer feature.

[0051]

568 Referring to FIG. 3C , in some implementations, the user interface elements of the Stories mobile payment application may advantageously be configured to provide the user with the ability to utilize custom payment parameters with a minimum number of user gestures applied to the user's mobile device. Ability to process purchases.

572 For example, a user may be provided with overloaded user interface elements, such as 325-326. For example, if the user has a QR payment code within the view of a camera included in the user's mobile device, the user can activate element 325 to take a snapshot of the QR code and use predetermined default settings to process the purchase based on the QR code . However, if the user wishes to customize payment parameters, the user may activate user interface element 326 (eg, press and hold continuously). In doing so, the application may provide a pop-up menu, eg, 327, that provides various payment customization options, such as those previously provided. For example, the user can drag the user's finger to the appropriate setting that the user likes, and release the user's finger from the touch screen of the user's mobile device to select that setting for payment processing. In alternative implementations, the payment settings options, such as 330, and QR capture activation buttons, such as 328a-b (such as 328b may provide even more settings than those displayed in the initial screen) may be combined with windows (such as 329) together in the user interface for capturing the QR code by the mobile device's camera. In an alternative implementation, the user's mobile

device can generate a hybrid QR code payment setup graphic, and the POS terminal (or user's trusted computing device) can capture the entire graphic for payment processing.

[0052]

589 Referring to Figure 3D, in some implementations, a user may advantageously be able to provide user settings in a device that generates a QR code for a purchase transaction, and then capture the QR code using the user's mobile device.

592 For example, a display device of a point-of-sale terminal may display a checkout screen, such as a web browser running on a client, eg 331, displaying a checkout web page, eg 332, of an online shopping website. In some implementations, a checkout screen may provide user interface elements, such as 333a-b, by which a user may indicate a desire to use Stories Mobile Payment. For example, if the user activates element 331a, the website can generate a QR code using the user's default settings and display the QR code (eg, 335) on the client's screen for the user to capture using the user's mobile device. In some implementations, the user can activate a user interface element, such as 333b, whereby the client can display a pop-up menu, such as 334, with additional options from which the user can select. For example, the website may provide the user with options similar to those discussed above in the description with reference to Figures 3B-C. In some implementations, the website can modify the QR code 335 in real time as the user modifies the settings provided by activating the user interface element 333b. Once the user has modified the settings using the pop-up menu, the user can capture a snapshot of the QR code to initiate the purchase transaction.

[0053]

607 Referring to FIG. 3E, in some implementations, SNAP can provide a user interface to the user to modify the user's snap mobile payment settings.

609 For example, the SNAP may provide a web interface, such as 341. For example, a user can use the web interface to modify the security settings, eg, 342, of the user's virtual wallet. For example, the user can browse a list of trusted devices, such as 344, through which the user can access the user's virtual wallet. In some implementations, the web interface can provide user interface elements to add trusted devices, such as 343. The web interface may also provide users with additional security options. For example, the user can set a security password (e.g. 345), change settings regarding when the user should be asked before authorizing a purchase transaction (e.g. 346), the type/style of representation of the security feature (e.g. 347), and the Security image (eg 348) on the terminal used in Snapchat mobile payment. In various implementations, the user can access other services including modifying user profile, account number, account preferences, adding cards, getting offers and coupons, locating ATM machines, and the like.

[0054]

622 Figures 4A-D show data flow diagrams illustrating an example snap mobile payment process in some embodiments of the SNAP.

624 Referring to FIG. 4A, in some implementations, a user such as 401 may wish to purchase a product, service, offer, etc. ("Product") from a merchant such as 403 through the merchant's online site or the merchant's

store. A user may communicate with a merchant server, e.g., 403, through a client, such as, but not limited to, a personal computer, mobile device, television, point-of-sale terminal, kiosk, ATM, etc. (e.g., 402). For example, a user may provide user input (eg, checkout input 411) into the client indicating that the user wishes to purchase a product. For example, a user in a merchant store may scan a product barcode for a product with a barcode scanner at a point-of-sale terminal. As another example, a user may select a product from a web catalog on a merchant website and add the product to a virtual shopping cart on the merchant website. The user may then indicate that the user wishes to checkout the items in the (virtual) shopping cart. The client may generate a checkout request, eg 412, and provide the checkout request (eg, 413) to the merchant server. For example, the client may provide the merchant server with a (secure) Hypertext Transfer Protocol ("HTTP(S)") GET message including product details in the form of data formatted according to Extensible Markup Language (XML). The following is an example HTTP(S) GET message for a merchant server including a checkout request in XML format:

[0056]

641 In some implementations, the merchant server can obtain the checkout request from the client and extract the checkout details (eg, XML data) from the checkout request.

643 For example, the merchant server may use a parser, such as the example parser discussed below with reference to FIG. 14 .

645 The merchant server can extract the product data as well as client data from the checkout request. In some implementations, the merchant server may query (e.g., 414) a merchant database (e.g., 404) to obtain product data (e.g., 415), such as product pricing, sales tax, offers, discounts, rewards, and/or other information to process the purchase trade. For example, the database may be a relational database responsive to Structured Query Language ("SQL") commands. The merchant server may execute a hypertext preprocessor ("PHP") script that includes SQL commands to query the database for product data. A list of exemplary PHP/SQL commands illustrating the substantive aspects of querying a database is provided below:

[0058]

655 In some implementations, in response to obtaining the product data, the merchant server may generate (eg, 416a) a QR payment code and/or secure display element according to the user's security settings (see, eg, 358).

658 The merchant server can provide the QR code to the client so that the client can display the QR code, and then the user can use the user's device to capture the QR code to obtain merchant and/or product data for generating a purchase transaction processing request .

661 In an alternative implementation, the merchant server may direct the client to communicate via an alternative communication protocol such as, but not limited to, Wi-Fi , Bluetooth , cellular network, SMS, email, and/or the like. The product and/or merchant data required to process the transaction to the user's device. For example, the merchant server may direct the client to initiate a plug-in on its system to provide an alternative communication service and transmit the product and/or merchant data to the user's device via the communication service.

[0059]

670 In implementations using QR codes, the merchant server may generate a QR code containing product information and merchant information required by the payment network to process the purchase transaction.

673 In some implementations, the QR code may include at least information required by the user device capturing the QR code to generate a purchase transaction processing request, such as a merchant identifier (e.g., merchant ID number, merchant name, store ID, etc.) and The session identifier for the user's shopping session associated with the store's website/store.

[0060]

680 In some implementations, the merchant server can generate in real-time a custom, user-specified merchant product XML data structure with a time-limited validity period, such as the exemplary "QR_data" XML data structure provided below:

[0062]

686 In some implementations, the XML data may include handles, aliases, tokens, or pointers to information stored on the payment network server, rather than encoding all the actual data needed to initiate the transaction for encoding into the QR code Information can advantageously be minimized.

689 In some implementations, the merchant can use the XML data to generate a QR code.

690 For example, the merchant server can use the PHP QR Code Open Source (LGPL) library available at <http://phpqrcode.sourceforge.net/> for generating QR codes, 2D barcodes.

692 For example, the merchant server may issue PHP commands similar to the exemplary commands provided below:

[0063]

697 < ?

698 PHP

[0064]

702 header('Content-Type: text/plain');

[0065]

706 //Create QR code image using data stored in Sdata variable

[0066]

710 QRoode::png(Sdata, 'qrcodeimg.png');

[0067]

714 ?

715 >

[0068]

719 In an alternative implementation, the merchant server may provide (eg, 416b) XML data with the request to the payment network server (eg, 406) to generate the QR code.

721 For example, the merchant server requests the generation of a QR code using an API call to the payment network server.

723 The payment network server may generate a QR code for the merchant server, eg, 416c, and provide (eg, 416d) the QR code to the merchant server.

725 For example, the payment network server may encode information provided by the merchant into the QR code, and may also advantageously include security information, time validity information, digital certificate information, bearer shipping messages, QR code generation/processing payment information, etc. encoded into that QR code.

[0069]

732 In some implementations, the payment network server provides the merchant server with encryption keys (eg, Rivest-Shamir-Adleman (RSA) private/public keys, digital certificates).

734 The merchant can use the encryption key to encrypt the custom, user-specific merchant product XML data structure to generate encrypted purchase data (eg, using the RSA algorithm).

736 The merchant server can then encode the encrypted data into a QR code. In various embodiments, the payment network server may advantageously employ this scheme to authenticate the merchant for any transaction processing request related to the user-merchant shopping session.

[0070]

742 In some implementations, the user device can be provided with a predesigned QR code associated with a verified, pre-authenticated merchant.

744 For example, a user may browse an online website on the user's device. The user device may generate an HTTP(S) GET request for a web page from a web server. In some implementations, the web server can generate a query for an advertisement to display on the web page in response to the user device's request for the web page. For example, a webpage server may retrieve a database or provide a request to an ad network server (eg, Akamai) to serve advertisements for embedding in the webpage. In some implementations, the ad network server may use keywords, metadata, etc. obtained from the webpage server (e.g., keywords or metadata associated with the webpage, user profile information, user ID, from the user's browsing history from cookies on that user's device, etc.). The advertising network may use the keyword to generate a query of

a database of advertisements associated with the keyword, and may obtain the advertisement to offer. In some implementations, the ad network server may provide (e.g., via an API call) information about such advertisements (e.g., merchant name, merchant ID, product name, product price information, related offers, etc.) to the payment network server. The payment network server may generate a QR code based on information provided by the ad network server so that a user device may take a snapshot of the QR code to initiate a communication with the QR code (e.g., provided to the payment network server by the ad network server) A purchase transaction of associated goods and/or services. The ad network server can provide the QR as part of the advertisement to the web server, which in turn can embed the advertisement including the QR code into the web page before serving the web page to the user device. In an alternative implementation, the ad network server/web server may transmit the URL or other identifier of the QR code (final) to the user device, and the user device may use the URL of the QR code (e.g., hosted on the payment web server) to generate a call (eg HTTP(S) GET request) to obtain the QR code and display it for the user.

[0071]

767 In some implementations, the merchant server can provide the QR code to the client, eg, 417.

768 For example, the merchant server may provide a hypertext markup language (“HTML”) page including references to the QR code image and/or secure element image, such as the following exemplary HTML page:

[0073]

773 In some implementations, the client can obtain the QR payment code (eg, 417) and display the QR code (eg, 418) on a display screen associated with the client device.

775 In some implementations, a user can use a user device, such as 405, to capture a QR code presented by the client device for payment processing.

777 For example, the user may provide a payment input into the user device such as 419. In various implementations, user input may include, but is not limited to, a single tap of a touchscreen interface (e.g., a single tap mobile app purchase embodiment), keypad entry, swiping a card, activating RFID-enabled/Hardware devices with NFC (e.g., electronic cards with multiple accounts, smartphones, tablets, etc.), mouse clicks, button presses on joysticks/game consoles, voice commands, single taps/clicks on touch-sensitive interfaces Multi-touch gestures, touching user interface elements on touch-sensitive displays, and more. For example, a user device may obtain tracking data from a user card (e.g., credit card, debit card, prepaid card, charge card, etc.), such as the exemplary tracking data provided below:

[0075]

788 In some implementations, the user device can determine whether an image has been captured describing the QR code.

790 Depending on whether a QR code has been captured, and (optionally) also on the content of the QR code, the user device may redirect the user (e.g. via a web browser application executing on the user device) to: a product, a merchant website, products on the merchant's website, the website, and include commands to add items to the user's shopping cart associated with the website, etc.

794 For example, a user device may execute a component such as the exemplary quick response code processing ("QRCP") component 600 described below with reference to the discussion of FIGS. 6A-B .

[0076]

799 In some implementations, when user payment input is obtained and the QR code is captured, the user device can generate a card authorization request 420 for provision to the payment network server (e.g., if the QR code includes a purchase coupon, offer, send invoices, personal payments from another virtual wallet user, etc.).

803 For example, the user device may provide a card authorization request (eg 421) on behalf of the user, an HTTP(S) GET message (eg 406) including product order details for payment to the web server, in the form of data in XML format. The following is an exemplary HTTP(S)GET message for the payment network server including a card authorization request in XML format:

[0078]

810 In some implementations, the card authorization request generated by the user device may include the minimum information required to process the purchase transaction.

812 For example, this can improve the efficiency of communicating the purchase transaction request, and can also advantageously improve the privacy protection provided to the user and/or merchant.

814 For example, in some implementations, the card authorization request may include at least a merchant ID, a session ID for the user and merchant's shopping session, and a device ID of a user device (eg, a smartphone) linked to the user's virtual wallet. In some implementations, the QR code and message sent to/from the QR code capture device may include a source ID (e.g., an identifier of the device that generated the QR code), session ID, merchant ID, item ID (e.g., model number) , the checkout amount, and/or the transaction device ID (eg, the user's smart phone device).

[0079]

823 In some implementations, the card authorization request may be provided by the merchant server or point-of-sale terminal rather than the user device.

825 In some implementations, a security-desiring user may request a payment network server via the user device to dynamically generate the primary account number that will be used with the user in the purchase transaction.

[0080]

831 ("PAN", for example, a credit card number) along with the Card Verification Value Code (dCVV_{TM}).

832 In response, the payment network server may generate a dCVV code (e.g., using random number generation, an MD5 hash of an input key, which may be generated using a user ID, merchant ID, session ID, timestamp, combinations thereof, etc.), and The user provides a session specific dCVV_{TM} code to use with the user's PAN number. For example, session-specific dCVV codes may have an expiration time (eg,

expire within one minute from issue). The user device can communicate the PAN and dCVV (eg, via Bluetooth, NFC, Wi-Fi, cellular, QR code, etc.) to the point-of-sale terminal, which can create a card authorization request. For example, the user device may generate a QR payment code with the PAN and dCVV numbers embedded therein, and the point-of-sale terminal may snap a snapshot of an image of the QR payment code generated by the user device. The point-of-sale terminal can then generate and provide the card authorization request to the payment network server. The payment network server may then compare the dCVV obtained from the merchant to the dCVV provided to the user device before the purchase transaction was initiated to confirm the transaction. If the dCVV codes from the two sources (payment network server and merchant) correspond correctly to each other, then the payment network server can continue processing the purchase transaction.

[0081]

849 In some implementations, the card authorization request from the user device may include encrypted data extracted from the QR code, which may have been encrypted by the merchant server as part of a merchant authentication scheme.

852 In some implementations, the Pay Network Server may obtain encrypted data from a card authorization request provided by a user device and attempt to decrypt the encrypted data, for example, using an RSA private/public key that the Pay Network Server initially provided to the merchant. The keys used by the server to encrypt the purchase data before embedding in the QR code are complementary. If the payment network server is able to decrypt the purchase data, the merchant is authenticated as a valid merchant. In some implementations, the payment network server can compare the purchase data decrypted from the card authorization with the data provided by the user/user device to determine whether the data from these different sources (user/user device, and merchant) are mutually correct. Thus, in some implementations, the payment network server can authenticate the merchant and associate the merchant with a particular user session or user device prior to processing the transaction.

[0082]

865 In some implementations, the payment network server may provide a notification to the user device that the transaction was verified and approved for the transaction.

867 In an alternative implementation, the payment network server may continue transaction processing. In some implementations, when the user is identified as being in a session with the merchant, the payment network server may communicate with the user device to provide the user with additional features. For example, in some implementations, the payment network server may provide communication with the user device (e.g., via an HTTP(S) POST message) to provide: the merchant's virtual storefront; A description of the merchant's aisle, a list of related items, etc. (see, eg, Figures 8E-G and the following description of additional embodiments).

[0083]

877 Referring to Figure 4B, in some implementations, the payment network server may process the transaction to

transfer purchase funds to an account stored on the merchant's acquirer.

879 For example, the acquirer may be a financial institution that maintains the merchant's account. For example, the results of transactions processed by the merchant may be deposited into an account maintained by the acquirer's server.

[0084]

885 In some implementations, the payment network server can generate a query, eg, 422, for the issuer server corresponding to the payment option selected by the user.

887 For example, a user's account may be linked to one or more issuing financial institutions ("issuers"), such as banking institutions, that issued the user's account. For example, such accounts include, but are not limited to, credit cards, debit cards, prepaid cards, checking, deposit, money market, certificates of deposit, savings (cash) value accounts, and the like. The publisher's publisher server, eg 4o8a-n, may hold user account details. In some implementations, a database such as payment network database 407 may store details of issuer servers associated with issuers. For example, the database may be a relational database responsive to Structured Query Language ("SQL") commands. The payment network server may query the payment network database for issuer server details. For example, the payment network server may execute a hypertext preprocessor ("PHP") script including SQL commands to query a database for details of the issuer server. A list of exemplary PHP/SQL commands illustrating the substantive aspects of querying a database is provided below:

[0086]

901 In response to obtaining the issuer server query, eg 422, the pay network database may provide the requested issuer server data to the pay network server, eg 423.

903 In some implementations, the payment network server can use the issuer server data to generate an authorization for each issuer server selected based on the predefined payment settings associated with the user's virtual wallet and/or the user's payment option input. request, such as 424, and provide card authorization requests, such as 425a-n, to the issuer server, such as 408a-n.

907 In some implementations, the authorization request may include details such as, but not limited to, costs to the user included in the transaction, user's card account details, user billing and/or shipping information, and the like. For example, the payment network server may provide an HTTP(S) POST message including an authorization request in XML format similar to the exemplary list provided below:

[0088]

914 In some implementations, the issuer server can parse the authorization request and based on the request details can query a database, such as user profile database 409a-n, for data associated with the account linked to the user.

917 For example, the publisher server may issue PHP/SQL commands similar to the examples provided below:

[0090]

- 921 In some implementations, after obtaining the user data, eg, 427a-n, the issuer server can determine whether the user can pay for the transaction with funds available on the account, eg, 428a-n.
- 923 For example, the issuer server may determine whether the user has sufficient balance remaining in the account, sufficient credit associated with the account, and the like.
- 925 Based on this determination, the issuer server may provide an authorization response to the payment network server, eg, 429a-n.
- 927 For example, the issuer server may provide an HTTP(S) POST message similar to the example above. In some implementations, if at least one issuer server determines that the user cannot pay for the transaction with available funds in the account, see, e.g., 430-431, then the payment network server may again request payment options from the user (e.g., by providing an authorization failure Message 431 to user equipment and request user equipment to provide new payment options), and retry the authorization of the purchase transaction. In some implementations, if the number of failed authorization attempts exceeds a threshold, the payment network server can exit the authorization process and provide an "authorization failed" message to the merchant server, user device, and/or client.

[0091]

- 938 Referring to Figure 4C, in some implementations, the payment network server may obtain an authorization message including notification of successful authorization, see eg 430, 433, and parse the message to extract authorization details.
- 941 When it is determined that the user has sufficient transaction funds, the payment network server may generate a transaction data record, such as 432, according to the authorization request and/or authorization response, and store details of the transaction and authorization regarding the transaction in the transaction database. For example, a payment web server could issue PHP/SQL commands similar to the following example listing to store transaction data in a database:

[0093]

- 949 In some implementations, the payment network server can forward the authorization success message, eg, 433a-b, to the user device and/or the merchant server.
- 951 The merchant can take this authorization message and determine from it that the user has sufficient funds in the card account to carry out the transaction.
- 953 The merchant server may add transaction records for the user to a batch of transaction data regarding authorized transactions. For example, the merchant may append XML data about the user's transactions to an XML data file, e.g., 434, including XML data for transactions that have been authorized for each user, and store the XML data file in a database (e.g., merchant database 404) , for example 435. For example, a batch XML data file could be of a structure similar to the sample XML data structure template provided below:

[0094]

961 < ?

962 XML version="1.0" encoding="UTF-8"? >

[0095]

966 <merchant_data>

[0096]

970 <merchant_id>3FBCR4INC</merchant_id>

[0097]

974 <merchant_name>Books&Things, Inc.</merchant_name>

[0098]

978 <merchant_auth_key>INNF484MCP59CHB27365</merchant_auth_key>

[0099]

982 <account_number>123456789</account_number>

[0100]

986 </merchant_data>

[0101]

990 <transaction_data>

[0102]

994 <transaction 1>

[0103]

998 ...

[0104]

1002 </transaction 1>

[0105]

1006 <transaction 2>

[0106]

1010 ...

[0107]

1014 </transaction 2>

[0108]

1018 .

[0109]

1022 .

[0110]

1026 .

[0111]

1030 <transaction n>

[0112]

1034 ...

[0113]

1038 </transaction n>

[0114]

1042 </transaction data>

[0115]

1046 In some implementations, the server may also generate a purchase receipt, such as 434, and provide the purchase receipt to the client, such as 436.

1048 The client may render and display the purchase receipt for the user, eg 437a.

1049 In some implementations, the user device 405 may also provide a notification of successful authorization to the user, eg, 437b.

1051 For example, a client/user device may render web pages, electronic messages, text/SMS messages, buffer voicemails, sound ringtones, and/or play audio messages, etc., and provide output including, but not limited to: sound, music , audio, video, images, tactile feedback, vibration alerts (e.g., vibration-enabled client devices such as smartphones), and the like.

[0116]

1058 Referring to Figure 4D, in some implementations, the merchant server can initiate clearing of a batch of authorized transactions.

1060 For example, the merchant server may generate a batch data request, such as 438 , and provide the request, such as 439 , to a database such as merchant database 404 .

1062 For example, a merchant server may query a relational database using PHP/SQL commands similar to the examples provided above.

1064 In response to the batch data request, the database can provide, eg, 440, the requested batch data.

1065 The server may generate a batch clearing request, eg, 441, using the batch data obtained from the database, and provide (eg, 442) the batch clearing request to the acquirer server, eg, 410.

1067 For example, the merchant server may provide the acquirer server with an HTTP(S) POST message that includes batch data in XML format in the message body.

1069 The acquirer server may use the obtained batch clearing request to generate a batch payment request, such as 443 , and provide the batch payment request to the payment network server, such as 444 .

1071 The payment network server may parse the batch of payment requests and extract transaction data, eg, 445, for each transaction stored in the batch of payment requests.

1073 The pay network server may store transaction data, such as 446, for each transaction in a database, such as pay network database 407.

1075 For each extracted transaction, the pay network server may query a database, such as pay network database 407, eg 447-448, for the address of the issuer server.

1077 For example, a payment web server may use PHP/SQL commands similar to the examples provided above.

1078 The payment network server may generate a single payment request, eg, 449, for each transaction for which transaction data was extracted, and provide the single payment request (eg, 450) to the issuer server (eg, 408).

1081 For example, a payment web server may provide an HTTP(S) POST request similar to the following example:

[0118]

1086 In some implementations, the issuer server generates a generateable payment command, eg, 451.

1087 For example, the issuer server may issue a command to debit funds from a user's account (or add a charge to

a user's credit card account).

1089 The issuer server may issue a payment command (eg, 452) to a database, eg, user profile database 409, that stores the user account information.

1091 The issuer server may provide (eg, 453) the funds transfer message to the payment network server, which may forward (eg, 454) the funds transfer message to the acquirer server.

1093 An exemplary HTTP(S) POST funds transfer message is provided below:

[0119]

1097 POST/clearance.php HTTP/1.1

[0120]

1101 Host:www.acquirer.com

[0121]

1105 Content-Type: Application/XML

[0122]

1109 Content-Length:206

[0123]

1113 <?

1114 XML version="1.0" encoding="UTF-8"?

1115 >

[0124]

1119 <deposit_ack>

[0125]

1123 <request_ID>CNI4ICNW2</request_ID>

[0126]

1127 <clear_flag>>true</clear_flag>

[0127]

1131 <timestamp>2011-02-22 17:00:02</timestamp>

[0128]

1135 <deposit_amount>\$34.78</deposit_amount>

[0129]

1139 </deposit_ack>

[0130]

1143 In some implementations, the acquirer server can parse the funds transfer message and associate the transaction (eg, using the request_ID field in the example above) to the merchant.

1145 The acquirer server may then transfer the funds specified in the funds transfer message to the merchant's account, eg, 455.

[0131]

1150 Figures 5A-E show logic flow diagrams illustrating exemplary aspects of implementing Snap Mobile Payments, such as Snap Mobile Payment Execution ("SMPE") component 500, in some embodiments of SNAP.

1153 Referring to Figure 5A, in some implementations, a user may wish to purchase a product, service, offer, etc. ("Product") from a merchant through the merchant's online site or in the merchant's store.

1155 The user can communicate with the merchant server through the client.

1156 For example, a user may provide user input (eg, 501) into the client indicating that the user wishes to checkout shopping items in a (virtual) shopping cart.

1158 The client can generate a checkout request, such as 502, and provide the checkout request to the merchant server.

1160 The merchant server may obtain a checkout request from the client, and extract checkout details (eg, XML data) from the checkout request, eg 503 .

1162 For example, the merchant server may use a parser such as the example parser described below with reference to the discussion of FIG. 14 .

1164 The merchant server extracts this product data along with the client data from the checkout request.

1165 In some implementations, the merchant server may query (eg, 504) a merchant database to obtain product data, eg, 505, such as product prices, sales tax, offers, discounts, rewards, and/or other information to process the purchase transaction.

[0132]

1171 In response to obtaining the product data, the merchant server may generate (eg, 506) a QR payment code

and/or secure display element (see, eg, 358) according to the user's security settings.

1173 For example, the merchant server may generate a QR code containing product information and merchant information required by the payment network to process the purchase transaction.

1175 For example, the merchant server may first generate a custom, user-specific merchant-product XML data structure with a time-limited validity period in real time, such as the exemplary "QR_data" XML data structure provided below:

[0135]

1181 In some implementations, merchants can utilize XML data to generate QR codes.

1182 For example, the merchant server can use the PHP QR Code Open Source (LGPL) library available at <http://phpqrcode.sourceforge.net/> for generating QR codes, 2D barcodes.

1184 For example, the merchant server may issue PHP commands similar to the exemplary commands provided below:

[0136]

1189 < ?

1190 PHP

[0137]

1194 header('Content-Type: text/plain');

[0138]

1198 //Create QR code image using data stored in \$data variable

[0139]

1202 QrCode::png(\$data, 'qrcodeimg.png');

[0140]

1206 ?

1207 >

[0141]

1211 The merchant server can provide the QR payment code to the client, eg 506.

1212 The client can obtain the QR payment code and display the QR code, eg 507, on a display screen associated with the client device.

1214 In some implementations, a user can use a user device, such as 509, to capture a QR code presented by the client device for payment processing.

1216 The client device can decode the QR code to extract the information embedded in the QR code.

1217 For example, a client device may use an application, such as the ZXing multi-format 1D/2D barcode image processing library available at <http://code.google.com/p/zxing/>, to extract information from the QR code.

1219 In some implementations, the user can provide payment input into the user device, eg, 508 .

1220 Upon obtaining user purchase input, the user device may generate a card authorization request, eg, 509, and provide the card authorization request to the payment network server.

[0142]

1225 Referring to Figure 5B, in some implementations, the payment network server can parse the card authorization request, eg, 510, and generate a query, eg, 511, for the issuer server corresponding to the payment option selected by the user.

1228 In some implementations, the payment network database may store details of issuer servers associated with issuers.

1230 In response to obtaining the issuer server query, the pay network database may provide, eg, 512, the requested issuer server data to the pay network server.

1232 In some implementations, the payment network server can use the issuer server data to generate authorization requests for each issuer server, eg, 425134, and provide the card authorization requests to the issuer servers.

[0143]

1238 In some implementations, the issuer server can parse the authorization request and, based on the details of the request, query the user profile database for data associated with the account linked to the user.

1240 In some implementations, upon obtaining the user data, the issuer server can determine whether the user can pay for the transaction with available funds in the account, eg, 517 .

1242 For example, the issuer server may determine whether the user has sufficient balance remaining in the account, has sufficient credit associated with the account, and the like.

1244 Based on this determination, the issuer server may provide an authorization response to the payment network server, eg, 518.

1246 In some implementations, if at least one issuer server determines (e.g., 519) that the user cannot pay for the transaction with available funds in the account, see e.g., 520, option "No," then the payment network server may again request payment options from the user (See eg 521, option "No", by providing an authorization failure message to the user equipment and requesting the user equipment to provide a new payment option), and retry the authorization of the purchase transaction. In some implementations, if the number of failed authorization attempts exceeds a threshold, see e.g. 521, option "Yes", then the payment network server may exit the authorization process and provide an "Authorization Failed" message to the merchant server, user device and /or client, eg 522.

[0144]

1257 In some implementations, the payment network server may obtain an authorization message including notification of successful authorization, see eg 520, option "Yes", and parse the message to extract authorization details.

1260 After determining that the user has sufficient transaction funds, the payment network server can generate transaction data records according to the authorization request and/or authorization response, such as 523, and store details of the transaction and authorization related to the transaction in the transaction database, such as 524 .

[0145]

1267 Referring to FIG. 5C , in some implementations, the payment network server may forward an authorization success message (eg, 525) to the user device and/or the merchant server, and sometimes through the acquirer server, eg, 526 .

1270 The merchant can parse the authorization message, eg 528, and from it determine that the user has sufficient funds in the card account to carry out the transaction, see eg 529. The merchant server may add a transaction record for the user to a batch of transaction data related to authorized transactions, see eg 530-531. In some implementations, the merchant server may also generate a purchase receipt, eg, 532, and provide the purchase receipt to the client. The client may render and display the purchase receipt, eg, 534, for the user. In some implementations, user device 405 may also provide a notification of successful authorization to the user.

[0146]

1280 Referring to Figures 5D-E, in some implementations, a merchant server can initiate clearing of a batch of authorized transactions.

1282 For example, the merchant server may generate a batch data request, such as 535, and provide the request (eg, 536) to a database, such as a merchant database. In response to the batch data request, the database can provide, eg, 536, the requested batch data. The server can use the batch data obtained from the database to generate a batch settlement request, eg 537, and provide the batch settlement request to the acquirer server. The acquirer server may generate (eg, 539) a batch payment request using the obtained batch clearing request and provide the batch payment request to the payment network server. The payment network server can parse the batch of payment requests and extract transaction data, eg, 540-542, for each transaction stored in the batch of payment requests. The pay network server may store the transaction data, eg 543-544, for each transaction in a database such as a pay network database. For each extracted transaction, the Pay Network Server may query (eg, 545-546) a database, such as a Pay Network Database, for the address of the Issuer Server. The payment network server may generate, eg, 547, a single payment request for each transaction for which transaction data was extracted, and provide the single payment request to the associated issuer server.

[0147]

1298 In some implementations, the issuer server can generate payment commands, eg, 548-549.

1299 For example, the issuer server may issue a command to debit funds from the user's account (or add a charge to the user's credit card account). The issuer server may issue the payment command to a database storing the user's account information (eg, a user profile database), eg, 549 . The issuer server may provide the funds transfer message to a payment network server, such as 551, that may forward the funds transfer message to the acquirer server. In some implementations, the acquirer server can parse the funds transfer message and associate the transaction (eg, using the request_ID field in the example above) to the merchant. The acquirer server may then transfer the funds specified in the funds transfer message to the merchant's account, eg, 553-555.

[0148]

1310 6A-B show logic flow diagrams illustrating example aspects of processing quick response codes, such as quick response code processing ("QRCP") component 600, in some embodiments of the SNAP.

1312 Referring to FIG. 6A , in some implementations, a virtual wallet application executing on a user device can determine whether a QR code has been captured in an image frame obtained by a camera operatively connected to the user device, and can also determine the QR code. The type and content of the code. Using this information, the virtual wallet application can redirect the user's user experience and/or initiate purchases, update aspects of the virtual wallet application, and the like. For example, the virtual wallet application may trigger the capture of image frames via a camera operatively connected to the user device, 601. The virtual wallet application can use an image segmentation algorithm to identify the foreground in the image, 602, and can crop the rest of the image to reduce background noise in the image, 603. The virtual wallet application can determine whether the foreground image includes a QR code from which data can be reliably read (e.g., if the image does not include a QR code, or if the QR code is partially cropped, blurred, etc. may not be reliably read fetch data), 604. For example, the virtual wallet application can use a code library, such as the ZXing multi-format 1D/2D barcode image processing library available at <http://code.google.com/p/zxing/>, to try and extract information. If the virtual wallet application can detect the QR code (605, option "yes"), the virtual wallet application can decode the QR code and extract data from the QR code. If the virtual wallet application cannot detect the QR code (605, option "No"), the virtual wallet application may attempt to perform optical character recognition on the image. For example, the virtual wallet application may perform optical character recognition, 606, using the Tesseract C++ open source OCR engine available at www.pixeltechnology.com/freewarw/tessnet2. The virtual wallet application can thus obtain the data encoded in the image and proceed if the data can be processed by the virtual wallet application. The virtual wallet application may query a database for the QR code type using the fields identified in the extracted data, 608. For example, the QR code may include invoices/bills, coupons, money orders (e.g., in P2P transfers), new account information packages, product information, purchase commands, URL navigation instructions, browser automated scripts, their combinations etc.

[0149]

1338 In some embodiments, the QR code may include data about the new account to be added to the virtual wallet application (see 609).

1340 The virtual wallet application may query the issuer of the new account (eg, obtained from the extracted data) for data associated with the new account, 610. The virtual wallet application may compare the data provided by the issuer with the data extracted from the QR code, 611. If the new account is confirmed (611, option "Yes"), the virtual wallet app can update the wallet credentials with the new account details, 613, and update the virtual wallet app's snapshot with data from the QR code History, 614.

[0150]

1348 Referring to FIG. 6B, in some embodiments, the QR code can include data (see 615) about bills, invoices, or coupons for purchases using the virtual wallet application, which can be queried with the virtual wallet application. The merchant associated with the purchase (as obtained from the extracted data) to query data associated with the bill, invoice, or coupon used for the purchase (e.g. offer details, offer ID, expiration time, etc. etc.), 616.

1353 The virtual wallet application can compare the data provided by the merchant with the data extracted from the QR code, 617. If the bill, invoice, or coupon for purchase is validated (618, option "Yes"), the virtual wallet application can generate a data structure that includes the QR code data (see, e.g., above referenced FIGS. 4-5 XML QR_data structure in the description of) to generate and provide a card authorization request, 619, and use the data from the QR code to update the snapshot history of the virtual wallet application 620.

[0151]

1362 In some embodiments, the QR code may include product information, commands, user navigation instructions, etc. for the virtual wallet application (see 621).

1364 The virtual wallet application can query a database of products using the information encoded in the QR. The virtual wallet application may provide various features including, but not limited to: displaying product information, redirecting the user to: a product page, a commerce website, a product page on a commerce website, adding items to a user's shopping cart on a commerce website, and the like. In some implementations, the virtual wallet application can perform a process such as that described above for any image frames that are pending and/or that the user selects for processing (eg, based on a snapshot history).

[0152]

1373 Figure 7 shows a user interface diagram illustrating an overview of example features of the virtual wallet application in some embodiments of the SNAP.

1375 FIG. 7 shows an illustration of various exemplary features of a virtual wallet mobile application 700 . Some of the features displayed include Wallet 701, Social Integration via TWITTER, FACEBOOK, etc., Quotes and Taxes 703, Snap Mobile Purchases 704, Alerts 705, and Security, Settings and Analytics 796. These features are explored in more detail below.

[0153]

1382 8A-G show user interface diagrams illustrating example features of the virtual wallet application in shopping mode, in some embodiments of the SNAP.

1384 Referring to Figure 8A, some embodiments of the virtual wallet mobile application help and greatly enhance the consumer's shopping experience. As shown in Figure 8A, the consumer has various shopping patterns available to peruse. In one implementation, for example, a user may initiate this shopping mode by selecting the store icon 810 at the bottom of the user interface. A user may search for and/or add items to the shopping cart 811 by typing items in the search field 812 . The user can also use the voice-activated shopping mode by speaking into the microphone 813 the name or description of the item to be retrieved and/or added to the shopping cart. In further implementations, the user may also select other shopping options 814 , such as current items 815 , billing 816 , address book 817 , merchants 818 and local proximity 819 .

[0154]

1395 In one embodiment, for example, a user may select option current item 815, as shown on the far left of the user interface of FIG. 8A.

1397 When the current item 815 option is selected, an intermediate user interface may be displayed. As shown, the middle user interface may provide a current list of items 815a-h in the user's shopping cart 811. A user may select an item, such as item 815a, to view product descriptions 815j for the selected item and/or other items from the same merchant. Price and total due information may also be displayed along with a QR code 815k that captures the information necessary to conduct a snap mobile purchase transaction.

[0155]

1405 Referring to FIG. 8B, in another embodiment, the user may select a billing 816 option.

1406 When the bill 816 option is selected, the user interface may display a list of bills and/or receipts 816a-h from one or more merchants. Additional information can be displayed next to each bill, such as date of visit, whether items from multiple stores are present, last bill payment date, automatic payment, number of items, etc. In one example, a wallet purchase statement 816a dated January 20, 2011 may be selected. The wallet shopping bill selection may display a user interface that provides various information about the selected bill. For example, the user interface may display a list of purchased items 816k, <<816i>>, the total number of items and corresponding values. For example, 7 items worth \$102.54 are on the selected wallet shopping statement. Users can now select any item and select Buy Again to add purchases to that item. The user may also refresh offers 816j from the last time to clear any invalid offers and/or search for new offers that may be suitable for the current purchase. As shown in Figure 8B, the user may select two items for repeat purchases. Once added, a message 816i may be displayed to confirm the addition of both items, which yields the total number of items in the shopping cart 14.

[0156]

1421 Referring to Figure 8C, in yet another embodiment, the user may select the address book option 817 to browse the address book 817a, which includes a list of contacts 817b and make any transfers or payments.

1423 In one embodiment, the address book may identify each contact using the contact's name and available

and/or preferred payment modes. For example, contact Amanda G. Payment may be via social payment (eg, via FACEBOOK) as represented by icon 817c. In another example, money may be transferred to Brian S. via a QR code as represented by QR code icon 817d. In another example, Charles B. Payments may be accepted via near field communication 817e, Bluetooth 817f and email 817g. Payment can also be made via USB 817h (eg, through a physical connection of the two mobile devices) and other social channels such as TWITTER.

[0157]

1433 In one implementation, the user may select JoeP.

1434 to pay. As shown in the UI, next to the Joe P. next to his name, JoeP. Features an email icon 8i7g, representing Joe P. Payment via email is accepted. When his name is selected, the user interface may display his contact information, such as email, phone, and so on. If the user wishes to contact Joe P. payment, the user can add another transfer mode 817j to his contact information and make a payment transfer. Referring to Figure 8D, the user may be provided with a screen 817k where the user may enter an amount to send to Joe, and add other text to provide Joe with context for the payment transaction 817l. The user may select the mode by which Joe may be contacted (eg, SMS, email, social networking) through graphical user interface element 817m. As a user type, text input may also be provided for browsing within the GUI element 817n. When the user has finished entering the necessary information, the user can press the send button 817o to send the social message to Joe. If Joe also has a virtual wallet application, Joe will be able to browse 817p social payment messages within the application or directly on the website of the social network (such as Twitter , , etc.). Messages may be aggregated from various social networks as well as other sources (eg, SMS, email). The redemption method appropriate for each messaging method may be indicated along with the social pay message. In the illustration of FIG. 8D , the SMS 817q received by Joe indicates that Joe can redeem the \$5 obtained via SMS by replying to the SMS and entering the hash tag value "#1234". In the same illustration, Joe has received a message 817r via that includes a URL link that Joe can activate to initiate a redemption of the \$25 payment.

[0158]

1457 Referring to FIG. 8E, in some other embodiments, a user may select a merchant 818 from a list of options in a shopping mode to browse a selection list of merchants 818a-e.

1459 In one implementation manner, the merchants in the list may be in contact with the wallet, or have a relationship with the wallet. In another implementation, merchants may include a listing of merchants that meet user-defined or other criteria. For example, the list may be the one curated by the user, the merchant that the user shopped most frequently or spent more than x total amount of money, or shopped for three consecutive months, and the like. In one implementation, the user may further select a merchant, such as Amazon 818a. The user can then navigate through the merchant's listings to discover items of interest, such as 818f-j. Directly through the wallet and without accessing the merchant's site from a separate page, the user

can select items 818j from Amazon's 818a catalog. As shown at the far right of the user interface of Figure 8D, the selected item can then be added to the shopping cart. Message 818k indicates that the selected item has been added to the shopping cart, and the updated quantity of the item in the shopping cart is now 13.

[0159]

1472 Referring to Figure 8F, in one embodiment, there may be a local proximity option that may be selected by the user to browse a listing of businesses that are geographically in close proximity to the user.

1474 For example, the list of merchants 819a-e may be merchants located close to the user. In one implementation, the mobile application can further identify when the user is in the store based on the user's location. For example, location icon 819d may be displayed next to a store (eg, Walgreens) when the user is in close proximity to the store. In one implementation, the mobile application may periodically refresh its location if the user leaves the store (eg, Walgreens). In a further implementation, a user may navigate through the mobile application to offers of selected Walgreens stores. For example, a user may use the mobile application to navigate to items 819f-j available on aisle 5 at Walgreens. In one implementation, the user can select corn 819i to add to cart 819k from his or her mobile application.

[0160]

1485 Referring to FIG. 8G, in another embodiment, the local proximity option 819 may include a map of the store, particularly a real-time map feature.

1487 For example, when a Walgreens store is selected, the user may activate the aisle map 819l that displays a map 819m showing the store organization and user location (indicated by yellow circles). In one implementation, a user can easily configure the map to add one or more other users (eg, the user's children) to share each other's locations within the store. In another implementation, the user may have the option to initiate a "store browsing" like street browsing in the map. Store Browsing 819n may display images/videos around the user. For example, if the user is about to enter hallway 5, the store browsing map may display a view of hallway 5. Additionally, the user can manipulate the orientation of the map using the navigation tool 819o to move the store view forward, backward, right, left, and rotate clockwise and counterclockwise.

[0161]

1498 9A-F show user interface diagrams illustrating example features of the virtual wallet application in payment mode in some embodiments of SNAP.

1500 Referring to FIG. 9A, in one embodiment, the wallet mobile application can provide the user via wallet mode 910 with multiple options for payment transactions. In one implementation, an exemplary user interface 911 for making a payment is shown. The user interface can clearly identify the amount 912 and currency 913 used for the transaction. The amount may be an amount payable and the currency may include real currencies such as dollars and euros, and also virtual currencies such as reward points. The amount of the transaction 914 may also be prominently displayed on the user interface. The user may select the funds tab 916 to select one or more forms of payment 917, which may include various credit, debit, gift, reward, and/or prepaid cards. The user may also have the option to pay in whole or in part with reward points. For

example, a graphical indicator 918 on the user interface shows the number of points available, and the graphical indicator 919 shows the number of points that will be used against the amount due 234.56 and the value of the points in the selected currency (USD, for example). Equivalent to 920.

[0162]

1514 In one implementation, the user can combine funds from multiple sources to pay for the transaction.

1515 The amount 915 displayed on the user interface may provide an indication of the amount of total funds covered thus far by the selected form of payment (eg, Discover Card and reward points). The user may select another payment form or adjust the amount to be debited from one or more payment forms until the amount 915 matches the amount due 914 . Once the user has settled on the amount to be debited from one or more payment forms, payment authorization can begin.

[0163]

1523 In one implementation, the user may select security authorization for the transaction by selecting the hide button 922 to effectively hide or anonymize some (e.g., pre-configured) or all identifying information so that when the user selects the pay button 921, the transaction Authorization is done securely and anonymously.

1527 In another implementation, the user may select a payment button 921, which may use standard authorization techniques for transaction processing. In another implementation, when the user selects the social button 923, a message about the transaction can be passed to one or more social networks (established by the user), which can post or announce the purchase transaction in a social forum , such as a poster or tweet. In one implementation, a user may select a social payment processing option 923. This indicator 924 may show authorization and sending of social sharing data in progress.

[0164]

1536 In another implementation, a restricted payment mode 925 may be activated for certain purchasing activities, such as prescribed purchases.

1538 This mode can be activated according to rules defined by issuers, insurance companies, merchants, payment processors, and/or other entities to facilitate the processing of particular goods and services. In this mode, the user can scroll down the list of payment forms 926 by following the Funds tab to select a particular account, such as a Flexible Payment Account (FSA) 927, Health Savings Account (HAS), etc., and the account that will be credited to the selected account amount. In one implementation, this restricted payment mode 1925 process may prohibit social sharing of purchase information.

[0165]

1547 In one embodiment, through the input funds user interface 928, the wallet mobile application may facilitate the entry of funds.

1549 For example, a user who is unemployed can access unemployment benefits funds 929 through the wallet

mobile application. In one implementation, the entity providing these funds may also configure rules for using these funds, as indicated by process indicator message 930 . The wallet can read and apply the rule in advance, and can reject any purchases with the unemployment fund that fail to meet the criteria set by the rule. Exemplary criteria include, for example, Merchant Category Code (MCC), transaction time, transaction location, and the like. For example, a transaction with a grocery merchant with MCC 5411 is approved, while a transaction with a bar merchant with MCC 5813 is declined.

[0166]

1559 Referring to Figure 9B, in one embodiment, the wallet mobile application can facilitate dynamic payment optimization based on factors such as user location, preference, and currency value of preference.

1561 For example, when the user is in the United States, the country indicator 931 may display a flag for the United States and may set the currency 933 to be the United States. In further implementations, the wallet mobile application may automatically rearrange the order in which payment forms 935 are listed to reflect the popularity or acceptability of various forms of payment. In one implementation, the ranking may reflect user preferences, which cannot be changed by the wallet mobile application.

[0167]

1569 Similarly, when a German user operates a wallet in Germany, the mobile wallet application user interface can be dynamically updated to reflect the operations 932 and currency 934 of that country.

1571 In further implementations, the wallet application may be rearranged in order where different payment forms 936 are listed based on acceptance levels in that country. Of course, the order of these forms of payment can be changed by the user to suit his or her own preferences.

[0168]

1577 Referring to Figure 9C, in one embodiment, a Payee tab 937 in the Wallet mobile application user interface may assist the user in selecting one or more payees to receive the funds selected in the Funds tab.

1579 In one implementation, the user interface can display a list of all payees 938 with whom the user has previously transacted or is available for transacting. The user can then select one or more payees. Payees 938 may include larger merchants such as Amazon.com Corporation, and individuals such as Jane P. Doe. Next to each payee name may be displayed a list of payment modes accepted by that payee. In one implementation, the user may select Payee Jane P. Doe 939 to receive payment. Once selected, the user interface can display additional identifying information related to the payee.

[0169]

1588 Referring to FIG. 9D, in one embodiment, a mode tab 1940 may assist in selecting the payment modes accepted by the payee.

1590 Multiple payment modes are available for selection. Exemplary modes include, Bluetooth 941, Wireless 942, SnapMobile via user-obtained QR code 943, Security Chip 944, TWITTER 945, Near Field

Communication (NFC) 946, Cellular 947, SnapMobile via user-provided QR code 948, USB949 and FACEBOOK 950, etc. In one implementation, only payment modes accepted by the payee may be selected by the user. Other non-accepted payment modes may be prohibited.

[0170]

1598 Referring to FIG. 9E , in one embodiment, an offer tab 951 may provide real-time offers for user selection, which relate to items in the user's shopping cart.

1600 The user may select one or more offers from the list of applicable offers 952 for redemption. In one implementation, some offers can be combined while others cannot. When the user selects an offer that cannot be combined with other offers, unselected offers can be disabled. In another implementation, an offer recommended by the wallet application's recommendation engine may be identified by an indicator, such as that shown at 953 . In another implementation, the user can read the details of the quote by expanding the quote line, as shown at 954 in the user interface.

[0171]

1609 Referring to FIG. 9F , in one embodiment, social tags 955 can help integrate wallet applications with social channels 956 .

1611 In one implementation, a user may select one or more social channels 956 and may log in to select a social channel from the wallet application by providing a social channel username and password 957 to the wallet application and logging in 958 . The user can then use social buttons 959 to send or receive money through the integrated social channels. In another implementation, users can send socially shared data, such as purchase information or links, through integrated social channels. In another embodiment, user-supplied login credentials may allow SNAP to participate in intercept resolution.

