

## **SYSTEM FOR PROCESSING AN ELECTRONIC PAYMENT REQUEST**

### Technical field

- 5 The present invention relates to a digital wallet provider system for processing electronic payment requests. The present invention also relates to a method for processing an electronic payment request.

### Background

- 10 Electronic payment systems have rapidly gained popularity in the developed world. This was driven in part by the growth of online shopping websites such as Amazon™ and auction websites such as eBay™ offering a wide range of products from a multitude of sellers resulting in competitively priced items available for purchase without a user having to leave their seat. Additionally, online banking systems have
- 15 also become popular. These systems allow consumers to perform a multitude of tasks such as transfer funds, paying third parties (including bills), and so on. This service is convenient as consumers no longer need to take time off their busy schedules to physically stand in line, for example at the bank or post office, to perform these transactions.
- 20 To complete an online electronic payment transaction, a user is typically required to have an existing account with the merchant, or if they do not have an existing account they may opt to sign up for one. If a user does not have an existing account with the merchant, this requirement to sign up for a new account may deter a user from
- 25 finalising a purchase as the registration process for some merchants may take time and effort to complete. Creating a new account typically requires a user to enter their personal details (name, shipping and mailing address, etc.) and payment information (credit card details) each time they sign up for a new account. Signing up for a new account may also result in a user inadvertently signing up for newsletters and
- 30 receiving unwanted spam emails. Finally, having an account for each merchant means a user has to keep track of a multitude of account information details and each may have varying login requirements (username and password) which could be frustrating for the user.

Digital wallets were introduced to mitigate some of the issues associated with maintaining a multitude of accounts for electronic transactions. Digital wallet service providers offer a service which allows a user to create one single account and associate user information (name, telephone number, home address, shipping  
5 address, etc) and payment options (credit card, debit card, etc.) to it. A user would only have to enter their information once to register for a digital wallet account. After registration, the user would then be able to use that digital wallet account to complete electronic transactions without having to sign up for a separate account with the merchant.

10

These systems work well in developed countries where most users have access to internet-enabled mobile computer devices. These mobile computer devices are capable of accessing an internet browser or downloading and running mobile applications such as ApplePay™, Android Pay™ or MasterPass™. Most users also have  
15 access to a computer device where they can easily access internet browsers capable of running secure websites which may be used to complete online payment transactions.

However, in certain countries, the majority of the population may not have access to internet-enabled computer devices. They would not be able to use these new  
20 electronic payment systems which are time-efficient and convenient. Additionally, merchants miss out on a large consumer group due to a lack of technology for this market. However, it is likely that most people in this particular consumer group do own a basic mobile phone (also known as a "dumb phone" or feature phone, in contrast to an internet-enabled smartphone). These basic mobile phones are  
25 marketed as lower-cost alternatives to smartphones and are especially popular in emerging markets. These phones are capable, as a bare minimum, to make and receive calls as well as compose, send and receive short message service (SMS) text messages.

30 It is generally desirable to overcome or ameliorate one or more of the above described difficulties, or to at least provide a useful alternative.

### Summary

In accordance with the present disclosure, there is provided a digital wallet provider system for processing electronic payment requests, the system including a server with  
5 one or more computer processors in communication with non-transitory computer readable data storage, which are configured to:

- (a) receive electronic payment request message data, with an associated telephone number, for initiating an electronic payment request;
- 10 (b) parse the message data to identify electronic payment request parameters;
- (c) use the associated telephone number to identify a digital wallet account stored in said data storage;
- (d) retrieve payment information from the digital wallet account;
- 15 (e) authenticate said payment information, wherein the step of authenticating payment information includes the following steps:
  - (e1) retrieving digital wallet account information associated with the telephone number associated with the electronic payment request message data from data storage;
  - 20 (e2) retrieving a primary account number (PAN) associated with the digital wallet account information; and
  - (e3) checking if the PAN associated with the digital wallet account information matches a predefined word associated with payment credentials of the electronic payment request parameters;
- 25 (f) send an electronic payment request to an authorization server;
- (g) receive data representing an electronic payment request approval status; and
- (h) send message data representing the electronic payment request approval status.
- 30

In accordance with the present disclosure, there is also provided a method for processing an electronic payment request performed by one or more computer processors of a digital wallet provider system executing instructions stored on non-

transitory computer readable data storage that, when executed, cause the system to perform the steps of:

- 5 (a) receiving electronic payment request message data, with an associated telephone number, for initiating an electronic payment request;
- (b) parsing the message data to identify electronic payment request parameters;
- (c) using the associated telephone number to identify a digital wallet account stored in said data storage;
- 10 (d) retrieving payment information from the digital wallet account;
- (e) authenticating said payment information, wherein the step of authenticating payment information includes the following steps:
  - (e1) retrieving digital wallet account information associated with the telephone number associated with the electronic payment request message data from data storage;
  - 15 (e2) retrieving a primary account number (PAN) associated with the digital wallet account information; and
  - (e3) checking if the PAN associated with the digital wallet account information matches a predefined word associated with payment credentials of the electronic payment request parameters;
  - 20
- (f) sending an electronic payment request to an authorization server;
- (g) receiving data representing an electronic payment request approval status; and
- 25 (h) sending message data representing the electronic payment request approval status.