[0172]

1620 Figure 10 shows a user interface diagram illustrating example features of the virtual wallet application in history mode, in some embodiments of the SNAP.

1622 In one embodiment, the user may select the history mode 1010 to browse the history of previous purchases and perform various actions on those previous purchases. For example, a user may enter merchant identifying information, such as name, product, MCC, etc., into the search bar 1011. In another implementation, the user can use the voice-activated retrieval feature by clicking on the microphone icon 1014 . The wallet application may query a storage area on the mobile device or elsewhere (eg, one or more databases and/or tables remote from the mobile device) for transactions matching the search keyword. The user interface can then display the results of the query, such as transaction 1015. The user interface may also identify the date 1012 of the transaction, the merchant and item 1013 involved in the transaction, the barcode of the receipt confirming that the transaction was made, the amount of the transaction, and any other relevant information.

[0173]

1635 In one implementation, a user may select a transaction, such as transaction 1015, to view details of that transaction.

1637 For example, the user can view details of items associated with the transaction and the amount 1016 of each item. In another implementation, the user can select the display option 1017 to view actions 1018 that the user can take with respect to the transaction or items in the transaction. For example, a user may add a photo to the transaction (eg, a picture of the user and the iPad the user purchased). In another implementation, if the user previously shared the purchase via a social channel, a post including the photo can be generated and sent to the social channel for publication. In one implementation, any sharing may be optional, and a user who does not share the purchase through social channels may still share the photo through one or more social channels he or she selects directly from the wallet application's history mode. In another implementation, the user can add the transaction to a group, such as user-created business expenses, household expenses, travel expenses, or other categories. Such a group can assist with year-end closing of expenses, submission of work expense reports, submission of value-added tax (VAT) refunds, personnel expenses, etc. In another implementation, the user may purchase one or more items purchased in the transaction. The user can then perform a transaction without going to the merchant's directory or site to discover the item. In another implementation, the user may also place one or more items in the shopping cart during the transaction for later purchase.

[0174]

1655 In another embodiment, the history mode may provide facilities for obtaining and displaying ratings 1019 for items in the transaction.

1657 The source of the rating can be the user, the user's friends (eg, from social channels, contacts, etc.), browsing aggregated from the webpage, and the like. In some implementations, the user interface may also allow users to post messages to other users of social channels (eg, TWITTER or FACEBOOK). For example, display area 1020 shows a FACEBOOK message exchange between two users. In one implementation, the user may share the link via message 1021. The selection of such a message with a link embedded into the product may allow the user to browse the product's description and/or purchase the product directly from the history mode.

[0175]

1667 In one embodiment, the history mode may also include tools for outputting receipts.

1668 The output receipt popup 1022 may provide a number of options for outputting receipts for transactions in the history. For example, the user may use one or more options 1025 including save (to local removable storage, to server, to cloud account, etc.), print to printer, fax, email, etc. A user can use his or her address book 1023 to look up email or fax numbers for output. The user may also specify format options 1024 for outputting receipts. Exemplary format options include, but are not limited to: text files (.doc, .txt, .rtf, .iif, etc.), spreadsheets (.csv, .xls, etc.), image files (.jpg, .tiff, .png, etc.), Portable Document Format (.pdf), Appendices (.ps), etc. The user can then click or tap output button 1027 to initiate receipt output.

[0176]

1678 11A-F show user interface diagrams illustrating example features of the virtual wallet application in snap mode, in some embodiments of the SNAP.

1680 Referring to FIG. 11A , in some embodiments, a user may select the snap mode 1101 to access the snap feature. In various embodiments, the virtual wallet application is able to snapshot and identify various items. For example, the virtual wallet application can snap and identify purchase invoices 1103, coupons 104, money (e.g., sent in person-to-person transfers) 1105, bills (e.g., utilities, etc.) 1106, receipts (e.g., for storage , expense report, etc.) 1107, payment account (eg, to add new credit/debit/prepaid card to the virtual wallet application) 1108. The user can return to the shopping screen at any time by activating the graphical user interface element 1102 . In some embodiments, the user can set the name of the shopping cart or wish list stored within the user's virtual wallet application to which the snapped items should be sent (see 1109). In some embodiments, the virtual wallet application may allow the user to create a new shopping cart or wish list to which the snapped items should be added.

[0177]

1693 In one embodiment, a user may select the snap mode 1110 to access its snap feature.

1694 The snap mode can handle any machine-readable data representation. Examples of such data may include linear and 2D barcodes, such as UPC codes and QR codes. These codes can be found on receipts, product packaging, etc. The snapshot mode can also process and manipulate pictures of receipts, products, offers, credit cards or other payment devices, and the like. FIG. 11A shows an exemplary user interface in snapshot mode. The user can use his or her mobile phone to take a picture of the QR code 1115 and/or barcode 1114. In one implementation, the bar 1113 and snapshot box 1115 can help the user to properly snap a snapshot of these codes. For example, as shown, snap frame 1115 does not capture all of code 1116 . Thus, the code captured in this browse is not parseable because the information in the code may be incomplete. This is indicated by a message on bar 1113 indicating that the snap mode is still looking for a code. The user can change the camera's zoom level 1117 to facilitate taking a snapshot of the QR code. When the code 1116 is fully framed by the snap box 1115, the message may be updated to read, for example, "Snapshot found." In one implementation, when the code is found, the user can use the mobile device camera to initiate code capture (see 1120). In another implementation, snapshot mode can automatically take a snapshot of the code using the mobile device camera (see 1119). In some implementations, the virtual wallet application can optionally apply a GPS tag (see 1118) to the QR code before storing it or using it in a transaction.

[0178]

1712 Referring to FIG. 11B , in one embodiment, the snap mode can facilitate payment redistribution posting transactions.

1714 For example, a user may purchase groceries and prescribed items from retailer Acme Supermarket. A user may inadvertently or for checkout convenience, for example, use his or her Visa card to pay for groceries and prescribed items. However, the user may have an FSA account that can be used to pay for prescribed items, and it will provide the user tax benefits. In this case, the user can use snapshot mode to initiate

transaction reallocation.

[0179]

1722 As shown, the user enters a search term (eg, billing) in the search bar 2121 .

1723 The user may then identify in tab 1122 the receipt 1123 that the user wishes to redistribute. Alternatively, the user can directly snap a picture of the barcode on the receipt, and the snapshot mode can generate and display the receipt 1123 using information from the barcode. Now the user can reassign 1125. In some implementations, the user may also challenge 1124 the transaction or file the receipt 1126.

[0180]

1730 In one implementation, when the reassign button 1125 is selected, the wallet application can perform optical character recognition (OCR) of the receipt.

1732 Each item in the receipt can then be reviewed to identify which payment device or account the item or items can be credited for taxes or other benefits such as cash back, reward points, and the like. In this example, there is a tax benefit if the prescription drug charged to the user's Visa card is charged to the user's FSA. The wallet application can then perform this reallocation as a finale. The reallocation process may include the wallet contacting the payment processor to credit the Visa card for the amount of the prescription drug and debit the same amount to the user's FSA account. In an alternative embodiment, a payment processor (eg, Visa or MasterCard) may obtain and OCR the receipt, identify the item and payment account for redistribution and perform the redistribution. In one implementation, the wallet application may request confirmation from the user to reallocate billing for the selected item to another payment account. Receipt 1127 may be generated after the reallocation process is complete. As discussed, the receipt shows that some charges have been moved from the Visa account to the FSA.

[0181]

1746 Referring to FIG. 11C , in one embodiment, snap mode can facilitate payment through payment codes such as barcodes or QR codes.

1748 For example, users can take a snapshot of the QR code of a transaction that has not yet been completed. The QR code can be displayed at a merchant POS terminal, website, or web application, and can be encoded with information identifying the item for purchase, merchant details, and other relevant information. When a user snaps such as a QR code, the snap mode can decode the information in the QR code and can use the decoded information to generate a receipt 1132 . Once the QR code is recognized, the navigation bar 1131 may indicate that the payment code is recognized. The user may now have the option to add to shopping cart 1133, pay with default payment account 1134 or pay with wallet 1135.

[0182]

1758 In one implementation, the user may decide to utilize a default 1134 payment.

1759 In this wallet example, the wallet application can then use the user's default payment method to complete the

purchase transaction. When the transaction is complete, a receipt can be automatically generated to prove the purchase. The user interface can also be updated to provide other options for processing completed transactions. Example options include social 1137 to share purchase information with others, redistribute 1138 as discussed with respect to FIG. 11B , and archive 1139 to store the receipt.

[0183]

1767 Referring to Figure 11D, in one embodiment, the snap mode can also help with quote identification, application and storage for future use.

1769 For example, in one implementation, a user can snap an offer code 1141 (eg, barcode, QR code, etc.). The wallet application can then generate offer text 1142 based on the information encoded in the offer code. Users can perform several actions on quote codes. For example, the user uses the lookup button 1143 to look up all merchants that accept the offer code, nearby merchants that accept the offer code, products from merchants that qualify for the offer code, and the like. The user can also use the add to cart button 1144 to apply the offer code to items currently in the shopping cart. Additionally, the user may also save the offer for future use by selecting the save button 1145 .

[0184]

1779 In one implementation, after an offer or coupon is applied 1146, the user may have the option to use a lookup to find eligible merchants and/or products, the user may enter the wallet using 1148, and the user may also save the offer Or Coupon 1146 for later use.

[0185]

1785 Referring to FIG. 11E , in one embodiment, the snapshot mode may also provide convenience for adding a funding source to the wallet application.

1787 In one implementation, payment cards such as credit cards, debit cards, prepaid cards, smart cards, and other payment accounts may have an associated code, such as a barcode or QR code.

1789 Such a code may have payment card information encoded therein including, but not limited to, name, address, payment card type, payment card account details, balance, spending limits, return balance, and the like. In one implementation, the code can be found on the face of the physical payment card. In another implementation, the code can be obtained by accessing an associated online account or another secure location. However, in another implementation, the code may be printed on the envelope accompanying the payment card. In one implementation, the user can snap a picture of the code. The wallet application can recognize the payment card 1151 and display textual information 1152 encoded in the payment card. The user can then perform verification of the information 1152 by selecting a verification button 1153 . In one implementation, the verification may include contacting the issuer of the payment card with information 1152 for confirmation of decoding, as well as any other relevant information. In one implementation, the user can add the payment card to the wallet by selecting the "Add to Wallet" button 1154 . Instructions to add a payment card to the wallet may cause the payment card to appear as one of the forms of payment for the funds tag 916 discussed with respect to FIG. 9A . The user may also cancel entering the payment card as

a funding source by selecting the cancel button 1155. When the payment card has been added to the wallet, the user interface may be updated to indicate completion of the entry via notification display 1156. The user can then access wallet 1157 to begin using the added payment card as a funding source.

[0186]

1808 Referring to FIG. 11F, in some implementations, the virtual wallet application can identify a product by processing the QR code, and can provide information related to the product, as well as information related to purchasing the product, ancillary services, and the like.

1811 For example, the virtual wallet application may provide a window 1161 in which the virtual wallet application may display images, product descriptions, prices, merchant information, etc. (see 1162). In some implementations, the virtual wallet application can provide a QR code that includes the displayed information so that another user can quickly snap the information to enter it into another virtual wallet application. In some implementations, the virtual wallet application can provide features so that the user can request doorman services (e.g., help when shopping), shipping services (e.g., so the user can leave the store without carrying the item out), 1164. In some implementations, the virtual wallet application can provide competitive prices from local merchants (eg, using the GPS location of the user device) or merchants on the Internet (see 1165). In some implementations, the virtual wallet application can provide users with features including but not limited to: browse previous stories, snap new codes, add GPS tags to codes, retrieve codes from earlier stories to use, manually Enter information about the QR code, attribute the QR code to an object (eg so that for organizational purposes QR codes for furniture products for the home can be grouped into a "bedroom furniture" object), etc. (see 1166). In some embodiments, the user can set the name of the shopping cart or wishlist stored within the user's virtual wallet application to which the snapped items should be sent (see 1167). In some embodiments, the virtual wallet application may allow the user to create a new shopping cart or wish list to which the snapped items should be added.

[0187]

1830 Figure 12 shows a user interface diagram illustrating example features of the virtual wallet application in offer mode in some embodiments of the SNAP.

1832 In some implementations, SNAP may allow users to retrieve offers for products and/or services from within the virtual wallet mobile application. For example, a user may enter text into graphical user interface ("GUI") element 1211, or issue a voice command by activating GUI element 1212 and speaking the command into the device. In some implementations, SNAP may provide an offer based on the user's previous behavior, demographics, current location, current shopping cart selections or purchased items, and the like. For example, if a user is in a physical store, or an online shopping site, and leaves the (virtual) store, the merchant associated with the store may wish to provide an enticement process to entice the customer to return to the (virtual) store. A merchant may provide 1213 such an offer. For example, the offer can offer a discount and can include an expiration time. In some implementations, other users can offer a gift (eg, 1214) to the user that the user can redeem. In some implementations, the offer section may include warnings about payment of outstanding funds to other users (e.g., 1215). In some implementations, the offer section can include a warning (eg, 1216) about requesting receipts of funds from other users. For example,

such features may identify funds that are receivable from other applications (eg, mailings, calendars, tasks, notes, reminders, alerts, etc.), or by manual input by the user into the virtual wallet application. In some implementations, the offers section may provide offers from participating merchants in SNAP, eg, 1217-1219, 1220. These offers can sometimes be aggregated using a combination of participating merchants, eg 1217. In some implementations, SNAP itself can provide offers, eg, 1220, for users to use with a particular form of payment from within the virtual wallet application.

[0188]

1853 13A-B show user interface diagrams illustrating exemplary features of the virtual wallet application in security and privacy mode, in some embodiments of SNAP.

1855 Referring to FIG. 13A, in some implementations, the user can view and/or change the user profile and/or the user's settings, such as by activating a user interface element. For example, a user can view/modify username (eg, 1311a-b), account number (eg, 1312a-b), user security access code (eg, 1313-b), user pin (eg, 1314-b), user address (eg, 1315 -b), social security number associated with the user (e.g. 1316-b), current device GPS location (e.g. 1317-b), user account at the merchant where the user is currently located (e.g. 1318-b), user's return Account (eg 1319-b), etc. In some implementations, the user can select which data fields and their associated values should be transmitted to facilitate the purchase transaction, thus providing the user with enhanced data security. For example, in the exemplary illustration in FIG. 13A, the user has selected Name 1311a, Account Number 1312a, Security Code 1313a, Merchant Account ID 1318a, and Rewards Account ID 1319a as fields to be sent as part of the notification to process the purchase transaction. In some implementations, the user can select the fields and/or data values sent as part of the notification to process the purchase transaction. In some implementations, the application may provide the user with multiple screens of data fields and/or stored associated values to select as part of the purchase order transmission. In some implementations, the application can provide SNAP with the user's GPS location. Based on the user's GPS location, SNAP can determine the user's environment (eg, whether the user is in a store, doctor's office, hospital, post office, etc.). Based on the circumstances, the user application may present the appropriate fields to the user from which the user may select fields and/or field values to send as part of the purchase order transmission.

[0189]

1876 For example, a user may walk into a doctor's office and wish to pay for co-pays for a doctor's appointment.

1877 In addition to basic transaction information, such as account number and name, the application can provide users with the ability to choose to transfer medical records, health information, which can be provided to medical providers, insurance companies, and transaction processors to reconcile between the parties pay. In some implementations, the records can be sent and encrypted in a data format compliant with the Health Insurance Act for Portability and Obligation (HIPAA), and only recipients authorized to view such records can have the appropriate decryption key to decrypt and view the records. Private User Information.

[0190]

1886 Referring to Figure 13B, in some implementations, an application executing on the user's device may provide a "VerifyChat" feature for fraud prevention.

1888 For example, SNAP can detect unusual and/or suspicious transactions. The SNAP can use the Verifychat feature to communicate with the user and verify the authenticity of the originator of the purchase transaction. In various implementations, SNAP can send email messages, text (SMS) messages, messages, Twitter tweets, text chats, voice chats, video chats (eg, Apple FaceTime), etc. to communicate with the user. For example, SNAP may initiate a video inquiry, e.g., 1321, for the user. For example, a user may need to present himself/herself via video chat, eg 1322. In some implementations, a customer service representative, such as agent 1324, can use the user's video to manually determine the user's authenticity. In some implementations, SNAP may use facial, biometric, etc. recognition methods (eg, using pattern classification techniques) to determine the user's identity. In some implementations, the application can provide fiducial markers (eg, crosshairs, target boxes, etc.) such as 1323 so that the user can provide video to aid in the automatic identification of the user's SNAP. In some implementations, the user may not have initiated the transaction, eg, the transaction was fraudulent. In this implementation, the user can cancel the query. SNAP may then cancel the transaction, and/or initiate a fraud investigation process on behalf of the user.

[0191]

1906 In some implementations, SNAP may use a text challenge process to determine the user's authenticity, e.g., 1325.

1908 For example, SNAP may communicate with users via text chat, SMS messages, emails, messages, Twitter tweets, and the like. SNAP can ask the user to ask questions, such as 1326. The application may provide user input interface elements (eg, virtual keyboard 1328) to answer query questions posed by SNAP. In some implementations, the inquiry question can be automatically and randomly selected by SNAP; in some implementations, a customer service representative can communicate with the user manually. In some implementations, the user may not have initiated the transaction, eg, the transaction was fraudulent. In this implementation, the user can cancel the text query. SNAP can then cancel the transaction, and/or initiate the fraud investigation process on behalf of the user.

[0192]

1920 SNAP controller

[0193]

1924 FIG. 14 shows a block diagram illustrating an embodiment of a SNAP controller 1401 .

1925 In this embodiment, the SNAP controller 1401 can be used to aggregate, process, store, retrieve, serve, identify, command, generate, match, and/or facilitate interaction with computers through various techniques, and/or other related data.

[0194]

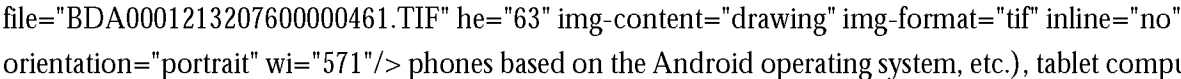
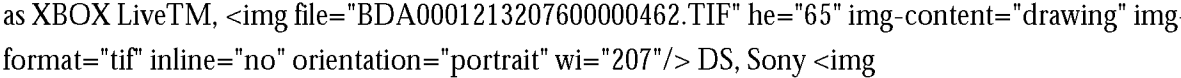
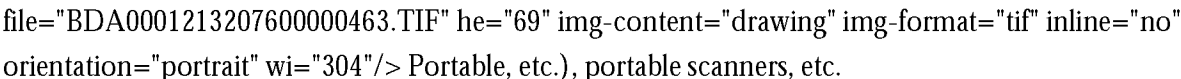
1931 Typically, users such as 1433a, which may be people and/or other systems, may engage information technology systems (eg, computers) to aid in information processing.

1933 In contrast, a computer employs a processor to process information; such a processor 1403 may be referred to as a central processing unit (CPU).

1935 One form of processor is known as a microprocessor. The CPU uses communication circuits to communicate binary-coded signals, which act as instructions to allow various operations. These instructions may be operations and/or data containing and/or referencing other instructions and data in various accessible processor and operable storage areas 1429 (e.g., registers, cache memory, random access memory, etc.) instruction. Such communicated instructions may be stored and/or transmitted in batches (eg, batches) of program and/or data components to facilitate desired operations. These stored instruction codes, such as programs, may engage CPU circuit elements and other motherboard and/or system components to perform desired operations. One type of program is a computer operating system, which may be executed by the CPU on a computer; the operating system allows and assists users in accessing and operating computer information technology and resources. Some of the resources that can be employed in an information technology system include: the input and output mechanisms through which data can be moved into and out of a computer; memory in which data can be saved; and processors through which information can be processed. These information technology systems can be used to collect data for later retrieval, analysis, and manipulation, which can be assisted by database programs. These information technology systems provide interfaces that allow users to access and operate various system elements.

[0195]

1953 In one embodiment, SNAP controller 1401 may be connected to and/or communicate with entities such as, but not limited to: one or more users from user input device 1411; peripheral device 1412; optional encryption process device 1428; and/or communication network 1413.

1956 For example, SNAP controller 1401 may connect to and/or communicate with users, such as 1433a, running client devices, such as 1433b, including but not limited to personal computers, servers, and/or various mobile devices, including but not limited to cellular phones, smart phones (such as  phones based on the Android operating system, etc.), tablet computers (such as Apple iPadTM, HP SlateTM, Motorola XoomTM, etc.), eBook readers (such as Amazon KindleTM, Barnes and Noble's NookTMMeReader etc.), laptops, notebooks, netbooks, game consoles (such as XBOX LiveTM,  DS, Sony  Portable, etc.), portable scanners, etc.

[0196]

1970 Networks are generally considered to include the interconnection and interoperation of clients, servers, and intermediate nodes in a graph topology.

1972 It should be noted that the term "server" is used throughout this application to generally refer to a computer, other device, program, or combination thereof, that processes and responds to requests from remote users across a communications network. Servers use their information to make requests to "clients". As used herein, the term "client" generally refers to a computer, program, other device, user, and/or combination thereof that is capable of processing and generating requests and obtaining and processing any responses from servers across a communication network. Computers, other devices, programs, or combinations thereof that facilitate information processing and requests, and/or send pieces of information from a source user to a target user, are commonly referred to as "nodes." Networks are generally thought of as facilitating the transfer of information from source to destination. Specifically, nodes that perform the task of pushing pieces of information from sources to destinations are often referred to as "routers." There are many forms of networks such as local area networks (LANs), piconets, wide area networks (WANs), wireless networks (WLANs), and so on. For example, the Internet is generally accepted as an interconnection of networks whereby remote clients and servers can access and interoperate with each other.

[0197]

1988 SNAP controller 1401 may be computer system based, which may include, but is not limited to, components such as computer system 1402 connected to memory 1429 .

[0198]

1993 computer system

[0199]

1997 Computer system 1402 may include clock 1430, central processing unit ("CPU" and/or "processor" (these terms are used interchangeably throughout this disclosure unless noted to the contrary)) 1403, memory 1429 (e.g., read-only memory (ROM) 1406, random access memory (RAM) 1405, etc.), and/or interface bus 1407, and almost often, though not necessarily, all interconnected and/or via one or more The transmission circuit path (the system bus 1404 on the (mother) board 1402 through which instructions (eg, binary coded signals) can be transmitted to achieve communication, operation, storage, etc.).

2003 The computer system may be connected to a power supply 1486; for example, the power supply may optionally be internal.

2005 Optionally, cryptographic processor 1426 and/or transceiver (eg, IC) 1474 may be connected to the system bus.

2007 In another embodiment, cryptographic processors and/or transceivers may be connected as internal and/or external peripherals 1412 via interface bus I/O. The transceiver, in turn, can be connected to the antenna 1475, thereby enabling wireless transmission and reception of various communications and/or sensor protocols; for example, the antenna can be connected to: Texas Instruments WiLink WL1283 transceiver chip (e.g., provides 802.11n, Bluetooth 3.0 , FM, Global Positioning System (GPS) (thus allowing the SNAP

controller to determine its location)); BroadcomBCM4329FKUBG transceiver chip (for example, providing 802.11n, Bluetooth 2.1+EDR, FM, etc.); BroadcomBCM4750IUB8 receiver chip (For example, GPS); Infineon Technologies X-Gold 618-PMB9800 (for example, providing 2G/3G HSDPA/HSUPA0 communication), etc. A system clock typically has a crystal oscillator and generates a reference signal through the circuit paths of the computer system. Clocks are typically connected to the system bus and various clock multipliers that increase or decrease the base operating frequency for other components interconnected in the computer system. The clock and various components in a computer system drive the signals that carry out information throughout the system. This sending and receiving of instructions to effectuate information throughout a computer system may generally be referred to as a communication. These communication instructions may also be transmitted, received, and caused to return and/or respond to communications beyond the example computer system to: communication networks, input devices, other computer systems, peripheral devices, and the like. It should be understood that in alternative embodiments, any of the above-described components may be connected directly to each other, to the CPU, and/or organized in numerous variations as exemplified by various computer systems.

[0200]

2029 The CPU includes at least one high-speed data processor sufficient to execute program components for executing user- and/or system-generated requests.

2031 The processor itself will often include various specialized processing units such as, but not limited to: integrated system (bus) controllers, memory management control units, floating point units, and even specialized processing subunits like graphics processing units, digital signal processing unit, etc. In addition, the processor may include internal fast-access addressable memory, and be able to map and address memory 1429 outside of the processor itself; memory may include, but is not limited to: fast registers, various levels of cache memory (e.g., 1, 2, Level 3, etc.), RAM, etc. A processor can access these memories by using a storage address space accessible through an instruction address, which the processor can construct and decode, allowing it to access a circuit path to a specific storage address space with a stored state. The CPU can be a microprocessor such as: AMD's Athlon, Duron and/or Opteron; ARM's application, embedded security processor; IBM and/or Motorola's DragonBall and PowerPC; IBM and Sony's Cell processor; Intel's Celeron, Core(2)Duo, Itanium, Pentium, Xeon, and/or Xscale processors. The CPU interacts with the memory by passing instructions according to conventional data processing techniques across conductive and/or transmission channels (eg (printed) electronic and/or optical circuits) to execute stored instructions (in other words, program code). This command passing facilitates communication within the SNAP controller and out across various interfaces. If processing requirements dictate greater speed and/or capacity, distributed processor (eg, distributed SNAP), mainframe, multi-core, parallel, and/or supercomputer architectures may similarly be employed. Alternatively, a small personal digital assistant (PDA) can be used if the configuration needs dictate greater portability.

[0201]

2052 Depending on the particular implementation, the features of SNAP may be implemented by implementing a microcontroller such as CAST's R8051XC2 microcontroller, Intel's MCS 51 (ie, 8051 microcontroller), or

the like.

2055 Also, to implement certain features of SNAP, some feature implementations may rely on embedded components such as: Application Specific Integrated Circuits ("ASICs"), Digital Signal Processing ("DSPs"), Field Programmable Gate Arrays ("FPGAs"), and/or similar embedded technologies. For example, any SNAP component set (distributed, etc.) and/or features may be implemented by a microprocessor and/or implemented by embedded components; for example, by an ASIC, coprocessor, DSP, FPGA, etc. Alternatively, some implementations of SNAP may be implemented with embedded components configured and used to implement various features or signal processing.

[0202]

2065 Depending on the particular implementation, embedded components may include software solutions, hardware solutions, and/or a combination hardware/software solutions.

2067 For example, the SNAP features discussed herein can be implemented by implementing an FPGA, which is a semiconductor device containing programmable logic elements called "logic blocks," and programmable interconnects, such as high-performance FPGAs from the Virtex family and/or low-level FPGAs produced by Xilinx. Cost Spartan series. After the FPGA is fabricated, the logic blocks and interconnects can be programmed by the customer or designer to implement any SNAP features. A hierarchy of programmable interconnects allows logic blocks to be interconnected as desired by the SNAP system designer/administrator, somewhat like a single programmable breadboard. The logic blocks of the FPGA can be programmed to perform operations on basic logic gates, such as AND and XOR, or more complex combinational operators such as decoders or simple math operations. In most FPGAs, logic blocks also include storage elements, which may be circuit flip-flops or more complete blocks of memory. In some cases, SNAPs can be developed on regular FPGAs and then ported to fixed versions that more closely resemble ASIC implementations. Alternative or cooperative implementations may migrate the SNAP controller features to the final ASIC instead of the FPGA, or migrate the SNAP controller features to the final ASIC in addition to the FPGA. According to all implementations of the aforementioned embedded components, a microprocessor may be envisaged as the "CPU" and/or "processor" for the SNAP.

[0203]

2085 power supply

[0204]

2089 The power supply 1486 may be any standard form used to power small electronic circuit board devices, such as the following batteries: alkaline, lithium hydride, lithium ion, lithium polymer, nickel cadmium, solar cells, and the like.

2092 Other types of AC or DC power sources may also be used.

2093 In the case of a solar cell, in one embodiment, the case provides an aperture through which the solar cell can capture photon energy. The battery 1486 is connected to at least one subsequent component of the interconnected SNAP, thereby providing electrical current to all subsequent components. In one example,

power supply 1486 is coupled to system bus unit 1404 . In an alternative embodiment, external power 1486 is provided through a connection through the I/O 1408 interface. For example, USB and/or IEEE 1394 connections carry data and power across the connection and are thus suitable power sources.

[0205]

2102 interface adapter

[0206]

2106 Interface bus 1407 accepts, connects, and/or communicates to a number of interface adapters, although generally not necessarily in the form of adapter cards, such as, but not limited to: input output interface (I/O) 1408, storage interface 1409, network interface 1410 etc.

2109 Optionally, cryptographic processor interface 1427 may similarly be connected to the interface bus.

2110 The interface bus provides communication of the interface adapters with each other and with other components of the computer system. Interface adapters are available for compatible interface buses. Interface adapters are usually connected to the interface bus through a slot structure. Conventional socket architectures can be used such as, but not limited to: Accelerated Graphics Port (AGP), Card Bus, (Extended) Industry Standard Architecture ((E)ISA), Micro Channel Architecture (MCA), NuBus, Peripheral Component Interconnect (Extended) (PCI(X)), PCI passthrough, Personal Computer Memory Card International Association (PCMCIA), etc.

[0207]

2120 The storage interface 1409 can accept, transfer, and/or connect to a plurality of storage devices, such as but not limited to: the storage device 1414, removable disk devices, and the like.

2122 The storage interface may employ connectivity protocols such as, but not limited to: (Ultra) (Serial) Advanced Technology Attachment (Packet Interface) ((Ultra) (Serial)ATA (PI)), (Enhanced) Integrated Drive Electronics ((E)IDE), Institute of Electrical and Electronics Engineers (IEEE) 1394, Fiber Channel, Small Computer System Interface (SCSI), Universal Serial Bus (USB), etc.

[0208]

2129 The network interface 1410 can accept, communicate and/or connect to a communication network 1413 .

2130 Through the communication network 1413, the SNAP controller is accessible by a user 1433a through a remote client 1433b (eg, a computer with a web browser). The network interface may employ connection protocols such as, but not limited to: direct connect, Ethernet (thick, thin, twisted pair 10/100/1000 10/100/1000Base T, etc.), token ring, such as IEEE802.11a- x wireless connection, etc. If processing requirements dictate greater overall speed and/or capacity, a distributed network controller (eg, distributed SNAP), fabric may similarly be employed to aggregate, load balance, and/or increase the communication bandwidth required by the SNAP controller. The communication network can be any one and/or combination of the following: direct interconnection; Internet; local area network (LAN); metropolitan area

network (MAN); operational mission as a node on the Internet (OMNI);); wireless network (eg, employing protocols such as but not limited to: Wireless Application Protocol (WAP), I-mode, etc.), etc. A network interface can be viewed as a specialized form of an input-output interface. Additionally, multiple network interfaces 1410 may be used to interface with various communication network types 1413 . For example, multiple network interfaces may be employed to allow communication via broadcast, multicast, and/or unicast networks.

[0209]

2147 Input output interface (I/O) 1408 accepts, communicates and/or connects to user input device 1411, peripheral device 1412, cryptographic processor device 1428, and the like.

2149 I/O can employ connection protocols such as but not limited to: Audio: Analog, Digital, Monaural, RCA, Stereo, etc.; Data: Apple Desktop Bus (ADB), IEEE 1394a-b, Serial, Universal Serial Bus (USB); infrared; joystick; keyboard; midi; optical; PC AT; PS/2; parallel; radio; video interface: Apple Desktop Connector (ADC), BNC, coaxial, component, composite, digital, DVI (DVI), High Definition Multimedia Interface (HDMI), RCA, RF Antenna, S-Video, VGA, etc.; Wireless Transceivers: 802.11a/b/g/n/x; Bluetooth; Cellular (e.g., Code Division Multi Address (CDMA), High Speed Packet Access (HSPA(+)), High Speed Downlink Packet Access (HSDPA), Global System for Mobile Communications (GSM), Long Term Evolution (LTE), WiMax, etc.); etc. A typical output device may include a video display, typically comprising a cathode ray tube (CRT) or liquid crystal display (LCD) based monitor, with an interface (such as DVI circuitry and cable) to accept a signal from a video interface. The video interface synthesizes information generated by the computer system and generates a video signal in a video storage frame based on the synthesized information. Another output device is a television, which accepts the signal from the video interface. Typically, the video interface provides composite video information through a video connection interface that accepts a video display interface (eg, an RCA composite video connector that accepts an RCA composite video cable; a DVI connector that accepts a DVI display cable, etc.).

[0210]

2167 User input device 1411 is often a type of peripheral device 1412 (see below) and may include: card reader, dongle, fingerprint reader, gloves, graphics tablet, joystick, keyboard, microphone, mouse, remote control , retina reader, touch screen (eg, capacitive, resistive, etc.), trackball, trackpad, sensor (eg, accelerometer, ambient light, GPS, gyroscope, proximity, etc.), stylus wait.

[0211]

2174 Peripherals 1412 may be connected to and/or communicated to I/O and/or other similar equipment, such as a network interface, storage interface, direct-to-interface bus, system bus, CPU, and the like.

2176 Peripherals can be external, internal and/or part of the SNAP controller.

2177 Peripherals can include: antennas, audio devices (e.g., line-in, line-out, microphone-in, speakers, etc.), cameras (e.g., still, video, webcam, etc.), dongles (e.g., for copying protection, use of digital signatures to ensure secure transactions, etc.), external processors (for additional capacity; e.g., encryption device 1428),

force feedback devices (e.g., vibrating motors), network interfaces, printers, scanners, storage devices, transceivers sensors (eg, cellular, GPS, etc.), video equipment (eg, goggles, monitors, etc.), video sources, helmets, etc. Peripherals often include various types of input devices (eg, video cameras).

[0212]

2186 It should be noted that while user input devices and peripherals may be employed, the SNAP controller may be embodied as an embedded, dedicated and/or monitor-less (ie headless) device where access will be provided via a network interface connection.

[0213]

2192 Cryptographic units, such as, but not limited to, microcontrollers, processors 1426, interfaces 1427, and/or devices 1428, can be attached to and/or communicate with the SNAP controller.

2194 An MC68HC16 microcontroller manufactured by Motorola may be used in and/or within the encryption unit.

2196 The MC68HC16 microcontroller uses 16-bit multiply and add instructions in a 16 MHz configuration and takes less than 1 second to execute 512-bit RSA private key operations. The cryptographic unit supports authentication of communications from interactive agents as well as allowing bearer transactions. The encryption unit can also be configured as part of the CPU. Equivalent microcontrollers and/or processors could also be used. Other commercially available dedicated encryption processors include: Broadcom's CryptoNetx and other security processors; Ncipher's nShield, SafeNet's Luna PCI (e.g., 7100) series; Semaphore Communication's 40MHz Roadrunner 184; Sun's encryption accelerator (e.g., Accelerator 6000PCIE Board, Accelerator 500Daughtercard); Via nanoprocessor (eg, L2100, L2200, U2400) line capable of executing 500+MB/s encrypted instructions; VLSI Technology's 33MHz 6868, etc.

[0214]

2208 memory

[0215]

2212 In general, any mechanism and/or embodiment that allows a processor to store and/or retrieve information can be considered memory 1429 .

2214 However, memory is an alternative technology and resource, and thus multiple memory embodiments may be employed in place of each other or in combination.

2216 It should be understood that various forms of memory 1429 may be employed by the SNAP controller and/or computer system. For example, a computer system may be configured in which the operation of the on-chip CPU memory (e.g., registers), RAM, ROM, and any other storage devices is provided by a paper punched tape or paper punched card mechanism; however, such an embodiment would result in Very slow operating speed. In a typical configuration, memory 1429 will include ROM 1406 , RAM 1405 , and storage device 1414 . Storage device 1414 may be any conventional computer system memory. Storage devices may

include drums; magnetic disk drives (fixed and/or removable); magneto-optical drives; optical drives (i.e., Blu-ray, CD-ROM/RAM/Recordable (R)/Writable (RW), DVD R/ RW, HD DVD R/RW, etc.); device arrays (e.g., redundant array of independent disks (RAID)); solid-state memory devices (USB memory, solid-state drive (SSD), etc.); other processor-readable storage media ; and/or other similar devices. Therefore, computer systems generally require and use memory.

[0216]

2230 parts set

[0217]

2234 Memory 1429 may contain a collection of program and/or database components and/or data such as, but not limited to: operating system component 1415 (operating system); information server component 1416 (information server); user interface component 1417 (user interface); Web browser component 1418 (web browser); database 1419; mail server component 1421; mail client component 1422; encryption server component 1420 (encryption server);

2239 These components may be stored and accessed from a storage device and/or from a storage device accessible through an interface bus.

2241 Although non-traditional program components, such as those of a collection of components, are typically stored in local storage device 1414, they may also be loaded and/or stored in storage devices such as peripheral devices, RAM, memory in remote storage facilities.

[0218]

2247 operating system

[0219]

2251 Operating system components 1415 are executable program components that facilitate operation of the SNAP controller.

2253 Typically, an operating system facilitates access to I/O, network interfaces, peripherals, storage devices, and so on.

2255 Operating systems can be highly fault-tolerant, scalable, and secure systems such as Apple Macintosh computer OS X (Server); AT&T Plan 9; Be OS; Unix and Unix-like system distributions (such as AT&T's UNIX; Berkley Software Distribution Program (BSD) variants, such as FreeBSD, NetBSD, OpenBSD, etc.; Linux distributions, such as Red Hat, Ubuntu, etc.); and/or similar operating systems. However, more restricted and/or less secure operating systems such as Apple Macintosh computer OS, IBM OS/2, Microsoft DOS, Microsoft Windows2000/2003/3.1/95/98/CE/Millennium/NT/ Vista/XP (server), Palm OS, etc. The operating system can communicate unidirectionally and/or bidirectionally with other components in the component set, including itself, and the like. The operating system most often communicates with other program components, user interfaces, and/or the like. For example, an operating system may contain,

communicate, generate, obtain, and/or provide program component, system, user, and/or data communications, requests, and/or responses. Once executed by the CPU, the operating system may allow interaction with communication networks, data, I/O, peripherals, program components, memory, user input devices, and the like. The operating system may provide a communication protocol that allows the SNAP controller to communicate with other entities over the communication network 1413 . The SNAP controller can use various communication protocols as the subcarrier transport mechanism for interaction, such as but not limited to: multicast, TCP/IP, UDP, unicast, etc.

[0220]

2274 information server

[0221]

2278 Information server component 1416 is a stored program component that is executed by the CPU.

2279 The information server may be a traditional Internet information server, such as but not limited to Apache based on Apache software, Internet information server of Microsoft Corporation, and the like.

2281 The Information Server may allow the execution of program components through facilities such as: Active Server Pages (ASP), ActiveX, (ANSI) (Objective-)C(++), C# and/or . NET, Common Gateway Interface (CGI) Scripting, Dynamic (D) Hypertext Markup Language (HTML), FLASH, Java, JavaScript, Practical Extractable Reporting Language (PERL), Hypertext Preprocessor (PHP), Pipeline, Python, Wireless Application Protocol (WAP), WebObjects, etc. The information server may support secure communication protocols such as, but not limited to: File Transfer Protocol (FTP); Hypertext Transfer Protocol (HTTP); Hypertext Transfer Protocol Secure (HTTPS), Secure Sockets Layer (SSL), messaging protocols (e.g. America Online Services (AOL) Instant Messenger (AIM), Application Exchange (APEX), ICQ, Internet Multithreaded Chat (IRC), Microsoft Networks (MSN) Messenger Service, Protocol for Presence and Instant Messaging (PRIM), Internet Engineering Task Force's (IETF's) Session Initiation Protocol (SIP), SIP for Instant Messaging and Presence Impact Extensions (SIMPLE), the open XML-based Extensible Messaging and Presence Protocol (XMPP) (i.e. Jabber or Open Mobile Alliance's (OMA's) Instant Messaging and Presence Service (IMPS), Yahoo! Instant Messenger Service, etc. The information server provides results in the form of web pages to the web browser and allows controlled generation of web pages through interaction with other program components. After the Domain Name System (DNS) resolved portion of the HTTP request is resolved to a particular Information Server, the Information Server resolves the request for information at the specified location on the SNAP Controller based on the remainder of the HTTP request. For example, a request such as `http://123.124.125.126/myInformation.html` may have the IP portion of the request "123.124.125.126", which resolves to an information server at that IP address through a DNS server; that information server may in turn resolve http request for the `/myInformation.html` portion of the request and resolve it to a location in memory containing the information "myInformation.html". In addition, other information used as a protocol can be employed across various ports, eg, FTP communication across ports, etc. The information server can communicate unidirectionally and/or bidirectionally with other components in the component set, including itself, and/or the like. Most information servers communicate constantly with the SNAP database 1419, operating system,

other program components, user interfaces, web browsers, and the like.

[0222]

2310 Access to the SNAP database can be achieved through a number of database bridging mechanisms, such as through scripting languages (eg, CGI) as listed below and through inter-application communication channels as listed below (eg, CORBA, WebObjects, etc.).

2313 Any data request by the web browser is parsed by the bridging mechanism into the appropriate syntax as required by SNAP. In one embodiment, the information server will provide a web form accessible by a web browser. An entry in a web form that is filled into a provided field is marked as having been entered into a particular field and is parsed accordingly. The entered terms are then passed along with the field labels, which instruct the parser to generate queries directed to the appropriate tables and/or fields. In one embodiment, based on the marked text entries, the parser can generate queries in standard SQL fashion by instantiating search strings with appropriate join/select commands, where the resulting commands are provided to SNAP as queries via a bridging mechanism. When query results are generated according to the query, the results are passed via the bridging mechanism and can be parsed by the bridging mechanism for formatting and generation of new result web pages. This new resulting web page is then provided to the information server, which can serve it to the requesting web browser.

[0223]

2327 Likewise, an information server may contain, communicate, generate, obtain, and/or provide program component, system, user, and/or data communications, requests, and/or responses.

[0224]

2332 user interface

[0225]

2336 Computer interfaces are similar in some respects to automotive operating interfaces.

2337 Automotive operating interface elements such as the steering wheel, transmission, and speedometer facilitate the access, operation, and display of vehicle resources and status.

2339 Computer interactive interface elements such as checkboxes, cursors, menus, scrollers, and windows (collectively and often referred to as widgets) similarly facilitate access, operation of data and computer hardware and operating system resources and state, and display.

2342 The operator interface is often called the user interface. Graphical User Interface (GUI) provides the baseline and means to graphically access and display information to the user, GUI such as Aqua of the Apple Macintosh computer operating system, OS/2 of International Business Machines Corporation, Windows 2000/2003/3.1/95 of Microsoft Corporation /98/CE/Millennium/NT/XP/Vista/7 (i.e. Aero), X-Windows for Unix (which may include, for example, additional Unix graphical interface libraries and layers such as the K Desktop Environment (KDE), mythTV, and GNU Network Object Model Environment (GNOME)), web

interface libraries (for example, ActiveX, AJAX, (D)HTML, FLASH, Java, JavaScript, etc., interface libraries such as but not limited to, Dojo, jQuery (UI), MooTools, Prototype, script.aculo.us, SWFObject, Yahoo UI, whatever can be used).

[0226]

2354 User interface component 1417 is a stored program component executed by the CPU.

2355 The user interface may be, for example, a conventional graphical user interface provided by and/or on top of the already discussed operating system and/or operating environment. A user interface may allow display, execution, interaction, processing, and/or operation of program components and/or system facilities through textual and/or graphical facilities. A user interface provides a facility by which a user can implement, interact with, and/or operate a computer system. A user interface can communicate unidirectionally and/or bidirectionally with other components within a component set, including itself, and/or the like. Most of the user interface often communicates with the operating system, other program components, and so on. The user interface may contain, communicate, generate, obtain and/or provide program component, system, user, and/or data communications, requests, and/or responses.

[0227]

2367 browser

[0228]

2371 Web browser component 1418 is a stored program component executed by the CPU.

2372 The web browser may be a conventional hypertext browsing application such as Microsoft Internet Explorer or Netscape Navigator.

2374 Secure web browsing can be provided over HTTPS, SSL, etc. utilizing 128-bit (or more) encryption. Web browsers allow the execution of program components through facilities such as ActiveX, AJAX, (D)HTML, FLASH, Java, JavaScript, web browser plug-in APIs (eg, FireFox, Safari Plug-in, etc. APIs), etc. Web browsers and similar information access tools can be integrated into PDAs, cell phones, and/or other mobile devices. A user's web browser can communicate unidirectionally and/or bidirectionally with other components within a component component set, including itself, and/or similar facilities. Most web browsers frequently communicate with information servers, operating systems, integrated program components (such as plug-ins), etc.; for example, it may contain, transmit, generate, obtain and/or provide program components, systems, users and/or data Communications, Requests and/or Responses. Also, instead of a web browser and an information server, a combined application can be developed to perform similar operations of both. Composite applications similarly implement retrieval of information from SNAP-enabled nodes and provision of information to users, user agents, etc. The composite application may be non-trivial on systems employing standard web browsers.

[0229]

[0230]

2394 The mail server component 1421 is a stored program component executed by the CPU 1403 .

2395 The mail server may be a conventional Internet mail server, such as but not limited to sendmail, Microsoft Exchange, and the like.

2397 The mail server may allow the execution of program components through facilities such as ASP, ActiveX, (ANSI) (Objective-)C(++), C#_ and/or . NET, CGI scripts, Java, JavaScript, PERL, PHP, pipes, Python, WebObjects, etc. The mail server can support communication protocols, such as but not limited to: Internet Message Access Protocol (IMAP), Message Application Programming Interface (MAPI)/Microsoft Exchange, post office protocol (POP3), Simple Mail Transfer Protocol (SMTP) and the like. The mail server may route, forward and process incoming and outgoing mail messages that have been sent, relayed and/or traversed through and/or to the SNAP.

[0231]

2407 Access to SNAP mail can be accomplished through multiple APIs provided by individual web server components and/or operating systems.

[0232]

2412 Also, a mail server may contain, communicate, generate, obtain, and/or provide program component, system, user, and/or data communications, requests, information, and/or responses.

[0233]

2417 mail client

[0234]

2421 Mail client component 1422 is a stored program component executed by CPU 1403 .

2422 The mail client can be a traditional mail browsing application, such as: Apple Mail, Microsoft Entourage, Microsoft Outlook, Microsoft Outlook Express, Mozilla, Thunderbird, etc.

2424 The mail client can support multiple transfer protocols, such as: IMAP, Microsoft Exchange, POP3, SMTP, etc.

2426 The mail client can communicate unidirectionally and/or bidirectionally with other components in the component set, including itself, and/or the like.

2428 Most mail clients routinely communicate with mail servers, operating systems, other mail clients, etc.; for example, it may contain, deliver, generate, obtain and/or provide program components, system, user and/or data communications, requests, Information and/or Responses. Mail clients typically provide facilities to compose and transmit e-mail messages.

[0235]

2435 encrypted server

[0236]

2439 Crypto server component 1420 is a stored program component executed by CPU 1403, crypto processor 1426, crypto processor interface 1427, crypto processor device 1428, and the like.

2441 A cryptographic processor interface would allow acceleration of encryption and/or decryption requested by the cryptographic element; however, the cryptographic element could alternatively run on a conventional CPU.