#### Brief Description of the Drawings

- 30 Embodiments of the invention are hereafter described, by way of non-limiting example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic diagram of a system for processing an electronic payment request initiated by an SMS message;

- 35 Figure 2 is a block diagram of a mobile device of the system shown in Figure 1;

Figure 3 is a schematic diagram showing components of an exemplary server of the system shown in Figure 1;

Figure 4 is a flow diagram showing the interoperation of the components of the system to execute the processing an electronic payment request initiated by an SMS message;

Figure 5 is a flow diagram showing the process of parsing the contents of the SMS message to identify electronic payment request parameters as shown in Figure 4;

Figure 6 is a flow diagram showing the process to authenticate the payment information as shown in Figure 4;

Figure 7a is an image of an exemplary auction product information used to generate a message to initiate an electronic payment request to place a bid;

Figure 7b is an image of an exemplary embodiment of a mobile device, generating for display the contents of a message data representing a payment request; and

Figure 7c is an image of an exemplary embodiment of a mobile device, generating for display the contents of a message data indicating that the electronic payment request is successful.

#### Detailed Description

The system 10 shown in Figure 1 allows electronic payment requests to be initiated by a user through a short message service (SMS) message, for example. The system 10 includes one or more of the following:

- (a) a mobile device 12;
- (b) a digital wallet provider system 14;
- (c) a merchant server 16; and
- (d) an authorization system 18.

Embodiments of the invention are below described with reference to initiating electronic payment requests by SMS message only. However, electronic payment requests may be initiated by other means, for example, email, a Multimedia Messaging System (MMS) message, a message sent through an instant messaging platform (such as iMessage, WhatsApp, Line, etc.), accessing a website on an internet browser, through an application running on a mobile computer device or using an

intelligent personal assistant (e.g. a voice command to a software agent such as Apple's Siri, Amazon's Alexa or Google Assistant).

5 The components of system 10 are in communication via the network 20. The communication network 20 may include the Internet, mobile telecommunications networks and/or local area networks.

10 The system 10 makes processing electronic payment requests simpler, faster and more convenient. The system 10 removes the need for sophisticated computer devices to complete an electronic payment request by allowing transactions to be made by a customer using their mobile device 12 that is capable of composing, sending and receiving SMS messages.

### **Mobile Device 12**

15

Figure 2 is a block diagram showing an exemplary mobile device 12 in which embodiments of the invention may be practiced. The mobile device 12 could be any mobile device capable of composing, sending and receiving SMS messages. The mobile device 12 may be a mobile computer device such as a smart phone, a personal data assistant (**PDA**), a palm-top computer, and multimedia Internet enabled cellular telephones. For ease of description, the mobile device 12 is described below, by way of non-limiting example, with reference to a mobile device in the form of an iPhone<sup>™</sup> manufactured by Apple<sup>™</sup>, Inc., such as the one shown in Figure 7b and 7c, or one manufactured by LG<sup>™</sup>, HTC<sup>™</sup> and Samsung<sup>™</sup>, for example.

25

As shown, the mobile device 12 includes the following components in electronic communication via a bus 206:

- 30 (a) a display 202;
- (b) non-volatile (non-transitory) memory 204;
- (c) random access memory ("RAM") 208;
- (d) N processing components 210;
- (e) a transceiver component 212 that includes N transceivers; and
- (f) user controls 214.

35

Although the components depicted in Figure 2 represent physical components, Figure 2 is not intended to be a hardware diagram. Thus, many of the components depicted in Figure 2 may be realized by common constructs or distributed among additional physical components. Moreover, it is certainly contemplated that other existing and  
5 yet-to-be developed physical components and architectures may be utilized to implement the functional components described with reference to Figure 2.

The display 202 generally operates to provide a presentation of content to a user, and may be realized by any of a variety of displays (e.g., CRT, LCD, HDMI, micro-projector  
10 and OLED displays).

In general, the non-volatile data storage 204 (also referred to as non-volatile memory) functions to store (e.g., persistently store) data and executable code.

15 In some embodiments for example, the non-volatile memory 204 includes bootloader code, modem software, operating system code, file system code, and code to facilitate the implementation components, known to those of ordinary skill in the art, which are not depicted nor described for simplicity.

20 In many implementations, the non-volatile memory 204 is realized by flash memory (e.g., NAND or ONENAND memory), but it is certainly contemplated that other memory types may be utilized as well. Although it may be possible to execute the code from the non-volatile memory 204, the executable code in the non-volatile memory 204 is typically loaded into RAM 208 and executed by one or more of the N  
25 processing components 210.

The N processing components 210 in connection with RAM 208 generally operate to execute the instructions stored in non-volatile memory 204. As one of ordinary skill in the art will appreciate, the N processing components 210 may include a video  
30 processor, modem processor, DSP, graphics processing unit (GPU), and other processing components.

The transceiver component 212 includes N transceiver chains, which may be used for communicating with external devices via wireless networks. Each of the N transceiver  
35 chains may represent a transceiver associated with a particular communication

scheme. For example, each transceiver may correspond to protocols that are specific to local area networks, cellular networks (e.g., a CDMA network, a GPRS network, a UMTS networks), and other types of communication networks.

- 5 It should be recognized that Figure 2 is merely exemplary and in one or more exemplary embodiments, the functions described herein may be implemented in hardware, software, firmware, or any combination thereof. If implemented in software, the functions may be stored on or transmitted over as one or more instructions or code encoded on a non-transitory computer-readable medium 204.
- 10 Non-transitory computer-readable media 204 includes both computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A storage medium may be any available medium that can be accessed by a computer.

#### 15 ***Digital Wallet Provider System 14***

As shown in Figure 3, the digital wallet provider system 14 may comprise a server 14. In some embodiments, the digital wallet provider system may comprise multiple servers in communication with each other, for example over a local area network or a

20 wide-area network such as the Internet. As described in the preceding section, the digital wallet provider system 14 is able to communicate with other components of the system 10 over the wireless communications network 20 using standard communication protocols.

- 25 The components of the digital wallet provider system 14 can be configured in a variety of ways. The components can be implemented entirely by software to be executed on standard computer server hardware, which may comprise one hardware unit or different computer hardware units distributed over various locations, some of which may require the communications network 20 for communication. A number of the
- 30 components or parts thereof may also be implemented by application specific integrated circuits (ASICs) or field programmable gate arrays.

In the example shown in Figure 3, the digital wallet provider system 14 is a commercially available server computer system based on a 32 bit or a 64 bit Intel

35 architecture, and the processes and/or methods executed or performed by the digital

wallet provider system 14 are implemented in the form of programming instructions of one or more software components or modules 722 stored on non-volatile (e.g., hard disk) computer-readable storage 724 associated with the digital wallet provider system 14. At least parts of the software modules 722 could alternatively be  
5 implemented as one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) and/or field programmable gate arrays (FPGAs).

The digital wallet provider system 14 includes at least one or more of the following standard, commercially available, computer components, all interconnected by a bus  
10 735:

- (a) random access memory (RAM) 726;
- (b) at least one computer processor 728, and
- (c) external computer interfaces 730:  
15
  - (i) universal serial bus (USB) interfaces 730a (at least one of which is connected to one or more user-interface devices, such as a keyboard, a pointing device (e.g., a mouse 732 or touchpad),
  - (ii) a network interface connector (NIC) 730b which connects the computer system 700 to a data communications network, such  
20 as the wireless communications network 20; and
  - (iii) a display adapter 730c, which is connected to a display device 734 such as a liquid-crystal display (LCD) panel device.

The digital wallet provider system 14 includes a plurality of standard software  
25 modules, including:

- (a) an operating system (OS) 736 (e.g., Linux or Microsoft Windows);
- (b) web server software 738 (e.g., Apache, available at <http://www.apache.org>);
- 30 (c) scripting language modules 740 (e.g., personal home page or PHP, available at <http://www.php.net>, or Microsoft ASP); and
- (d) structured query language (SQL) modules 742 (e.g., MySQL, available from <http://www.mysql.com>), which allow data to be stored in and retrieved/accessed from an SQL database 716.

Advantageously, the database 716 forms part of the computer readable data storage 724. Alternatively, the database 716 is located remote from the server 14 shown in Figure 3.