2444 Cryptographic elements allow encryption and/or decryption of provided data. Cryptographic elements allow symmetric and asymmetric (eg, Pretty Good Protection (PGP)) encryption and/or decryption. The encryption technology that can be used by the encryption element is such as but not limited to: digital certificate (for example, X.509 authentication framework), digital signature, double signature, envelope, password access protection, public key management and so on. Cryptographic elements will facilitate many (encryption and/or decryption) security protocols such as but not limited to: checksum, Data Encryption Standard (DES), Elliptic Curve Cryptography (ECC), International Data Encryption Algorithm (IDEA), message Digest (MD5, which is a form of hashing), Cipher, Rivest Cipher (RC5), Rijndael, RSA (which is an Internet encryption and authentication system using an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977), Secure Hash Algorithm (SHA), Secure Sockets Layer (SSL), Secure Hypertext Transfer Protocol (HTTPS), etc. Using these encrypted security protocols, SNAP can encrypt all incoming and/or outgoing communications and can utilize wider communication networks as nodes within a Virtual Private Network (VPN). The cryptographic element facilitates the processing of "security authorization", whereby access to resources is prohibited by security protocols, wherein the cryptographic element implements authorized access to secure resources. Additionally, the cryptographic element may provide a unique identifier of the content, for example using and MD5 hashing to obtain a unique signature for a digital audio file. A cryptographic element may communicate unidirectionally and/or bidirectionally with other components within a component set, including itself, and/or the like. The cryptographic element supports cryptographic mechanisms that allow secure transmission of information across communication networks to allow SNAP components to engage in secure transactions, if desired. The cryptographic element facilitates secure access to resources on SNAP and facilitates access to secure resources on remote systems; ie it can act as a client and/or server to secure resources. Most cryptographic components often communicate with information servers, operating systems, other program components, etc. The cryptographic element may contain, communicate, generate, obtain, and/or provide program component, system, user, and/or data communications, requests, and/or responses.

[0237]

2472 SNAP database

[0238]

2476 The SNAP database component 1419 can be embedded in the database and the data it stores.

2477 The database is a stored program component, which is executed by the CPU; the stored program component configures the CPU in part to process the stored data.

2479 The database may be a traditional, fault-tolerant, relational, scalable, secure database, such as Oracle or Sybase. Relational databases are an extension of flat files. A relational database consists of a series of related tables. Tables are joined to each other by key fields. The use of key fields allows tables to be combined through indexes relative to the key fields; that is, the key fields serve as dimensional pivots for the combined information of the various tables. Relationships typically identify links between tables by means of matching primary keys. A primary key represents a field that uniquely identifies a table row in a relational database. More precisely, they uniquely identify table rows on the "one" side of a one-to-many relationship.

[0239]

2489 Alternatively, SNAP databases can be implemented using various standard data structures, such as arrays, hashes, (linked) lists, structures, structured text files (eg XML), tables, etc.

2491 These data structures can be stored in memory and/or in (structure) files. In another alternative, an object-oriented database such as Frontier, ObjectStore, Poet, Zope, etc. can be used. An object database may comprise a plurality of object collections grouped and/or linked by common attributes; they are related to other object collections by some common attributes. Object-oriented databases perform similarly to relational databases, except that their objects are not just pieces of data, but can have other types of functionality encapsulated within a given object. The use of SNAP database 1419 may be integrated into another component, such as SNAP component 1435, if the SNAP database is implemented as a data structure. Likewise, databases can be implemented as a mix of data structures, objects, and relational structures. Databases can be consolidated and/or distributed in myriad variations by standard data processing techniques. Parts of the database, such as tables, may be exported and/or imported and thus decentralized and/or integrated.

[0240]

2505 In one embodiment, the database component 1419 includes several tables 1419a-o.

2506 The user table 1419a may include fields such as, but not limited to: `user_id`, `ssn`, `dob`, `first_name`, `last_name`, `age`, `state`, `address_firstline`, `address_secondline`, `zipcode`, `devices_list`, `contact_info`, `contact_type`, `alt_contact_info`, `alt_contact_type`, and the like. A user form may support and/or track multiple entity accounts on SNAP. The device table 1419b may include fields such as, but not limited to: `device_ID`, `device_name`, `device_IP`, `device_MAC`, `device_type`, `device_model`, `device_version`, `device_OS`, `device_apps_list`, `device_securekey`, `wallet_app_installed_flag`, and the like. The Apps table 1419c may include fields such as, but not limited to: `app_ID`, `app_name`, `app_type`, `app_dependencies`, and the like. Account table 1419d may include fields such as, but not limited to: `account_number`, `account_security_code`, `account_name`, `issuer_acquirer_flag`, `issuer_name`, `acquirer_name`, `account_address`, `routing_number`, `access_API_call`, `linked_wallets_list`, and the like. Merchant table 1419e

may include fields such as, but not limited to: merchant_id, merchant_name, merchant_address, ip_address, mac_address, auth_key, port_num, security_settings_list, etc. Issuer table 1419f may include fields such as, but not limited to: issuer_id, issuer_name, issuer_address, ip_address, mac_address, auth_key, port_num, security_settings_list, and the like. The acquirer table 1419g may include fields such as, but not limited to: account_firstname, account_lastname, account_type, account_num, account_balance_list, billingaddress_line1, billingaddress_line2, billing_zipcode, billing_state, shipping_preferences, shippingaddress_line1, shippingaddress_line2, shipping_zipcode, etc.

2523 The payment gateway table 1419b may include fields such as, but not limited to: gateway_ID, gateway_IP, gateway_MAC, gateway_secure_key, gateway_access_list, gateway_API_call_list, gateway_services_list, and the like. Transaction table 1419i may include fields such as but not limited to: order_id, user_id, timestamp, transaction_cost, purchase_details_list, num_products, products_list, product_type, product_params_list, product_title, product_summary, quantity, user_id, client_system_id, client_ip, client_type, client_atversion_moding, app_installed_flag, user_id, account_firstname, account_lastname, account_type, account_num, account_priority_account_ratio, billingaddress_line1, billingaddress_line2, billing_zipcode, billing_state, shipping_preferences, shippingaddress_line1, shippingaddress_line2, shipping_zipcode, shipping_state, merchant_id, merchant_name, merchant_auth_key等。 The batch table 1419j may include fields such as, but not limited to: batch_id, transaction_id_list, timestamp_list, cleared_flag_list, clearance_trigger_settings, and the like. Ledger table 1419k may include fields such as, but not limited to: request_id, timestamp, deposit_amount, batch_id, transaction_id, clear_flag, deposit_account, transaction_summary, payor_name, payor_account, and the like.

2537 Products table 1419l may include fields such as, but not limited to: product_ID, product_title, product_attributes_list, product_price, tax_info_list, related_products_list, offers_list, discounts_list, rewards_list, merchants_list, merchant_availability_list, and the like. The offer form 1419m may include fields such as, but not limited to: offer_ID, offer_title, offer_attributes_list, offer_price, offer_expiry, related_products_list, discounts_list, rewards_list, merchants_list, merchant_availability_list, and the like. The behavior data table 1419n may include fields such as but not limited to: user_id, timestamp, activity_type, activity_location, activity_attribute_list, activity_attribute_values_list, and the like. Analysis table 1419o may include fields such as, but not limited to: report_id, user_id, report_type, report_algorithm_id, report_destination_address, and the like.

[0241]

2549 In one embodiment, the SNAP database can interact with other database systems.

2550 For example, using a distributed database system, query and data access by retrieving SNAP components can handle the combination of SNAP database, integrated data security layer database as a single database entity.

[0242]

2555 In one embodiment, the user program may contain various user interface primitives that may be used to update SNAP.

2557 Likewise, various accounts may require custom database tables depending on the environment in which

SNAP may need to serve, as well as the type of client. It should be noted that any unique field can be specified as the key field throughout. In an alternative embodiment, these tables have been dispersed into their own databases and their respective database controllers (ie, a single database controller for each of the above tables). Using standard data processing techniques, one can further distribute the database via several computer systems and/or storage devices. Similarly, by consolidating and/or distributing the various database components 1419a-o, the configuration of decentralized database controllers may be changed. SNAP can be configured to track various settings, inputs and parameters through the database controller.

[0243]

2568 The SNAP database can communicate unidirectionally and/or bidirectionally with other components within the component set, including itself, and/or similar facilities.

2570 Most SNAP databases communicate frequently with SNAP components, other program components, and the like. A database may contain, maintain and provide information about other nodes and data.

[0244]

2575 SNAP

[0245]

2579 SNAP component 1435 is a stored program component executed by the CPU.

2580 In one embodiment, a SNAP component includes any and/or all combinations of aspects of SNAP discussed in the preceding figures.

2582 Thus, SNAP implements the access, acquisition and provision of information, services, transactions, etc. across various communication networks.

[0246]

2587 The SNAP component can convert real-time generated merchant-product quick response codes into virtual wallet card-based transaction purchase notifications, etc. and use of SNAP through the SNAP component.

2589 In one embodiment, the SNAP component 1435 takes input (e.g., checkout input 411; product data 414; payment input 419; issuer server data 423; user data 427a-n, etc.) and transforms the input through the SNAP component (e.g., SMPE 1441; QRCP 1442, etc.) are outputs (eg, QR payment code 417; card authorization request 421; authorization response 429a-n; authorization success message 433a-b; batch additional data 435; purchase receipt 436, etc.).

[0247]

2597 SNAP components that allow information access between nodes can be developed using standard development tools and languages such as, but not limited to: Apache components, Assembly, ActiveX, executable binary, (ANSI) (Objective-)C (++), C #_and / or.

2600 NET, database adapters, CGI scripts, Java, JavaScript, drawing tools, procedural and object-oriented development tools, PERL, PHP, Python, shell scripts, SQL commands, web application server extensions, web development environments and libraries (e.g., Microsoft Corporation ActiveX; Adobe AIR, FLEX&FLASH; AJAX; (D)HTML; Dojo, Java; JavaScript; jQuery (UI); MooTools; etc.), WebObjects, etc. In one embodiment, the SNAP server employs an encryption server to encrypt and decrypt communications. A SNAP element can communicate unidirectionally and/or bidirectionally with other components within a component set, including itself, and/or the like. Most SNAP components constantly communicate with SNAP databases, operating systems, other program components, and so on. A SNAP may contain, communicate, generate, obtain and/or provide program component, system, user and/or data communications, requests and/or responses.

[0248]

2613 Distributed SNAP

[0249]

2617 The structure and/or operation of any SNAP node controller component can be combined, merged and/or distributed in any number of ways to aid in development and/or configuration.

2619 Similarly, component sets can be combined in any number of ways to aid deployment and/or development.

2620 To achieve this, components can be integrated into a common code base or into a facility where components can be dynamically loaded in an integrated fashion on demand.

[0250]

2625 Component sets can be combined and/or distributed in myriad variations through standard data processing and/or development techniques.

2627 Multiple instances of any of the program components in a program component set may be instantiated on a single node, and/or across multiple nodes to improve performance through load balancing and/or data processing techniques. Additionally, a single instance may also be distributed across multiple controllers and/or storage devices; eg, a database. All program component instances and controllers working together may do so through standard data process communication techniques.

[0251]

2635 The configuration of the SNAP controller will depend on the environment in which the system is deployed.

2636 Factors such as, but not limited to, budget, capacity, location, and/or utilization of underlying hardware resources may enforce deployment requirements and configurations. Regardless of whether the configuration results in more consolidated and/or integrated program components, results in more distributed families of program components, and/or results in a combination between consolidated and distributed configurations, data may be communicated, obtained, and/or provided. Depending on the set of program components, component instances incorporated into the common code base can pass, obtain,

and/or provide data. These can be achieved through in-application data handling communication techniques such as but not limited to: data references (eg pointers), internal message passing, object instance variable communication, shared memory space, variable passing, and the like.

[0252]

2648 If the component set components are mutually discrete, independent and/or external, then passing, obtaining and/or providing data and/or to other components can be achieved through in-application data processing communication techniques, such as but not limited to: Application programming interface (API) information transfer; (distributed) component object model ((D)COM), (distributed) object linking and embedding ((D)OLE), etc.), common object request agent architecture (CORBA), Jini local and remote APIs, Javascript Object Notation (JSON), Remote Method Reference (RMI), SOAP, process pipes, shared files, etc.

2655 Messages sent between discrete components for inter-application communication, or within the storage space of a single component for intra-application communication, can facilitate the creation and parsing of the grammar. Grammars can be developed using development tools, such as lex, yacc, XML, etc., which allow grammar generation and parsing functions, which in turn can form the basis of communication messages within and between components.

[0253]

2663 For example, the syntax can be set to recognize a token for an HTTP post directive, such as:

[0254]

2667 w3c-post http://...

2668 Value1

[0255]

2672 Where Value1 is identified as a parameter because "http://" is part of the syntax and subsequent is considered part of the posted value.

2674 Similarly, using this syntax, the variable "value1" can be inserted into the "http://" post command and then sent.

2676 The grammar itself may be presented as structured data that is interpreted and/or used to generate parsing mechanisms (such as grammar description text files processed by lex, yacc, etc.). Likewise, once a parsing mechanism has been spawned and/or instantiated, it itself processes and/or parses structured data such as, but not limited to: characters delineating text (e.g. tags), HTML, structured text streams, XML, etc. data. In another embodiment, the inter-application data processing protocol itself may have integrated and/or readily available parsers (eg, JSON, SOAP, etc. parsers) that may be used to parse (eg, communicate) data. Furthermore, parse syntax can be used on top of message parsing, but also for parsing: databases, datasets, data stores, structured data, etc. Again, the desired configuration will depend on the context, environment,

and needs of system development.

[0256]

2688 For example, in some implementations, the SNAP controller may be a PHP script that implements a Secure Sockets Layer ("SSL" socket server) executed by the message server, which listens for data that the client may send (e.g., data encoded in JSON format) incoming traffic on the server port.

2691 Once the incoming communication is identified, the PHP script can read the incoming message from the client device, parse the received JSON-encoded data to extract information from the JSON-encoded text data into PHP script variables, and query it using the Structured Query Language ("SQL ") to store the data (eg, client identification information, etc.) and/or the extracted information in a relational database accessible by Basically written as PHP/SQL commands to accept JSON-encoded input data from a client device over an SSL connection, parse the data to extract variables, and store the data to a database An exemplary list is provided below:

[0258]

2701 Likewise, the following resources are available to provide exemplary embodiments showing SOAP parser implementations:

[0259]

2706 <http://www.xav.com/perl/site/lib/SOAP/Parser.html>

[0260]

2710 <http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?>

2711 [topic=/com.ibm](#)

[0261]

2715 .

2716 [IBMDI.doc/referenceguide295.htm](#)

[0262]

2720 and other parser implementations:

[0263]

2724 <http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?>

2725 [topic-/com.ibm](#)

[0264]

2729 .

2730 [IBMDI.doc/referenceguide259.htm](#)

[0265]

2734 All of these are therefore included here by reference.

[0266]

2738 In order to solve various problems and develop technologies, it is used for snapshot mobile payment devices, methods and systems (including cover, title, subtitle, technical field, background technology, summary of the invention, description of drawings, detailed description, claims, abstract , drawings, appendices and/or others) of this application throughout are shown by various schematic embodiments in which the claimed innovations can be practiced.

2743 The advantages and features of the present application are merely representative examples of embodiments, not exhaustive and/or exclusive.

2745 They exist only to aid in understanding and to teach the principles as claimed.

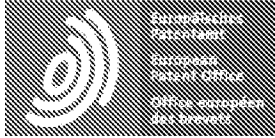
2746 It should be understood that they do not represent all innovations as claimed.

2747 Accordingly, certain aspects of the disclosure are not discussed here.

2748 Alternative embodiments have not necessarily been presented for specific parts of the invention or otherwise undescribed alternative embodiments may be available to contemplate disclaimed components of an alternative embodiment.

2751 It will be appreciated that many of those non-described embodiments employ the same principles of the invention and that others are equivalent. Accordingly, it is to be understood that other embodiments may be utilized and functional logical, operational, organizational, structural and/or topological modifications may be made without departing from the scope and/or spirit of this disclosure. Accordingly, all examples and/or embodiments are considered to be non-limiting throughout this disclosure. No inference should be drawn to consider those embodiments discussed here relative to those not discussed here, except for the sake of reducing space and repetition. For example, it should be understood that the logical and/or topological structure of any group of any program component (collection of components), other components and/or provided component arrangements as shown in the figures and/or fully described is not limited to a fixed operating order and/or permutation, but any order disclosed is exemplary and all equivalents, regardless of order are contemplated by this disclosure. Furthermore, it should be understood that such components are not limited to serial execution, but that multiple threads, processes, services, servers, and/or those that can execute asynchronously, synchronously, in parallel, concurrently, synchronously, etc. are contemplated by this disclosure. Thus, some components may be mutually exclusive in that they cannot both exist in a single embodiment. Similarly some components are applicable to one aspect of the invention and not applicable to other aspects. Additionally, the disclosure includes other novel methods that are not presently claimed. All rights reserved to the presently unclaimed applicant for a new method, including the right to claim such a

new method, file addition application, continuation, continuation in part, severance, and/or its equivalents. Thus, it should be understood that advantages, embodiments, examples, functions, components, logical operations, organization, structures, topologies and/or other aspects of the disclosure are not intended to be limited to or limited to the disclosure defined by the claims On the equivalent of claims. It should be understood that various implementations of SNAP depend on the specific needs and/or characteristics of SNAP individual and/or business users, database configurations and/or relational models, data types, data transfer and/or network frameworks, syntax structures, etc. Example can be implemented which allows a lot of flexibility and customization. For example, aspects of SNAP may be adapted for restaurant ordering, online shopping, shopping in brick and mortar stores, secure information processing, healthcare information systems, and the like. While the various embodiments and discussions of SNAP have been directed to electronic purchase transactions, however, it should be understood that the embodiments herein can be readily configured and/or customized for a wide variety of other applications and/or implementations Way.



Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

CLAIMS CN106803175A

1.

13 A computer-implemented snapshot payment method comprising:

14 obtaining user input at the mobile computing device to initiate a purchase transaction;

15 acquiring image frames by an image acquisition device operatively connected to said mobile computing device;

16 identify the payment code depicted within the captured image frame;

17 generating a purchase transaction request via the mobile computing device using the identified payment code;

18 providing the purchase transaction request for payment processing; and

19 A purchase receipt is obtained for the purchase transaction.

2.

23 The method of claim 1, further comprising:

24 An image of the payment code is provided for purchase transaction processing.

3.

28 The method of claim 1, further comprising:

29 acquiring video including said image frames by said image acquisition device included in said user mobile device;

31 extracting said image frames from the acquired video; and

32 The image frame is analyzed to determine whether the image frame includes the described payment code.

4.

36 The method of claim 1, wherein the user input is a touch screen gesture on a touch screen operatively connected to the mobile computing device.

5.

41 The method of claim 1, wherein the payment code is a one-dimensional barcode.

6.

45 The method of claim 1, wherein the payment code is a two-dimensional barcode including a quick response code.

7.

50 The method of claim 1, further comprising:

51 extract purchase session data from said payment code; and

52 Wherein the purchase transaction request is generated through the user's mobile device using the extracted purchase session data.

8.

57 The method of claim 7, wherein the purchasing session data includes a merchant identifier and a session identifier for a user shopping session with a merchant associated with the merchant identifier.

9.

62 The method of claim 8, wherein the session identifier is configured as a token parameter in a Uniform Resource Locator for data about a user's shopping session with the merchant.

10.

67 The method of claim 1, further comprising:

68 Obtain payment information associated with a virtual wallet account for payment processing;

69 Wherein the generated purchase transaction request includes the payment information associated with the virtual wallet account.

11.

74 The method of claim 10, wherein the payment information includes a dynamically generated card verification value code.

12.

79 The method of claim 11, further comprising:

80 providing a request to the server for the dynamically generated card verification value code; and
81 The dynamically generated card verification value code is obtained from the server in response to providing
the request.

13.

86 The method of claim 12, wherein the dynamically generated card verification value has an expiration time and
corresponds to a user shopping session with the merchant.

14.

91 The method of claim 1, wherein the payment code depicted within the captured image frame is captured from
a display of a media device and encodes data to purchase the requested media content.

15.

96 The method of claim 14, wherein the media device is a television.

16.

100 The method of claim 15, wherein the television is part of an in-flight entertainment system.

17.

104 The method of claim 16, wherein the media device is displaying a web page.

18.

108 A computer-implemented snapshot payment system comprising:

109 processor; and

110 a memory configured to communicate with the processor and store processor-executable instructions to:

111 obtaining user input at the mobile computing device to initiate a purchase transaction;

112 acquiring image frames by an image acquisition device operatively connected to said mobile computing
device;

114 identify the payment code depicted within the captured image frame;

115 generating a purchase transaction request via the mobile computing device using the identified payment code;

116 providing the purchase transaction request for payment processing; and

117 A purchase receipt is obtained for the purchase transaction.

19.

121 A computer-readable tangible medium storing computer-executable snapshot payment instructions to:

122 obtaining user input at the mobile computing device to initiate a purchase transaction;
123 acquiring image frames by an image acquisition device operatively connected to said mobile computing device;
125 identify the payment code depicted within the captured image frame;
126 generating a purchase transaction request via the mobile computing device using the identified payment code;
127 providing the purchase transaction request for payment processing; and
128 A purchase receipt is obtained for the purchase transaction.

20.

132 A computer-implemented snapshot payment device, comprising means for:
133 obtaining user input at the mobile computing device to initiate a purchase transaction;
134 acquiring image frames by an image acquisition device operatively connected to said mobile computing device;
136 identify the payment code depicted within the captured image frame;
137 generating a purchase transaction request via the mobile computing device using the identified payment code;
138 providing the purchase transaction request for payment processing; and
139 A purchase receipt is obtained for the purchase transaction.

21.

143 A computer-implemented reverse snapshot payment method comprising:
144 obtaining user input at the user device to initiate a purchase transaction with a merchant;
145 obtain user payment information for processing said purchase transaction;
146 generating, by the user device, a payment code image using payment information for processing the purchase transaction;
148 displaying the payment code image for a point-of-sale terminal via a display operatively connected to the user device to capture an image of the payment code image; and
150 A purchase receipt is obtained for the purchase transaction.

22.

154 A computer-implemented group decomposition snapshot payment method, comprising:
155 obtaining user input at the user's user device to initiate a group purchase transaction;
156 obtaining purchase data for said group purchase transaction;
157 generating, by said user device, a disassembled payment code image using purchase data for said group purchase transaction;
159 wherein said disassembled payment code image includes information about another user's payment amount;
and
161 The split payment code image is displayed for another user device of the other user by a display operatively connected to the user device to obtain an image of the split payment code image.

23.

166 A computer-implemented person-to-person snapshot payment method comprising:
167 obtaining user input at the user's user device to initiate a person-to-person transaction;
168 obtaining a transfer amount for said person-to-person transaction;
169 generating, by said user device, a payment code image using a transfer amount for said person-to-person transaction;
171 wherein said payment code image includes information about the amount transferred by another user; and
172 The payment code image is displayed for another user device of the other user by a display operatively connected to the user device to obtain an image of the payment code image.

24.

177 A computer-implemented method of mobile selling on snaps, comprising:
178 obtaining a user checkout request at the point-of-sale device;
179 obtaining user shopping cart information about a merchant for use in processing purchase transactions associated with said user's checkout request;
181 using the user shopping cart information to generate a payment code image through the user device;
182 via a display operatively connected to the point-of-sale device, displaying the payment code image for user equipment to capture an image of the payment code image; and
184 An authorization notification is obtained for the purchase transaction.

25.

188 A computer-implemented reverse snapshot mobile selling method comprising:
189 obtaining a user checkout request at the point-of-sale device;
190 acquiring an image frame by an image acquisition device operatively connected to said point-of-sale device;
191 identify the payment code depicted within the captured image frame;
192 generating a purchase transaction request through said point-of-sale device using the identified payment code;
193 providing the purchase transaction request for payment processing; and
194 An authorization notification is obtained for the purchase transaction.



(12)发明专利申请

(10)申请公布号 CN 106803175 A

(43)申请公布日 2017.06.06

(21)申请号 201710037081.6

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038

(22)申请日 2012.02.16

代理人 张劲松

(30)优先权数据

61/443,624 2011.02.16 US

61/512,248 2011.07.27 US

61/522,213 2011.08.10 US

61/527,576 2011.08.25 US

(51)Int.Cl.

G06Q 20/36(2012.01)

(62)分案原申请数据

201280018719.7 2012.02.16

(71)申请人 维萨国际服务协会

地址 美国加利福尼亚

(72)发明人 A·哈曼德 I·卡彭科

M·加夫利洛夫 A·施里瓦斯塔瓦

M·卡尔森 P·哈里拉马尼

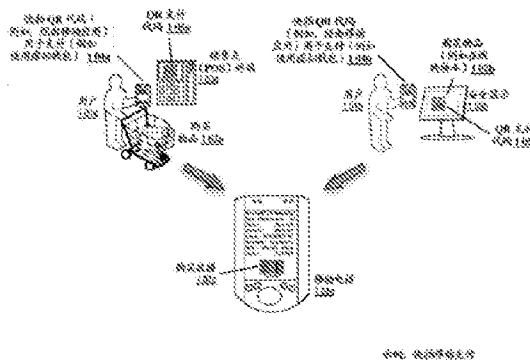
权利要求书3页 说明书46页 附图53页

(54)发明名称

快拍移动支付装置,方法和系统

(57)摘要

本发明公开了快拍移动支付装置,方法和系统。快拍移动支付装置、方法和系统(“SNAP”)经由SNAP部件传送实时产生的商家-产品快速响应代码到基于虚拟钱包卡的交易购买通知。在一个实施例中,该SNAP从移动设备获得出现在销售点设备的显示屏上的QR代码的快照。所述SNAP解码所述QR代码来获得包括在用户的结帐请求中的产品信息,以及商家信息以用于处理和提供该QR代码的商家的用户购买交易。所述SNAP访问用户虚拟钱包来获得用户账户信息以处理与商家的用户购买交易。所述SNAP利用该产品信息、商家信息和用户账户信息产生卡授权请求,SNAP提供其到支付网络用于交易处理。此外,所述SNAP获得确认用户购买交易的处理的购买收据。



CN 106803175 A

1. 一种计算机实现的快拍支付方法,包括:
在移动计算设备处获得用户输入来启动购买交易;
通过操作地连接至所述移动计算设备的图像获取设备获取图像帧;
识别在所获取的图像帧内描述的支付代码;
使用所识别的支付代码,通过所述移动计算设备产生购买交易请求;
提供所述购买交易请求用于支付处理;以及
获得用于所述购买交易的购买收据。
2. 如权利要求1所述的方法,还包括:
提供所述支付代码的图像用于购买交易处理。
3. 如权利要求1所述的方法,还包括:
通过包括在所述用户移动设备中的所述图像获取设备获取包括所述图像帧的视频;
从所获取的视频提取所述图像帧;以及
分析所述图像帧来确定所述图像帧是否包括所描述的支付代码。
4. 如权利要求1所述的方法,其中所述用户输入是在操作地连接至所述移动计算设备的触摸屏上的触摸屏手势。
5. 如权利要求1所述的方法,其中所述支付代码是一维条形码。
6. 如权利要求1所述的方法,其中所述支付代码是包括快速响应代码的二维条形码。
7. 如权利要求1所述的方法,还包括:
从所述支付代码提取购买会话数据;以及
其中所述购买交易请求是使用所提取的购买会话数据,通过所述用户移动设备产生的。
8. 如权利要求7所述的方法,其中所述购买会话数据包括商家标识符,以及用于和与所述商家标识符相关联的商家的用户购物会话的会话标识符。
9. 如权利要求8所述的方法,其中所述会话标识符被配置为用作关于和所述商家的用户购物会话的数据的统一资源定位符中的令牌参数。
10. 如权利要求1所述的方法,还包括:
获得与虚拟钱包帐户相关联的支付信息用于支付处理;
其中所产生的购买交易请求包括与所述虚拟钱包帐户相关联的所述支付信息。
11. 如权利要求10所述的方法,其中所述支付信息包括动态产生的卡验证值代码。
12. 如权利要求11所述的方法,还包括:
提供对动态产生的卡验证值代码的请求到服务器;以及
响应提供所述请求,从所述服务器获得所述动态产生的卡验证值代码。
13. 如权利要求12所述的方法,其中动态产生的卡验证值具有期满时间并且对应于和商家的用户购物会话。
14. 如权利要求1所述的方法,其中在所获取的图像帧内描述的所述支付代码是从媒体设备的显示器获取的,并且编码数据来购买所要求的媒体内容。
15. 如权利要求14所述的方法,其中所述媒体设备是电视。
16. 如权利要求15所述的方法,其中所述电视是飞机上娱乐系统的一部分。
17. 如权利要求16所述的方法,其中所述媒体设备正显示网页。

18. 一种计算机实现的快拍支付系统,包括:
处理器;以及
存储器,配置为与所述处理器通信并存储处理器可执行指令以:
在移动计算设备处获得用户输入来启动购买交易;
通过操作地连接至所述移动计算设备的图像获取设备获取图像帧;
识别在所获取的图像帧内描述的支付代码;
使用所识别的支付代码,通过所述移动计算设备产生购买交易请求;
提供所述购买交易请求用于支付处理;以及
获得用于所述购买交易的购买收据。
19. 一种计算机可读的有形介质,存储计算机可执行的快拍支付指令以:
在移动计算设备处获得用户输入来启动购买交易;
通过操作地连接至所述移动计算设备的图像获取设备获取图像帧;
识别在所获取的图像帧内描述的支付代码;
使用所识别的支付代码,通过所述移动计算设备产生购买交易请求;
提供所述购买交易请求用于支付处理;以及
获得用于所述购买交易的购买收据。
20. 一种计算机实现的快拍支付装置,包括装置以用于:
在移动计算设备处获得用户输入来启动购买交易;
通过操作地连接至所述移动计算设备的图像获取设备获取图像帧;
识别在所获取的图像帧内描述的支付代码;
使用所识别的支付代码,通过所述移动计算设备产生购买交易请求;
提供所述购买交易请求用于支付处理;以及
获得用于所述购买交易的购买收据。
21. 一种计算机实现的反向快拍支付方法,包括:
在用户设备处获得用户输入来启动和商家的购买交易;
获得用于处理所述购买交易的用户支付信息;
通过所述用户设备使用用于处理所述购买交易的支付信息产生支付代码图像;
通过操作地连接至所述用户设备的显示器,为销售点终端显示所述支付代码图像以获取所述支付代码图像的图像;以及
获得用于所述购买交易的购买收据。
22. 一种计算机实现的群组分解快拍支付方法,包括:
在用户的用户设备处获得用户输入来启动群组购买交易;
获得用于所述群组购买交易的购买数据;
通过所述用户设备,使用用于所述群组购买交易的购买数据产生分解支付代码图像;
其中所述分解支付代码图像包括有关另一个用户的支付金额的信息;以及
通过操作地连接至所述用户设备的显示器,为所述另一个用户的另一个用户设备显示所述分解支付代码图像以获取所述分解支付代码图像的图像。
23. 一种计算机实现的个人对个人的快拍支付方法,包括:
在用户的用户设备处获得用户输入来启动个人对个人的交易;

获得用于所述个人对个人的交易的转帐金额；
通过所述用户设备,使用用于所述个人对个人的交易的转帐金额产生支付代码图像；
其中所述支付代码图像包括有关另一个用户的转帐金额的信息；以及
通过操作地连接至所述用户设备的显示器,为所述另一个用户的另一个用户设备显示所述支付代码图像以获取所述支付代码图像的图像。

24. 一种计算机实现的快拍移动销售方法,包括:
在销售点设备处获得用户结帐请求；
获得关于商家的用户购物车信息用于处理与所述用户结帐请求相关的购买交易；
通过所述用户设备,使用所述用户购物车信息产生支付代码图像；
通过操作地连接至所述销售点设备的显示器,显示所述支付代码图像以使用户设备获取所述支付代码图像的图像；以及
获得所述购买交易的授权通知。

25. 一种计算机实现的反向快拍移动销售方法,包括:
在销售点设备处获得用户结帐请求；
通过操作地连接至所述销售点设备的图像获取设备获取图像帧；
识别在所获取的图像帧内描述的支付代码；
使用所识别的支付代码,通过所述销售点设备产生购买交易请求；
提供所述购买交易请求用于支付处理；以及
获得所述购买交易的授权通知。

快拍移动支付装置,方法和系统

[0001] 本申请是基于申请号为201280018719.7、申请日为2012年2月16日、发明名称为“快拍移动支付装置,方法和系统”的专利申请的分案申请。

[0002] 本专利申请公开文档(在下文中称“说明书”)描述指导各个新的革新(在下文中是新发明新技术和/或新方法)的发明方面并包含附属于版权,掩模工作和/或其它知识产权保护的材料。当它出现在公开的专利局文件/记录中时,这种知识产权的各个所有人不反对任何人作出专利公开文档的传真再现,但在别的方面保留所有权利。

[0003] 优先权声明

[0004] 本申请按照35USC\$119,要求了下列优先权:于2011年2月16日申请的序号为61/443,624、标题为“移动捕获结帐装置、方法和系统”,代理人编号为P-42032PRV|20270-127PV的美国临时专利申请;2011年7月27日申请的序号为61/512,248,标题为“快拍移动支付装置,方法和系统”,代理人编号为10US01|20270-175PV的美国临时专利申请;2011年8月10日申请的序号为61/522,213,标题为“通用移动支付平台、装置、方法和系统”,代理人编号为10US03|20270-175PV2的美国临时专利申请;以及2011年8月25日申请的序号为61/527,576,标题为“快拍移动支付装置、方法和系统”,代理人编号为10US02|20270-175PV1的美国临时专利申请。将前述的申请的整个教导在此引入,以供参考。

技术领域

[0005] 本发明一般地涉及用于电子购买交易的装置、方法和系统,具体而言,涉及快拍移动支付装置、方法和系统(“SNAP”)。

背景技术

[0006] 顾客交易通常需要顾客从商品陈列架或网站选择产品,然后在结帐柜台或网页上结帐。产品信息通常是从网页目录或进入销售点终端设备中被选择出来的。在物理零售环境中,产品信息是通过利用集成的条形码扫描器在销售点记录器上扫描物品条型码而自动输入的,以及顾客通常被配有多个支付选项,诸如现金、支票、信用卡或借记卡。一旦支付被提出并同意,所述销售点记录器在商家的计算机系统中存储所述交易,以及产生表示所述交易圆满结束的收据。

附图说明

[0007] 根据本发明的发明方面,所述附录和/或附图非限制的举例说明了根据本发明的各个示例、发明的方面:

[0008] 图1A-F示出了说明了在SNAP的一些实施例中的基于快拍移动支付的购买交易的示例方面的框图;

[0009] 图2A-F示出了在所述SNAP的一些实施例中,说明帮助快拍移动支付的快拍移动支付应用的示例特征的应用程序用户界面图;

[0010] 图3A-E示出了在所述SNAP的一些实施例中,说明用于捕获产品条型码、保护用户

数据并防止欺诈的快拍移动支付应用的示例特征的应用程序用户界面图；

[0011] 图4A-D示出了在所述SNAP的一些实施例中,说明示例快拍移动支付过程的数据流程图；

[0012] 图5A-E示出了在所述SNAP的一些实施例中,说明实行快拍移动支付的示例方面的逻辑流程图,例如快拍移动支付执行(“SMPE”)部件500；

[0013] 图6A-B示出了在所述SNAP的一些实施例中,说明处理快速响应代码的示例方面的逻辑流程图,例如快速响应代码处理(“QRCP”)部件600；

[0014] 图7示出了在所述SNAP一些实施例中,说明虚拟钱包应用的示例特征的概述的用户界面图；

[0015] 图8A-G示出了在所述SNAP的一些实施例中,说明购物模式中的虚拟钱包应用的示例特征的用户界面图；

[0016] 图9A-F示出了在所述SNAP的一些实施例中,说明支付模式中的虚拟钱包应用的示例特征的用户界面图；

[0017] 图10示出了在所述SNAP一些实施例中,说明历史模式中的虚拟钱包应用的示例特征的用户界面图；

[0018] 图11A-F示出了在所述SNAP的一些实施例中,说明快拍模式中的虚拟钱包应用的示例特征的用户界面图；

[0019] 图12示出了在所述SNAP一些实施例中,说明报价模式中的虚拟钱包应用的示例特征的用户界面图；

[0020] 图13A-B示出了在所述SNAP的一些实施例中,说明安全和隐私模式中的虚拟钱包应用的示例特征的用户界面图；

[0021] 图14示出了说明SNAP控制器的实施例的框图。

[0022] 所述附图内的每个附图标记的前沿的数字表示其中附图标记被引入和/或详细描述的附图。因而,附图标记101的详细论述将在附图1中出现和/或被引用,附图标记201被引进附图2中等等。

具体实施方式

[0023] 快拍移动支付(SNAP)

[0024] 所述快拍移动支付装置、方法和系统(在下文中“SNAP”)通过SNAP部件将实时产生的商家产品的快速响应代码转换为基于卡的虚拟钱包的交易购买通知。图1A-F示出了说明在SNAP的一些实施例中的基于快拍移动支付的购买交易的示例方面的框图。参见附图1A,在一些实现方式中,例如101a-b的用户可能希望在例如103a的商家商店或在例如103b的商家网站购买产品。例如,在商家商店,用户可在例如103a的商店中的销售点(“POS”)终端上扫描多个产品(例如102a)的条型码,然后指示用户希望结帐的扫描物品。在一些实现方式中,所述POS终端经由支付网络产生包括扫描的产品物品相关的信息,以及用于处理所述购买交易的商家信息的快速响应(“QR”)代码,例如105a。用户使用诸如智能电话的用户设备可捕获由所述POS终端产生的所述QR代码的图像。例如,所述用户设备可以具有用于迅速获取所述商家产品QR代码的应用。所述用户设备可使用从所述QR代码中提取的信息,连同有关绑定到用户设备的虚拟钱包的信息一起来启动购买交易。例如,所述用户设备可使

用从所述QR代码中提取的所述产品和商家信息以及来自所述虚拟钱包的金融支付信息来建立购买交易请求,并将所述请求提交到支付网络(例如,信用卡处理网络)。

[0025] 在一些实现方式中,所述用户设备可使用捕获QR代码的替换方法来从所述POS终端获得信息。例如,所述POS终端可经由蓝牙™、Wi-Fi、SMS、文本信息、电子邮件、和/或其它通信方法来传递提交购买交易请求到支付网络所需的信息到用户设备。

[0026] 在一些实现方式中,用户101b可能希望对存储在例如102b的在线商店网站上的虚拟购物车中的物品结账。例如,用户可以使用安全显示器(例如,所述用户的信任计算设备的一部分)浏览所述网站。当指示用户希望对所述虚拟购物车的物品结账,所述网站可提供包括有关所述虚拟购物车中的产品和商家信息的信息的QR代码。例如,在其中所述用户使用安全显示器的情况中,为安全目的,QR代码可以被显示在所述安全显示器内的随机位置。所述用户可获取所显示的QR代码的快照,并使用来自与所述用户设备相关联的虚拟钱包的支付信息来创建购买交易请求以便由支付网络处理。当购买交易完成时,支付网络直接向用户设备106、商店中的所述POS终端和/或所述安全显示器(用于安全的在线购物情况)提供例如107的购买收据,作为交易处理完成的确认。因此,在一些实现方式中商家可以在处理所述购买交易时被屏蔽以免获得用户的个人和/或私人信息,同时使用用于呈现商家产品QR代码的安全显示器来确保所述用户的虚拟钱包的完整性。

[0027] 在各个实现方式中,这种支付处理可以被用于各式各样的交易。例如,在餐厅用餐的用户可获得包括QR支付代码的帐单,QR支付代码包括关于包括在该账单中的餐费的细节,以及该餐厅的商家ID。在没有向该餐厅披露关于该用户的任何金融或个人信息的情况下,用户可使用用户的智能电话给该餐厅账单拍快照,以及使用用户的虚拟钱包为支付该餐厅账单。

[0028] 参见附图1B,在一些实现方式中,例如110,用户111可能希望使用反向快拍移动支付过程来结账存储在(在线)商店例如112中的(虚拟)购物车中的物品。例如,用户可使用作为用户的信任计算设备的一部分的安全显示器,例如113,或经由实体商店中的POS终端浏览网站。当指示用户希望结账所述虚拟购物车中的物品时,用户可经由连接至该用户的虚拟钱包的用户移动设备上的移动应用生成(例如114)包括有关该用户的支付方式、报价、回报、和/或其它方面的信息的QR代码115b。该用户可提供显示在用户移动设备上的该QR代码给安装在信任计算设备(或POS终端)上的网络摄像机(或其它QR代码捕捉设备和/或机制)。用户的信任计算设备或POS终端可获得由该用户的移动设备产生的该QR代码的快照,例如116,并且利用来自该用户产生的QR代码的支付信息来创建购买交易请求,以用于支付网络进行处理。当完成该购买交易时,该支付网络可直接向用户移动设备、商店中的POS终端和/或安全显示器(用于安全的在线购物情况)提供购买收据,作为交易处理完成的确认。因此,在一些实现方式中,该用户将能使用由该用户的移动设备产生的QR代码作为塑料支付卡(例如信用、借记、预付卡)的替代,或作为其它诸如近场通信、蓝牙®等等的金融信息传输机制的代替。在一些实现方式中,该QR代码可以是一次性匿名的信用卡号码的代表(例如,参见与附图3B相关联的说明)。

[0029] 在一些实现方式中,第一用户121b可能希望支付给第二用户121a某金额(或等价物,例如虚拟货币、替代货币、回报、里程、点数等等),例如P2P快拍移动支付120。第二用户121a可产生限制时间有效性的QR代码,例如122,包括关于将被转帐的该金额以及链接到第

二用户的金融账户的隐私记号/别名的信息。第二用户可向第一用户显示产生的该QR代码(例如,通过维持第二用户的移动电话向第一用户显示该QR代码;通过电子邮件、社交网络消息、推特等等发送该QR代码)。第一用户使用第一用户的移动电话给该QR代码拍快照,例如123,并且使用该金额、第二用户的链接到金融账户的隐私记号/别名、以及链接到该第一用户的移动电话的第一用户的虚拟钱包,来产生用于由该支付网络处理的购买交易请求。当该交易完成时,该支付网络可向作为交易当事方的用户提供交易通知收据。在作为替代的实现方式中,该两个用户可经由该QR代码的备用方法共享在该QR代码中编码的数据,包括但不限于:近场通信(NFC)、Wi-Fi™、蓝牙™、蜂窝网络、SMS、电子邮件、文本消息和/或其它通信协议。

[0030] 通常,应该理解的是,在快拍移动支付的各个实现方式中,这种记号、别名和/或处理可以被有利地使用。例如,希望参与反向快拍移动支付过程(参见,例如附图1B,元件110)的用户可产生包含关于指向存储在支付网络系统的服务器上的金融支付信息的句柄(handle)的信息的QR代码。例如,快拍移动支付的一些实现方式可使用支付象征过程来产生和/或处理句柄,支付象征过程与编号为13/153,301、标题为“支付象征装置方法以及系统”的美国申请所描述的内容相似,此处该内容通过引用被明确地包括在此。此外,在一些实现方式中,该句柄可根据简洁消息传递协议编码信息,诸如在编号为6,837,425,标题为“简洁协议以及解决便携式消费者设备和基础设备之间基本上离线消息传递的方法”的美国专利中描述的,此处通过引用其整个内容被明确地包括在此。在一些反向快拍移动支付实现方式中,用户可提供包含有该句柄并显示在用户的移动设备上的该QR代码给安装在信任计算设备(或POS终端)上的网络摄像机(或其它QR代码捕捉设备和/或机制)。该用户信任的计算设备或POS终端可获得由该用户的移动设备产生的QR代码的快照,例如116,并为由该支付网络处理的购买交易请求提供从该QR代码中提取的句柄给商家服务器。为了使用该句柄处理该购买交易,该商家服务器可产生卡授权请求(诸如参考附图4A在以下的讨论中进一步描述的),并提供该卡授权请求给支付网络。当完成该购买交易时,该支付网络可直接向用户移动设备、该商店中的该POS终端和/或该安全显示器(例如用于安全的在线购物情况)提供购买收据,作为使用该句柄的交易处理完成的确认。

[0031] 在一些实现方式中,用户警告机制可以被建立到快拍移动支付购买交易处理流程中。例如,在一些实现方式中,商家服务器可嵌入专用于该交易的URL到卡授权请求中。例如,在一些实现方式中,POS终端、远程设备和/或台式计算机可在卡授权请求中将该URL嵌入到可选的层3数据中。该URL可指向存储在作为卡授权请求的主体的专用于该交易的商家服务器上的网页。例如,由该URL指向的网页可包括关于该购买交易的细节,例如被购买的产品、进货成本、时间期满、订单处理的状态等。因此,通过传递该网页的URL给该支付网络,商家服务器可向该支付网络提供该交易的细节。在一些实现方式中,该支付网络可提供通知给用户,诸如支付收据、交易授权确认消息、运输通知等。在这种消息中,该支付网络可提供该URL给用户设备。该用户可在用户的设备上导航到该URL来获得关于该用户的购买的警告,以及其他的消息,诸如报价、优惠券、相关产品、回报通知等。

[0032] 在一些实现方式中,多个用户可经由快拍移动支付可参与群组支付来分解偿付(tender),例如130。在一些实现方式中,用户之一131a可获得在例如133的POS终端处生成的(或例如在诸如用餐账单的纸上呈现的)QR支付代码(例如134)的快照(例如132)。该用户

可又生成QR分解支付代码,包含有关于该偿付已经被分解为的金额的信息。该用户131a可呈现该分解的偿付QR代码135给其他用户131b-c,用户131b-c可获得该分解的偿付QR代码的快照,例如136。在一些实现方式中,为了该原始QR代码的支付,该用户131b-c可以经由该支付网络偿还用户131a,或用户131b-c可以经由该分解的偿付QR代码进行直接支付给该商家(例如,当该用户131a给该商家的QR代码拍快照的时候,没有立即发生支付处理)。在一些实现方式中,该商家可为用户131a-c直接提供分解偿付QR代码。

[0033] 在一些实现方式中,通过使用作为替代的通信机制可以实现群组移动支付,而不是使用QR代码。例如,在一些实现方式中,该POS终端133可使用诸如蓝牙™的通信协议来与用户131a-c通信。该POS终端可串行或并行地与每一个用户建立独立的通信会话。通过这些独立的通信会话,POS终端可传输该用户的设备所需要的产品和/或商家数据来产生各个购买交易处理请求。因此,通过这些独立的通信会话,POS终端可将与用户131a-c相关联的群组偿付分解成单个支付金额。

[0034] 参见附图1C,在一些实现方式中,为了认证/验证目的,以及为了提供用于公开个人和/或私人信息的数字准许,可以使用快拍移动付帐方式。例如,拜访他/她的医生143的用户142可能被要求提供正式准许来向该医生公开个人信息(例如病历)。该医生的终端(例如144)可产生包含有这个医生数字凭证以及有关被请求的用户的病历的类型/内容的信息的QR代码。用户可通过该用户的移动设备对该QR代码拍快照。用户的移动设备可根据该QR代码产生记录释放的请求,以及用作该请求是从个人信任设备(例如该用户的移动设备)获得的验证。在作为替代的实现方式中,用户能够选择该用户意欲向医疗供应商披露的个人信息,以及该用户的移动设备可产生一QR代码以用于该医生的终端来获得快照以便检索该用户的医疗信息。在一些实现方式中,该QR代码也可以包括支付信息(例如用户的支付帐户信息,或该医生的收单机构信息)以及有关个人信息的受控释放的信息。

[0035] 在一些实现方式中,SNAP可通过预先填充可变更的QR支付代码来辅助P2P交易,例如150。例如,具有公开的简档页面(例如151)的第一用户可放置QR代码的图像在公开的简档中,例如152。例如,该QR代码可包括预先确定的支付金额用于通过获取该QR代码的快照发起的购买交易。在一些实现方式中,该预定的金额可以是\$0(例如,\$0QR支付代码)。第二用户可使用移动设备来捕捉该QR支付代码的快照,并可通过第二用户的移动设备来设置第二用户意欲支付第一用户的金额。第二用户的移动设备可给用于交易处理的支付网络提供在该QR代码内编码的信息以及第二用户选择的支付金额。

[0036] 应该理解的是,可以使用此处描述的快拍移动支付的各个方面以用于信息的任何受控交换和/或支付。例如,参考附图1D,在一些实现方式中,用户可通过快拍移动支付获得按次计费的节目,例如160。例如,电视显示器可提供包括节目信息(例如162)的广告以及QR支付代码用于获得该节目内容,例如161。该QR代码包括标识该节目信息的信息,以及标识该电视预订者帐户信息、电视机地址等的信息。该用户可获得该QR代码的快照,并提供嵌入在该QR代码中的信息以及该用户的移动设备的信息(例如,链接到该用户的虚拟钱包的预订者帐号、付款帐户信息等)。当通过支付网络处理支付信息时,该支付网络可将支付完成的指示提供给电视节目供应商,并且该电视节目供应商可放出节目内容到用户的电视。作为另一例子,相似流程可以被用于飞机上的娱乐活动,例如170,其中飞机上的屏幕可提供节目信息172以及QR支付代码171以供用户快拍来用于飞机上娱乐活动的启动。作为另一例

子, 广告牌、壁挂、海报、商店内广告、临时围墙等等, 例如180, 可包括用于产品/服务的报价, 以及包括商家信息和标识购买量的产品信息的QR代码等。用户可利用链接到该用户的虚拟钱包的用户的移动设备来对该QR代码拍快照, 以购买该产品和/或服务, 以及, 如果合适, 该产品可以被直接按照与该支付网络交换的作为用户的移动设备发送的购买请求的一部分的购买信息说明的地址运往用户地址处。作为另一例子, 报纸, 例如185, 可包括报价、广告、工作邮寄等, 其包含有QR代码, 例如186, 其中包含有用户利用支付网络发起购买交易所必须的信息。应该理解的是, 在此处论述的任何其它实现方式和/或他们的等价物中, 可以使用实现此处实现方式中论述的快拍移动支付的任何方面, 和/或他们的等价物。

[0037] 参见附图1E-F, 在一些实现方式中, 处理购买交易所需的数据可以通过替换QR代码的方法来提供, 包括但不限于: 近场通信(NFC)、Wi-Fi™、蓝牙™、蜂窝网络、SMS、电子邮件、文本消息和/或其它通信协议。例如, 在一些实现方式中, 通过在客户端设备上执行的网络浏览器进行在线购物的用户, 例如190, 可能希望从在线商店网站(例如191)对物品的购买进行支付。该网站可包括用户界面元件, 用户可激活其来发起购物结帐和支付。当该用户激活该用户元件时, 显示在线购物网站的客户端可提供消息给商家的服务器来发起安全购买交易处理。运行该在线购物网站的商家服务器可建立安全连接(例如安全套接字层连接)到支付网络(例如192)的支付网络服务器。并且, 该支付网络服务器可建立安全连接到该客户端。例如, 该客户端可包括安全I/O芯片, 其仅仅允许通过该客户端和该支付网络的支付网络服务器建立安全连接。通过安全连接, 该支付网络服务器可提供指令到该客户端来请求用户启动该用户的用户设备上的虚拟钱包移动应用, 参见例如附图1F, 196。该客户端可因此提供请求给用户来启动该用户的用户设备(例如193)上的虚拟钱包移动应用。当用户启动该用户设备上的虚拟钱包移动应用时, 该用户设备和该客户端可互相建立安全连接(例如通过蓝牙™、Wi-Fi、蜂窝等等)。在一些实现方式中, 该客户端和用户设备可以被预先配置来互相快速地建立该安全通信通道。通过该安全通信通道, 该客户端可提供数据给用户的移动设备, 或反之亦然, 来帮助该购买交易的启动。该用户的移动设备(或客户端)上的虚拟钱包应用然后可以产生购买交易启动消息并提供这消息到支付网络服务器以用于处理该购买交易。当交易处理完成时, 支付网络服务器可提供支付完成的通知到该客户端, 例如附图1F的197, 或到该用户设备。

[0038] 图2A-F示出了在该SNAP的一些实施例中, 示出帮助快拍移动支付的快拍移动支付应用的示例特征的应用程序用户界面图。参见附图2A, 在一些实现方式中, 用户可能希望对存储在在线商家网站的虚拟购物车中一个或多个物品结帐。例如, 用户可以使用浏览器应用, 例如201, 来视觉化该商家网站的结帐页面, 例如202。该结帐网页可描述该结帐定单的细节, 例如203, 并可为用户提供一个或多个选项来为存储物品的购买提供支付。在一些实现方式中, 该结帐网页可包括选项来使用快拍移动支付过程支付该购买, 例如204。

[0039] 参见附图2B, 在一些实现方式中, 当选择使用该快拍移动支付过程的选项时, 商家结帐网页, 例如206, 可通过该浏览器应用205提供QR代码, 例如209, 其包括有关虚拟购物车中物品的信息和商家信息以便支付网络处理该购买交易(例如链接到商家的收单机构金融账户的私人记号/别名)。在一些实现方式中, 该网页可以通过用户的信任计算设备的安全显示器来显示。例如, 作为安全措施, 该显示器内的QR代码框架的位置, 例如207, 可以被随机地改变来防止该QR代码的快照被通过欺诈手段(例如对该信任计算设备的篡改)获得。在

一些实现方式中,由用户预先选择的安全图像,例如208,可以被显示在屏幕上以便用户可以验证为是准确的。在一些实现方式中,在提供图像到信任计算设备以前,该图像可以由SNAP加密。在一些实现方式中,信任计算设备可以是保存解密并且成功地在安全显示器上向用户显示该图像的所需要的解密密钥的唯一设备。

[0040] 参见附图2C,在一些实现方式中,这种包含QR代码的商家产品信息可以被销售点(“POS”)终端使用,例如210a-b。例如,在实体店中,当该用户指示其希望对用户的物理购物车中的物品结账时,POS终端可显示QR代码,例如211a-b,其包括购买支付金额,例如212a-b。例如,该QR代码可包括根据可扩展标记语言(“XML”)格式化的数据,诸如以下示例的数据结构:

[0041]

```

<QR_data>
  <order_ID>4NFD4RG94</order_ID>
  <timestamp>2011-02-22 15:22:43</timestamp>
  <expiry_lapse>00:00:30</expiry_lapse>
  <transaction_cost>834.78</transaction_cost>
  <user_ID>john.q.public@gmail.com</user_ID>
  <client_details>
    <client_IP>192.168.23.126</client_IP>
    <client_type>smartphone</client_type>
    <client_model>HTC Hero</client_model>
    <OS>Android 2.2</OS>
    <app_installed_flag>true</app_installed_flag>
  </client_details>
  <secure_element>www.merchant.com/securedyn/0394733/123.png</secure_element>
  <purchase_details>
    <num_products>1</num_products>
    <product>
      <product_type>book</product_type>
      <product_params>
        <product_title>XML for dummies</product_title>
        <ISBN>938-2-14-168710-0</ISBN>
        <edition>2nd ed.</edition>
        <cover>hardbound</cover>
        <seller>bestbuybooks</seller>
      </product_params>
      <quantity>1</quantity>
    </product>
  </purchase_details>
  <merchant_params>
    <merchant_id>3F8CR4INC</merchant_id>
    <merchant_name>Books & Things, Inc.</merchant_name>
    <merchant_auth_key>1NMF484KCF59CH827365</merchant_auth_key>
  </merchant_params>
</QR_data>

```

[0042] 参见附图2D,在一些实现方式中,用户可使用智能电话(例如213)获得被显示在安全显示器或该POS终端的屏幕上的该QR代码的快照。例如,该用户的智能电话可以在其上运行以检测和捕捉QR代码(例如216a)的应用,例如214。例如,该用户可使用注册特征,例如215,来在该智能电话的显示器内对其该QR代码。在一些实现方式中,该应用可为用户提供放大(例如217)或缩小(例如218)该QR代码的能力,来确保该QR代码的图像符合该智能电话的屏幕的尺寸。当在该智能电话的显示器内对其QR代码时,用户将能使用用户界面元件例如219来获得该QR代码的快照。该用户可使用该智能电话的显示器上的用户界面元件220取

消该快拍移动支付过程。

[0043] 参见附图2E,在一些实现方式中,当获得该商家产品QR代码的快照时,用户的智能电话可提取存储在该QR代码内的产品以及商家数据,并使用链接到该用户的智能电话的用户虚拟钱包的账号来产生购买交易请求,以用于由支付网络处理。当完成由该支付网络使用户的智能电话提供的信息处理该支付交易时,商家网站222(通过该浏览器应用221)可为该用户提供购买收据225。参见附图2F,在其中用户在实体店使用该快拍移动支付过程的实现方式中,该POS终端可为用户显示购买收据。在一些实现方式中,该支付网络可直接给该用户的智能电话提供买方收据。

[0044] 图3A-E示出了在该SNAP的一些实施例中,举例说明用于捕获产品条形码、保证用户数据安全并防止欺诈的快拍移动支付应用的示例部件的应用程序用户界面图。参见附图3A,在一些实现方式中,在用户的设备上执行的应用可包括为该用户提供各个特征的应用接口。在一些实现方式中,该应用可以被配置为识别产品标识符(例如条形码、QR代码等等),例如301。例如,该应用可以被配置为捕捉商家产品QR代码以用于快拍移动支付处理,如上参考附图2A-F所讨论的。在一些实现方式中,可能需要用户登陆到该应用来启动它的特征。一旦被启动,摄像机可为该用户提供亲身般一次轻敲购买特征。例如,该客户端设备可具有摄像机,应用通过其可获取图像,视频数据、流现场视频等,例如303。该应用可以被配置为分析输入数据并检索(例如301)产品标识符,例如304,诸如QR代码209、211a-b、216a和227。在一些实现方式中,该应用可覆盖十字线、目标框,和/或类似对准参考标记,例如305,以使用户可使用该参考标记对准该产品标识符,从而帮助产品标识符的识别和解释。在一些实现方式中,该应用可包括接口元件来允许用户在产品识别模式和产品报价接口显示屏幕之间来回切换(参见例如306),以使用户在捕捉产品标识符以前可准确地研究对用户可用的交易。在一些实现方式中,该应用可为用户提供浏览先前的产品标识符捕捉(参见例如307)的能力,以便该用户将能更好地决定哪个产品标识符是用户希望捕捉的。在一些实现方式中,用户可能希望取消产品购买;该应用可为用户提供用户界面元件(例如308)来取消产品标识符识别过程并返回到用户原来使用的先前界面屏幕。在一些实现方式中,可以例如以列表形式(参见例如309)为该用户提供关于产品、用户设置、商家、报价等的信息,以使用户可以更好理解用户的购买选项。在应用中可提供各种其他特征(参见例如310)。

[0045] 参见附图3B,在一些实现方式中,该应用可包括用户的位置的指示(例如商家商店的名称、地理位置,与商家商店内的走廊有关的信息,等等),例如311。该应用可提供用于产品购买的应付金额的指示,例如312。在一些实现方式中,该应用可为用户提供各种选项来支付用于购买产品的金额。例如,该应用可使用GPS坐标来确定该用户所在的商家商店,并指引用户到该商家的网站。在一些实现方式中,SNAP可提供API来直接参与商家以帮助交易处理。在一些实现方式中,标记商家的SNAP应用可以被开发具有SNAP功能,其可直接连接用户到商家的交易处理系统。例如,用户可从各个卡供应商(例如313)的多个卡(例如信用卡、借记卡、预付卡等等)中选择。在一些实现方式中,该应用可给用户提供的选项来使用包括在用户的银行帐户例如支票、存款、金融市场、当前帐户等等(例如314)中的资金支付购买金额。在一些实现方式中,用户可以通过该应用设置默认选项来设置哪个卡、银行帐户等要用于该购买交易。在一些实现方式中,这种缺省选项的设置可允许用户通过单个点击、轻敲、扫和/或其它校正的用户输入动作发起该购买交易,例如315a。在一些实现方式中,当用户

使用这种选项的时候,该应用可使用该用户的默认设置来发起该购买交易。在一些实现方式中,该应用允许用户使用其它帐号(例如Google™结帐,Paypal™帐号等等)来支付该购买交易,例如316。在一些实现方式中,该应用允许用户使用回报点、航线里程、旅馆积分、电子优惠券、打印的优惠券(例如通过与产品标识符相似的方式捕捉打印的优惠券)等等来支付该购买交易,例如317-318。在一些实现方式中,该应用在发起购买交易以前提供选项来提供快速授权,例如319。在一些实现方式中,该应用可在用户已经选择某选项来发起该购买交易以后提供进度指示符来提供关于该交易的进度的指示,例如320。在一些实现方式中,该应用可给用户关于该用户先前通过该应用进行的购买的历史信息,例如321。在一些实现方式中,该应用可给用户选项来与其它用户共享关于该购买的信息(例如,通过电子邮件、SMS、Facebook[®]上的墙贴、Twitter™上的推特,等等)和/或控制与商家、收单机构、支付网络等等共享的信息,以处理该购买交易,例如322。在一些实现方式中,该应用可给用户选项来显示由客户端设备捕捉的产品识别信息(例如以便在离开商店时显示该产品信息的客户服务代表),例如324。在一些实现方式中,该用户、应用、设备和/或SNAP在处理中可能遇到错误。在这种情况下,用户将能和客户服务代表聊天(例如VerifyChat 323)来解决该购买交易过程中的困难。

[0046] 在一些实现方式中,用户可选择使用一次性的匿名信用卡号码来进行交易,例如参见315b。例如SNAP可使用一组预先指定的匿名卡细节(参见,例如“AnonCard1”,“AnonCard2”)。作为另一例子,SNAP可能例如实时产生一组一次性的不记名卡细节来安全地完成购买交易(例如Anon It 1X)。在这种实现方式中,该应用可自动设置用户简档设置,以使用户的任何个人识别信息将不能被提供给商家和/或其它实体。在一些实现方式中,用户需要输入用户名和密码来启动不记名特征。

[0047] 参见附图3C,在一些实现方式中,该快拍移动支付应用的用户界面元件可以有利地被配置成以应用于该用户的移动设备的最小数量的用户手势来为用户提供利用自定义支付参数处理购买的能力。例如,可以为用户提供超负荷用户界面元件,例如325-326。例如,如果用户在包括在用户的移动设备中的摄像机的视角内具有QR支付代码,那么该用户可激活元件325来给QR代码拍快照并使用预先确定的默认设置来基于该QR代码处理该购买。然而,如果用户希望自定义支付参数,那么该用户可启动用户界面元件326(例如按压并连续保持)。这样做时,该应用可提供弹出菜单,例如327,其提供各种支付定制选择,诸如先前提供的那些。例如,用户可拖动用户手指到用户喜欢的适当设置,并从用户的移动设备的触摸屏释放用户手指来选择该设置用于支付处理。在可选实现方式中,该支付设置选项,例如330,以及QR捕捉激活按钮,例如328a-b(例如328b可提供比显示在初始屏幕中的那些甚至更多的设置)可以和窗口(例如329)一起被包括在用户界面中,以用于通过移动设备的摄像机捕捉该QR代码。在作为替代的实现方式中,该用户的移动设备可产生混合QR代码支付设置图形,并且POS终端(或用户的信任计算设备)可捕捉该整个图形用于支付处理。

[0048] 参见附图3D,在一些实现方式中,用户可以有利地能够在产生用于购买交易的QR代码的设备中提供用户设置,然后使用该用户的移动设备捕捉该QR代码。例如,销售点终端的显示设备可以显示结帐屏幕,诸如在客户端上运行的网络浏览器,例如331,显示在线购物网站的结帐网页,例如332。在一些实现方式中,结帐屏幕可提供用户界面元件,例如333a-b,借此用户可以指示使用快拍移动支付的希望。例如,如果用户激活元件331a,该网

站可使用用户的默认设置产生QR代码,并在客户端的屏幕上显示该QR代码(例如335)来便于用户使用用户的移动设备捕捉。在一些实现方式中,用户能激活用户界面元件,例如333b,借此客户端可显示具有用户可从中选择的附加选项的弹出菜单,例如334。例如,网站可给用户与上述参见附图3B-C的说明中所讨论的相似的选项。在一些实现方式中,当用户修改通过激活该用户界面元件333b而提供的设置时,该网站可实时修改该QR代码335。一旦用户已经使用弹出菜单修改了设置,用户就可捕捉该QR代码的快照来发起购买交易处理。

[0049] 参见附图3E,在一些实现方式中,SNAP可向用户提供用户界面来修改用户的快拍移动支付设置。例如,该SNAP可提供网络界面,例如341。例如,用户能使用该网络界面修改该用户的虚拟钱包的安全设置,例如342。例如,该用户可浏览信任设备的列表,例如344,用户通过该列表可访问该用户的虚拟钱包。在一些实现方式中,该网络界面可提供用户界面元件来添加信任设备,例如343。该网络界面也可以为用户提供附加安全选项。例如,该用户能够设置安全密码(例如345),更改关于在授权购买交易以前用户何时应被询问的设置(例如346),安全特征的表示的类型/风格(例如347),以及将被显示在快拍移动支付中使用的终端上的安全图像(例如348)。在各个实现方式中,用户能访问包括修改用户简档、帐号、帐号偏好、添加卡、获得报价以及优惠券、定位ATM机等等的其它服务。

[0050] 图4A-D示出了在该SNAP的一些实施例中,说明示例快拍移动支付过程的数据流程图。参见附图4A,在一些实现方式中,例如401的用户可能希望通过商家在线站点或商家的商店,从例如403的商家购买产品、服务、报价等(“产品”)。用户可通过客户端,诸如但不限于个人计算机、移动设备、电视、销售点终端、商亭、ATM等(例如402),与例如403的商家服务器通信。例如,用户可提供指示用户希望购买产品的用户输入(例如结帐输入411)到客户端中。例如,商家商店中的用户可通过在销售点终端的条形码扫描器扫描产品的产品条形码。作为另一例子,用户可从商家网站的网页目录选择产品,并添加产品到该商家网站上的虚拟购物车。用户然后可以指示用户希望结帐该(虚拟)购物车中的物品。客户端可产生例如412的结帐请求,并提供该结帐请求(例如413)到商家服务器。例如,客户端可以根据可扩展标记语言(XML)格式化的数据的形式为商家服务器提供包括产品细节的(安全)超文本传输协议(“HTTP(S)”)GET消息。以下是用于商家服务器的包括XML格式的结帐请求的示例HTTP(S)GET消息:

```

GET /checkout.php HTTP/1.1
Host: www.merchant.com
Content-Type: Application/XML
Content-Length: 718
<?XML version = "1.0" encoding = "UTF-8"?>
<checkout_request>
  <session_ID>48FY48G94</session_ID>
  <timestamp>2011-03-23 15:22:43</timestamp>
  <user_ID>john.q.public@gmail.com</user_ID>
  <client_details>
    <client_IP>192.168.33.126</client_IP>
    <client_type>smartphone</client_type>
    <client_model>HTC Hero</client_model>
    <OS>Android 2.2</OS>
    <app_installed_flag>true</app_installed_flag>
  </client_details>
  <purchase_details>
    <num_products>1</num_products>
    <product>
      <product_type>book</product_type>
      <product_params>
        <product_title>XML for dummies</product_title>
        <ISSN>938-2-14-168710-0</ISSN>
        <edition>2nd ed.</edition>
        <cover>hardbound</cover>
        <seller>beathuybooks</seller>
      </product_params>
      <quantity>1</quantity>
    </product>
  </purchase_details>
</checkout_request>

```

[0052] 在一些实现方式中,该商家服务器可从客户端获得该结账请求,并从该结账请求提取该结账细节(例如,XML数据)。例如,商家服务器可使用解析器,诸如如下参见附图14所论述的示例解析器。该商家服务器可从该结账请求提取 该产品数据以及客户端数据。在一些实现方式中,该商家服务器可查询(例如414)商家数据库(例如404)来获得产品数据(例如415),诸如产品定价、营业税、报价、折扣、回报和/或其它信息来处理该购买交易。例如,数据库可以是响应于结构化查询语言(“SQL”)命令的关系型数据库。商家服务器可执行包括SQL命令的超文本预处理器(“PHP”)脚本来查询产品数据的数据库。以下提供了说明查询数据库的实质方面的示例性PHP/SQL命令列表:

```

[0053]
<?PHP
header('Content-Type: text/plain');
mysql_connect("254.93.179.112", $DBserver, $password); // access database server
mysql_select_db("PRODUCTS.SQL"); // select database table to search
//create query
$query = "SELECT product_info product_price tax_info_list offers_list
discounts_list rewards_list FROM ProdTable WHERE product LIKE '%" $prod";
$result = mysql_query($query); // perform the search query
mysql_close("PRODUCTS.SQL"); // close database access
?>

```

[0054] 在一些实现方式中,响应于获得产品数据,商家服务器可根据用户的安全设置(参见例如358)产生(例如416a)QR支付代码和/或安全显示元件。该商家服务器可提供该QR代码到客户端,以便客户端可显示该QR代码,然后用户就可使用用户的设备捕捉该QR代码来获得商家和/或产品数据,以用于产生购买交易处理请求。在作为替代的实现方式中,商家服务器可指引客户端通过作为替代的通信协议(诸如但不限于:Wi-Fi™、蓝牙™、蜂窝网

络、SMS、电子邮件和/或类似通信协议)来传递处理该交易所需的产品和/或商家数据到用户的设备。例如,商家服务器可指引客户端来在它的系统上发起插件,以提供作为替代的通信业务,并通过该通信业务传输该产品和/或商家数据到用户的设备。

[0055] 在使用QR代码的实现方式中,商家服务器可产生包含支付网络处理购买交易所需的产品信息以及商家信息的QR代码。在一些实现方式中,该QR代码可至少包括捕捉该QR代码的用户设备所需的信息来产生购买交易处理请求,诸如商家标识符(例如,商家ID号、商家名称、商店ID等等)以及用于与商店网站/实体店相关联的用户购物会话的会话标识符。

[0056] 在一些实现方式中,该商家服务器可实时产生自定义的、用户指定的商家产品XML数据结构,该数据结构具有限制时间的有效期,诸如以下提供的示例性“QR_data”XML数据结构:

[0057]

```
<QR_data>
  <order_ID>4HFU48G94</order_ID>
  <timestamp>2011-02-22 15:22:43</timestamp>
  <expiry_lapse>00:00:30</expiry_lapse>
  <transaction_cost>934.78</transaction_cost>
  <alerts_URL>www.merchant.com/shopcarts.php?sessionID=AEBB4356</alerts_URL>
  <user_ID>john.q.public@gmail.com</user_ID>
  <client_details>
    <client_IP>192.168.23.136</client_IP>
    <client_type>smartphone</client_type>
    <client_model>HTC Hero</client_model>
    <OS>Android 2.2</OS>
    <app_installed_flag>true</app_installed_flag>
  </client_details>
  <secure_element>www.merchant.com/securedyn/0394733/123.png</secure_element>
  <purchase_details>
    <num_products>1</num_products>
    <product>
      <product_type>book</product_type>
      <product_params>
        <product_title>XML for dummies</product_title>
        <ISBN>938-2-14-168710-8</ISBN>
        <edition>2nd ed.</edition>
        <cover>hardbound</cover>
        <seller>bestbuybooks</seller>
      </product_params>
      <quantity>1</quantity>
    </product>
  </purchase_details>
  <merchant_params>
    <merchant_id>3FBCH4INC</merchant_id>
    <merchant_name>Books & Things, Inc.</merchant_name>
    <merchant_auth_key>1SMF4848CF59CHR27365</merchant_auth_key>
  </merchant_params>
</QR_data>
```

[0058] 在一些实现方式中,该XML数据可包括句柄、别名、记号或指向存储在支付网络服务器上的信息的指针,而不是编码发起该交易所需的所有实际数据,以便编码到该QR代码中的信息可以有利地被最小化。在一些实现方式中,该商家可使用该XML数据产生QR代码。例如,商家服务器可使用在<http://phpqrcode.sourceforge.net/>可用的PHP QR代码开源(LGPL)库用于产生QR代码、2维条形码。例如,该商家服务器可发布与以下提供的示例性命令相似的PHP命令:

[0059] <?PHP


```
[0060] header('Content-Type:text/plain');
[0061] //Create QR code image using data stored in Sdata variable
[0062] QRroode::png(Sdata,'qrcodeimg.png');
[0063] ?>
```

[0064] 在作为替代的实现方式中,该商家服务器可随着请求一起提供(例如416b)XML数据到支付网络服务器(例如406)来产生QR代码。例如,商家服务器使用API调用到该支付网络服务器来请求QR代码的生成。支付网络服务器可产生用于该商家服务器的QR代码,例如416c,并提供(例如416d)该QR代码到该商家服务器。例如,支付网络服务器可将由商家提供的信息编码到QR代码中,并且也可有利地将安全信息、时间有效性信息、数字证书信息、不记名发货消息、QR代码产生/处理付费信息等等编码到该QR代码中。

[0065] 在一些实现方式中,支付网络服务器为商家服务器提供加密密钥(例如Rivest-Shamir-Adleman (RSA) 私有/公共密钥,数字证书)。商家可使用该加密密钥来加密该自定义的、用户特定的商家产品XML数据结构,以产生加密的购买数据(例如使用RSA算法)。该商家服务器然后将该加密的数据编码到QR代码中。在各种实施例中,对于与用户-商家购物会话相关的任何交易处理请求,该支付网络服务器可有利地采用这种方案来验证商家。

[0066] 在一些实现方式中,可以向用户设备提供预先设计的与验证、预先验证的商家相关联的QR代码。例如,用户可以在用户的设备上浏览在线网站。该用户设备可从网页服务器产生用于网页的HTTP(S)GET请求。在一些实现方式中,该网页服务器可响应于该用户设备的对网页的请求,产生用于广告的查询来显示在该网页上。例如,网页服务器可检索数据库或提供请求到广告网络服务器(例如,Akamai)来提供用于嵌入到该网页中的广告。在一些实现方式中,该广告网络服务器可使用从网页服务器中获得的关键字、元数据等(例如,与该网页相关联的关键字或元数据、用户简档信息、用户ID、来自存储在该用户设备上的cookie的用户浏览历史,等等)。该广告网络可使用关键字来产生与该关键字相关联的广告的数据库的查询,并且可获得广告来提供。在一些实现方式中,该广告网络服务器可提供(例如通过API调用)关于这种广告的信息(例如,商家名称,商家ID,产品名称,产品价格信息,相关报价,等等)到支付网络服务器。该支付网络服务器可基于由该广告网络服务器提供的信息产生QR代码,以使用户设备可对该QR代码拍快照来发起与该QR代码(例如,由该广告网络服务器提供到该支付网络服务器的)相关联的货物和/或服务的购买交易。广告网络服务器可提供该QR作为广告的一部分到该网页服务器,网页服务器又可在向用户设备提供网页以前,嵌入包括该QR代码的广告到该网页中。在作为替代的实现方式中,广告网络服务器/网页服务器可传输该QR代码(最终的)的URL或其它标识符到用户设备,并且该用户设备可使用该QR代码的URL(例如,托管在该支付网络服务器上)产生调用(例如HTTP(S)GET请求)来获得该QR代码并为用户显示它。

[0067] 在一些实现方式中,商家服务器可提供该QR代码到该客户端,例如417。例如,商家服务器可提供包括引用该QR代码图像和/或安全元件图像的超文本标记语言(“HTML”)页面,诸如以下示例性的HTML页面:

```
[0068] <html>
      
      
    </html>
```

[0069] 在一些实现方式中,客户端可获得该QR支付代码(例如417)并在与客户端设备相关联的显示屏幕上显示该QR代码(例如418)。在一些实现方式中,用户可使用用户设备,例如405,来捕捉由该客户端设备呈现的QR代码以用于支付处理。例如,用户可提供支付输入到用户设备例如419中。在各个实现方式中,用户输入可包括但不限于:触摸屏接口的单次轻敲(例如,一次轻敲移动应用购买实施例)、键盘输入、扫卡、在该用户设备内激活支持RFID/NFC的硬件设备(例如,具有多个帐号的电子卡、智能电话、书写板等等)、鼠标点击、在操纵杆/游戏控制台上压下按钮、语音命令、触敏接口上的单次/多次触摸手势、触动触敏显示器上的用户界面元件,等等。例如,用户设备可从用户卡(例如信用卡、借记卡、预付卡、赠帐卡等等)获得追踪数据,诸如以下提供的示例性追踪数据:

```

88123456789012345*PUBLIC/Q.Q.*99011200000000000000**801*****?*
[0070] (wherein '123456789012345' is the card number of 'Q.Q. Public' and has a CVV
number of 901, '990112' is a service code, and '**' represents decimal digits
which change randomly each time the card is used.)

```

[0071] 在一些实现方式中,用户设备可确定图像是否已经捕捉了描述QR代码。根据是否已经捕捉了QR代码,以及(可选地)也根据该QR代码的内容,该用户设备可重定向用户(例如通过在该用户设备上执行的网页浏览器应用)到:产品、商家网站、商家网站上的产品、网站以及包括命令来添加物品到与该网站相关联的用户购物车等。例如,用户设备可执行一部件,诸如如下参见附图6A-B的讨论所描述的示例性快速响应代码处理(“QRCP”)部件600。

[0072] 在一些实现方式中,当获得用户支付输入并捕捉了QR代码时,该用户设备可以产生用于提供到支付网络服务器的卡授权请求420(例如,如果该QR代码包括购买优惠券、报价、发货单、来自另一个虚拟钱包用户的个人支付等等)。例如,用户设备可以以XML格式的数据的形式提供代表该用户的卡授权请求(例如421)、包括用于支付网络服务器的产品订购细节的HTTP(S)GET消息(例如406)。以下是用于该支付网络服务器的包括XML格式的卡授权请求的示例性HTTP(S)GET消息:

```

GET /purchase.php HTTP/1.1
Host: www.merchant.com
Content-Type: Application/XML
Content-Length: 1308
<?XML version = "1.0" encoding = "UTF-8"?>
<purchase_order>
  <order_ID>48FU4RG94</order_ID>
  <alerts_URL>www.merchant.com/shopcart.php?sessionID=AEBB4356</alerts_URL>
  <timestamp>2011-02-22 15:22:43</timestamp>
  <user_ID>john.q.public@gmail.com</user_ID>
  <client_details>
    <client_IP>192.168.23.126</client_IP>
    <client_type>smartphone</client_type>
    <client_model>HTC Hero</client_model>
    <OS>Android 2.2</OS>
    <app_installed_flag>true</app_installed_flag>
  </client_details>
  <purchase_details>
    <num_products>1</num_products>
    <product>
      <product_type>book</product_type>
      <product_params>
        <product_title>XML for dummies</product_title>
        <ISBN>938-2-14-168710-0</ISBN>
        <edition>2nd ed.</edition>
        <cover>hardbound</cover>
        <seller>bestbuybooks</seller>
      </product_params>
      <quantity>1</quantity>
    </product>
  </purchase_details>
  <merchant_params>
    <merchant_id>3FB0P418C</merchant_id>
    <merchant_name>Books & Things, Inc.</merchant_name>
    <merchant_auth_key>1M9F484MCP59C8E27365</merchant_auth_key>
  </merchant_params>
  <account_params>
    <account_name>John Q. Public</account_name>
    <account_type>credit</account_type>
    <account_sum>123456789012345</account_sum>
    <billing_address>123 Green St., Norman, OK 98765</billing_address>
    <phone>123-456-7899</phone>
    <sign>/jpg/</sign>
    <confirm_type>email</confirm_type>
    <contact_info>john.q.public@gmail.com</contact_info>
  </account_params>
  <shipping_info>
    <shipping_address>same as billing</shipping_address>
    <ship_type>expedited</ship_type>
    <ship_carrier>FedEx</ship_carrier>
    <ship_account>123-45-678</ship_account>
    <tracking_flag>true</tracking_flag>
    <sign_flag>false</sign_flag>
  </shipping_info>
</purchase_order>

```

[0073]

[0074] 在一些实现方式中,由用户设备产生的卡授权请求可包括处理该购买交易所需的最少信息。例如,这可提高传递该购买交易请求的效率,并且也可以有利地提高提供到该用户和/或商家的隐私保护。例如,在一些实现方式中,该卡授权请求可至少包括商家ID、用于用户和商家的购物会话的会话ID,以及链接到该用户的虚拟钱包的用户设备(例如智能电话)的设备ID。在一些实现方式中,发送到/来自于该QR代码捕捉设备的QR代码和消息可包括源ID(例如产生该QR代码的设备的标识符)、会话ID、商家ID、物品ID(例如型号)、结帐金额,和/或交易设备ID(例如,用户的智能电话设备)。

[0075] 在一些实现方式中,卡授权请求可以由该商家服务器或销售点终端提供,而不是用户设备。在一些实现方式中,期望安全的用户可通过该用户设备请求支付网络服务器以

便动态地产生将在该购买交易中与该用户的主要帐户号

[0076] (“PAN”，例如，信用卡号码)一起使用的卡验证值代码(dCVV™)。作为响应，该支付网络服务器可产生dCVV™代码(例如，使用随机数生成、输入键的MD5散列，其可以利用用户ID、商家ID、会话ID、时间戳、它们的组合等产生)，并为该用户提供会话特定的dCVV™代码来与用户的PAN号码一起使用。例如，会话特定的dCVV™代码可以具有期满时间(例如，从发布开始的一分钟内失效)。该用户设备可(例如，通过蓝牙™、NFC、Wi-Fi、蜂窝、QR代码等等)将该PAN和dCVV传递到销售点终端，销售点终端可创建卡授权请求。例如，该用户设备可产生嵌有该PAN和dCVV号码的QR支付代码，并且销售点终端可对该用户设备产生的QR支付代码的图像拍快照。该销售点终端然后可以产生和提供该卡授权请求到支付网络服务器。该支付网络服务器然后可以比较从商家获得的dCVV和在该购买交易被发起以前提供到该用户设备的dCVV来确认该交易。如果来自该两个源(支付网络服务器和商家)的dCVV代码互相正确地对应，那么该支付网络服务器可继续处理该购买交易。

[0077] 在一些实现方式中，该来自用户设备的卡授权请求可包括从该QR代码提取的加密数据，其可以已经由该商家服务器作为商家验证方案的一部分而加密。在一些实现方式中，该支付网络服务器可从由用户设备提供的卡授权请求获得加密数据，并试图解密该加密数据，例如，利用RSA私有/公共密钥，其对于支付网络服务器开始提供给商家服务器用于在嵌入到该QR代码中以前加密购买数据的密钥是互补的。如果支付网络服务器能够解密该购买数据，那么商家被认证为有效商家。在一些实现方式中，支付网络服务器可以比较从该卡授权解密的购买数据和由用户/用户设备提供的数据，以确定来自这些不同源(用户/用户设备，和商家)的数据是否互相正确地对应。因此，在一些实现方式中，该支付网络服务器能验证该商家，并在处理交易以前关联该商家到特定的用户会话或用户设备。

[0078] 在一些实现方式中，支付网络服务器可提供通知给用户设备，通知该交易被验证并批准交易。在作为替代的实现方式中，支付网络服务器可继续进行交易处理。在一些实现方式中，当标识用户处于与商家会话中时，支付网络服务器可以与用户设备通信来为用户提供额外的特征。例如，在一些实现方式中，支付网络服务器可提供与用户设备的通信(例如，通过HTTP(S) POST消息)，以提供：商家的虚拟店面；与包括在卡授权请求中的产品相关联的商家的走廊的描述、相关物品的列表等(参见，例如附图8E-G以及附加实施例的以下描述)。

[0079] 参见附图4B，在一些实现方式中，支付网络服务器可处理交易以便转帐购买资金到存储在商家的收单机构上的帐户中。例如，收单机构可以是维护商家的帐户的金融机构。例如，由商家处理的交易结果可以被存放到由收单机构的服务器维护的帐户中。

[0080] 在一些实现方式中，该支付网络服务器可以为对应于用户所选的支付选项的发布方服务器产生查询，例如422。例如，用户的帐户可以被链接到一个或多个发布用户的帐户的发布方金融机构(“发布方”)，诸如银行机构。例如，这种帐户包括但不限于：信用卡、借记卡、预付卡、支票、存款、金融市场、存款凭证、积蓄(现金)值帐户等。发布方的发布方服务器，例如4o8a-n，可保持用户帐号的细节。在一些实现方式中，例如支付网络数据库407的数据库可存储与发布方相关联的发布方服务器的细节。例如，该数据库可以是响应于结构化查询语言(“SQL”)命令的关系型数据库。该支付网络服务器可为了发布方服务器细节而查询支付网络数据库。例如，该支付网络服务器可执行包括SQL命令的超文本预处理器

(“PHP”)脚本来查询数据库以查询发布方服务器的细节。以下提供了说明查询数据库的实质方面的示例性PHP/SQL命令列表:

```
<?PHP
header('Content-Type: text/plain');
mysql_connect("254.53.175.112", $DBserver, $password); // access database server
mysql_select_db("ISSUERS.SQL"); // select database table to search
//create query for issuer server data
[0081] $query = "SELECT issuer_name issuer_address issuer_id ip_address mac_address
        auth_key port_num security_settings_list FROM issuertable WHERE account_num
        LIKE '% $accountnum'";
$result = mysql_query($query); // perform the search query
mysql_close("ISSUERS.SQL"); // close database access
?>
```

[0082] 响应于获得该发布方服务器查询,例如422,该支付网络数据库可提供所请求的发布方服务器数据到支付网络服务器,例如423。在一些实现方式中,支付网络服务器可使用发布方服务器数据来为基于与该用户的虚拟钱包相关联的预定义的支付设置和/或用户的支付选项输入而选择的每个发布方服务器产生授权请求,例如424,并提供卡授权请求,例如425a-n到该发布方服务器,例如408a-n。在一些实现方式中,授权请求可包括细节,诸如但不局限于:包含在交易中的对用户的成本、用户的卡帐户细节、用户帐单和/或发货信息,等。例如,支付网络服务器可提供包括与以下提供的示例性列表相似的XML格式的授权请求的HTTP(S)POST消息:

```
POST /authorization.php HTTP/1.1
Host: www.issuer.com
Content-Type: Application/XML
Content-length: 634
<?XML version = "1.0" encoding = "UTF-8"?>
<card_query_request>
  <query_id>VMB136FK</query_id>
  <timestamp>2011-02-22 15:22:44</timestamp>
  <purchase_summary>
    <num_products>1</num_products>
    <product>
      <product_summary>Book - XML for dummies</product_summary>
      <product_quantity>1</product_quantity>
    </product>
  </purchase_summary>
  <transaction_cost>822.61</transaction_cost>
  <account_params>
    <account_type>checking</account_type>
    <account_num>1234567890123456</account_num>
  </account_params>
  <merchant_params>
    <merchant_id>3FBC8410E</merchant_id>
    <merchant_name>Books & Things, Inc.</merchant_name>
    <merchant_auth_key>10MF464MC859C8827365</merchant_auth_key>
  </merchant_params>
</card_query_request>
```

[0084] 在一些实现方式中,发布方服务器可解析该授权请求,并基于该请求细节可查询数据库,例如用户简档数据库409a-n,以查询与链接到该用户的账户相关联的数据。例如,发布方服务器可发布与以下提供的示例相似的PHP/SQL命令:

[0085]

```
<?PHP
header('Content-Type : text/plain');
mysql_connect ("254.93.179.112", $DBserver, $password) ; // access
database server mysql_select_db ("USERS . SQL" ) ; // select database table to
search
//create query for user data
$query = "SELECT user_id user_name user_balance account_type FROM
UserTable
WHERE account_num LIKE '% ' $accountnum" ;
$result = mysql_query ( $query) ; // perform the search query
mysql_close ( "USERS . SQL" ) ; // close database access
?>
```

[0086] 在一些实现方式中,在获得该用户数据后,例如427a-n,该发布方服务器可确定用户是否可以利用帐户上可用的资金支付该交易,例如428a-n。例如,发布方服务器可确定用户在帐户中是否具有足够的余额剩余、与该帐户相关联的足够信用等。基于该确定,发布方服务器可提供授权响应到支付网络服务器,例如,429a-n。例如,发布方服务器可提供与上面示例相似的HTTP(S) POST消息。在一些实现方式中,如果至少一个发布方服务器确定用户不能利用帐户中的可用资金支付该交易,参见例如430-431,那么该支付网络服务器可再次从用户请求支付选项(例如,通过提供授权失败消息431到用户设备并请求用户设备提供新支付选项),并再尝试该购买交易的授权。在一些实现方式中,如果授权尝试的失败次数超出阈值,该支付网络服务器可退出授权处理,并提供“授权失败”消息到商家服务器、用户设备和/或客户端。

[0087] 参见附图4C,在一些实现方式中,支付网络服务器可获得包括成功授权的授权的授权消息,参见例如430、433,并解析该消息以提取授权细节。当确定用户拥有足够的交易资金时,支付网络服务器可根据该授权请求和/或授权响应产生交易数据记录,例如432,并在交易数据库中存储该交易的细节和关于该交易的授权。例如,支付网络服务器可发布与以下示例列表相似的PHP/SQL命令来在数据库中存储交易数据:

```

<?PHP
header('Content-Type: text/plain');
mysql_connect("254.32.183.103", $DBserver, $password); // access database server
mysql_select("TRANSACTIONS.SQL"); // select database to append
mysql_query("INSERT INTO PurchasesTable (timestamp, purchase_summary_list,
num_products, product_summary, product_quantity, transaction_cost,
account_params_list, account_name, account_type, account_num,
[0088] billing_address, zipcode, phone, sign, merchant_params_list, merchant_id,
merchant_name, merchant_auth_key)
VALUES (time(), $purchase_summary_list, $num_products, $product_summary,
$product_quantity, $transaction_cost, $account_params_list, $account_name,
$account_type, $account_num, $billing_address, $zipcode, $phone, $sign,
$merchant_params_list, $merchant_id, $merchant_name, $merchant_auth_key)");
// add data to table in database
mysql_close("TRANSACTIONS.SQL"); // close connection to database
?>

```

[0089] 在一些实现方式中,支付网络服务器可转发授权成功消息,例如433a-b,到用户设备和/或商家服务器。商家可获得该授权消息并根据它确定用户在卡帐户中拥有足够的资金来进行该交易。该商家服务器可为用户添加交易记录到关于授权的交易的一批交易数据。例如,该商家可附加关于该用户交易的XML数据到包括用于已经为各个用户授权的交易的数据的XML数据文件,例如434,并在数据库(例如商家数据库404)中存储该XML数据文件,例如435。例如,批XML数据文件可以是与以下提供的示例XML数据结构模板相似的结构:

```

[0090] <?XML version="1.0" encoding="UTF-8"?>
[0091] <merchant_data>
[0092] <merchant_id>3FBCR4INC</merchant_id>
[0093] <merchant_name>Books&Things,Inc.</merchant_name>
[0094] <merchant_auth_key>1NNF484MCP59CHB27365</merchant_auth_key>
[0095] <account_number>123456789</account_number>
[0096] </merchant_data>
[0097] <transaction_data>
[0098] <transaction 1>
[0099] ...
[0100] </transaction 1>
[0101] <transaction 2>
[0102] ...
[0103] </transaction 2>
[0104] .
[0105] .
[0106] .
[0107] <transaction n>
[0108] ...
[0109] </transaction n>
[0110] </transaction data>

```

[0111] 在一些实现方式中,服务器也可以产生购买收据,例如434,并提供该购买收据到客户端,例如436。该客户端可为用户呈递并显示该购买收据,例如437a。在一些实现方式中,用户设备405也可以提供成功授权的通知到用户,例如437b。例如,客户端/用户设备可

呈递网页、电子消息、文本/SMS消息、缓冲语音邮件、发出铃声、和/或播放音频消息等等，并提供包括但不限于以下各项的输出：声音、音乐、音频、视频、图像、触觉反馈、振动警告（例如，诸如智能电话等的支持振动的客户端设备），等等。

[0112] 参见附图4D，在一些实现方式中，商家服务器可发起一批授权交易的清算。例如，商家服务器可产生批数据请求，例如438，并提供该请求，例如439，到例如商家数据库404的数据库。例如，商家服务器可使用与上面提供的示例相似的PHP/SQL命令来查询关系数据库。响应于该批数据请求，该数据库可提供所请求的批数据，例如440。服务器可利用从数据库中获得的批数据产生批清算请求，例如441，并提供（例如442）该批清算请求到收单机构服务器，例如410。例如，商家服务器可为收单机构服务器提供在消息主体中包括XML格式的批数据的HTTP(S) POST消息。该收单机构服务器可利用所获得的批清算请求产生批支付请求，例如443，并提供该批支付请求到支付网络服务器，例如444。支付网络服务器可解析该批支付请求并为存储在该批支付请求中的每个交易提取交易数据，例如445。支付网络服务器可在例如支付网络数据库407的数据库中为每个交易存储交易数据，例如446。对于每个提取的交易，支付网络服务器可查询例如支付网络数据库407的数据库，例如447-448，以查询发布方服务器的地址。例如，支付网络服务器可使用与上面提供的示例相似的PHP/SQL命令。支付网络服务器可为每个被提取了交易数据的交易产生单个支付请求，例如449，并提供该单个支付请求（例如450）到发布方服务器（例如408）。例如，支付网络服务器可提供与以下示例相似的HTTP(S) POST请求：

```
POST /requestpay.php HTTP/1.1
Host: www.issuer.com
Content-Type: Application/XML
Content-Length: 768
<?XML version = "1.0" encoding = "UTF-8"?>
<pay_request>
  <request_id>CH141CNWZ</request_id>
  <timestamp>2011-02-22 17:00:01</timestamp>
  <pay_amount>$34.78</pay_amount>
  <account_params>
    <account_name>John Q. Public</account_name>
    <account_type>credit</account_type>
    <account_num>123456789012345</account_num>
    <billing_address>123 Green St., Norman, OK 90765</billing_address>
    <phone>123-456-7809</phone>
    <sign>/jqp/</sign>
  </account_params>
  <merchant_params>
    <merchant_id>37BCR4TNC</merchant_id>
    <merchant_name>Books & Things, Inc.</merchant_name>
    <merchant_auth_key>1MUP4846C259CMB27365</merchant_auth_key>
  </merchant_params>
  <purchase_summary>
    <num_products>1</num_products>
    <product>
      <product_summary>Book - XML for dummies</product_summary>
      <product_quantity>1</product_quantity>
    </product>
  </purchase_summary>
</pay_request>
```

[0113]

[0114] 在一些实现方式中，发布方服务器产生可产生支付命令，例如451。例如，发布方服务器可发布命令来从用户帐户扣除资金（或添加费用到用户信用卡帐户）。该发布方服务器可发布支付命令（例如452）到存储该用户帐户信息的数据库，例如，用户简档数据库409。发布方服务器可提供资金转帐消息（例如453）到支付网络服务器，支付网络服务器其可转发（例如454）该资金转帐消息到收单机构服务器。下面提供示例性HTTP(S) POST资金转帐消

息:

```
[0115] POST/clearance.php HTTP/1.1
[0116] Host:www.acquirer.com
[0117] Content-Type:Application/XML
[0118] Content-Length:206
[0119] <?XML version="1.0"encoding="UTF-8"?>
[0120] <deposit_ack>
[0121] <request_ID>CNI4ICNW2</request_ID>
[0122] <clear_flag>true</clear_flag>
[0123] <timestamp>2011-02-22 17:00:02</timestamp>
[0124] <deposit_amount>$34.78</deposit_amount>
[0125] </deposit_ack>
```

[0126] 在一些实现方式中,收单机构服务器可解析该资金转帐消息,并关联该交易(例如,利用在上述例子中的request_ID字段)到商家。该收单机构服务器然后可以移转资金转帐消息中指定的资金到商家的账户,例如455。

[0127] 附图5A-E示出了说明在SNAP的一些实施例中,执行快拍移动支付的示例性方面的逻辑流程图,例如快拍移动支付执行(“SMPE”)部件500。参见附图5A,在一些实现方式中,用户可能希望通过商家在线站点或在商家商店中从商家购买产品、服务、报价等(“产品”)。该用户可通过客户端与商家服务器通信。例如,用户可提供用户输入(例如501)到客户端中,指示用户希望结帐(虚拟)购物车中的购物物品。客户端可产生结帐请求,例如502,并提供该结帐请求到商家服务器。商家服务器可从该客户端获得结帐请求,并从该结帐请求提取结帐细节(例如XML数据),例如503。例如,商家服务器可使用诸如如下参见附图14的讨论所描述的示例解析器的解析器。商家服务器从结帐请求中提取该产品数据以及客户端数据。在一些实现方式中,商家服务器可查询(例如504)商家数据库来获得产品数据,例如505,诸如产品价格、营业税、报价、折扣、回报,和/或其它信息来处理该购买交易。

[0128] 响应于获得该产品数据,该商家服务器可根据用户的安全设置产生(例如506)QR支付代码和/或安全显示元件(参见例如358)。例如,商家服务器可产生包含有支付网络处理该购买交易所要求的产品信息以及商家信息的QR代码。例如,该商家服务器可首先实时产生自定义的、用户特定的具有时间受限的有效期的商家-产品XML数据结构,诸如下面提供的示例性“QR_data”XML数据结构:

```
[0129] <QR_data>
  <session_ID>49FB48G94</session_ID>
  <timestamp>2011-02-22 15:22:43</timestamp>
  <expiry_lapse>00:00:30</expiry_lapse>
  <transaction_cost>$34.78</transaction_cost>
  <user_ID>john.q.public@gmail.com</user_ID>
  <client_details>
    <client_IP>192.168.23.136</client_IP>
    <client_type>smartphone</client_type>
    <client_model>HTC Hero</client_model>
    <OS>Android 2.2</OS>
```

```

    <app_installed_flag>true</app_installed_flag>
  </client_details>
  <secure_element>www.merchant.com/securedyn/0394733/123.png</secure_element>
  <purchase_details>
    <num_products>1</num_products>
    <product>
      <product_type>book</product_type>
      <product_params>
        <product_title>XML for dummies</product_title>
        <ISBN>998-0-14-188710-9</ISBN>
        <edition>2nd ed.</edition>
        <cover>hardbound</cover>
        <seller>bestbuybooks</seller>
      </product_params>
      <quantity>1</quantity>
    </product>
  </purchase_details>
  <merchant_params>
    <merchant_id>3F8C841DC</merchant_id>
    <merchant_name>Books & Things, Inc.</merchant_name>
    <merchant_auth_key>1MIF454MCPS9C8B27365</merchant_auth_key>
  </merchant_params>
  <QR_data>

```

[0131] 在一些实现方式中，商家可利用XML数据产生QR代码。例如，商家服务器可使用在 <http://phpqrcode.sourceforge.net/> 可用的PHP QR代码开源 (LGPL) 库以用于产生QR代码、2维条形码。例如，商家服务器可发布与以下提供的示例性命令相似的PHP命令：

[0132] <?PHP

[0133] header('Content-Type:text/plain');

[0134] //Create QR code image using data stored in \$data variable

[0135] QRcode::png(\$data,'qrcodeimg.png');

[0136] ?>

[0137] 商家服务器可提供该QR支付代码到客户端，例如506。客户端可获得该QR支付代码，并在与客户端设备相关联的显示屏幕上显示该QR代码，例如507。在一些实现方式中，用户可使用用户设备，例如509，来捕捉由该客户端设备呈现的QR代码以用于支付处理。该客户端设备可解码该QR代码以提取嵌入在该QR代码中的信息。例如，客户端设备可使用在 <http://code.google.com/p/zxing/> 可用的应用程序，诸如ZXing多格式1D/2D条形码图像处理库，以从该QR代码提取信息。在一些实现方式中，用户可提供支付输入到用户设备中，例如508。当获得用户购买输入时，该用户设备可产生卡授权请求，例如509，并提供该卡授权请求到支付网络服务器。

[0138] 参见附图5B，在一些实现方式中，支付网络服务器可解析该卡授权请求，例如510，并为对应于用户所选的支付选项的发布方服务器产生查询，例如511。在一些实现方式中，支付网络数据库可存储与发布方相关联的发布方服务器的细节。响应于获得该发布方服务器查询，支付网络数据库可提供，例如，512，所请求的发布方服务器数据到该支付网络服务器。在一些实现方式中，该支付网络服务器可使用发布方服务器数据来为每个发布方服务器产生授权请求，例如，425134，并提供卡授权请求到发布方服务器。

[0139] 在一些实现方式中，发布方服务器可解析该授权请求，并基于该请求的细节，可为与链接到该用户的帐户相关联的数据查询用户简档数据库。在一些实现方式中，当获得该用户数据后，发布方服务器可确定该用户是否可以利用帐户中的可用资金支付交易，例如517。例如，发布方服务器可确定用户是否具有足够余额剩余在帐户中、是否具有与该帐户相关联的足够信用等。基于该确定，发布方服务器可提供授权响应到支付网络服务器，例如

518. 在一些实现方式中, 如果至少一个发布方服务器确定 (例如519) 用户不能利用帐户中的可用资金支付该交易, 参见例如520, 选项“否”, 那么该支付网络服务器可再次从用户请求支付选项 (参见例如521, 选项“否”, 通过提供授权失败消息到用户设备并请求用户设备提供新支付选项), 并再尝试该购买交易的授权。在一些实现方式中, 如果授权尝试的失败次数超出阈值, 参见例如521, 选项“是”, 那么该支付网络服务器可退出该授权处理, 并提供“授权失败”消息到该商家服务器、用户设备和/或客户端, 例如522。

[0140] 在一些实现方式中, 该支付网络服务器可获得包括成功授权的授权的授权消息, 参见例如520, 选项“是”, 并解析该消息以提取授权细节。当确定用户拥有足够的交易资金后, 支付网络服务器可根据该授权请求和/或授权响应产生交易数据记录, 例如523, 并在交易数据库中存储该交易的细节和涉及该交易的授权, 例如524。

[0141] 参见附图5C, 在一些实现方式中, 该支付网络服务器可转发授权成功消息 (例如525) 到用户设备和/或商家服务器, 有时通过收单机构服务器转发, 例如526。该商家可解析该授权消息, 例如528, 并根据它确定用户在卡帐户中拥有足够资金来进行该交易, 参见例如529。该商家服务器可为用户添加一条交易记录到涉及授权交易的一批交易数据中, 参见例如530-531。在一些实现方式中, 该商家服务器也可以产生购买收据, 例如532, 并提供该购买收据到客户端。该客户端可为用户呈递并显示该购买收据, 例如534。在一些实现方式中, 用户设备405也可以提供成功授权的通知给用户。

[0142] 参见附图5D-E, 在一些实现方式中, 商家服务器可发起一批授权交易的清算。例如, 该商家服务器可产生批数据请求, 例如535, 并提供该请求 (例如536) 到数据库, 例如商家数据库。响应于该批数据请求, 该数据库可提供所请求的批数据, 例如536。服务器可利用从数据库获得的批数据产生批清算请求, 例如537, 并提供该批清算请求到收单机构服务器。收单机构服务器可利用该获得的批清算请求产生 (例如539) 批支付请求, 并提供该批支付请求到该支付网络服务器。该支付网络服务器可解析该批支付请求, 并为存储在该批支付请求中的每个交易提取交易数据, 例如540-542。该支付网络服务器可为例如支付网络数据库的数据库中的每个交易存储该交易数据, 例如543-544。对于每个提取的交易, 支付网络服务器可查询 (例如545-546) 例如支付网络数据库的数据库以查询发布方服务器的地址。该支付网络服务器可为每个被提取交易数据的交易产生单个支付请求, 例如547, 并提供该单个支付请求到关联的发布方服务器。

[0143] 在一些实现方式中, 发布方服务器可产生支付命令, 例如548-549。例如, 发布方服务器可发布命令来从用户帐户扣除资金 (或添加费用到用户的信用卡帐户)。发布方服务器可发布支付命令到存储用户的帐户信息的数据库 (例如用户简档数据库), 例如549。该发布方服务器可提供资金转帐消息到可转发该资金转帐消息到收单机构服务器的支付网络服务器, 例如551。在一些实现方式中, 收单机构服务器可解析该资金转帐消息, 并关联该交易 (例如, 利用在上述例子中的request_ID字段) 到商家。该收单机构服务器然后可以移转资金转帐消息中指定的资金到商家的账户, 例如553-555。

[0144] 图6A-B示出了在该SNAP的一些实施例中, 说明处理快速响应代码的示例方面的逻辑流程图, 例如快速响应代码处理 (“QRCP”) 部件600。参见附图6A, 在一些实现方式中, 在用户设备上执行的虚拟钱包应用可确定在操作地连接至该用户设备的照相机获得的图像帧中是否已经捕捉到QR代码, 并也可以确定该QR代码的类型、内容。利用这种信息, 该虚拟钱

包应用可重定向用户的用户体验和/或发起购买、更新该虚拟钱包应用的方面等等。例如,该虚拟钱包应用可通过操作地连接至用户设备的照相机触发图像帧的捕捉,601。该虚拟钱包应用可使用图像分割算法来标识图像中的前景,602,并可裁剪图像的其余部分以减少图像中的背景噪声,603。该虚拟钱包应用可确定前景图像是否包括QR代码,根据该QR代码可以可靠地读取数据(例如,如果图像不包括QR代码,或该QR代码被部分地裁剪、模糊等等可能无法可靠地读取数据),604。例如,该虚拟钱包应用可使用代码库,诸如在<http://code.google.com/p/zxing/>可获得的比如ZXing多格式1D/2D条形码图像处理库,以尝试并从该QR代码提取信息。如果该虚拟钱包应用能够检测出QR代码(605,选项“是”),那么该虚拟钱包应用可解码该QR代码,并从该QR代码提取数据。如果该虚拟钱包应用不能检测出QR代码(605,选项“否”),那么该虚拟钱包应用可在图像上试图执行光学字符识别。例如,该虚拟钱包应用可使用在www.pixeltechnology.com/freewarw/tesseract2可获得的Tesseract C++开源OCR引擎,来执行光学字符识别,606。因此该虚拟钱包应用可获得编码在该图像中的数据,并如果该数据可以被虚拟钱包应用处理则可继续进行。该虚拟钱包应用可利用在提取的数据中标识的字段查询数据库,以查询该QR代码类型,608。例如,该QR代码可包括发货单/帐单、优惠券、汇单(例如,P2P移账中的)、新帐户信息包、产品信息、购买命令、URL导航指令、浏览器自动脚本、它们的组合等。

[0145] 在一些实施例中,该QR代码可包括关于将被添加到该虚拟钱包应用的新帐户的数据(参见609)。该虚拟钱包应用可查询该新帐户(如从提取的数据中获得)的发布方,以查询与该新帐户相关联的数据,610。该虚拟钱包应用可比较发布方提供的数据和从该QR代码提取的数据,611。如果该新帐户被确认(611,选项“是”),则该虚拟钱包应用可利用该新帐户的细节更新该钱包凭证,613,并利用来自该QR代码的数据更新该虚拟钱包应用的快拍历史,614。

[0146] 参见附图6B,在一些实施例中,该QR代码可包括关于使用该虚拟钱包应用的帐单、发货单或用于购买的优惠券的数据(参见615),该虚拟钱包应用可查询与该购买(如从提取的数据中获得的)相关联的商家,以查询与该帐单、发货单或用于购买的优惠券相关联的数据(例如报价细节、报价ID、期满时间等等),616。该虚拟钱包应用可比较商家提供的数据和从该QR代码提取的数据,617。如果该帐单、发货单或用于购买的优惠券被确认(618,选项“是”),那么该虚拟钱包应用可产生包括该QR编码数据的数据结构(参见例如上述参考图4-5的说明中的XML QR_data结构)以用于产生并提供卡授权请求,619,并且使用来自该QR代码的数据更新该虚拟钱包应用的快拍历史620。

[0147] 在一些实施例中,该QR代码可包括用于该虚拟钱包应用的产品信息、命令、用户导航指令等等(参见621)。该虚拟钱包应用可使用编码在QR中的信息查询产品数据库。该虚拟钱包应用可提供各种特征,包括但不限于:显示产品信息、重定向用户到:产品页面、商业网站、商业网站上的产品页面、在商业网站添加物品到用户购物车等等。在一些实现方式中,该虚拟钱包应用可执行诸如上面描述的过程以用于待处理的和/或用户选择用于处理(例如根据快拍历史)的任何图像帧。

[0148] 图7示出了在该SNAP一些实施例中,说明虚拟钱包应用的示例特征的概述的用户界面图。图7示出了虚拟钱包移动应用700的各种示例性特征的说明。显示的一些特征包括钱包701、经由TWITTER、FACEBOOK等等的社交融合、报价和税703、快拍移动购买704、警告

705以及安全、设置和分析796。以下更加详细地探索这些特征。

[0149] 图8A-G示出了在该SNAP的一些实施例中,说明购物模式中的虚拟钱包应用的示例特征的用户界面图。参见附图8A,该虚拟钱包移动应用的一些实施例帮助并极大地增强了消费者的购物体验。如图8A所示,消费者可获得各种购物模式来细读。在一种实现方式中,例如,用户可通过在用户界面底部选择商店图标810来启动该购物模式。用户可在检索字段812中键入物品来搜索和/或添加物品到购物车811。用户也可以通过说出将被检索和/或添加到购物车的物品的名称或描述到麦克风813中来使用语音激活的购物模式。在进一步的实现方式中,用户也可以选择其它购物选项814,比如当前物品815,帐单816,地址簿817,商家818和本地邻近819。

[0150] 在一个实施例中,例如,用户可选择选项当前物品815,如图8A的用户界面的最左边所示。当选择了当前物品815选项时,可以显示中间的用户界面。如图所示,中间的用户界面可提供用户的购物车811中的物品815a-h的当前列表。用户可选择一个物品,例如物品815a,来浏览所选物品和/或来自相同商家的其他物品的产品说明815j。也可以随着捕捉实施快拍移动购买交易必需的信息的QR代码815k一起显示价格和总的应付信息。

[0151] 参见图8B,在另一个实施例中,用户可选择帐单816选项。当选择帐单816选项后,用户界面可显示来自一个或多个商家的帐单和/或收据816a-h的列表。紧挨着每一个帐单可以显示附加信息,诸如访问日期、是否呈现来自多个商店的物品、最后帐单支付日期、自动支付、物品数量等。在一个例子中,可选择日期为2011年1月20日的钱包购物帐单816a。该钱包购物帐单选择可显示提供关于所选择的帐单的各种信息用户界面。例如,用户界面可显示购买的物品816k的列表, <<816i>>, 物品总数量和相应价值。例如,7个物品价值\$102.54处于选择的钱包购物帐单上。用户现在可选择任何物品并选择再次购买来添加购买该物品。用户也可以从最后时间刷新报价816j来清除任何无效的报价和/或搜索可适合当前购买的新报价。如图8B中示出的,用户可选择两个物品用于重复购买。一旦添加,可显示消息816i来确认两个物品的添加,其得出处于购物车14中的物品的总数。

[0152] 参见图8C,在又一个实施例中,用户可选择地址簿选项817来浏览地址簿817a,其包括联系人817b的列表和产生任何汇款或支付。在一个实施例中,地址簿可使用联系人的姓名和可用的和/或优选的支付模式来标识每个联系人。例如,联系人Amanda G. 可以是经由如图标817c表示的社交支付(例如经由FACEBOOK)来支付。在另一个示例中,钱可以经由如QR代码图标817d表示的QR代码被转送到Brian S.。在另一示例中,Charles B. 可经由近场通信817e、蓝牙817f和电子邮件817g接受支付。支付也可以经由USB 817h(例如,通过两个移动设备的物理连接)和其它诸如TWITTER的社交渠道进行。

[0153] 在一种实现方式中,用户可选择Joe P. 来支付。如用户界面中所示,紧挨着Joe P. 的名字旁边,Joe P. 具有电子邮件图标817g,表示Joe P. 接受经由电子邮件的支付。当选择他的名字时,用户界面可显示他的联系信息,诸如电子邮件、电话等等。如果用户希望通过非电子邮件的方法对Joe P. 支付,则该用户可添加另一个转帐模式817j到他的联系信息并进行支付转帐。参见图8D,用户可以配有屏幕817k,其中用户可以输入金额来发送给Joe,以及添加其它文本来将上下文提供给Joe以用于支付交易817l。用户可以通过图形用户界面元件817m选择可以联系Joe的模式(例如SMS、电子邮件、社交网络)。作为用户类型,也可以提供文本输入以便在GUI元件817n内浏览。当用户已经完成必要信息的输入时,用户可以按

下发送按钮817o来发送该社交消息给Joe。如果Joe也具有虚拟钱包应用,Joe将能在该应用内或直接在社交网络(例如Twitter™, Facebook®等等)的网站浏览817p社交支付消息。消息可从各个社交网络以及其它源(例如SMS、电子邮件)聚集。适合于每个消息传递方式的兑换方法可以与社交支付消息一起被指示。在图8D的说明中,Joe接收的SMS 817q表示Joe可以通过答复SMS并输入散列标签值“#1234”来兑换经由SMS获得的\$5。在相同说明中,Joe已经经由Facebook®接收到消息817r,其中包括Joe可以激活来启动\$25支付的兑换的URL链接。

[0154] 参见图8E,在一些其它的实施例中,用户可从购物模式中的选项的列表选择商家818来浏览商家818a-e的选择列表。在一种实现方式中,列表中的商家可以与该钱包发生联系,或与钱包具有联系关系。在另一个实现方式中,商家可包括满足用户定义或其他标准的商家列表。例如,该列表可以是用户确定的(curated)一个、用户最频繁购物或花费多于x总量的金额或连续三个月购物的商家等。在一种实现方式中,用户可进一步选择一个商家,例如Amazon 818a。然后用户可以通过商家的清单导航来发现感兴趣的物品,诸如818f-j。直接通过钱包以及在从独立的页面访问商家站点的情况下,用户可从Amazon818a的目录选择物品818j。如图8D的用户界面的最右端所示,然后将所选物品添加到购物车。消息818k表示所选物品已经被添加到购物车,以及现在购物车中的物品的更新数量是13。

[0155] 参见附图8F,在一个实施例中,可以有本地邻近选项,其可以由用户选择来浏览地理上非常邻近于用户的商家列表。例如,商家819a-e的列表可以是位置接近于该用户的商家。在一种实现方式中,该移动应用可基于用户的位置进一步标识用户何时在商店中。例如,当用户非常邻近该商店时,位置图标819d可以紧挨着商店(例如,Walgreens)被显示。在一种实现方式中,如果用户离开该商店(例如,Walgreens),该移动应用可周期性地刷新它的位置。在进一步实现方式中,用户可通过该移动应用导航选择的Walgreens商店的报价。例如,用户可使用该移动应用导航到Walgreens的走廊5上可获得的物品819f-j。在一种实现方式中,用户可从他或者她的移动应用选择玉米819i来添加到购物车819k。

[0156] 参见图8G,在另一个实施例中,本地邻近选项819可包括商店地图,尤其是实时地图特征。例如,当选择Walgreens商店时,用户可启动显示出商店组织结构和用户位置(由黄色圆圈指示)的地图819m的走廊地图819l。在一种实现方式中,用户可容易地配置地图来添加一个或多个其它用户(例如,用户的孩子)来共享在商店内的彼此的位置。在另一个实现方式中,用户可以具有选项来在地图中启动类似街道浏览的“商店浏览”。商店浏览819n可显示用户周围的图像/视频。例如,如果用户即将进入走廊5,商店浏览地图可显示走廊5的视图。此外,用户可使用导航工具819o操纵地图的方向来向前、向后、向右、向左,以及顺时针和逆时针方向旋转移动该商店视图。

[0157] 附图9A-F显示在SNAP的一些实施例中,说明在支付模式中的虚拟钱包应用的示例特征的用户接口图。参见图9A,在一个实施例中,该钱包移动应用可经由钱包模式910给用户用于支付交易的多个选项。在一种实现方式中,示出了用于进行支付的示例性用户界面911。该用户界面可清楚地标识用于该交易的金额912和货币913。该金额可以是应付金额并且该货币可包括诸如美元和欧元的真实货币,以及也包括诸如回报点的虚拟货币。交易914的金额也可以被显著地显示在该用户界面上。用户可选择资金标签916来选择一个或多个支付形式917,其可包括各个信用、借记、赠品、回报和/或预付卡。该用户也可以具有利

用回报点支付全部或部分的选项。例如,该用户界面上的图形指示符918示出了可用点的数目,该图形指示符919示出了将使用的对应付金额234.56的点数以及该点数在选择的货币(USD,例如)中的等价920。

[0158] 在一种实现方式中,该用户可从多个源组合资金来支付该交易。显示在该用户界面上的金额915可提供迄今由选择的支付形式(例如,发现卡以及回报点)所覆盖的总资金的金额的指示。用户可选择另一个支付形式或调整将从一个或多个支付形式借记的金额,直到金额915匹配应付金额914。一旦用户定下将从一个或多个支付形式借记的金额,则可开始付款授权。

[0159] 在一种实现方式中,用户可通过选择隐匿按钮922来选择交易的安全授权,来有效地隐匿或匿名一些(例如预先配置的)或全部识别信息,以便当用户选择支付按钮921的时候,交易授权是以安全且匿名的方式进行的。在另一个实现方式中,用户可选择支付按钮921,其可以使用标准授权技术用于交易处理。在另一实现方式中,当用户选择社交按钮923的时候,关于该交易的消息可以被传递到一个或多个社交网络(由用户建立的),其可在社交论坛中发布或宣布该购买交易,诸如墙报或tweet。在一种实现方式中,用户可选择社交支付处理选项923。该指示符924可示出进行中的授权和发送社交共享数据。

[0160] 在另一个实现方式中,对于某些购买活动可以激活限制支付模式925,诸如规定购买。可以根据由发布方、保险公司、商家、支付处理方和/或其它实体定义的规则来激活该模式,来帮助特殊货物和服务的处理。在此模式中,用户可按照资金标签向下翻卷支付形式926的列表来选择特殊的帐户,诸如灵活支付帐户(FSA)927、健康储蓄帐户(HAS)等,以及将被记入选择的帐户的金额。在一种实现方式中,这种限制支付模式925处理可禁止购买信息的社交共享。

[0161] 在一个实施例中,通过输入资金用户界面928,钱包移动应用可帮助资金的输入。例如,失业的用户可通过钱包移动应用获得失业救济资金929。在一种实现方式中,提供这些资金的实体也可以配置使用这些资金的规则,如处理指示符消息930所示。该钱包可事先读取并应用该规则,并可拒绝未能满足该规则设定的标准的利用该失业基金的任何购买。示例性标准包括,例如,商家种类编码(MCC),交易时间,交易位置等。举例来说,与具有MCC 5411的杂货商家的交易是被批准的,而与具有MCC 5813的酒吧商家的交易是被拒绝的。

[0162] 参见附图9B,在一个实施例中,该钱包移动应用可基于诸如用户位置、偏好以及偏好的币值因素,帮助动态支付优化。例如,当用户处于美国的时候,该国指示符931可显示美国的标记并可设置货币933为美国。在此外的实现方式,钱包移动应用可自动重排顺序,其中支付形式935被列出以反映各种形式的支付的流行程度或可接受度。在一种实现方式中,该排列可反映用户的偏好,其不能由该钱包移动应用改变。

[0163] 类似地,当德国用户在德国操作钱包的时候,该移动钱包应用用户界面可以被动态地更新来反映德国的操作932和货币934。在此外的实现方式中,钱包应用可重排顺序,其中不同的支付形式936被基于那个国家的接受水平而列出。当然,这些支付形式的顺序可以由用户更改来适应他或者她自己的偏好。

[0164] 参见附图9C,在一个实施例中,钱包移动应用用户界面中的收款人标签937可帮助用户选择一个或多个接收在资金标签中选择的资金的收款人。在一种实现方式中,该用户界面可显示全部收款人938的列表,用户已经早先与他们做过交易,或者可以用来交易。用

户然后可以选择一个或多个收款人。收款人938可包括较大商家诸如Amazon.com公司,和个人诸如Jane P.Doe。紧挨着每个收款人名字可以显示该收款人接受的支付模式的列表。在一种实现方式中,用户可选择收款人Jane P.Doe 939来接收支付。一旦选择,该用户界面可显示涉及该收款人的附加标识信息。

[0165] 参见附图9D,在一个实施例中,模式标签1940可帮助选择该收款人接受的支付模式。多个支付模式可用于选择。示例性模式包括,蓝牙941、无线942、借助用户获得的QR代码的快拍移动943、安全芯片944、TWITTER945、近场通信(NFC)946、蜂窝947、借助用户提供的QR代码的快拍移动948、USB949和FACEBOOK 950,等等。在一种实现方式中,仅仅是由收款人接受的支付模式可以被用户选择。其它非接受的支付模式可以是禁止的。

[0166] 参见附图9E,在一个实施例中,报价标签951可提供实时报价用于用户选择,其与用户的购物车中的物品有关。用户可从适用报价952的列表选择一个或多个报价用于兑换。在一种实现方式中,一些报价可以被组合,而其它不能。当用户选择不能和其他报价组合的报价的时候,未选择的报价可以被禁止。在另一种实现方式中,由钱包应用的推荐引擎推荐的报价可以由指示符标识,诸如953所显示的那个。在另一种实现方式中,用户可通过扩展报价行来读取报价的细节,如用户界面中的954所示。

[0167] 参考图9F,在一个实施例中,社交标签955可帮助整合钱包应用与社交渠道956。在一种实现方式中,用户可选择一个或多个社交渠道956并且可以通过提供社交渠道用户名和密码957到钱包应用并且登陆958来登陆以从钱包应用选择社交渠道。用户然后通过整合的社交渠道来使用社交按钮959发送或接收金额。在另一种实现方式中,用户可通过整合的社交渠道发送社交共享数据,诸如购买信息或链接。在另一个实施例中,用户提供的登录凭证可允许SNAP来参加截取解析。

[0168] 图10示出了在该SNAP的一些实施例中,说明历史模式中的虚拟钱包应用的示例特征的用户接口图。在一个实施例中,用户可以选择历史模式1010来浏览先前购买历史并对那些先前购买执行各种动作。例如,用户可在检索条1011中输入商家识别信息,诸如名称、产品、MCC等。在另一个实现方式中,用户可通过点击麦克风图标1014来使用语音激活的检索特征。钱包应用可查询该移动设备或其它地方(例如,远离该移动设备的一个或多个数据库和/或表格)中的存储区域来查询匹配该检索关键词的交易。该用户界面然后可以显示诸如交易1015的查询的结果。用户界面也可以识别该交易的日期1012、涉及该交易的商家以及物品1013、确认进行了交易、该交易的金额和任何其它相关信息的收据的条型码。

[0169] 在一种实现方式中,用户可选择例如交易1015的交易来浏览该交易的细节。例如,用户可以浏览与该交易相关联的物品的细节和每个物品的金额1016。在另一种实现方式中,用户可选择显示选项1017来浏览对于该交易或该交易中的物品用户可采取的动作1018。例如,用户可添加照片到该交易(例如用户和用户购买的iPad的图片)。在另一种实现方式中,如果用户早先通过社交渠道共享了该购买,可以产生包括该照片的帖子并发送到该社交渠道用于公布。在一种实现方式中,任何共享可以是可选择的,以及不通过社交渠道共享该购买的用户仍然可以通过他或者她直接从钱包应用的历史模式选择的一个或多个社交渠道共享该照片。在另一个实现方式中,用户可以添加该交易到群组,诸如用户建立的公司开支、家庭开支、差旅开支或其它类别。这种群组可以帮助开支的年终结算、工作开支报告的提交、增值税(VAT)退税的提交、人员开支等。在另一实现方式中,用户可以购买交易

中购买的一个或多个物品。用户然后可以在没有去往商家目录或站点来发现该物品的情況下执行交易。在另一种实现方式中,用户也可以在交易中将一个或多个物品放入购物车用于以后购买。

[0170] 在另一个实施例中,该历史模式可以提供便利以用于获得并显示该交易中的物品的评价1019。该评价的来源可以是用户、用户的朋友(例如,来自社交渠道、联系人等等)、从该网页聚集的浏览等。在一些实现方式中,该用户界面也可以允许用户张贴消息到社交渠道(例如TWITTER或FACEBOOK)的其它用户。例如,显示区域1020显示两个用户之间的FACEBOOK消息交换。在一种实现方式中,用户可通过消息1021共享链接。具有嵌入到产品的链接的这种消息的选择可允许用户浏览该产品的说明和/或直接从历史模式购买该产品。

[0171] 在一个实施例中,该历史模式也可以包括用于输出收据的工具。输出收据弹出1022可提供用于输出历史中的交易的收据的多个选项。例如,用户可以使用一个或多个选项1025,其包括保存(到本地移动存储器、到服务器、到云帐户等)、打印到打印机、传真、电子邮件等。用户可以使用他或者她的地址簿1023来查找用于输出的电子邮件或传真号码。用户也可以指定格式选项1024用于输出收据。示例性格式选项包括但不限于:文本文件(.doc,.txt,.rtf,.iif等等)、电子数据表(.csv,.xls等等)、图像文件(.jpg,.tff,.png,等等)、便携式文档格式(.pdf)、附录(.ps)等。用户然后可以点击或轻敲输出按钮1027来启动收据输出。

[0172] 图11A-F示出了在该SNAP的一些实施例中,说明快拍模式中的虚拟钱包应用的示例特征的用户接口图。参见附图11A,在一些实施例中,用户可以选择快拍模式1101来访问快拍特征。在各种实施例中,虚拟钱包应用能够快拍并识别各种物品。例如,虚拟钱包应用能快拍并识别购买发票1103、优惠券104、钱(例如,个人对个人转帐中发送的)1105、账单(例如,公用事业,等等)1106、收据(例如用于存储,开支报告,等等)1107、支付帐户(例如,以添加新的信用/借计/预付卡到该虚拟钱包应用)1108。用户能够通过激活图形用户界面元件1102而随时返回到购物屏幕。在一些实施例中,用户能设置存储在快拍的物品应被发送到(参见1109)的用户的虚拟钱包应用内的购物车或希望列表的名称。在一些实施例中,该虚拟钱包应用可允许用户创建快拍的物品应被添加到的新的购物车或希望列表。

[0173] 在一个实施例中,用户可以选择快拍模式1110来访问它的快拍特征。该快拍模式可以处理任何机器可读的数据表示。这种数据的示例可包括线性和2D条形码,诸如UPC码和QR代码。这些代码可以在收据、产品包装等上找到。该快拍模式也可以处理和操作收据、产品、报价、信用卡或其它支付设备等的图片。图11A示出了快拍模式中的示例性用户界面。用户可以使用他或者她的移动电话来对QR代码1115和/或条型码1114拍照。在一种实现方式中,条1113和快拍框1115可以帮助用户正确地对这些代码拍快照。例如,如图所示,快拍框1115未捕捉代码1116的全部。因而,在这次浏览中捕捉的代码不是可解析,因为该代码中的信息可能是不完整的。这通过表示该快拍模式仍然在寻找代码的条1113上的消息来表示。用户可以更改照相机的变焦水平1117来促进对QR代码拍快照。当代码1116被快拍框1115完全地框住时,条消息可以被更新为例如“快拍发现”。在一种实现方式中,当找到该代码后,用户可以使用移动设备照相机来启动代码捕捉(参见1120)。在另一个实现方式中,快拍模式可以使用该移动设备照相机自动给该代码拍快照(参见1119)。在一些实现方式中,虚拟钱包应用可以在存储QR代码或在交易中使用它以前可选地应用全球定位系统标签(参见

1118) 到该QR代码。

[0174] 参见图11B, 在一个实施例中, 快拍模式可有助于支付再分配张贴交易。例如, 用户可从零售商Acme超市购买杂货和规定物品。用户可以无意中或为了结帐方便, 例如, 使用他或者她的Visa卡来支付杂货和规定物品。然而, 该用户可能具有可用于支付规定物品的FSA帐户, 以及其将提供用户税款利益。在这种情况下, 该用户可以使用快拍模式来启动交易再分配。

[0175] 如图所示, 用户在检索条2121中输入检索项(例如, 帐单)。用户然后可以在标签1122中识别用户希望再分配的收据1123。作为替代地, 用户可以直接给收据上的条形码的图片拍快照, 并且快拍模式可以使用来自该条形码的信息产生并显示收据1123。现在用户可以重新分配1125。在一些实现方式中, 用户也可以对交易提出质疑1124或存档该收据1126。

[0176] 在一种实现方式中, 当选择了重新分配按钮1125时, 钱包应用可以执行收据的光学字符识别(OCR)。收据中的每个物品然后可以被审查来识别一个或多个物品可以被记入到哪个支付设备或账户以用于税款或诸如现金返还、回报点等等的其它收益。在此例子中, 如果被记入到用户的Visa卡的处方药物被记入到用户的FSA, 则有税款收益。钱包应用然后可以执行该再分配作为末端。该再分配处理可以包括钱包联系支付处理方来贷记处方药物的金额到该Visa卡并借记相同金额到用户的FSA帐户。在作为替代的实施方式中, 支付处理方(例如Visa or MasterCard)可获得并OCR该收据, 识别物品和支付帐户以用于再分配并执行该再分配。在一种实现方式中, 钱包应用可请求用户确认将所选物品的计费再分配给另一个支付帐户。在再分配处理完成以后可以产生收据1127。如所讨论的, 该收据示出一些费用已经从Visa账户移动到FSA。

[0177] 参见图11C, 在一个实施例中, 快拍模式可以通过诸如条形码或QR代码的支付代码帮助支付。例如, 用户可以对还没完成的交易的QR代码拍快照。该QR代码可以被显示在商家POS终端处、网站, 或网页应用, 并可以被与识别用于购买物品的信息、商家细节以及其它相关的信息一起编码。当用户快拍诸如QR代码的时候, 快拍模式可以解码该QR代码中的信息并可以使用该解码的信息来产生收据1132。一旦该QR代码被识别, 导航条1131可以指出支付代码被识别。现在用户可以具有选项来添加到购物车1133、利用默认支付帐户支付1134或利用钱包支付1135。

[0178] 在一种实现方式中, 用户可以决定利用默认1134支付。在这个钱包示例中, 钱包应用然后可以使用用户的默认支付方法来完成该购买交易。当完成该交易后, 可以自动产生收据用于证明购买。用户界面也可以被更新以提供其它选项用于处理已完成交易。示例选项包括社交1137来与别人共享购买信息, 如关于图11B所讨论的重新分配1138以及存档1139来存储该收据。

[0179] 参见图11D, 在一个实施例中, 快拍模式也可以帮助报价识别、应用以及存储以备将来之用。例如, 在一个实现方式中, 用户可以快拍报价代码1141(例如, 条形码、QR代码等)。钱包应用然后可以根据编码在该报价代码中的信息产生报价文本1142。用户可以对报价代码执行多个动作。例如, 用户使用查找按钮1143来查找接受该报价代码的所有商家、接受该报价代码的附近商家、来自取得该报价代码资格的商家的产品等。用户也可以使用该添加到购物车按钮1144来应用该报价代码到当前在购物车中的物品。此外, 用户也可以通

过选择保存按钮1145来保存该报价以备将来之用。

[0180] 在一种实现方式中,报价或优惠券1146被应用之后,用户可具有选项来使用查找来查找取得资格的商家和/或产品,该用户可以使用1148进入该钱包,以及用户也可以保存该报价或优惠券1146用于后来使用。

[0181] 参见图11E,在一个实施例中,快拍模式也可以提供便利以用于添加资金来源到钱包应用。在一个实现方式中,诸如信用卡、借记卡、预付卡、智能卡的支付卡以及其它支付帐户可具有关联代码,诸如条形码或QR代码。这种代码可具有编码在其中的支付卡信息,包括但不限于,名称,地址,支付卡类型,支付卡帐户细节,余额,花费限制,回报余额等。在一种实现方式中,该代码可以在物理支付卡的表面被发现。在另一个实现方式中,可以通过访问关联的在线帐户或另一个安全位置获得该代码。然而,在另一个实现方式中,该代码可以被打印在伴随支付卡的信封上。在一种实现方式中,用户可以快拍该代码的图片。钱包应用可以识别支付卡1151并显示编码在支付卡中的文本信息1152。该用户然后通过选择验证按钮1153执行该信息1152的验证。在一种实现方式中,该验证可以包括联系该支付卡的发布方用于确认解码的信息1152以及任何其它相关信息。在一种实现方式中,用户可以通过选择“添加到钱包”按钮1154来添加该支付卡到钱包。添加支付卡到钱包的指令可以促使支付卡作为按照图9A所讨论的资金标签916的支付形式之一出现。用户也可以通过选择取消按钮1155取消输入支付卡作为资金来源。当支付卡已经被添加到钱包时,用户界面可以被更新以通过通知显示1156来指示输入完成。用户然后可以访问钱包1157以开始使用添加的支付卡作为资金来源。

[0182] 参见附图11F,在一些实现方式中,该虚拟钱包应用可通过处理该QR代码识别产品,以及可提供与该产品有关的信息,以及与用于购买该产品、辅助服务等有关的信息。例如,该虚拟钱包应用可提供窗口1161,其中该虚拟钱包应用可显示图像、产品说明书、价格、商家信息等(参见1162)。在一些实现方式中,该虚拟钱包应用可提供包括所显示的信息的QR代码,以便另一个用户可以迅速地快拍该信息来输入它到另一个虚拟钱包应用中。在一些实现方式中,该虚拟钱包应用可提供特征以便用户可以请求门卫服务(例如,当购物时候的帮助)、发货服务(例如,因此用户可以在不需要携带该物品出去的情况下离开商店),1164。在一些实现方式中,该虚拟钱包应用可提供本地商家(例如,使用用户设备的GPS位置)或因特网上的商家的竞争价格(参见1165)。在一些实现方式中,该虚拟钱包应用可向用户提供包括但不限于以下各项的特征:浏览先前快拍,快拍新代码,添加GPS标签到代码,检索早先快拍的代码来使用,手工输入与QR代码有关的信息,把该QR代码归属于对象(例如以便为了组织目的,用于家庭的家具产品的QR代码可以被分组为“卧室家具”对象),等等(参见1166)。在一些实施例中,用户能设置存储在快拍的物品应被发送到的用户虚拟钱包应用内的购物车或希望列表的名称(参见1167)。在一些实施例中,该虚拟钱包应用可允许用户创建快拍的物品应被添加到的新的购物车或希望列表。

[0183] 图12示出了在该SNAP一些实施例中,说明报价模式中虚拟钱包应用的示例特征的用户接口图。在一些实现方式中,SNAP可允许用户从该虚拟钱包移动应用内部检索产品和/或服务的报价。例如,用户可输入文本到图形用户界面(“GUI”)元件1211中,或通过激活GUI元件1212发布语音命令并且讲出命令到设备中。在一些实现方式中,SNAP可基于用户的先前行为、人口统计、当前位置、当前购物车选择或购买物品等提供报价。例如,如果用户处于

实体店,或在线购物网站,以及离开该(虚拟)商店,那么与该商店相关联的商家可能希望提供诱惑处理来怂恿顾客返回该(虚拟)商店。商家可提供这种报价1213。例如,该报价可提供折扣,并可以包括期满时间。在一些实现方式中,其它用户可提供赠品(例如1214)给该用户,其中该用户可以兑换。在一些实现方式中,报价部分可以包括关于对其它用户(例如1215)未完成的资金的支付警告。在一些实现方式中,该报价部分可以包括关于从其它用户请求资金收据的警告(例如1216)。例如,这种特征可以识别从其它应用可接收的资金(例如邮寄,日程表,任务,注释,提醒程序,警告等等),或通过由用户人工输入到该虚拟钱包应用中。在一些实现方式中,报价部分可从SNAP中的参与商家提供报价,例如1217-1219,1220。这些报价可以有时使用参与商家的组合而聚集,例如1217。在一些实现方式中,SNAP本身可以从虚拟钱包应用内为用户随使用特定的支付形式的用户而提供报价,例如1220。

[0184] 图13A-B显示在SNAP的一些实施例中,说明在安全和隐私模式中虚拟钱包应用的示例性特征的用户界面图。参见图13A,在一些实现方式中,用户能浏览和/或更改用户简档和/或用户的设置,例如通过激活用户接口元件。例如,用户能浏览/修改用户名(例如1311a-b)、帐号(例如1312a-b)、用户安全访问码(例如1313-b)、用户pin(例如1314-b)、用户地址(例如,1315-b)、与用户相关联的社会安全号码(例如1316-b)、当前设备GPS位置(例如1317-b)、用户当前所处商店的商家的用户帐户(例如1318-b)、用户的回报帐户(例如1319-b)等。在一些实现方式中,用户能选择哪些数据字段和它们的关联值应被传输从而帮助该购买交易,因此为用户提供增强的数据安全性。例如,在图13A中的示例性说明中,用户已经选择姓名1311a、帐号1312a、安全代码1313a、商家帐户ID 1318a和回报帐户ID 1319a作为将被作为通知的一部分而发送的字段来处理该购买交易。在一些实现方式中,该用户可以套接这些字段和/或数据值,其作为通知的一部分被发送来处理该购买交易。在一些实现方式中,应用可以为用户提供数据字段和/或存储的关联值的多个屏幕来选择为购买定单传输的一部分。在一些实现方式中,应用可以给SNAP提供用户的GPS位置。基于用户的GPS位置,SNAP可以确定用户的环境(例如,用户是否处于商店,医生办公室,医院,邮政办公室等等)。基于该环境,用户应用可以呈现适当字段给用户,用户根据其可以选择字段和/或字段值来作为购买定单传输的一部分发送。

[0185] 例如,用户可能进入医生办公室并希望支付医生预约的共付医疗费。除基本交易信息之外,诸如帐号和名称,该应用可以给用户提供能力来选择传送病历、健康信息,其可以被提供给医疗供应商、保险公司,以及交易处理方来对账当事人之间的支付。在一些实现方式中,该记录可以以符合轻便和义务的健 康保险行动(HIPAA)的数据格式发送并加密,以及只有被授权浏览这种记录的接收方可以具有适当解密密钥来解密并浏览该私人用户信息。

[0186] 参见图13B,在一些实现方式中,在用户的设备上执行的应用可以提供“VerifyChat”特征用于防欺诈。例如,SNAP可以检测出不寻常的和/或可疑的交易。该SNAP可使用该Verifychat特征来与用户通信,并验证该购买交易的发起人的真实性。在各个实现方式中,SNAP可以发送电子邮件消息、文本(SMS)消息、Facebook®消息、Twitter™的tweet、文本聊天、语音聊天、视频聊天(例如,苹果FaceTime)等来与该用户通信。例如,SNAP可以为用户启动视频询问,例如1321。例如,用户可需要通过视频聊天呈现他/她自己,例如1322。在一些实现方式中,客户服务代表例如代理1324可以使用该用户的视频人工地确定

该用户的真实性。在一些实现方式中,SNAP可以使用面部、生物测定等识别方法(例如使用模式分类技术)来确定用户的身份。在一些实现方式中,应用可以提供基准标记(例如十字线、目标框等等)例如1323,以使用户可以提供视频以帮助用户的SNAP的自动识别。在一些实现方式中,用户可能尚未启动交易,例如该交易是欺诈的。在这种实现方式中,用户可以取消该询问。SNAP然后可以取消该交易,和/或代表该用户启动欺诈调查过程。

[0187] 在一些实现方式中,SNAP可以使用文本询问过程来确定用户的真实性,例如1325。例如,SNAP可以通过文本聊天、SMS消息、电子邮件、**Facebook**®消息、Twitter™的tweet等与用户通信。SNAP可以对用户提出询问问题,例如1326。该应用可以提供用户输入界面元件(例如虚拟键盘1328)来回答SNAP提出的询问问题。在一些实现方式中,该询问问题可以由SNAP自动随机地选择;在一些实现方式中,客户服务代表可以人工地与用户通信。在一些实现方式中,用户可能尚未启动该交易,例如该交易是欺诈的。在这种实现方式中,用户可以取消该文本询问。SNAP然后可以取消该交易,和/或替代表用户启动欺诈调查过程。

[0188] SNAP控制器

[0189] 图14显示说明SNAP控制器1401的实施例的框图。在此实施例中,SNAP控制器1401可用来聚集、处理、存储、检索、服务、识别、命令、产生、匹配、和/或通过各种技术帮助与计算机交互,和/或其它相关数据。

[0190] 通常,例如1433a的用户,其可以是人员和/或其它系统,可以接合信息技术系统(例如计算机)来帮助信息处理。反之,计算机采用处理器来处理信息;这种处理器1403可以被称为中央处理单元(CPU)。处理器的一个形式被称为微处理器。CPU使用通信电路来传递二进制编码信号,其作为指令来允许各种操作。这些指令可以是在各种可访问的处理器和可操作存储区1429(例如寄存器、高速缓冲存储器、随机存取存储器等等)中的包含和/或引用其它指令和数据的操作和/或数据指令。这种通信指令可以作为程序和/或数据分量分批(例如批指令)存储和/或传输来帮助所需操作。这些存储的指令代码,例如程序,可以接合CPU电路元件以及其它母板和/或系统组件来执行所需操作。一种程序类型是计算机操作系统,其可以由计算机上的CPU执行的;该操作系统允许并帮助用户访问和运行计算机信息技术和资源。信息技术系统中可以采用的一些资源包括:通过其数据可进出计算机的输入和输出机制;数据可保存在其中的存储器;以及信息可以通过其处理的处理器。这些信息技术系统可以被用来收集数据以用于以后的检索、分析、以及操作,其可通过数据库程序来帮助。这些信息技术系统提供允许用户访问并运行各种系统元件的接口。

[0191] 在一个实施例中,SNAP控制器1401可以被连接至和/或与实体通信,所述实体诸如但不限于:来自用户输入设备1411的一个或多个用户;外围设备1412;可选加密处理设备1428;和/或通信网络1413。例如,SNAP控制器1401可以连接至和/或与用户通信,例如1433a,运行客户端设备,例如1433b,客户端设备包括但不限于:个人计算机、服务器和/或各种移动设备,包括但不限于蜂窝电话、智能电话(例如**iPhone**®, **Blackberry**®, 基于安卓操作系统的电话等等)、平板计算机(例如,Apple iPad™, HP Slate™, 摩托罗拉Xoom™等等)、eBook阅读器(例如Amazon Kindle™、Barnes以及Noble的Nook™eReader等等)、膝上型计算机、笔记本、上网本、游戏控制台(例如XBOX Live™, **任天堂**®DS、索尼**PlayStation**® Portable等等)、便携式扫描仪等。

[0192] 通常认为网络包括客户端、服务器、以及图形拓扑中的中间节点的互连和互操作。

应该注意的是,本申请始终使用的术语“服务器”通常指的是计算机、其它设备、程序或它们的组合,其处理并响应穿过通信网络的远程用户的请求。服务器使用他们的信息来请求“客户端”。正如此处使用的那样,术语“客户端”通常指代计算机、程序、其它设备、用户和/或它们的组合,其能够处理并产生请求以及获得和处理任何从服务器穿过通信网络的响应。帮助信息处理和请求,和/或将信息片段从源用户发送到目标用户的计算机、其它设备、程序、或它们的组合通常称为“节点”。网络通常被认为帮助从源点到目的地的信息传输。具体来讲,从来源推动信息片段到目的地的任务的节点通常被叫作“路由器”。存在许多网络形式,诸如局域网(LANs)、微微网、广域网(WANs),无线网络(WLANs),等等。例如,因特网通常被接受为多个网络的互连,借此远程客户端和服务器可以彼此访问和互操作。

[0193] SNAP控制器1401可以是基于计算机系统的,其可包括但不局限于诸如连接至存储器1429的计算机系统1402的组件。

[0194] 计算机系统

[0195] 计算机系统1402可包括时钟1430、中央处理单元(“CPU”和/或“处理器”(这些术语在整个公开里可互换的使用除非相反地注释))1403、存储器1429(例如,只读存储器(ROM)1406、随机存取存储器(RAM)1405,等等),和/或接口总线1407,并且几乎经常,尽管不一定,全部互联和/或通过一个或多个具有导电和/或其它方式的传输电路路径(指令(例如,二进制编码信号)通过其可传输来实现通信、操作、存储,等等)的(母)板1402上的系统总线1404传递。该计算机系统可以被连接至电源1486;例如,可选地,该电源可以是内部的。可选地,加密处理器1426和/或收发器(例如,IC)1474可以被连接至系统总线。在另一个实施例中,加密处理器和/或收发器可以通过接口总线I/O被连接为内部和/或外部外围设备1412。收发器又可以被连接至天线1475,由此实现各种通信的无线发射和接收和/或传感器协议;例如,天线可以连接至:Texas Instruments WiLink WL1283收发器芯片(例如,提供802.11n,蓝牙3.0,FM,全球定位系统(GPS)(由此允许SNAP控制器确定它的位置));Broadcom BCM4329FKUBG收发器芯片(例如,提供802.11n,蓝牙2.1+EDR,FM,等等);Broadcom BCM4750IUB8接收器芯片(例如,GPS);Infineon Technologies X-Gold 618-PMB9800(例如,提供2G/3G HSDPA/HSUPA通信)等。系统时钟通常具有晶体振荡器并通过该计算机系统的电路路径产生基准信号。时钟通常被连接到系统总线以及将增减基准操作频率用于该计算机系统中互联的其它部件的各种时钟倍乘器。计算机系统时钟和各种部件驱动实现遍及该系统的信息的信号。这种实现遍及计算机系统的信息的指令的发送和接收通常可以称为通信。这些通信指令此外可以被传输、接收,以及促使超出实例计算机系统返回和/或应答通信到:通信网络、输入设备、其他的计算机系统、外围设备等。应该理解的是,在替换实施例中,任何上述部件可以被互相直接连接、连接至CPU和/或按照各种计算机系统举例说明的很多变化来组织。

[0196] CPU包括至少一个足以执行用于执行用户和/或系统产生的请求的程序部件的高速数据处理单元。处理器本身往往将包括各种专业化处理单元,诸如但不局限于:集成系统(总线)控制器、存储器管理控制单元、浮点单元,并且甚至类似图形处理单元的专业化处理子单元、数字信号处理单元等。此外,处理器可包括内部快速存取可寻址存储器,并能够映射和寻址处理器本身以外的存储器1429;内存可包括但不局限于:快速寄存器,各级高速缓冲存储器(例如1、2、3级,等等),RAM等等。处理器可以通过使用通过指令地址可访问的存储

地址空间访问这些存储器,处理器可以构造并解码所述指令,允许它访问去往具有存储状态的具体存储地址空间的电路路径。CPU可以是微处理器,诸如:AMD的Athlon,Duron和/或Opteron;ARM的应用,嵌入式安全处理器;IBM和/或Motorola的DragonBall以及PowerPC;IBM和Sony的Cell处理器;Intel的Celeron,Core (2) Duo,Itanium,Pentium,Xeon,和/或Xscale等处理器。CPU通过根据常规数据处理技术穿过导电和/或传输渠道(例如(印刷)电子和/或光学电路)以执行存储指令(换言之,程序代码)的指令传递与存储器进行交互。这种指令传递帮助了SNAP控制器内的和穿过各种界面以外的通信。如果处理要求规定较大速度和/或容量,可以类似采用分布式处理器(例如,分布式SNAP),大型机,多核,并联,和/或超级计算机体系结构。作为替代地,如果配置需要规定较大的可移植性,则可以采用小型个人数字助理(PDA)。

[0197] 根据特定的实现方式,SNAP的特征可以通过实施诸如CAST的R8051XC2微控制器的微控制器、Intel的MCS 51(即,8051微控制器)等来实现。同时,为实施SNAP的某些特征,一些特征实现方式可依赖嵌入式部件,诸如:专用集成电路(“ASIC”),数字信号处理(“DSP”),现场可编程门阵列(“FPGA”),和/或类似的嵌入式技术。例如,任何SNAP部件集(分布式等)和/或特征可以通过微处理器实现和/或通过嵌入式部件实现;例如,通过ASIC,协处理器,DSP,FPGA等。作为替代地,SNAP的一些实现方式可以利用被配置并用于实现各种特征或信号处理的嵌入式部件实现。

[0198] 根据该特定的实现方式,嵌入式部件可包括软件解决方案,硬件解决方案,和/或硬件/软件解决方案的组合。例如,在此讨论的SNAP特征可以通过实现FPGA来实现,FPGA是包含叫做“逻辑块”的可编程逻辑部件的半导体器件,和可编程互联,诸如高性能FPGA Virtex系列和/或Xilinx生产的低成本Spartan系列。在FPGA被制造之后,逻辑块和互联可以由顾客或设计者编程来实施任何SNAP特征。可编程互联的层级允许逻辑块根据SNAP系统设计者/管理者的需要被互相连接,有点像单片可编程面包板。FPGA的逻辑块可以被编程为执行基本逻辑门的运算,诸如AND和XOR,或更多诸如解码器或简单数学操作的复杂的组合运算符。在大部分的FPGA中,逻辑块还包括存储元件,其可以是电路触发器或存储器的更完整的块。在一些情况下,SNAP可以在规则FPGA上研发,然后移植到更类似ASIC实现方式的固定版本中。作为替代的或协同的实现方式可以迁移SNAP控制器特征到最后的ASIC而不是FPGA,或除FPGA之外还迁移SNAP控制器特征到最后的ASIC。根据前述嵌入式部件的所有实现方式,微处理器可以设想为用于SNAP的“CPU”和/或“处理器”。

[0199] 电源

[0200] 电源1486可以是用于给小型电子电路板设备供电的任何标准形式,诸如下列电池:碱性的,氢化锂,锂离子,锂聚合物,镉镍,太阳能电池等。也可以使用其它类型的交流或直流电源。在太阳能电池的情况下,在一个实施例中,该情况提供孔隙,太阳电池通过其可捕获光子能量。该电池1486与至少一个互联的SNAP的随后部件相连,由此提供电流到所有随后部件。在一个例子中,电源1486与系统总线部件1404相连。在可替代的实施例中,通过穿过I/O 1408界面的连接提供外部电源1486。例如,USB和/或IEEE 1394连接运送数据和功率穿过该连接并因此是合适的电源。

[0201] 接口适配器

[0202] 接口总线1407可接受、连接、和/或传递到多个接口适配器,尽管通常不一定以适

配卡的形式,诸如但不限于:输入输出接口(I/O) 1408,存储接口1409,网络接口1410等。可选的,加密处理器接口1427类似地可以连接至接口总线。该接口总线为彼此以及计算机系统的其它部件提供接口适配器的通信。接口适配器适用于兼容式接口总线。接口适配器通常与接口总线通过插槽结构连接。可以采用传统插槽结构,诸如但不限于:加速图形端口(AGP),卡总线,(扩展的)工业标准结构(EISA),微通道结构(MCA),NuBus,外围部件互连(扩展的)(PCI(X)),PCI直通,个人计算机存储器卡国际联合会(PCMCIA),等。

[0203] 存储接口1409可接受、传递、和/或连接至多个存储设备,诸如但不限于:存储设备1414,可移除磁盘设备等。存储接口可采用连接协议,诸如但不限于:(超)(串行)先进技术附件(分组接口)((超)(串行)ATA(PI)),(增强的)集成驱动电子线路(EIDE),电气与电子工程师协会(IEEE)1394,光纤信道,小型计算机系统接口(SCSI),通用串行总线(USB),等。

[0204] 网络接口1410可接受、传递和/或连接至通信网络1413。通过通信网络1413,SNAP控制器可由用户1433a通过远程客户端1433b(例如,具有网络浏览器的计算机)访问。网络接口可采用连接协议,诸如但不限于:直接连接,以太网(厚,薄,双绞线10/100/1000 10/100/1000Base T等),令牌环网,诸如IEEE802.11a-x的无线连接等。如果处理要求规定较大的总速度和/或容量,可类似地采用分布式网络控制器(例如,分布式SNAP)、结构来汇聚、负载平衡和/或提高SNAP控制器需要的通信带宽。通信网络可以是下列任何一个和/或组合:直接互连;因特网;局域网(LAN);城域网(MAN);作为因特网上的节点的运行任务(OMNI);自定义安全连接;广域网(WAN);无线网络(例如,采用诸如但不限于:无线应用协议(WAP),I-模式等的协议)等。网络接口可以被视为输入输出接口的专用形式。此外,多个网络接口1410可用来与各种通信网络类型1413接合。例如,可以采用多个网络接口来允许经由广播、多播、和/或单播网络的通信。

[0205] 输入输出接口(I/O) 1408可接受、传递和/或连接至用户输入设备1411,外围设备1412,加密处理设备1428等。I/O可采用连接协议,诸如但不限于:音频:模拟,数字,单耳,RCA,立体声等;数据:苹果台式总线(ADB),IEEE 1394a-b,串行,通用串行总线(USB);红外;游戏杆;键盘;midi;光学;PC AT;PS/2;并联;无线电;视频接口:苹果台式连接器(ADC),BNC,同轴,部件,合成,数字,数字视频接口(DVI),高清晰度多媒体接口(HDMI),RCA,RF天线,S-Video,VGA,等;无线收发器:802.11a/b/g/n/x;蓝牙;蜂窝(例如,码分多址(CDMA),高速包存取(HSPA(+)),高速下行链路包存取(HSDPA),全球移动通信系统(GSM),长期演化(LTE),WiMax,等等);等。一种典型输出设备可包括视频显示器,其典型地包括基于阴极射线管(CRT)或液晶显示器(LCD)的监视器,具有从视频接口接受信号的接口(例如DVI电路和电缆)。视频接口合成由计算机系统产生的信息并基于合成的信息在视频存储框架中产生视频信号。另一个输出设备是电视机,其从视频接口接受信号。通常,视频接口通过接受视频显示接口(例如,接受RCA复合视频电缆的RCA复合视频连接器;接受DVI显示电缆的DVI连接器,等等)的视频连接接口提供复合视频信息。

[0206] 用户输入设备1411往往是一种外围设备1412(参见下文)并可包括:卡读取器,保护锁,指纹读取器,手套,图形写字板,游戏杆,键盘,麦克风,鼠标,远程控制器,视网膜读取器,触摸屏(例如,电容性的,电阻性的,等等),轨迹球,轨迹板,传感器(例如,加速度计,环境光,GPS,陀螺仪,邻近等等),输入笔等。

[0207] 外围设备1412可被连接和/或传递到I/O和/或其他类似装备,诸如网络接口,存储接口,直接到接口总线,系统总线,CPU等。外围设备可以是外部的,内部的和/或SNAP控制器的一部分。外围设备可以包括:天线,音频设备(例如,线路输入,线路输出,麦克风输入,扬声器,等等),照相机(例如,静态,视频,网络摄像机,等等),保护锁(例如,用于拷贝保护,利用数字签名确保安全交易等),外部处理器(用于附加的容量;例如,加密装置1428),力反馈设备(例如,振动马达),网络接口,打印机,扫描仪,存储设备,收发器(例如,蜂窝,GPS,等等),视频设备(例如,护目镜,监视器,等等),视频源,头盔等。外围设备经常包括各种类型的输入设备(例如,摄像机)。

[0208] 应该注意的是,尽管可以采用用户输入设备和外围设备,SNAP控制器可以体现为嵌入式、专用和/或更少监视器(即无头的)设备,其中将经由网络接口连接提供访问。

[0209] 加密单元诸如但不局限于:微控制器,处理器1426,接口1427,和/或设备1428,可以附着在和/或与该SNAP控制器通信。由摩托罗拉公司制造的MC68HC16微控制器可以用于和/或在加密单元内。MC68HC16微控制器以16 MHz配置的方式使用16位乘法和加法指令以及需要不到1秒来执行512位RSA私钥运算。加密单元支持来自交互代理以及允许不记名交易的通信的认证。加密单元也可以被配置为CPU的一部分。也可以使用等价微控制器和/或处理器。其他的可以购买到的专用加密处理器包括:Broadcom的CryptoNetx以及其它安全处理器;Ncipher的nShield,SafeNet的Luna PCI(例如,7100)系列;Semaphore Communication的40MHzRoadrunner 184;Sun的加密加速器(例如,加速器6000PCIe板,加速器500Daughtercard);Via纳米处理器(例如,L2100,L2200,U2400)线,其能够执行500+MB/s的加密指令;VLSITechnology的33MHz 6868等。

[0210] 存储器

[0211] 通常,允许处理器实行存储和/或检索信息的任何机制和/或实施例都可看作存储器1429。然而存储器是可代替的技术和资源,因此可以互相替代或结合地采用多个存储器实施例。应该理解的是,SNAP控制器和/或计算机系统可以采用各种形式的存储器1429。例如,计算机系统可以被配置,在其中片上CPU存储器(例如,寄存器),RAM,ROM和任何其它存储设备的操作是由纸张穿孔带或纸张穿孔卡片机制提供的;然而,这种实施例将导致非常慢的操作速度。在典型配置中,存储器1429将包括ROM 1406, RAM 1405,和存储设备1414。存储设备1414可以是任何传统计算机系统存储器。存储设备可以包括鼓;(固定和/或可移除的)磁盘驱动器;磁光驱动器;光驱(即,蓝光,CD-ROM/RAM/可记录(R)/可写(RW),DVD R/RW,HD DVD R/RW等等);设备阵列(例如,独立盘的冗余阵列(RAID));固态存储器设备(USB存储器,固态驱动(SSD)等等);其它处理器可读存储介质;和/或其他类似的设备。因此,计算机系统通常需要并使用存储器。

[0212] 部件集

[0213] 存储器1429可包含程序和/或数据库部件和/或数据的集合,诸如但不局限于:操作系统部件1415(操作系统);信息服务器部件1416(信息服务器);用户接口部件1417(用户接口);网页浏览器部件1418(网页浏览器);数据库1419;邮件服务器部件1421;邮件客户端部件1422;加密服务器部件1420(加密服务器);SNAP部件1435等(即,合称为部件集)。这些部件可以从存储设备和/或从通过接口总线可访问的存储设备存储并访问。尽管非传统程序部件,诸如 部件集合的那些,通常被存储在本地存储设备1414中,但他们也可以通过通

信网络、ROM、各种形式的存储器等被载入和/或存储在诸如外围设备、RAM、远程存储设施的存储器中。

[0214] 操作系统

[0215] 操作系统部件1415是使SNAP控制器的操作变得容易的可执行程序部件。通常,操作系统有助于I/O、网络接口、外围设备、存储设备等的访问。操作系统可以是高度容错、可扩展和安全的系统,诸如苹果Macintosh计算机OS X(服务器);AT&T Plan 9;Be OS;Unix和Unix-like系统分发(诸如AT&T的UNIX;Berkley软件分布程序(BSD)变体,诸如FreeBSD, NetBSD, OpenBSD等;Linux分布,诸如Red Hat, Ubuntu等);和/或类似操作系统。然而,也可以采用更多限制和/或更少安全性的操作系统,诸如苹果Macintosh计算机OS, IBM OS/2, Microsoft DOS, Microsoft Windows 2000/2003/3.1/95/98/CE/Millennium/NT/Vista/XP(服务器), Palm OS等。操作系统可单向和/或双向与部件集中的其他的部件通信,包括本身,等。操作系统最通常与其他的程序部件、用户接口和/或类似部件通信。例如,操作系统可包含、传递、产生、获得、和/或提供程序部件、系统、用户、和/或数据通信、请求和/或响应。一旦由CPU执行,操作系统可允许与通信网络、数据、I/O、外围设备、程序部件、存储器、用户输入设备等交互。操作系统可提供通信协议,其允许SNAP控制器通过通信网络1413与其他的实体通信。SNAP控制器可以使用各种通信协议作为用于交互的副载波传输机制,诸如但不限于:多播, TCP/IP, UDP, 单播等。

[0216] 信息服务器

[0217] 信息服务器部件1416是存储的由CPU执行的程序部件。信息服务器可以是传统因特网信息服务器,诸如但不限于Apache软件基础的Apache, 微软公司的因特网信息服务器等。信息服务器可通过一些设施允许程序部件的执行,诸如:有效服务器页(ASP), ActiveX, (ANSI) (Objective-) C(++), C#和/或.NET, 公共网关接口(CGI)脚本, 动态(D)超文本标记语言(HTML), FLASH, Java, JavaScript, 实际提取报告语言(PERL), 超文本预处理器(PHP), 管道, Python, 无线应用协议(WAP), WebObjects等。信息服务器可支持安全通信协议, 诸如但不限于:文件传输协议(FTP);超文本传输协议(HTTP);安全超文本传输协议(HTTPS), 安全套接层(SSL), 消息传递协议(例如美国在线服务公司(AOL)的即时消息器(AIM), 应用交换(APEX), ICQ, 因特网多线交谈(IRC), 微软网络(MSN)消息器服务, 存在和即时消息协议(PRIM), 因特网工程任务组的(IETF的)会话启动协议(SIP), 用于即时消息和存在影响扩展的SIP(SIMPLE), 开放式基于XML的可扩展消息和存在协议(XMPP)(即Jabber或开放的移动联盟的(OMA的)即时消息和存在服务(IMPS)), 雅虎即时消息器服务等。信息服务器提供网页形式的结果到网页浏览器, 并且允许通过与其它程序部件交互的网页的受控生成。在HTTP请求的域名系统(DNS)解析部分被解决为特定的信息服务器之后, 信息服务器基于HTTP请求的其余部分, 在SNAP控制器上的指定位置解析对信息的请求。例如, 诸如http://123.124.125.126/myInformation.html的请求可能具有请求的IP部分“123.124.125.126”, 其通过DNS服务器被解析为那个IP地址处的信息服务器;那个信息服务器此外可能又解析请求的“/myInformation.html”部分的http请求并且将它解析为包含信息“myInformation.html”的存储器中的位置。此外, 用作协议的其它信息可以跨各种端口来采用, 例如, 跨端口的FTP通信等。信息服务器可以单向和/或双向地与部件集中的其它部件通信, 包括本身, 和/或类似设施。大部分的信息服务器经常与SNAP数据库1419, 操作系

统,其他的程序部件,用户接口,网页浏览器等通信。

[0218] 对SNAP数据库的访问可以通过多个数据库桥接机制实现,诸如通过如以下列举的脚本语言(例如,CGI)以及通过如以下列举的应用间通信信道(例如CORBA,WebObjects,等等)。通过网页浏览器的任何数据请求通过该桥接机制被解析为如SNAP需要的适当语法。在一个实施例中,信息服务器将提供网页浏览器可访问的网页表格。网页表格中被填进所提供的字段的条目被标志为已经被输入特定的字段并且因而被解析。输入的术语然后被随着字段标签传递,其命令分析器产生指向适当表格和/或字段的查询。在一个实施例中,基于标志的文本条目,分析器可以通过利用适当的join/select命令实例化检索串而产生标准SQL方式的查询,其中经由桥接机制提供结果命令到SNAP作为查询。当根据该查询产生查询结果后,该结果被经由桥接机制传递,并且可以由该桥接机制解析以用于格式化以及新结果网页的生成。这种新结果网页然后被提供到信息服务器,信息服务器可以将它提供到发出请求的网页浏览器。

[0219] 同样,信息服务器可包含、传递、产生、获得和/或提供程序部件、系统、用户、和/或数据通信、请求、和/或响应。

[0220] 用户接口

[0221] 计算机接口在某些方面与汽车操作接口相似。汽车操作接口元件,诸如方向盘,变速器,以及速度计有助于汽车资源和状态的访问,操作以及显示。计算机交互接口元件,诸如复选框,光标,菜单,卷轴和窗口(合称为以及通常称为窗口小部件)类似地有助于数据和计算机硬件和操作系统资源和状态的访问,容量,操作,和显示。操作接口通常被叫做用户接口。图形用户接口(GUI)提供图形地向用户访问和显示信息的基线和装置,GUI诸如是苹果Macintosh计算机操作系统的Aqua,国际商业机器公司的OS/2,微软公司的Windows2000/2003/3.1/95/98/CE/Millennium/NT/XP/Vista/7(即Aero),Unix的X-Windows(例如,其可包括附加Unix图形接口库以及诸如K台式环境(KDE)的层,mythTV以及GNU网络对象模型环境(GNOME)),网页接口库(例如,ActiveX,AJAX,(D)HTML,FLASH,Java,JavaScript等等,接口库诸如但不限于,Dojo,jQuery(UI),MooTools,Prototype,script.aculo.us,SWFObject,雅虎用户接口,任何可以被使用的)。

[0222] 用户接口部件1417是由CPU执行的存储程序部件。用户接口可以是由例如已经讨论的操作系统和/或操作环境提供的和/或在已经讨论的操作系统和/或操作环境之上的传统图形用户接口。用户接口可以允许通过文本和/或图形设施显示,执行,交互,处理,和/或操作程序部件和/或系统设施。用户接口提供设施,用户通过其能实施、相互作用和/或运行计算机系统。用户接口可以单向和/或双向地与部件集内的其他部件通信,包括本身,和/或类似设施。大部分的用户接口经常与操作系统、其他的程序部件等通信。该用户接口可包含、传递、产生、获得和/或提供程序部件、系统、用户、和/或数据通信、请求、和/或响应。

[0223] 网页浏览器

[0224] 网页浏览器部件1418是由CPU执行的存储程序部件。网页浏览器可以是传统超文本浏览应用,诸如Microsoft Internet Explorer或Netscape Navigator。安全网页浏览可以通过HTTPS,SSL等利用128位(或更多)加密来提供。网页浏览器允许程序部件通过设施的执行,诸如ActiveX,AJAX,(D)HTML,FLASH,Java,JavaScript,网页浏览器插件APIs(例如,Firefox,Safari Plug-in 等API)等。网页浏览器和类似信息访问工具可以被集成到PDA,

蜂窝电话,和/或其他的移动设备。用户网页浏览器可以单向和/或双向地与部件部件集内的其他部件通信,包括本身,和/或类似设施。大部分的网页浏览器经常与信息服务器,操作系统,集成的程序部件(例如插件)等通信;例如,它可包含、传递、产生、获得和/或提供程序部件、系统、用户和/或数据通信、请求和/或响应。同样,代替网页浏览器和信息服务器,也可以开发组合应用来执行二者的相似操作。组合应用类似地实施从支持SNAP的节点实施信息的获得和提供信息到用户,用户代理等。该组合应用可以在采用标准网页浏览器的系统上是无关紧要的。

[0225] 邮件服务器

[0226] 邮件服务器部件1421是由CPU 1403执行的存储程序部件。邮件服务器可以是传统因特网邮件服务器,诸如但不限于sendmail、Microsoft Exchange等。邮件服务器可通过一些设施允许程序部件的执行,诸如ASP,ActiveX,(ANSI)(Objective-)C(++),C#_和/.NET,CGI脚本,Java,JavaScript,PERL,PHP,pipes,Python,WebObjects等。邮件服务器可支持通信协议,诸如但不限于:Internet消息访问协议(IMAP),消息应用编程接口(MAPI)/Microsoft Exchange,post office protocol(POP3),简单邮件传送协议(SMTP)等。邮件服务器可以路由,转发和处理输入和输出邮件消息,其已经被发送,中继和/或穿越通过和/或到该SNAP。

[0227] 对SNAP邮件的访问可以通过由单个网页服务器部件和/或操作系统提供的多个API实现。

[0228] 同时,邮件服务器可包含、传递、产生、获得和/或提供程序部件、系统、用户、和/或数据通信、请求、信息和/或响应。

[0229] 邮件客户端

[0230] 邮件客户端部件1422是由CPU 1403执行的存储程序部件。邮件客户端可以是传统邮件浏览应用,诸如:Apple Mail,Microsoft Entourage,Microsoft Outlook,Microsoft Outlook Express,Mozilla,Thunderbird等。邮件客户端可支持多个传输协议,诸如:IMAP,Microsoft Exchange,POP3,SMTP等。邮件客户端可单向和/或双向地与部件集中的其他的部件通信,包括本身,和/或类似设施。大部分的邮件客户端经常与邮件服务器、操作系统、其它邮件客户端等通信;例如,它可包含、传递、产生、获得和/或提供程序部件、系统、用户和/或数据通信、请求、信息和/或响应。邮件客户端通常提供设施来编写并传输电子邮件消息。

[0231] 加密服务器

[0232] 加密服务器部件1420是由CPU 1403、加密处理器1426、加密处理器接口1427、加密处理器设备1428等执行的存储程序部件。加密处理器接口将允许加密元件请求的加密和/或解密的加速;然而,作为选择,加密元件可以运行在传统CPU上。加密元件允许所提供数据的加密和/或解密。加密元件允许对称的和非对称的(例如,Pretty Good Protection(PGP))加密和/或解密。加密元件可采用的加密技术诸如但不限于:数字证书(例如,X.509认证框架),数字签名,双重签名,信封,密码存取保护,公钥管理等。加密元件将有助于很多(加密和/或解密)安全协议,诸如但不限于:校验和,数据加密标准(DES),椭圆曲线加密(ECC),国际数据加密算法(IDEA),消息摘要(MD5,其是散列运算的一种方式),密码,Rivest Cipher(RC5),Rijndael,RSA(其是使用1977年由Ron Rivest,Adi Shamir和

Leonard Adleman开发的算法的因特网加密和认证系统),安全散列算法(SHA),安全套接层(SSL),安全超文本传输协议(HTTPS)等。采用这些加密安全协议,SNAP可以加密所有输入和/或输出通信并可以利用更宽的通信网络用作虚拟专用网络(VPN)内的节点。加密元件有助于“安全授权”的处理,借此通过安全协议禁止对资源的访问,其中,该加密元件实施对安全资源的授权访问。此外,加密元件可提供内容的唯一标识符,例如采用以及MD5散列来为数字音频文件获得唯一签名。加密元件可以单向和/或双向地与部件集内的其他部件通信,包括本身,和/或类似设施。如果需要,加密元件支持允许信息穿过通信网络的安全传输来允许SNAP部件参加安全交易的加密机制。加密元件有助于SNAP上的资源的安全访问以及有助于远程系统上的安全资源的访问;即它可以作为安全资源的客户端和/或服务器。大部分的加密元件经常与信息服务器,操作系统,其他的程序部件等通信。该加密元件可包含、传递、产生、获得和/或提供程序部件、系统、用户和/或数据通信、请求、和/或响应。

[0233] SNAP数据库

[0234] SNAP数据库部件1419可以被嵌入在数据库及其所存储的数据中。数据库是存储程序部件,其由CPU执行;存储程序部件部分配置CPU来处理所存储的数据。数据库可以是传统、容错、关联、可扩展、安全的数据库,诸如Oracle或Sybase。关系数据库是平面文件的扩展。关系数据库包含一系列相关表。表通过键字段互相连接。键字段的使用允许通过相对于键字段的索引而组合表;即,键字段作为用于各种表的组合信息的维数支点。关系通常借助于匹配初级键来识别表之间的链接。初级键表示唯一地识别关系数据库中的表的行。更确切的说,他们唯一地识别一对多关系的“一”侧的表行。

[0235] 可替代地,SNAP数据库可以使用各种标准数据结构实现,诸如阵列,散列,(链)表,结构,结构文本文件(例如XML),表格等。这些数据结构可以存储在存储器中。在另一个替换中,可以使用面向对象的数据库,诸如Frontier,ObjectStore,Poet,Zope,等。对象数据库可包括多个对象集合,其通过公共属性被分组和/或链接起来;他们通过一些公共属性与其它对象集合相关。面向对象数据库与关系数据库类似地执行,除了其对象不只是数据片段,而可以具有给定对象内封装的功能的其他类型。如果SNAP数据库实现为数据结构,则SNAP数据库1419的使用可以被集成到另一个部件中,诸如SNAP部件1435。同样,数据库可以实现为数据结构、对象以及关系结构的混合。数据库可以通过标准数据处理技术以无数的变化被合并和/或分布。数据库的一些部分,例如表格,可以被输出和/或输入并因此分散和/或集成。

[0236] 在一个实施例中,该数据库部件1419包括若干表格1419a-o。用户表格1419a可包括字段,诸如但不限于:user_id,ssn,dob,first_name,last_name,age,state,address_firstline,address_secondline,zipcode,devices_list,contact_info,contact_type,alt_contact_info,alt_contact_type,等。用户表格可支持和/或追踪SNAP上的多个实体帐户。设备表格1419b可包括字段,诸如但不限于:device_ID,device_name,device_IP,device_MAC,device_type,device_model,device_version,device_OS,device_apps_list,device_securekey,wallet_app_installed_flag,等。Apps表格1419c可包括字段,诸如但不限于:app_ID,app_name,app_type,app_dependencies,等。帐户表格1419d可包括字段,诸如但不限于:account_number,account_security_code,account_name,issuer_acquirer_flag,issuer_name,acquirer_name,account_address,routing_number,

access_API_call,linked_wallets_list等。商家表格1419e可包括 字段,诸如但不局限于:merchant_id,merchant_name,merchant_address,ip_address,mac_address,auth_key,port_num,security_settings_list,等。发布方表格1419f可包括字段,诸如但不局限于:issuer_id,issuer_name,issuer_address,ip_address,mac_address,auth_key,port_num,security_settings_list等。收单机构表格1419g可包括字段,诸如但不局限于:account_firstname,account_lastname,account_type,account_num,account_balance_list,billingaddress_line1,billingaddress_line2,billing_zipcode,billing_state,shipping_preferences,shippingaddress_line1,shippingaddress_line2,shipping_zipcode,shipping_state等。支付网关表格1419b可包括字段,诸如但不局限于:gateway_ID,gateway_IP,gateway_MAC,gateway_secure_key,gateway_access_list,gateway_API_call_list,gateway_services_list,等。交易表格1419i可包括字段,诸如但不局限于:order_id,user_id,timestamp,transaction_cost,purchase_details_list,num_products,products_list,product_type,product_params_list,product_title,product_summary,quantity,user_id,client_id,client_ip,client_type,client_model,operating_system,os_version,app_installed_flag,user_id,account_firstname,account_lastname,account_type,account_num,account_priority_account_ratio,billingaddress_line1,billingaddress_line2,billing_zipcode,billing_state,shipping_preferences,shippingaddress_line1,shippingaddress_line2,shipping_zipcode,shipping_state,merchant_id,merchant_name,merchant_auth_key等。批表格1419j可包括字段,诸如但不局限于:batch_id,transaction_id_list,timestamp_list,cleared_flag_list,clearance_trigger_settings等。分类账表格1419k可包括字段,诸如但不局限于:request_id,timestamp,deposit_amount,batch_id,transaction_id,clear_flag,deposit_account,transaction_summary,payor_name,payor_account等。产品表格1419l可包括字段,诸如但不局限于:product_ID,product_title,product_attributes_list,product_price,tax_info_list,related_products_list,offers_list,discounts_list,rewards_list,merchants_list,merchant_availability_list等。报价表格1419m可包括字段,诸如但不局限于:offer_ID,offer_title,offer_attributes_list,offer_price,offer_expiry,related_products_list,discounts_list,rewards_list,merchants_list, merchant_availability_list,等。行为数据表格1419n可包括字段,诸如但不局限于:user_id,timestamp,activity_type,activity_location,activity_attribute_list,activity_attribute_values_list等。分析表格1419o可包括字段,诸如但不局限于:report_id,user_id,report_type,report_algorithm_id,report_destination_address等。

[0237] 在一个实施例中,SNAP数据库可以与其它数据库系统交互。例如,采用分布式数据库系统,通过检索SNAP部件进行的查询以及数据访问可以处理SNAP数据库、集成的数据安全层数据库的组合为单个数据库实体。

[0238] 在一个实施例中,用户程序可包含各种用户接口图元,其可用来更新SNAP。同样,根据SNAP可能需要服务的环境以及客户端类型,各种帐户可能需要自定义数据库表。应该注意的是,任何唯一字段可以被指定为通篇的键字段。在作为替代的实施例中,这些表格已

经被分散到他们自己的数据库和它们各自的数据库控制器中(即,用于每一个上述表格的单个数据库控制器)。采用标准数据处理技术,人们可以进一步经由若干计算机系统和/或存储设备分发该数据库。类似地,通过合并和/或分布各种数据库部件1419a-o,分散的数据库控制器的配置可以被改变。SNAP可以被配置为通过数据库控制器跟踪各种设置、输入和参数。

[0239] SNAP数据库可以单向和/或双向地与部件集内的其他部件通信,包括本身,和/或类似设施。大部分的SNAP数据库经常与SNAP部件、其他的程序部件等通信。数据库可包含、维持和提供关于其它节点和数据的信息。

[0240] SNAP

[0241] SNAP部件1435是由CPU执行的存储程序部件。在一个实施例中,SNAP部件包括在前面附图中讨论的SNAP的各方面的任何一个和/或所有组合。因而,SNAP跨各种通信网络实施信息、服务、交易等的访问,获得和供应。

[0242] SNAP部件可通过SNAP部件转换实时产生的商家-产品快速响应代码为基于虚拟钱包卡的交易购买通知等和SNAP的使用。在一个实施例中,SNAP部件1435进行输入(例如,结帐输入411;产品数据414;支付输入419;发布方服务器数据423;用户数据427a-n等),并通过SNAP部件转换输入(例如,SMPE 1441;QRCP 1442等)为输出(例如,QR支付代码417;卡授权请求421;授权响应429a-n;授权成功消息433a-b;批附加数据435;购买收据436等)。

[0243] 允许节点间信息访问的SNAP部件可以通过采用标准开发工具和语言开发,诸如但不局限于:Apache部件,Assembly,ActiveX,可执行的二进制,(ANSI)(Objective-)C(++),C#和/或.NET,数据库适配器,CGI脚本,Java,JavaScript,绘图工具,面向过程和对象的开发工具,PERL,PHP,Python,shell脚本,SQL命令,网页应用服务器扩展,网页开发环境和库(例如,微软公司的ActiveX;Adobe AIR,FLEX&FLASH;AJAX;(D)HTML;Dojo,Java;JavaScript;jQuery(UI);MooTools;Prototype;script.aculo.us;简单对象存取协议(SOAP);SWFObject;雅虎用户接口等),WebObjects等。在一个实施例中,SNAP服务器采用加密服务器来加密和解密通信。SNAP元件可单向和/或双向地与部件集内的其他部件通信,包括本身,和/或类似设施。大部分的SNAP部件经常与SNAP数据库、操作系统、其他的程序部件等通信。SNAP可包含、传递、产生、获得和/或提供程序部件、系统、用户和/或数据通信、请求和/或响应。

[0244] 分布式SNAP

[0245] 任何SNAP节点控制器部件的结构和/或操作可以以任意多种方式组合、合并和/或分布来帮助开发和/或配置。类似地,可以以任意多种方式组合部件集以帮助部署和/或开发。为实现这一点,可以集成部件到公共代码基础中或到可以按需以集成的方式动态地加载部件的设施中。

[0246] 部件集可以被以无数的变化通过标准数据处理和/或开发技术而合并和/或分布。程序部件集中的程序部件的任一项的多个实例可以被实例化在单个节点上,和/或跨多个节点以通过负载平衡和/或数据处理技术提高性能。此外,单个实例也可以是跨多个控制器和/或存储设备分布的;例如,数据库。一起工作的所有程序部件实例和控制器可以通过标准数据进程通信技术这样做。

[0247] SNAP控制器的配置将取决于系统部署的环境。这些因素诸如但不局限于:预算,容

量,位置和/或底层硬件资源的使用可以实施部署要求和配置。不考虑配置是否导致更多合并和/或集成程序部件,导致更多分布的程序部件系列,和/或导致合并和分布式配置间的组合,数据可以被传递,获得,和/或提供。根据程序部件集,合并到公共代码基础中的部件实例可以传递,获得,和/或提供数据。这些可通过应用内数据处理通信技术来实现,诸如但不限于:数据引用(例如指针),内部消息传递,对象实例变量通信,共享存储器空间,变量传递等。

[0248] 如果部件集部件是相互分立的、独立的和/或外部的,那么传递、获得和/或提供数据与和/或到其他的部件可以通过应用内数据处理通信技术实现,诸如但不限于:应用程序接口(API)信息传递;(分布式)部件对象模型((D)COM),(分布式)对象链接与嵌入((D)OLE)等),公共对象请示代理体系结构(CORBA),Jini本地和远程应用程序接口,Javascript对象注释(JSON),远程方法引用(RMI),SOAP,进程管道,共享文件等。应用间内通信的分立部件之间或在应用内通信的单个部件的存储空间内部发送的消息可以有助于语法的创建和解析。语法可以使用开发工具开发,诸如lex,yacc,XML等,其允许语法生成和解析功能,其又可以形成部件内部和之间的通信消息的基础。

[0249] 例如,语法可以设置为识别HTTP张贴指令的令牌,例如:

[0250] w3c-post http://...Value1

[0251] 其中Value1识别为一种参数,因为“http://”是语法体系的一部分,并且后续被认为是张贴值的一部分。类似地,利用这种语法,变量“value1”可以插入到“http://”张贴命令中然后被发送。语法体系本身可以呈现为结构化数据,其被解释和/或用于产生解析机制(例如lex,yacc等等处理的语法描述文本文件)。同样,一旦产生和/或实例化了解析机制,它本身处理和/或解析结构化数据,诸如但不限于:描绘文本的字符(例如标签),HTML,结构化文本流,XML等结构化数据。在另一个实施例中,应用间数据处理协议本身可具有集成和/或容易地可用的解析器(例如,JSON,SOAP,等解析器),其可以用于解析(例如,通信)数据。此外,解析语法可以被使用在消息解析之上,但也可以用于解析:数据库,数据集,数据存储,结构化数据等。再次,期望的配置将取决于语境,环境,以及系统开发的需要。

[0252] 例如,在一些实现方式中,SNAP控制器可以通过信息服务器执行实现安全套接层(“SSL”套接服务器)的PHP脚本,其侦听客户端可以发送数据(例如以JSON格式编码的数据)的服务器端口上的输入通信。一旦识别输入通信,PHP脚本可以从客户端设备读取输入消息,解析该接收的JSON编码的数据以便从JSON编码的文本数据提取信息到PHP脚本变量中,并在使用结构化查询语言(“SQL”)可访问的关系数据库中存储该数据(例如,客户端识别信息,等等)和/或提取的信息。基本上以PHP/SQL命令的形式写入,来通过SSL连接从客户端设备接受JSON编码的输入数据、解析数据以便提取变量,并存储数据到数据库的示例性列表如下提供:

[0253]

```

<?PHP
header('Content-Type: text/plain');

// set ip address and port to listen to for incoming data
$address = '192.168.0.100';
$port = 255;

// create a server-side SSL socket, listen for/accept incoming communication
$sock = socket_create(AF_INET, SOCK_STREAM, 0);
socket_bind($sock, $address, $port) or die('Could not bind to address');
socket_listen($sock);
$client = socket_accept($sock);

// read input data from client device in 1024 byte blocks until end of message
do {
    $input = "";
    $input = socket_read($client, 1024);
    $data .= $input;
} while($input != "");

// parse data to extract variables
$obj = json_decode($data, true);

// store input data in a database
mysql_connect("201.408.185.132", $DBserver, $password); // access database server
mysql_select("CLIENT_DB.SQL"); // select database to append
mysql_query("INSERT INTO UserTable (transmission)
VALUES ($data)"); // add data to UserTable table in a CLIENT database
mysql_close("CLIENT_DB.SQL"); // close connection to database
?>

```

[0254] 同样,下列资源可用来提供关于SOAP解析器实现方式的示例性实施例:

[0255] <http://www.xav.com/perl/site/lib/SOAP/Parser.html>

[0256] [http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?](http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm)
topic=/com.ibm

[0257] .IBMDI.doc/referenceguide295.htm

[0258] 以及其它解析器实现方式:

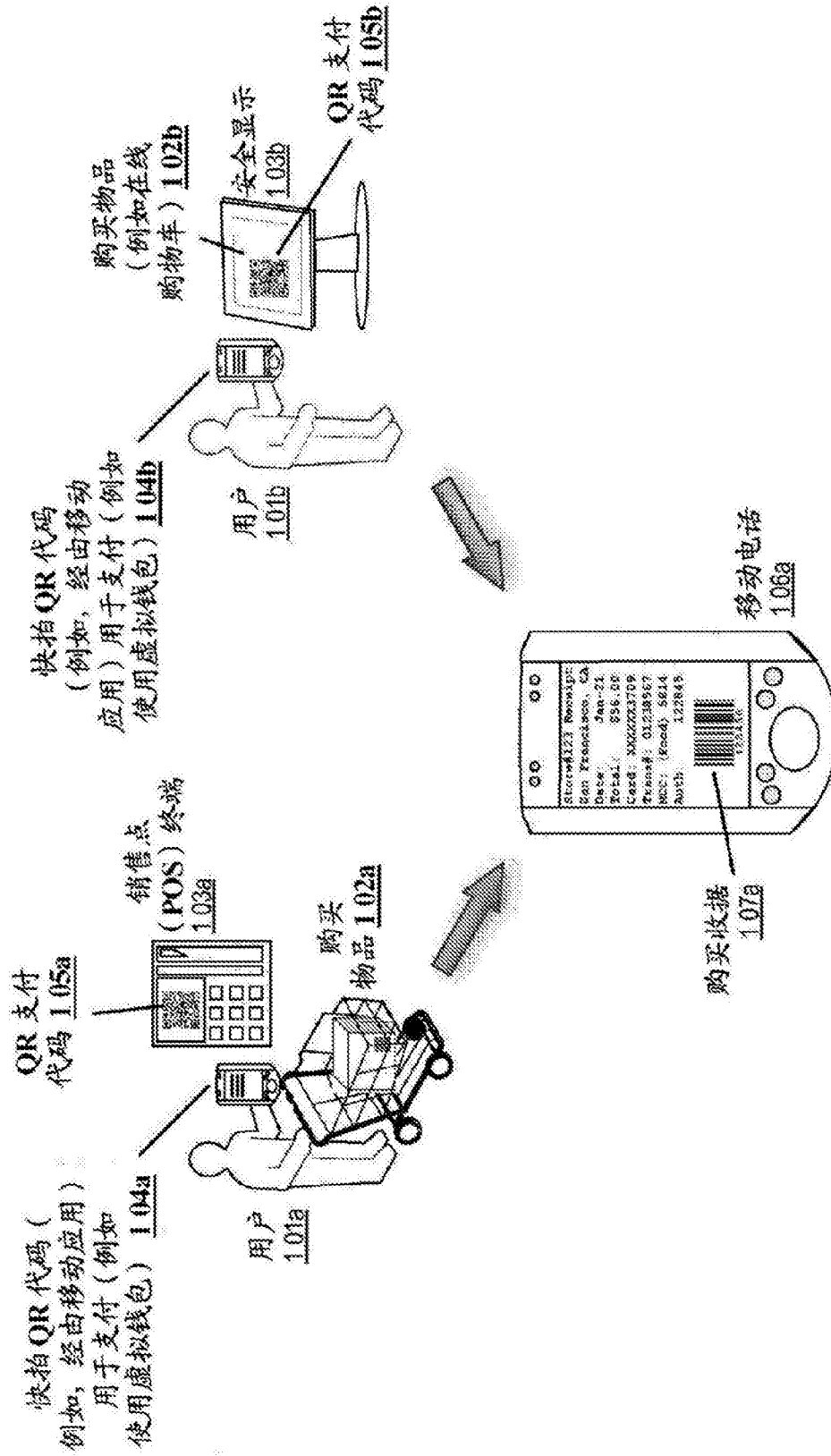
[0259] [http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?](http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm)
topic=/com.ibm

[0260] .IBMDI.doc/referenceguide259.htm

[0261] 因此通过引用将所有这些包括在此。

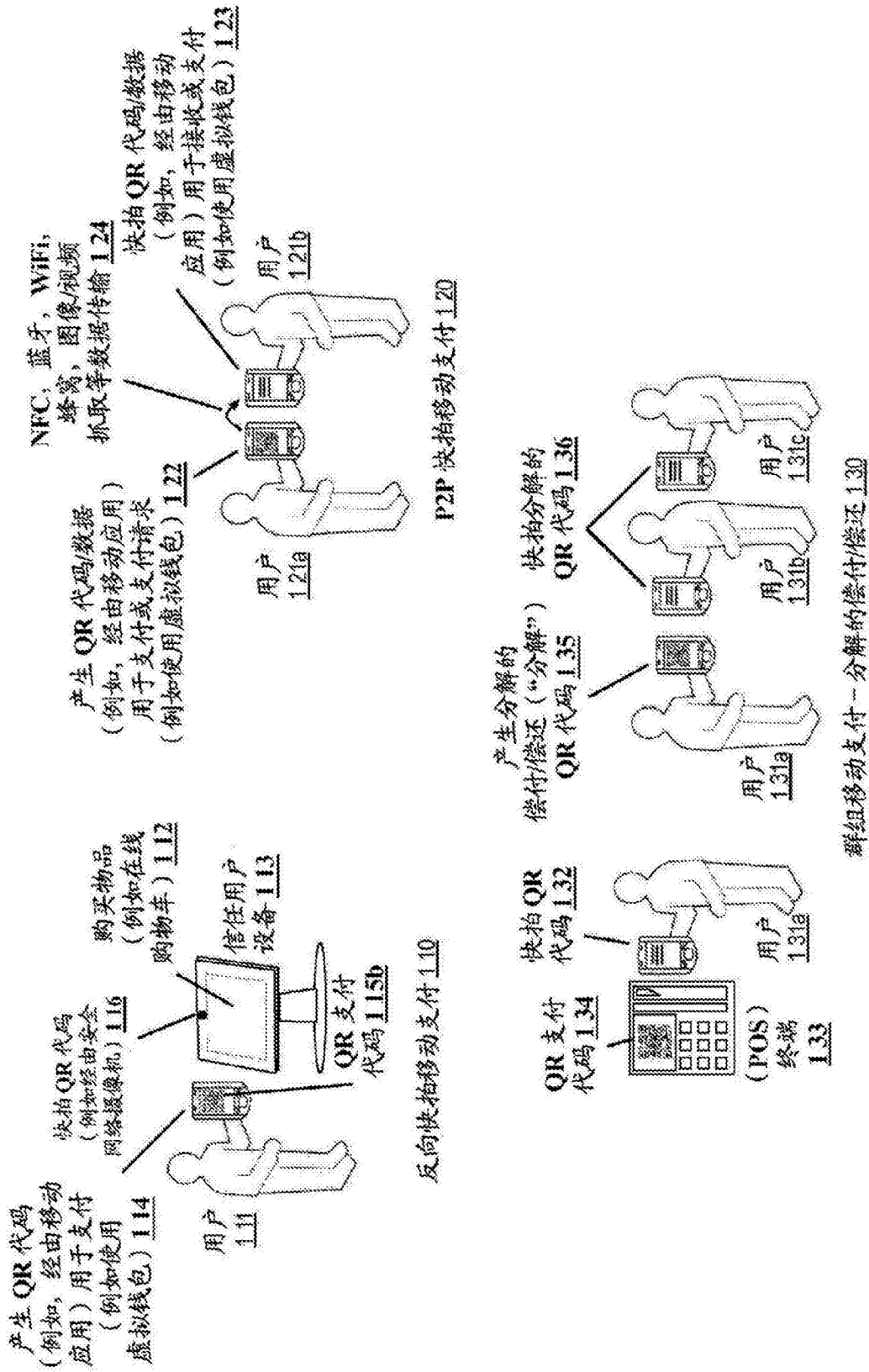
[0262] 为了解决各种问题并发展技术,用于快拍移动支付装置、方法和系统(包括封面,标题,小标题,技术领域,背景技术,发明内容,附图说明,具体实施方式,权利要求,摘要,附图,附录和/或其他)的本申请的全部通过各种示意图实施例显示,其中所要求的创新可以被实行。本申请的优点和特征仅是实施例的代表性示例,不是穷举和/或排他的。他们存在仅仅用于帮助理解和教导如权利要求所述的原理。应该理解的是,他们不是代表所有如权利要求所述的创新。因而公开内容的某些方面没有在此论述。替代性的实施例未必已经呈现用于本发明的具体部分或此外未描述的替代性的实施例可以被可获得用于设想替代性的实施例的放弃的部件。将理解的是,许多那些未描述的实施例采用本发明相同原理及其他是等价的。因此,应该理解的是,在不脱离该公开内容的范围和/或精神的情况下可以使用其它实施例以及产生功能逻辑,操作,组织的,结构和/或拓扑修改。因而,在整个公开内容中,所有示例和/或实施例被认为是非限制的。没有推断应被引起考虑在此论述的那些

实施例相对于在此未论述的那些,除为了降低空间以及重复起见以外的。例如,应该理解的是,任何程序部件(部件集合)的任何群组的逻辑和/或拓扑结构,如附图和/或全部所描述的其它部件和/或提供部件设置不局限于固定的运行顺序和/或排列,而是任何公开的顺序是示例性以及都等价,不考虑顺序是该公开内容设想的。此外,应该理解的是,这种部件不局限于串行执行,而是多个线程,处理,服务,服务器,和/或那些能异步地、同步、并行、同时,同步执行的那些,等是该公开内容设想的。因而,一些部件可以相互对立的,因为它们不能同时存在于单个实施例中。类似地一些部件适用于本发明的一种方面,以及不适用的其它方面。此外,公开内容包括其它目前未要求的新方法。对目前未经要求的新方法申请人保留所有权利,包括要求这种新方法、文件增补申请、继续、部分地继续、分割和/或它的同类的权利。因而,应该理解的是,该公开内容的优势,实施例,示例,功能,部件,逻辑操作,组织,结构,拓扑和/或其它方面不是设想限制在权利要求书所定义的公开内容上或限制在相当于权利要求书上。应该理解的是,根据SNAP个人和/或企业用户,数据库配置和/或关系模型,数据类型,数据传输和/或网络框架,语法结构等的特定的需要和/或特性,SNAP的各种实施例可以被实施,其允许许多灵活性和定制。例如,SNAP的各方面可以修改以适合于饭店订餐,在线购物,在实体店中购物,安全信息处理,保健信息系统等。然而当SNAP的各种实施例和讨论已经指向电子购买交易时,应该理解的是,此处的实施例可以被容易地配置和/或自定义用于各式各样的其它应用和/或实现方式。



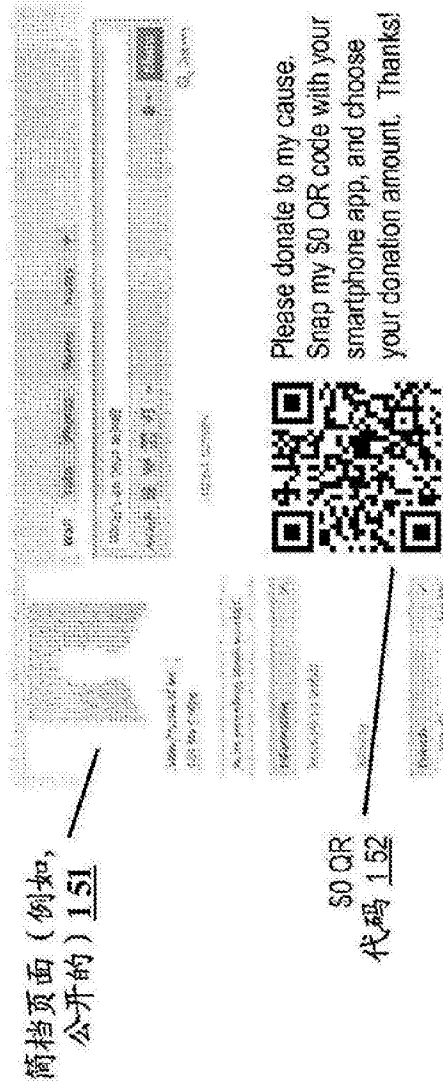
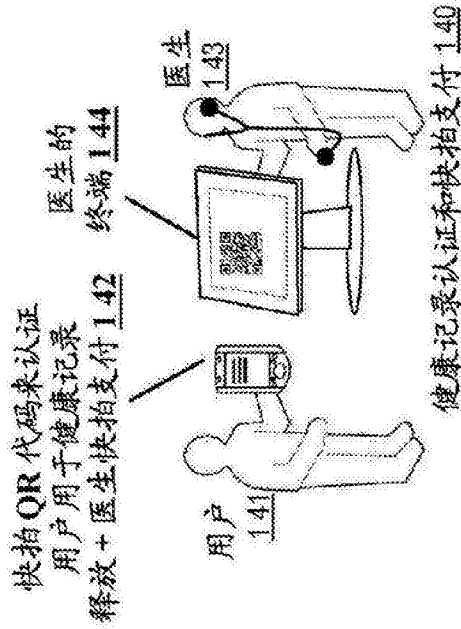
示例: 快拍移动支付

图1A



示例: 快拍移动支付

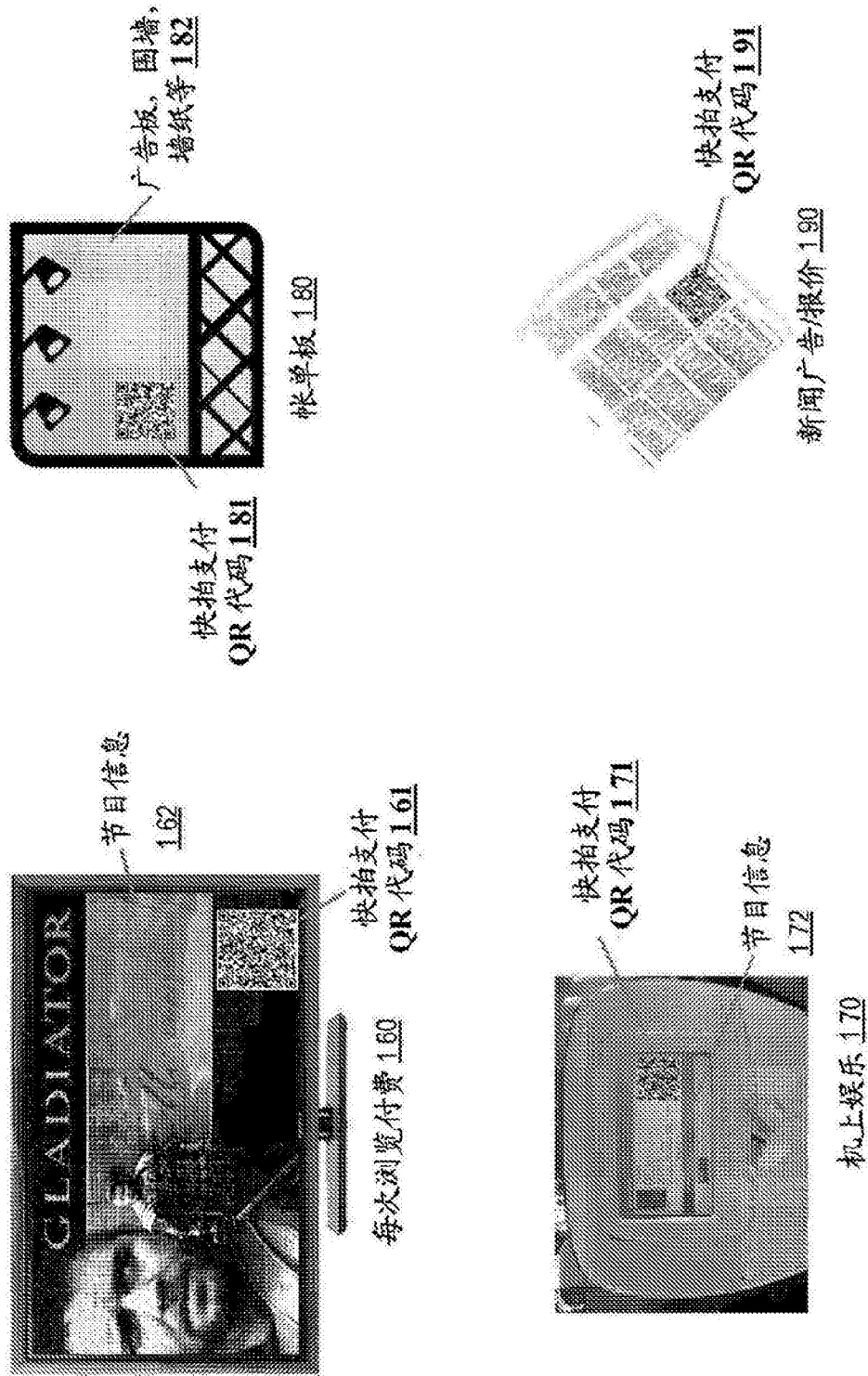
图1B



预先提交的/可修改的快拍支付 1.50

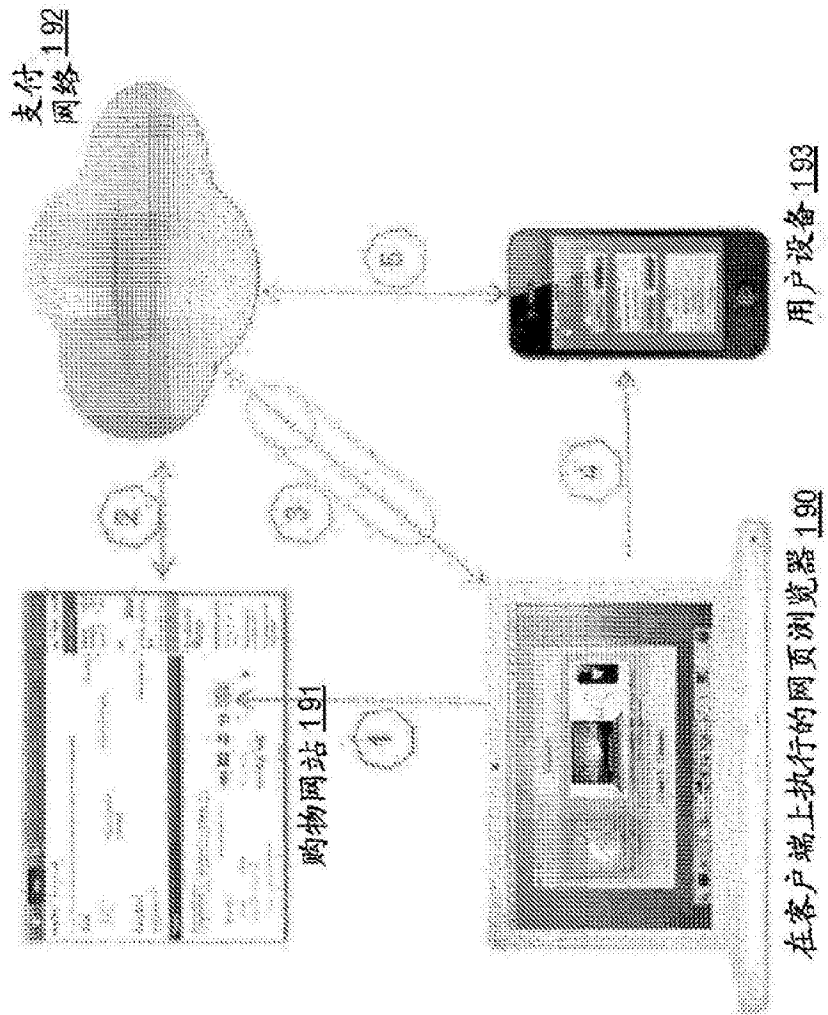
示例: 快拍移动支付

图1C



示例: 快拍移动支付

图1D



示例：快拍移动支付

图1E

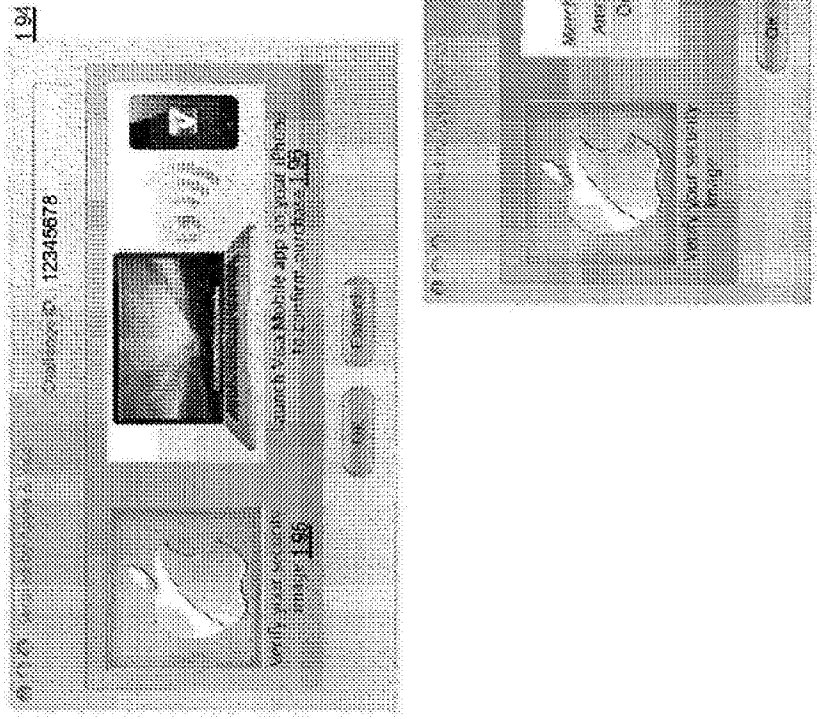
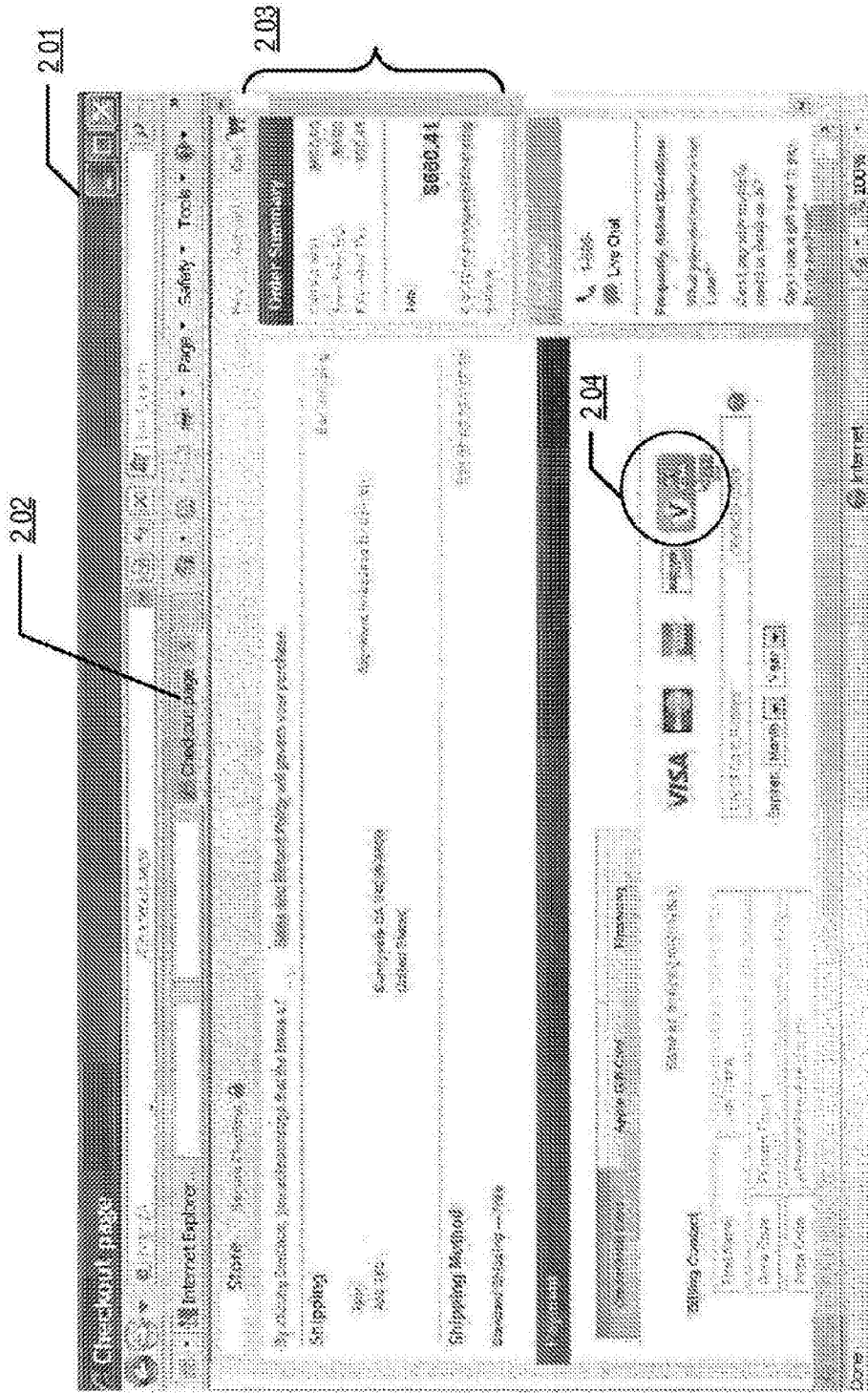


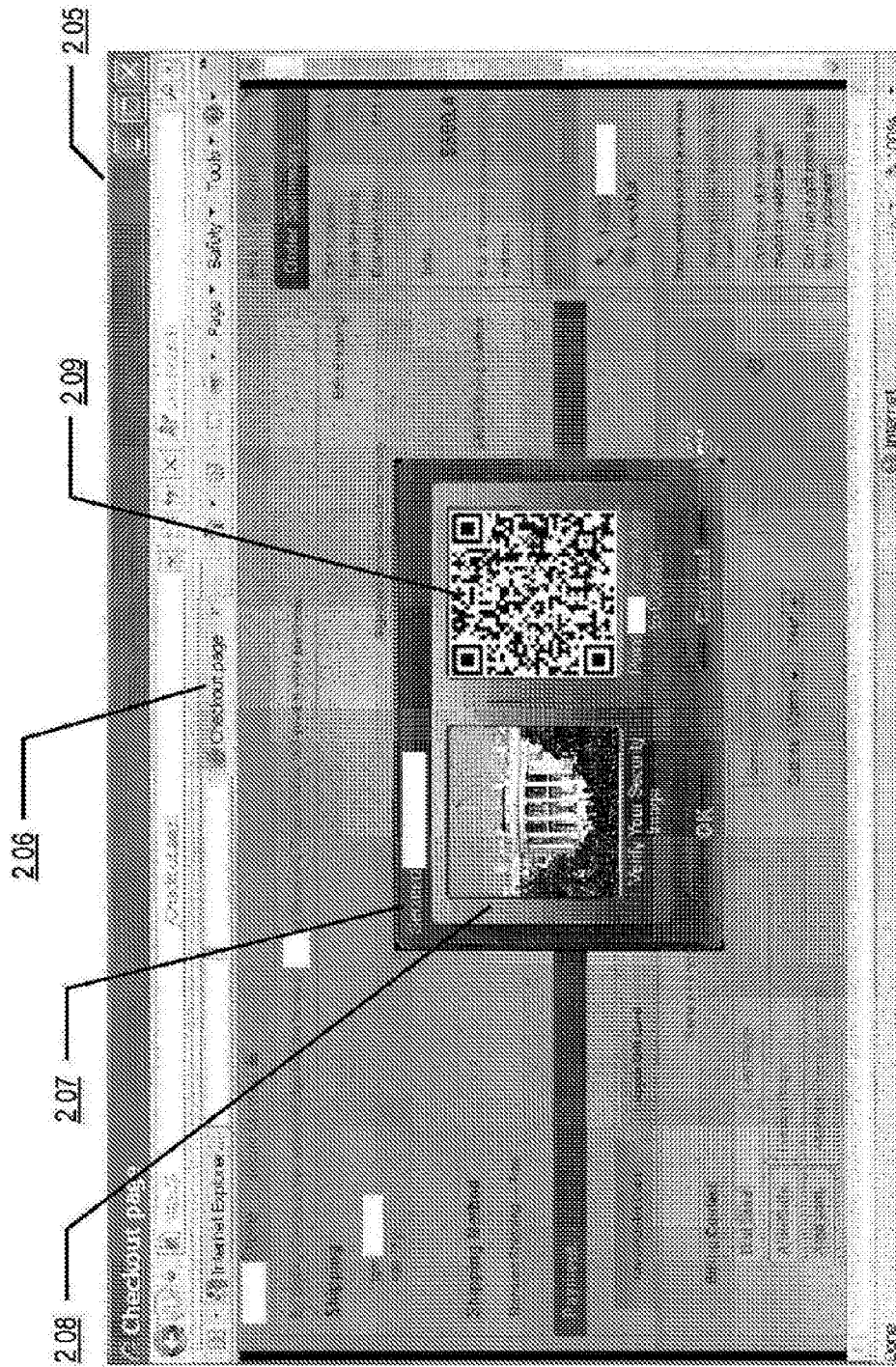
图1F

示例: 快拍移动支付



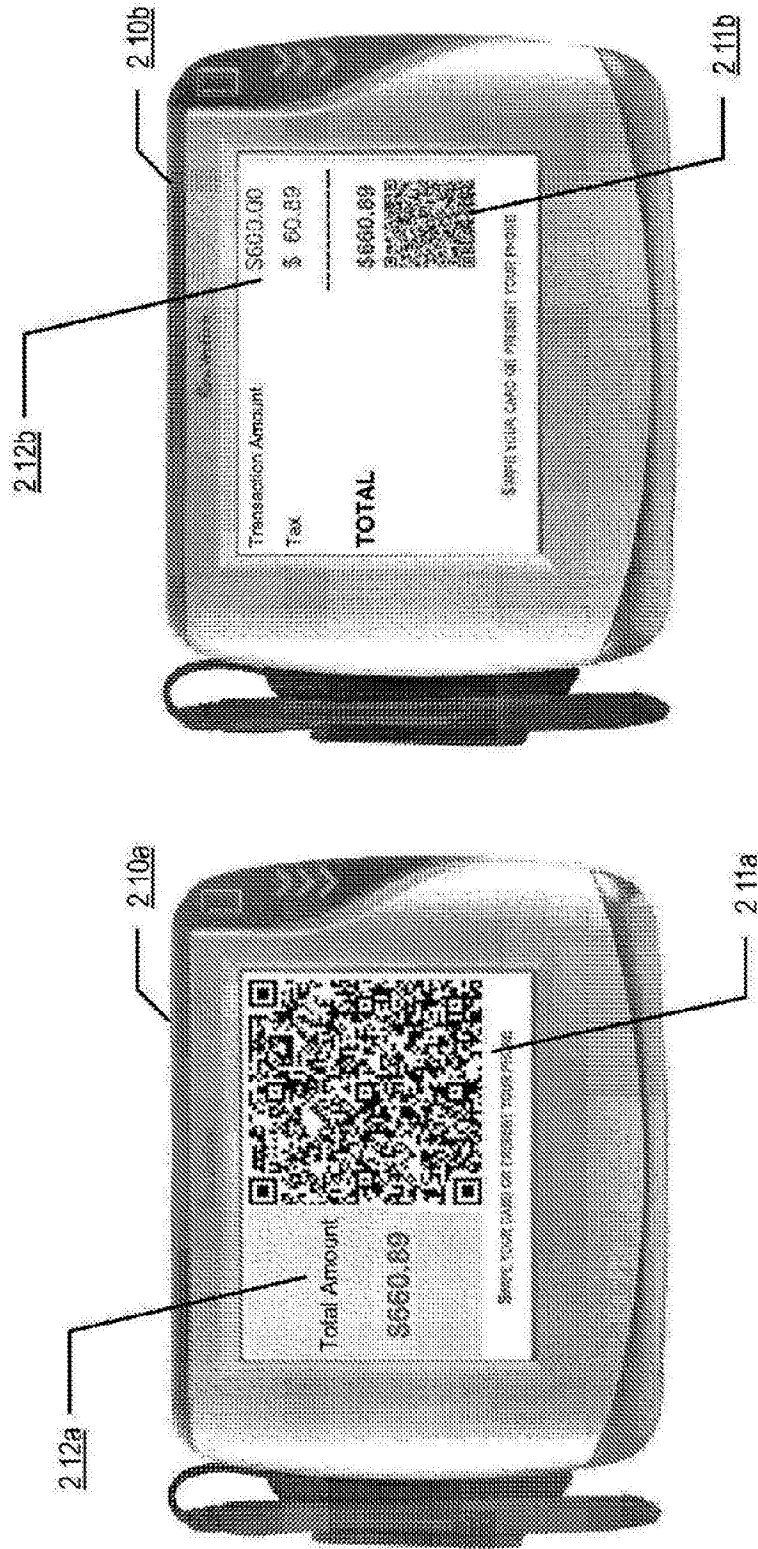
示例：快拍移动支付用户界面

图2A



示例：快拍移动支付网络界面

图2B



示例：快拍移动支付POS终端界面

图2C

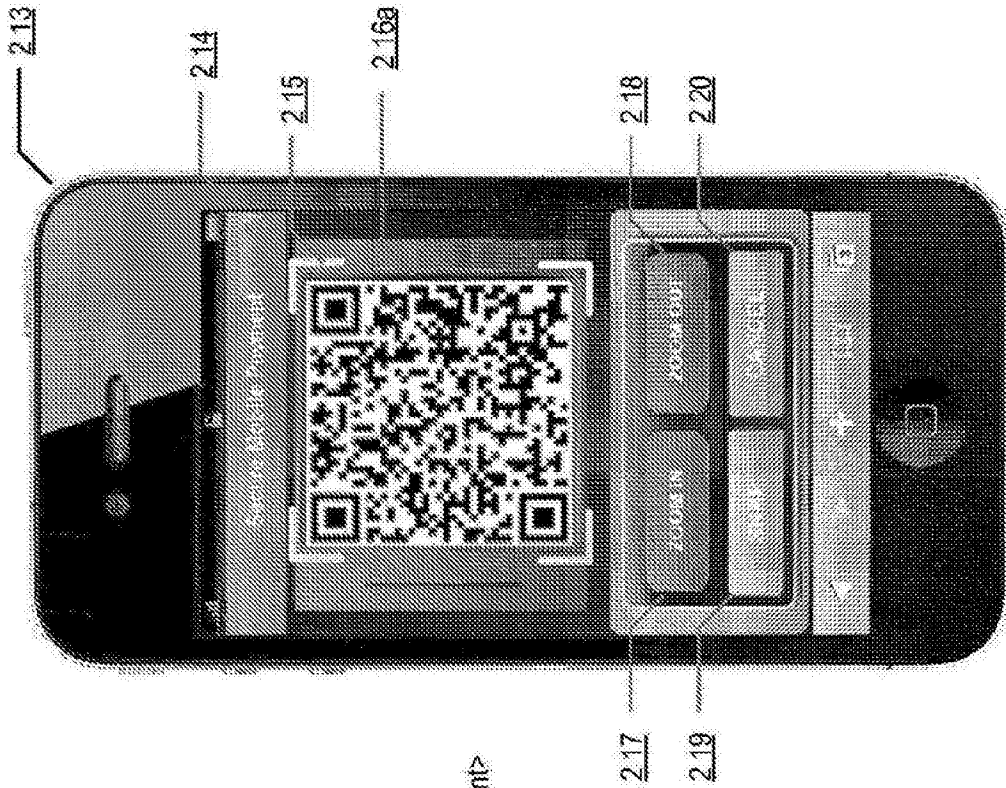
示例 QR 代码数据内容 2.16b

```

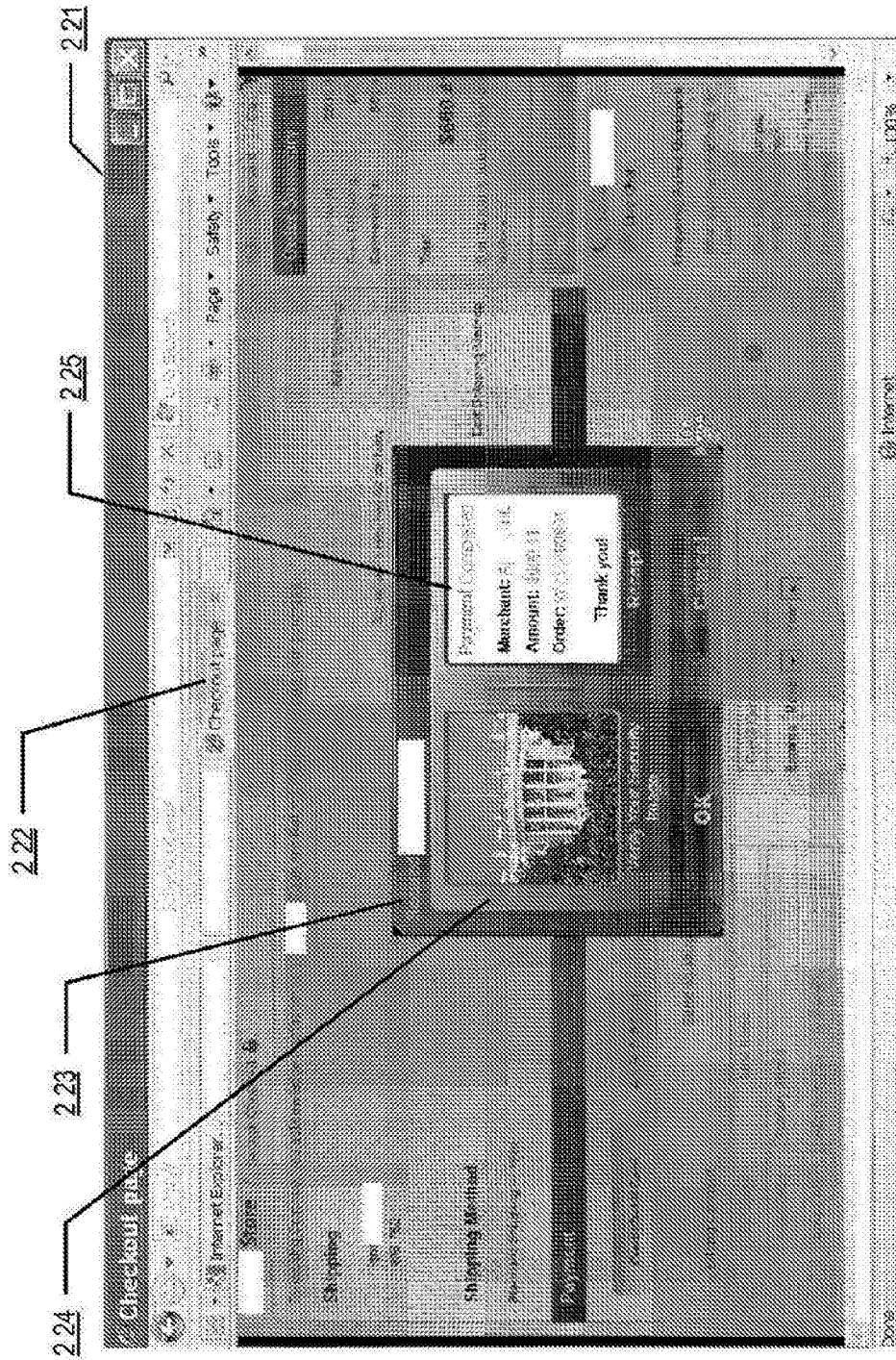
<data>
  <merchant_id>AE783</merchant_id>
  <merchant_name>Acme, Inc.</merchant_name>
  <store_id>88234</store_id>
  <store_url>www.shop.acme.com</store_url>
  <terminal_id>userdevice1</terminal_id>
  <transaction_id>AFE1213344</transaction_id>
  <timestamp>2011-04-01:23:59:59</timestamp>
  <transaction_amount>$660.89</transaction_amount>
  <digital_sign>
    45e2085fa20496c91df574dc56652e145
  </digital_sign>
</data>

```

图 2D



示例：快拍移动支付用户界面



示例：快拍移动支付网络收据

图2E

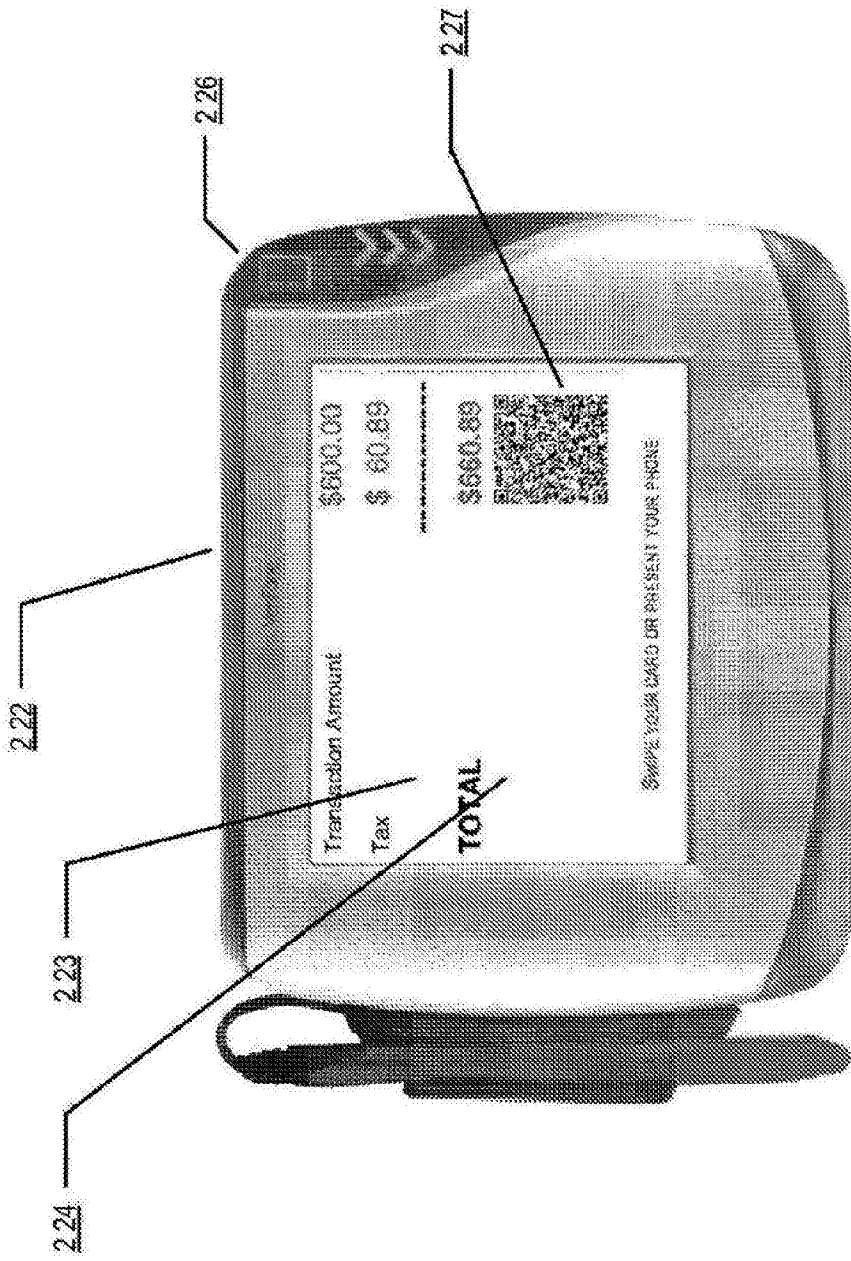
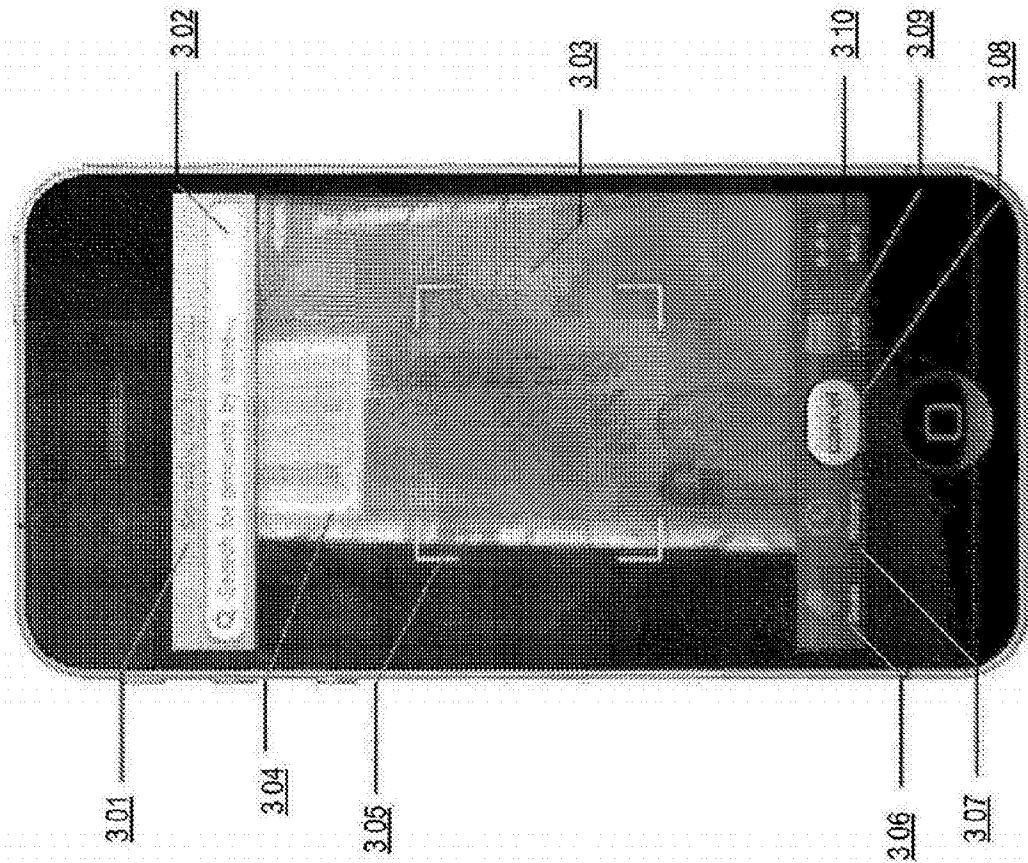


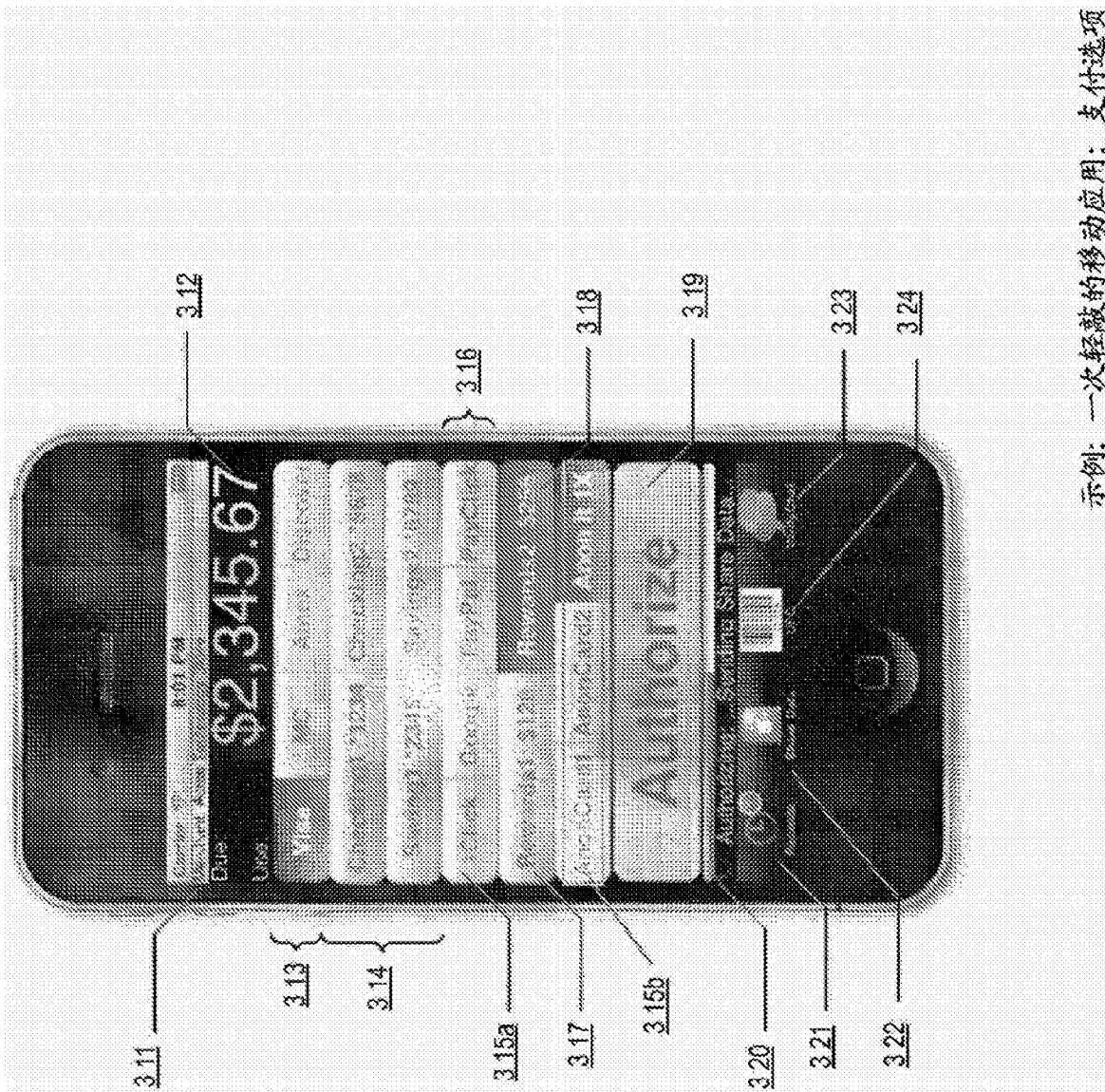
图2F

示例：快拍移动支付网络收据



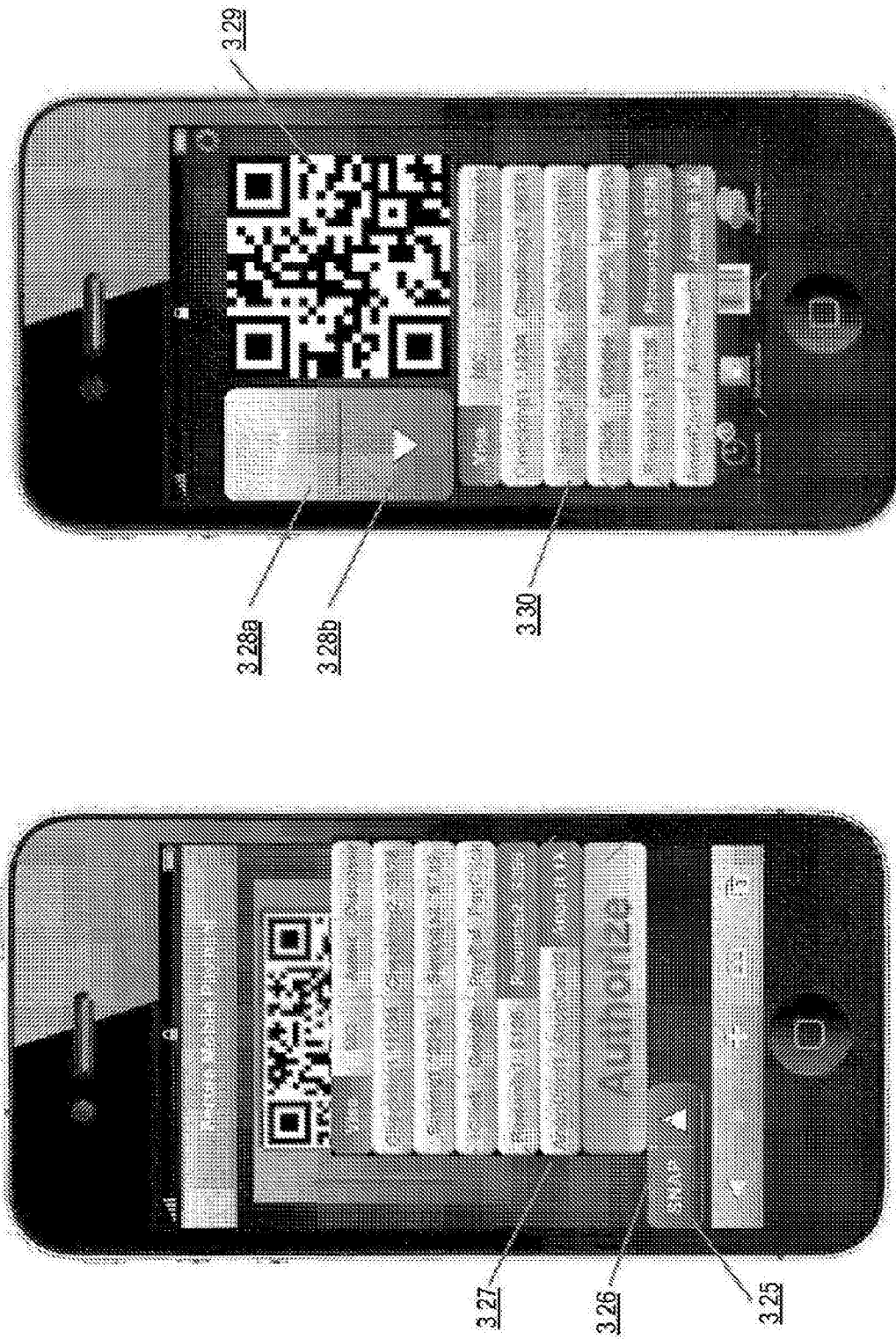
示例：一次轻敲的移动应用：条码捕捉

图3A



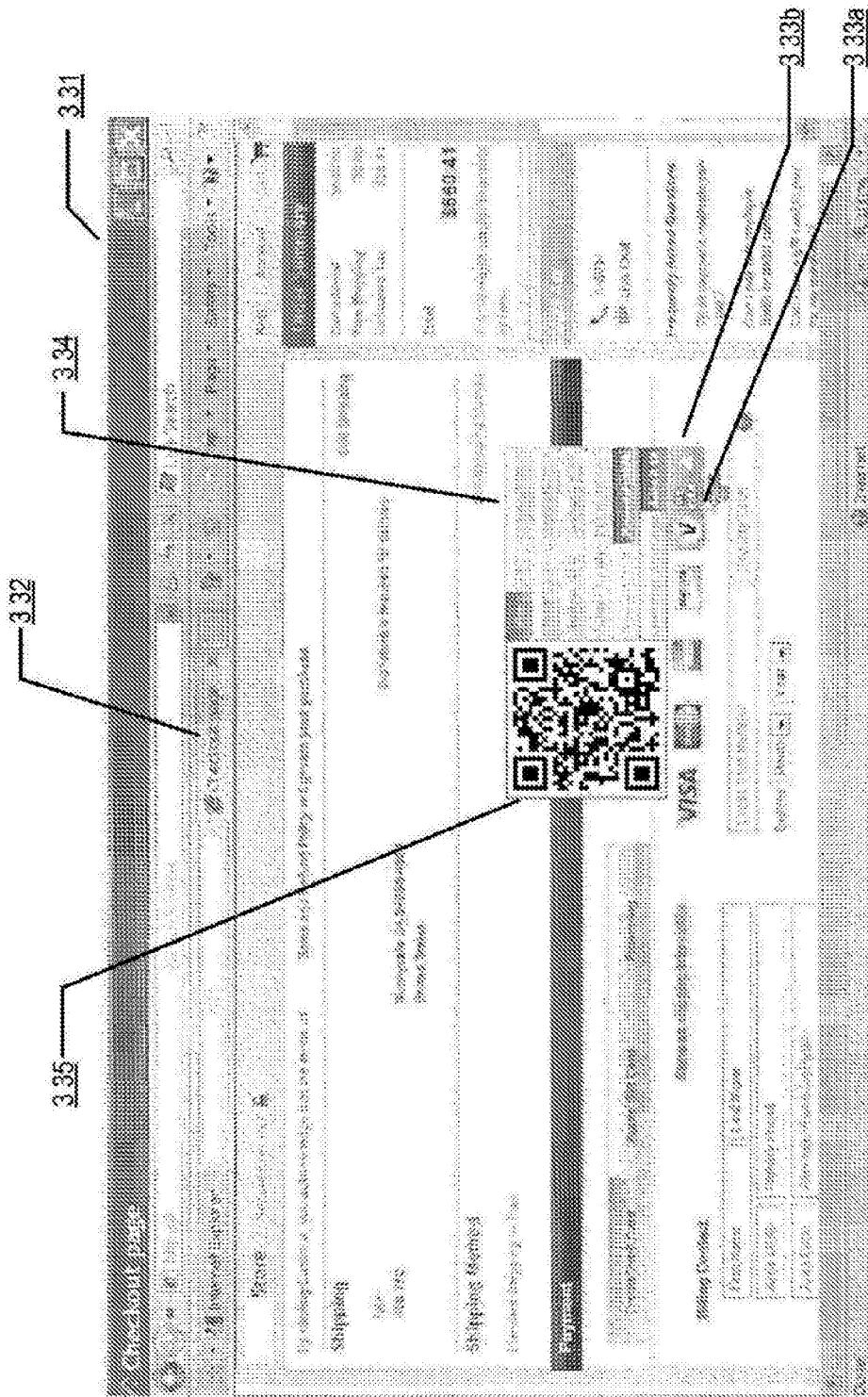
示例：一次轻敲的移动应用：支付选项

图3B



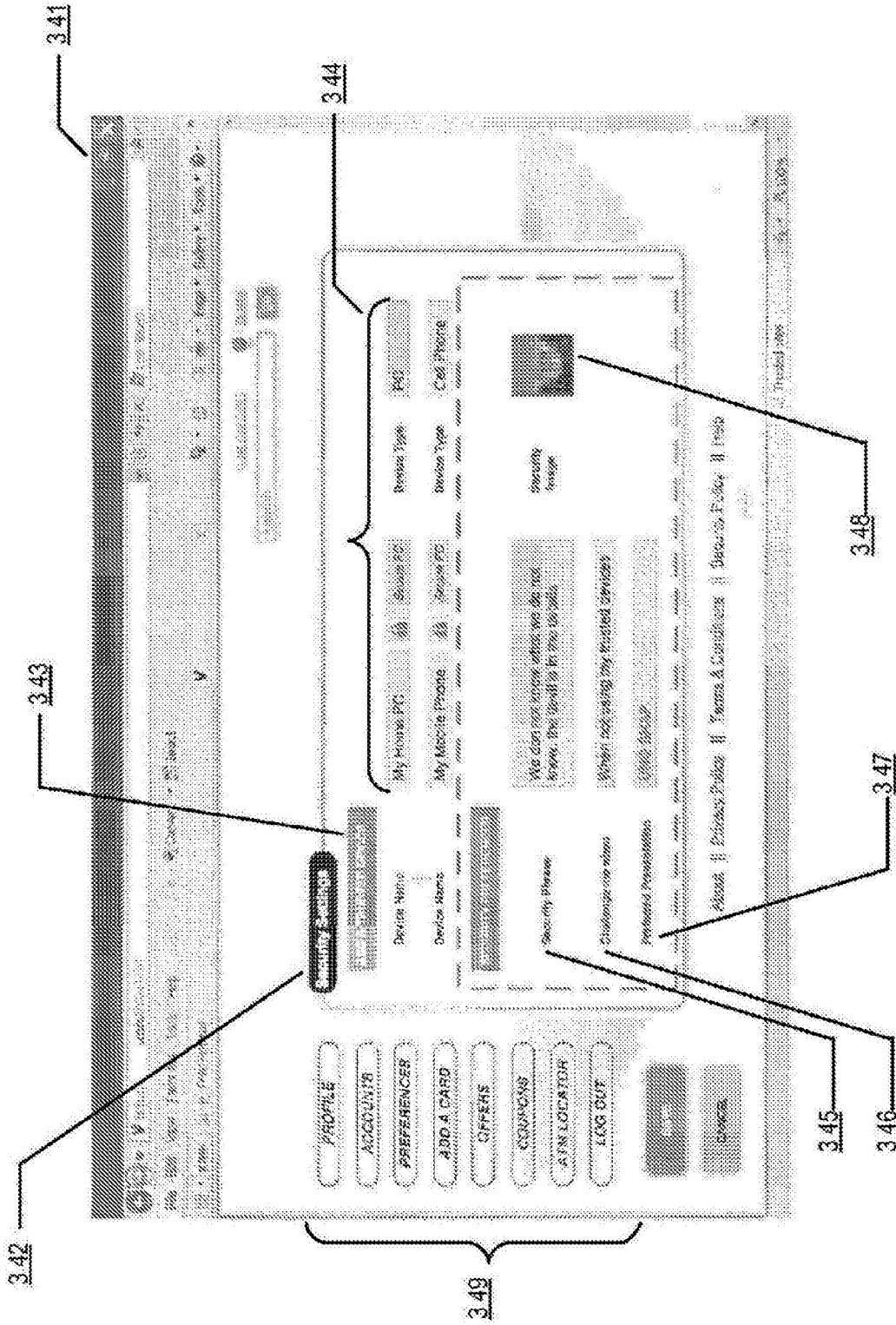
示例：一次轻敲的移动应用：支付选项

图3C



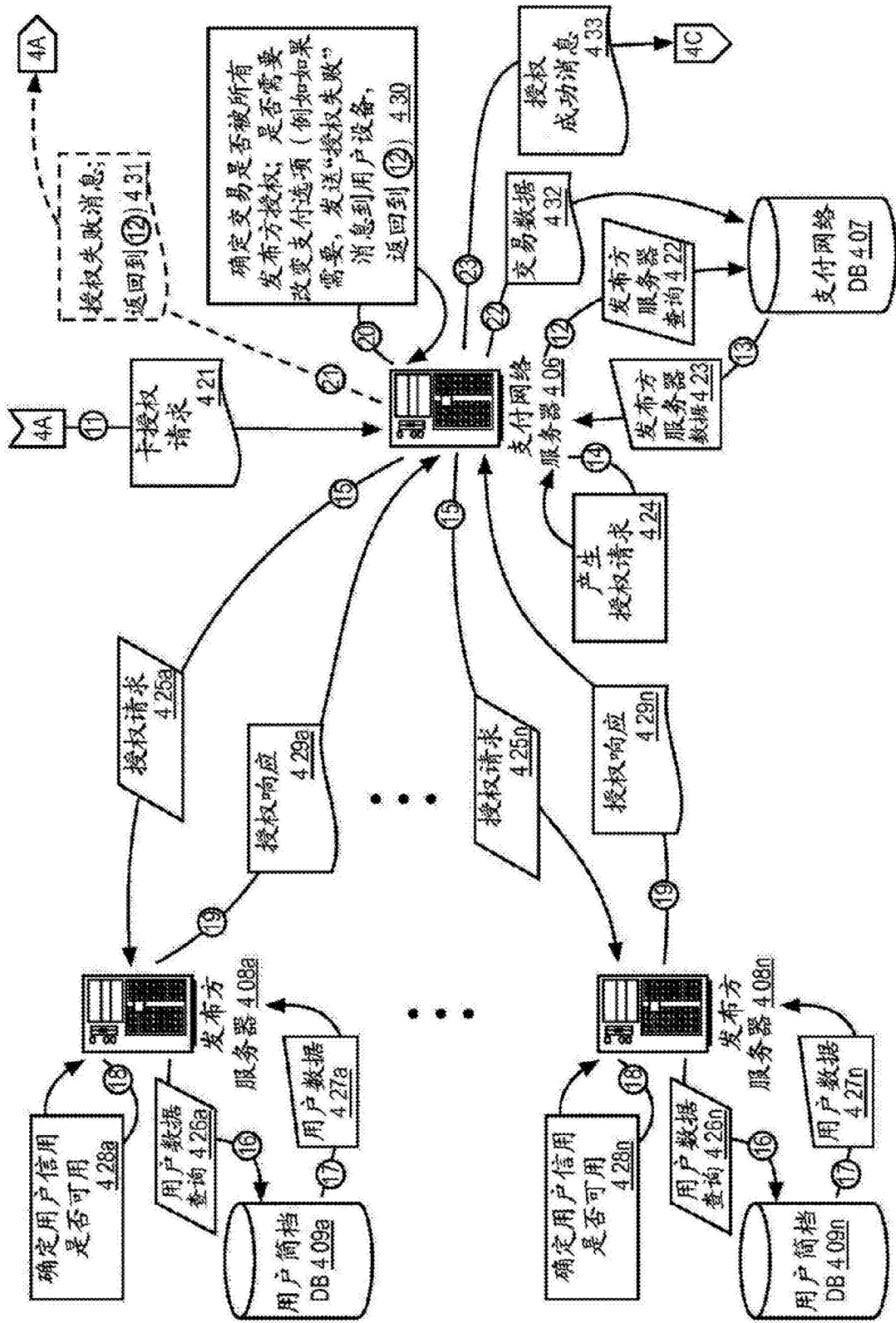
一次轻敲的移动应用：网站上的支付选项

图3D



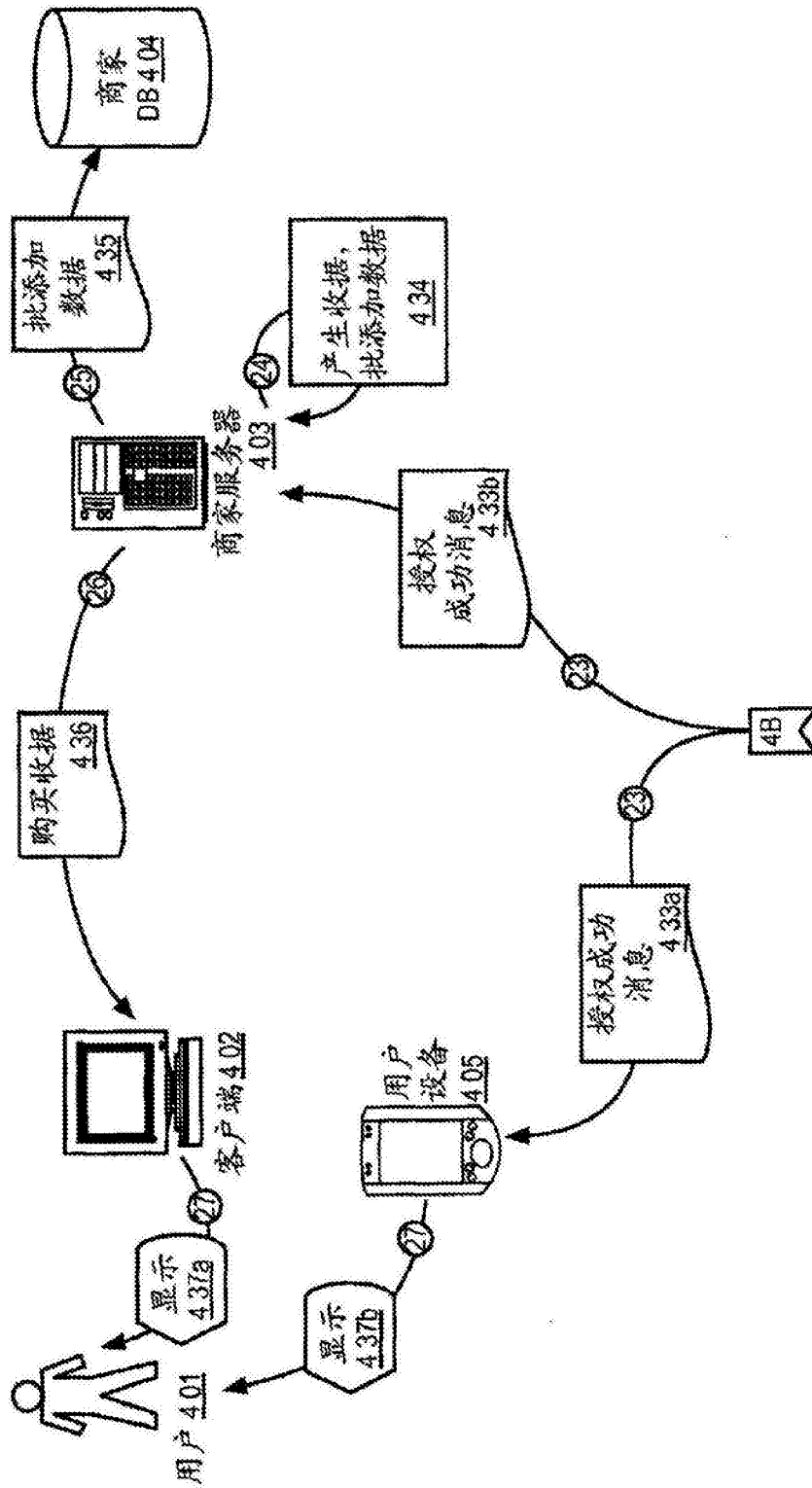
示例: 快拍移动支付: 安全/欺诈保护

图3E



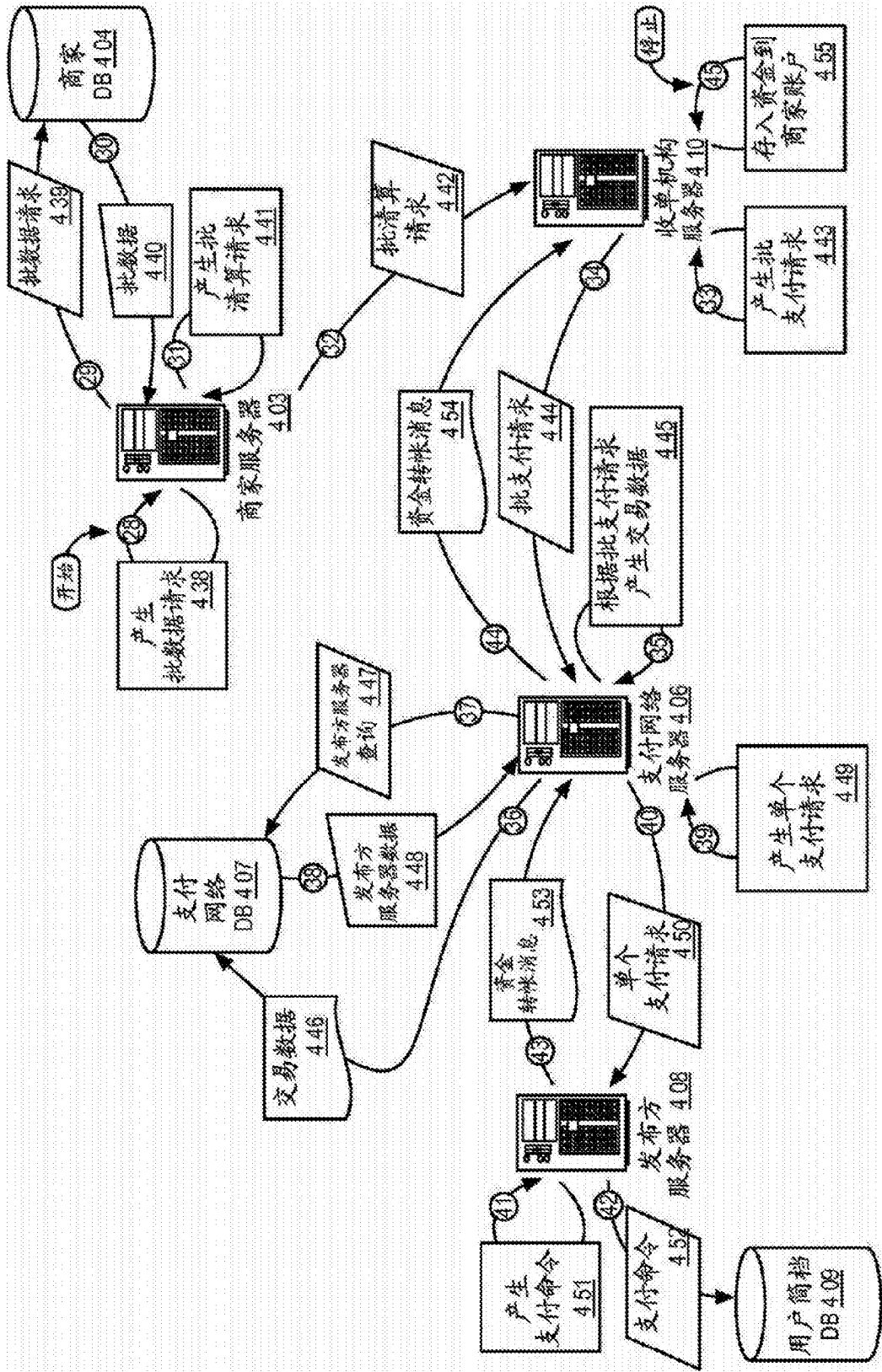
示例：快拍移动支付

图4B



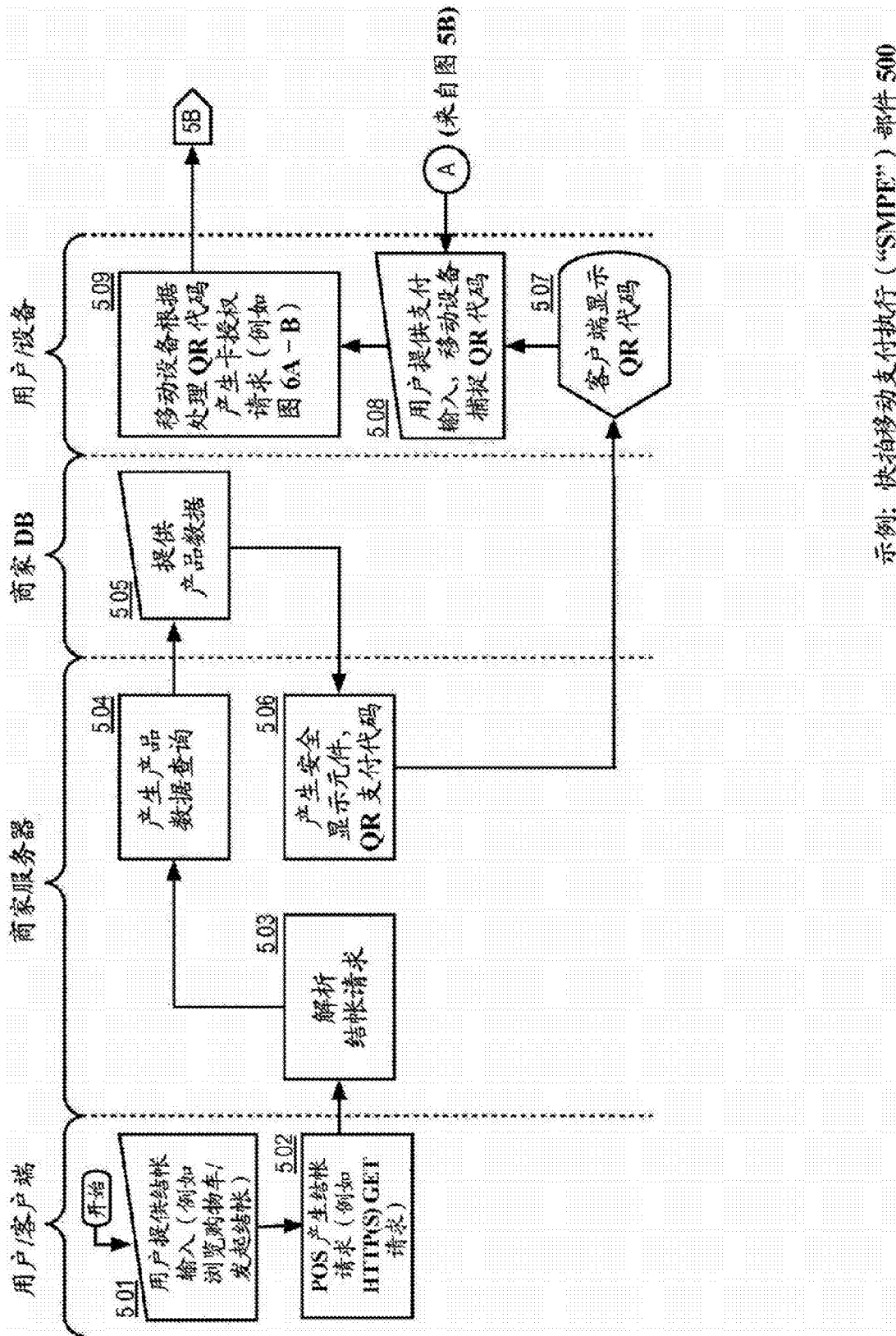
示例：快拍移动支付

图4C



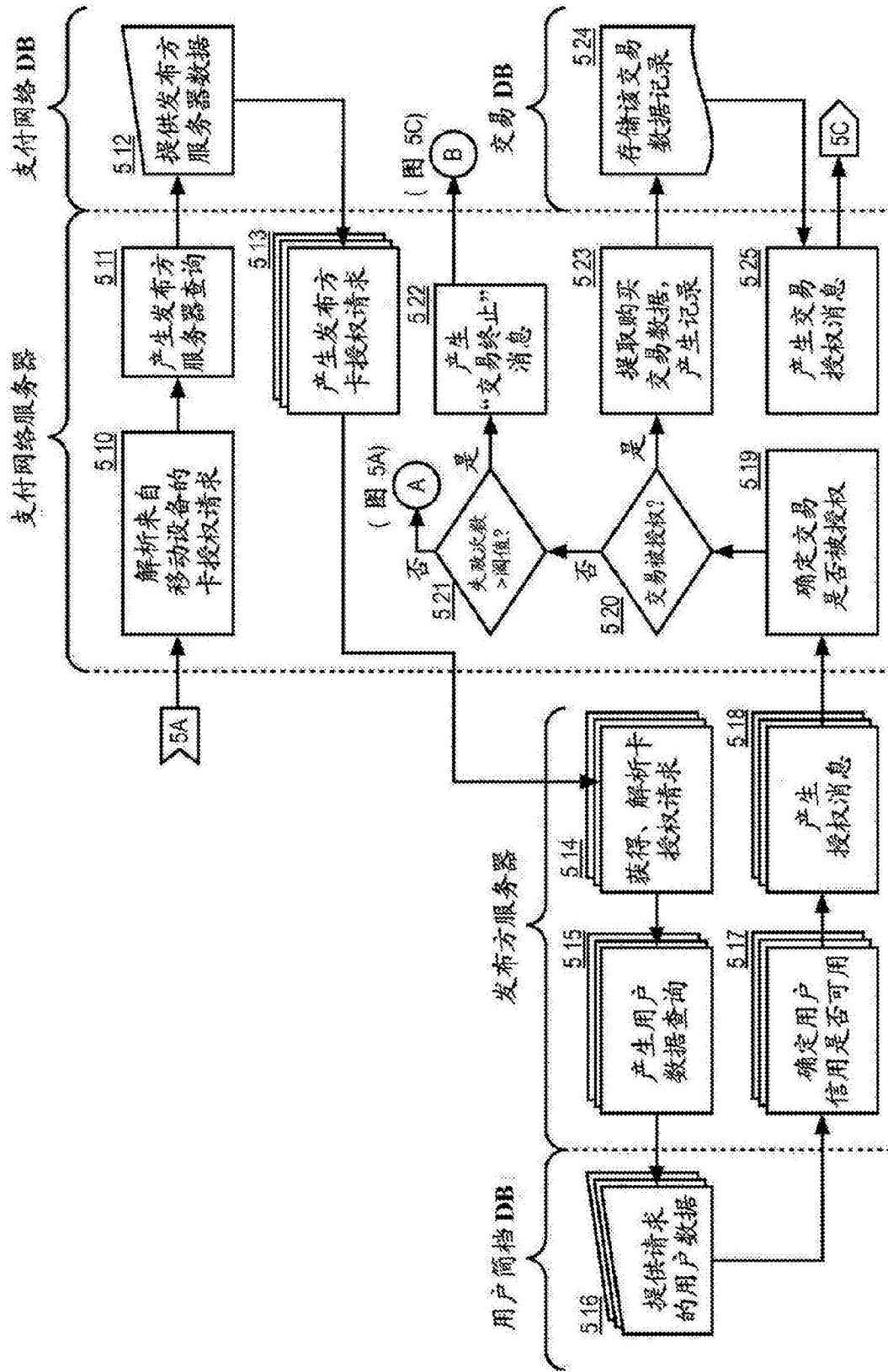
示例：快拍移动支付

图4D



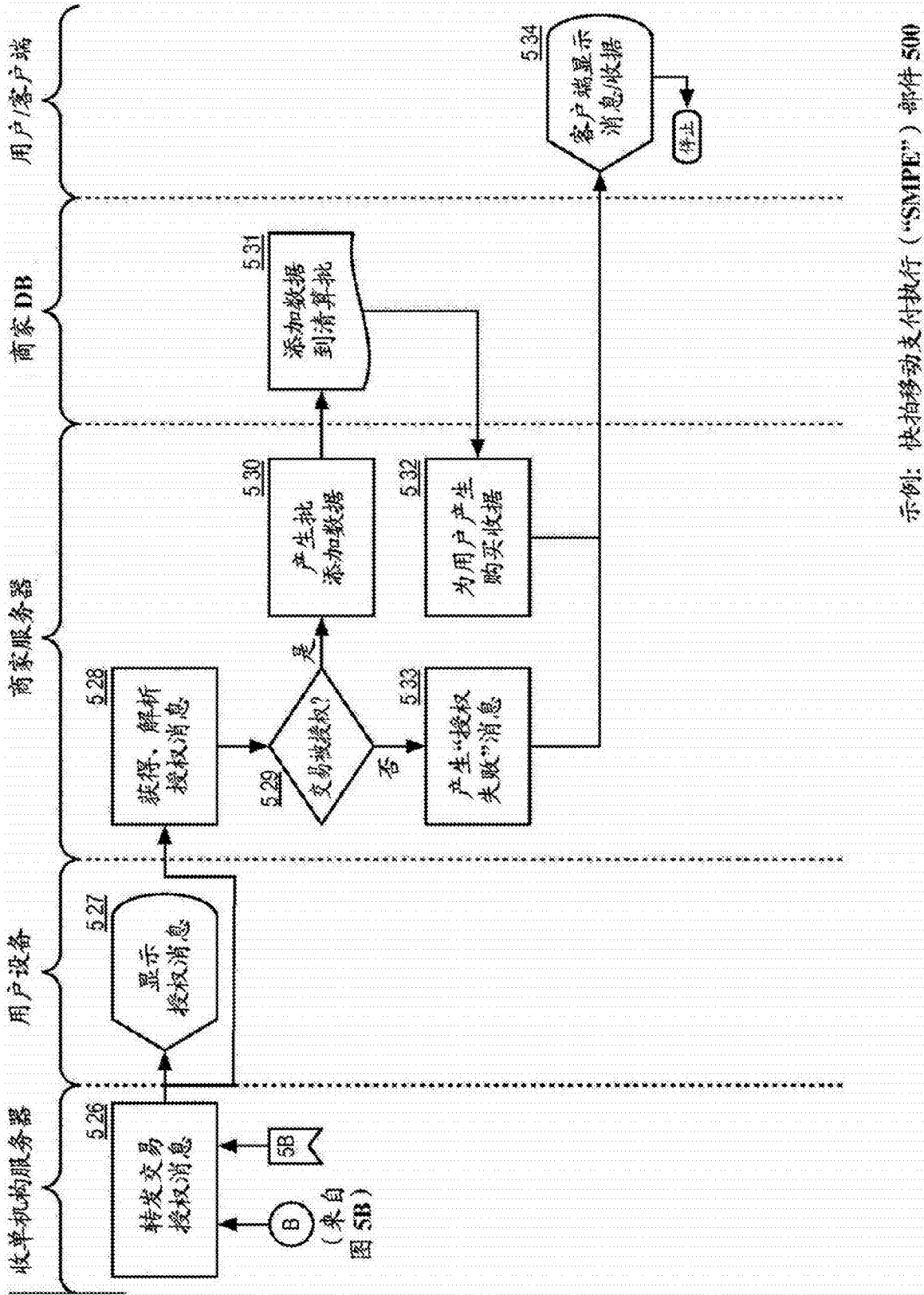
示例: 快拍移动支付执行 (“SMPE”) 部件 500

图5A



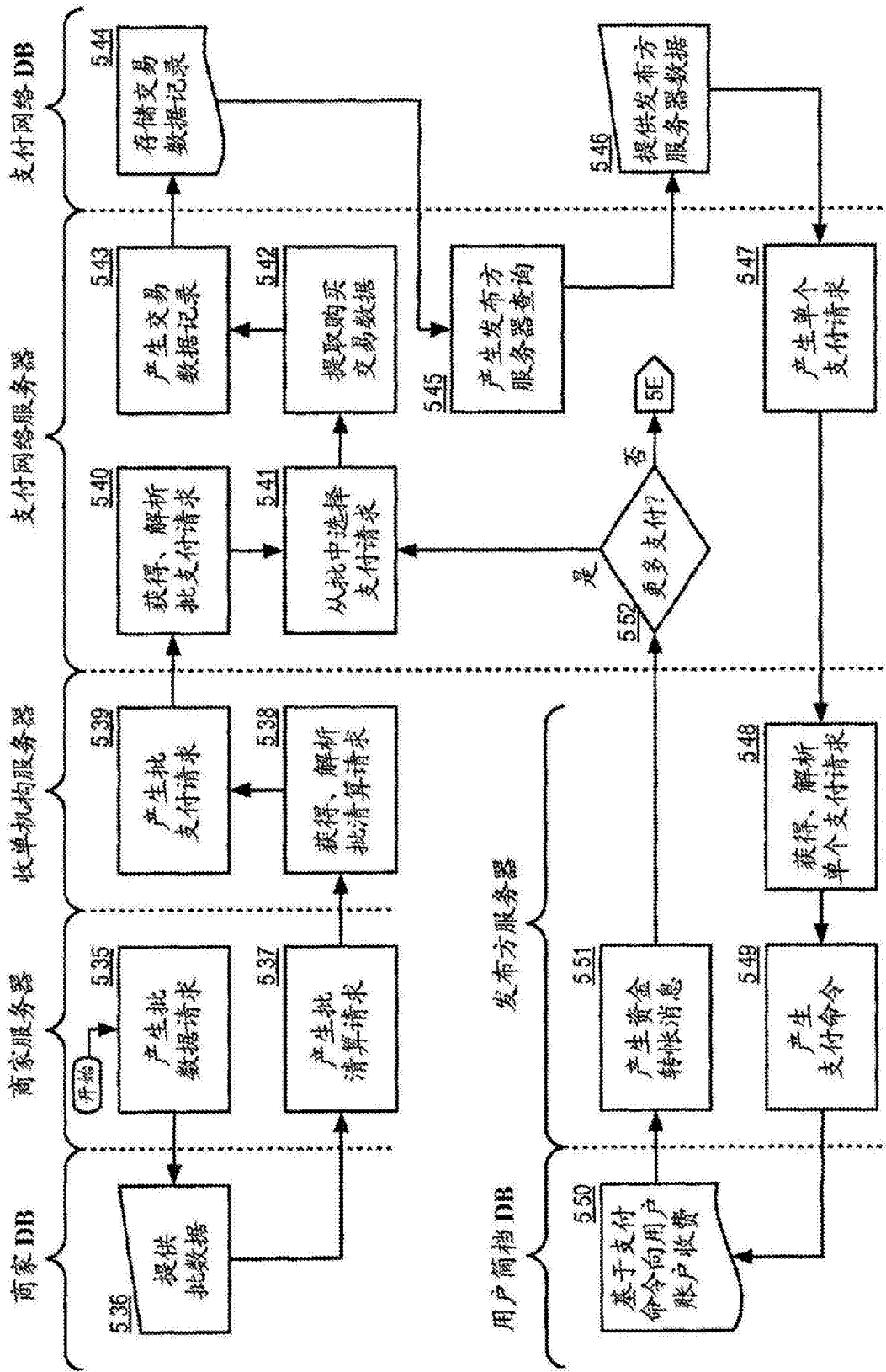
示例: 快拍移动支付执行 (“SMPE”) 部件 500

图5B



示例: 快拍移动支付执行 (“SMPE”) 部件 500

图5C



示例：快拍移动支付执行 (“SMPE”) 部件 500

图5D

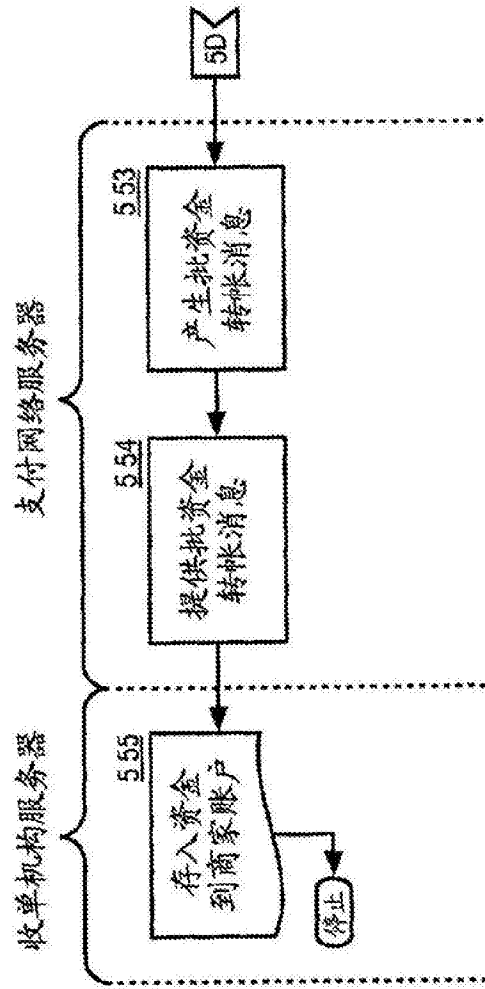
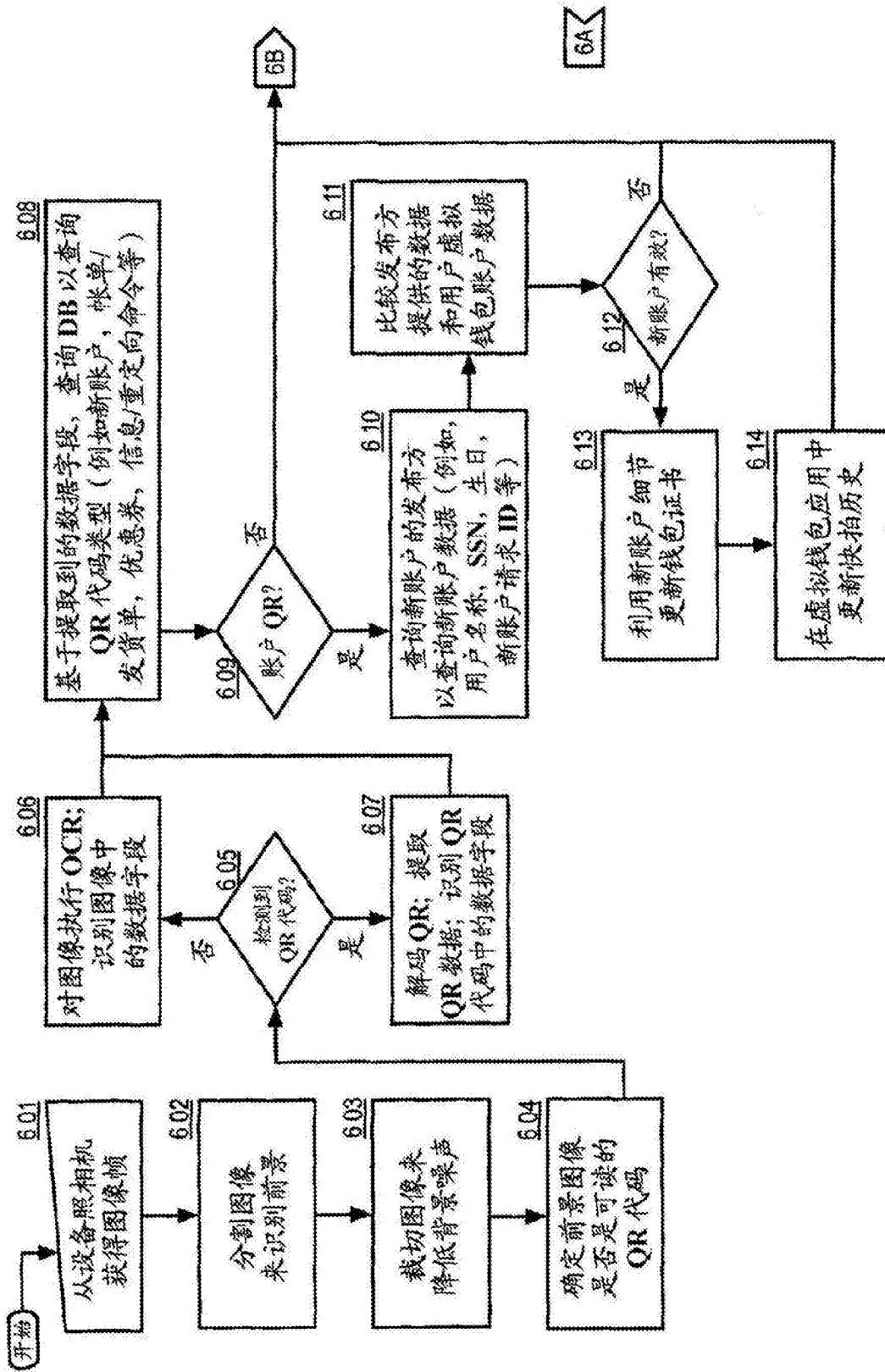


图5E

示例：快拍移动支付执行 (“SMPE”) 部件 500



示例: 快速响应代码处理 (“QRCP”) 部件 600

图6A

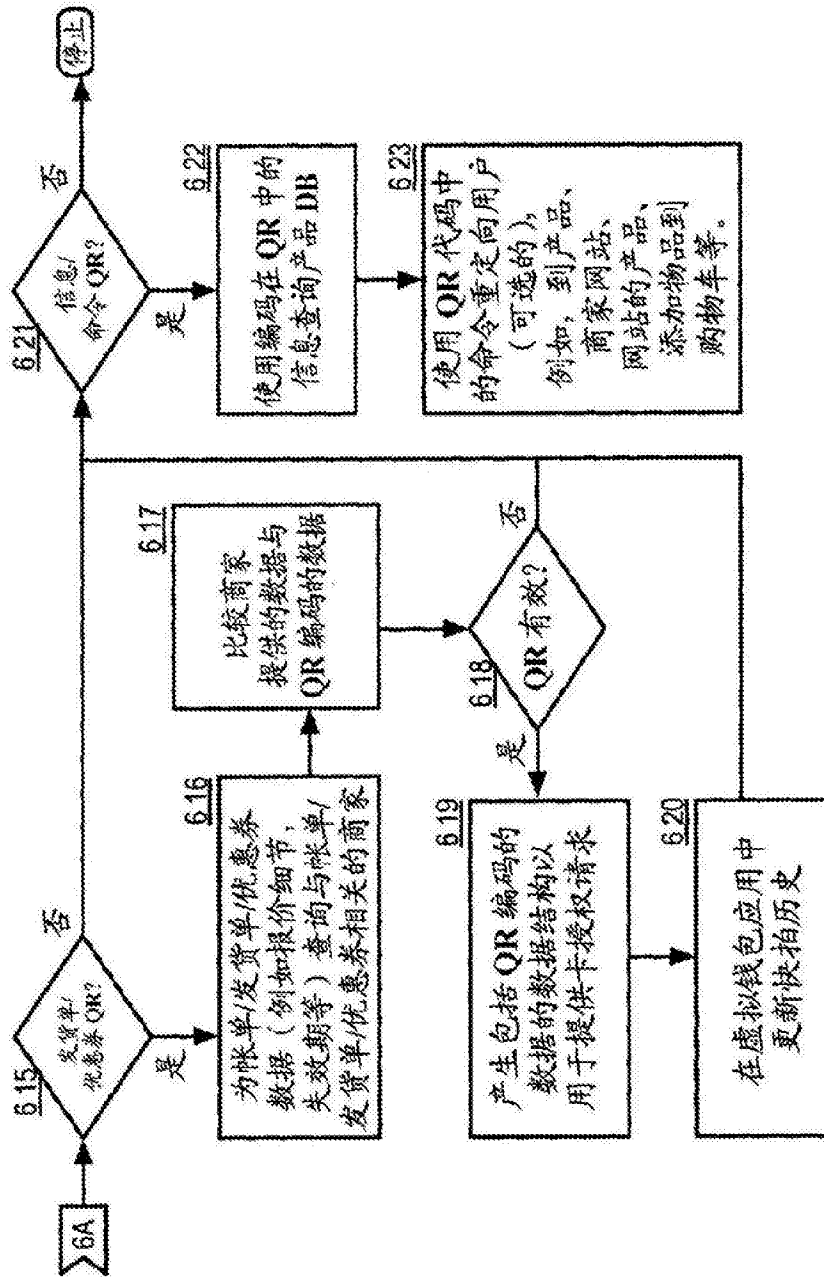
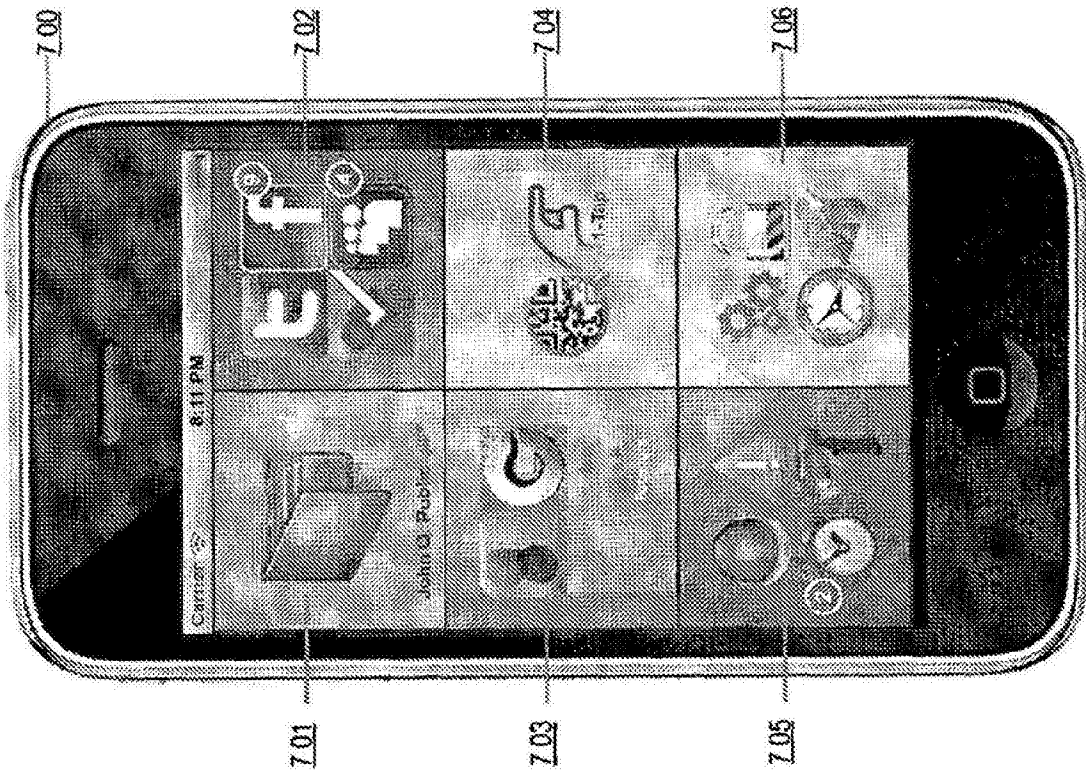


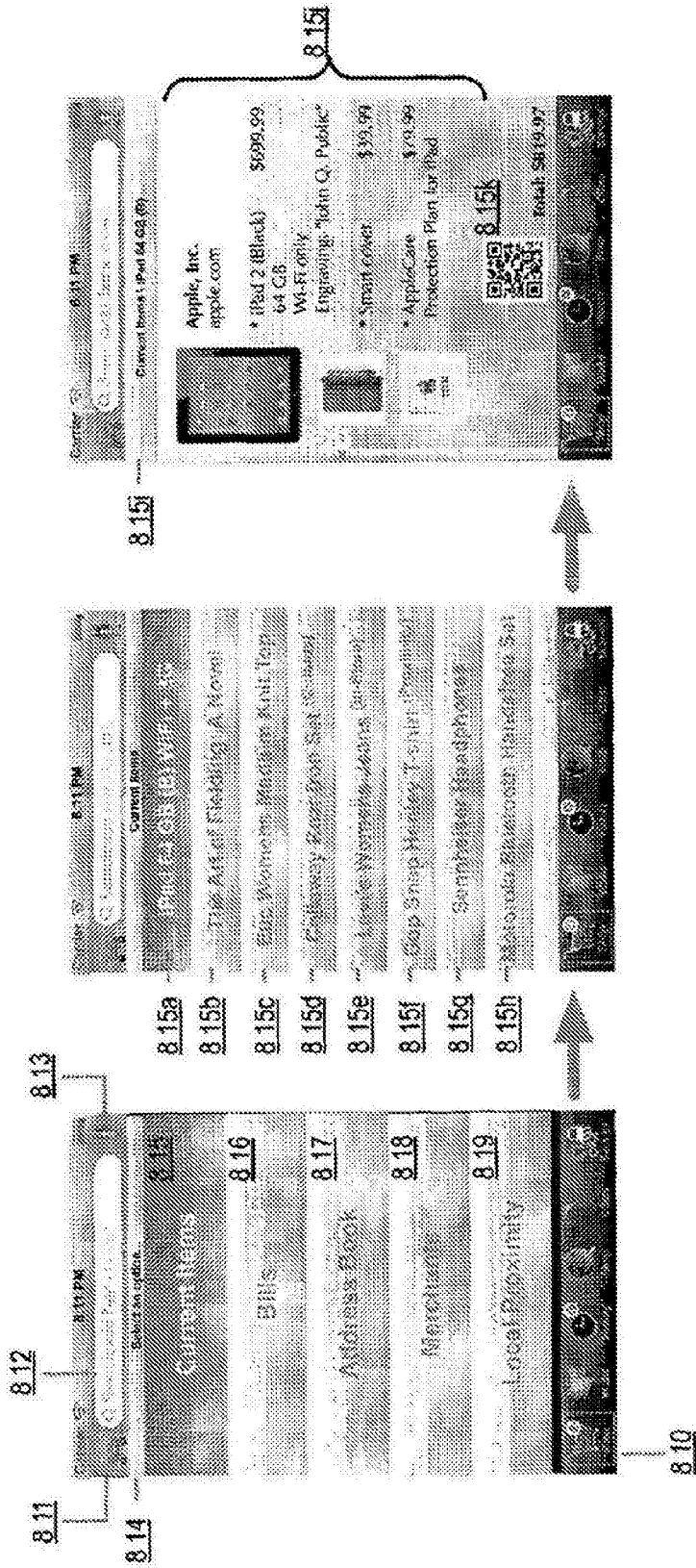
图6B

示例: 快速响应代码处理 (“QRCP”) 部件 600



示例：虚拟钱包移动应用 - 特征浏览

图7



示例：虚拟钱包移动应用 - 购物模式

图8A