- 5 The boundaries between the modules and components in the software modules 722 are exemplary, and alternative embodiments may merge modules or impose an alternative decomposition of functionality of modules. For example, the modules discussed herein may be decomposed into submodules to be executed as multiple computer processes, and, optionally, on multiple computers. Moreover, alternative  
10 embodiments may combine multiple instances of a particular module or submodule. Furthermore, the operations may be combined or the functionality of the operations may be distributed in additional operations in accordance with the invention. Alternatively, such actions may be embodied in the structure of circuitry that implements such functionality, such as the micro-code of a complex instruction set  
15 computer (CISC), firmware programmed into programmable or erasable/programmable devices, the configuration of a field-programmable gate array (FPGA), the design of a gate array or full-custom application-specific integrated circuit (ASIC), or the like.
- 20 Each of the blocks of the flow diagrams of the processes of the digital wallet provider system 14 may be executed by a module (of software modules 722) or a portion of a module. The processes may be embodied in a non-transient machine-readable and/or computer-readable medium for configuring a computer system to execute the method. The software modules may be stored within and/or transmitted to a computer system  
25 memory to configure the computer system to perform the functions of the module.

The digital wallet provider system 14 normally processes information according to a program (a list of internally stored instructions such as a particular application program and/or an operating system) and produces resultant output information via  
30 input/output (I/O) devices 730. A computer process typically includes an executing (running) program or portion of a program, current program values and state information, and the resources used by the operating system to manage the execution of the process. A parent process may spawn other, child processes to help perform the overall functionality of the parent process. Because the parent process specifically  
35 spawns the child processes to perform a portion of the overall functionality of the

parent process, the functions performed by child processes (and grandchild processes, etc.) may sometimes be described as being performed by the parent process.

### ***Authorization System 18***

5

The authorization system 18 is able to communicate with the digital wallet provider system 14 through standard communication protocols provided for by communications network 20, in order to receive requests for payment authorization, process such requests, and convey responses back to the digital wallet provider system 14.

10

For example, the authorization system 18 may comprise an acquirer system (which may in turn comprise a core banking system in communication with an acquirer processor system), a payment network (such as Mastercard, Visa or China Unionpay) and an issuer system (which may comprise a core banking system and an issuer processor system).

15

The authorization system 18 may receive the payment authorization request via the acquirer system, which routes the request via the payment network to the issuer system in a manner known in the art. The request may be formatted according to the ISO 8583 standard, for example, and may include a primary account number (PAN) of the payment instrument being used for the transaction, a merchant identifier (MID), and an amount of the transaction, as well as other transaction-related information as will be known by those skilled in the art. The issuer system receives the request, applies authorization logic to approve or decline the request, and sends an authorization response (approve or decline, optionally with a code indicating the reason for the decline) back to the acquirer system via the payment network in known fashion. The acquirer system then communicates the authorization response to the digital wallet provider system 14.

20

25

Alternatively, in some embodiments, the authorization system 18 may receive the payment authorization request via the issuer system, which approves or declines the request (which again may be in ISO 8583 format, and comprise a PAN, MID, transaction amount etc.) and sends a response directly back to the digital wallet provider system 14.

30  
35

In addition to processing requests for payment in which funds are actually transferred from the cardholder's account (maintained in the issuer's core banking system) to the merchant's account (maintained in the acquirer's core banking system), the authorization system 18 may process a pre-authorization (or "pre-auth") request, in which funds are not transferred on approval of the request, but are instead placed on hold. The pre-auth can later be completed, for example by the merchant server 16 or the digital wallet provider system 14, in order to release the funds. Alternatively, the pre-auth can be cancelled, thus effectively cancelling the transaction.

#### 10 ***Merchant Server 16***

The merchant server 16 may be a server system operated by a merchant to process auction bids subsequent to authorization of electronic payment requests. The merchant server 16 is able to communicate with the digital wallet provider system 14 through standard communication protocols provided for by communications network 20. The merchant server 16 may transmit configuration information to digital wallet provider system 14 to define the format of auction bid data so that the digital wallet provider system 14 can accurately parse payment requests received via SMS or other messaging formats, and correctly identify the merchant and bid amount for the purposes of pre-authorizing the bid amount. One such example of configuration information transmitted to the merchant server 16 to the digital wallet provider system 14 is described with reference to Figures 5, 6, 7a, 7b and 7c below.

#### ***Digital Wallet Registration Process***

Before a person can use the system 10 to effect a payment request, the person must first have registered for a valid digital wallet (DW) account such as MasterPass™ or Apple Pay™, or an issuer wallet operated by a financial institution such as a bank, for example. Depending on the DW system, the user may sign up for an account in various ways e.g. through an internet browser accessing a website provided by the DW provider system 14 running on a computer or through a mobile app running on a mobile computer device. These systems are known in the art and as such will not be described in further detail. This embodiment of the invention requires the user to have access to the internet once, which is to complete the registration for the DW account.

As part of the DW account registration process, the user typically registers at least one valid payment card associated with the DW account. The system 10 can be used with any suitable payment card such as credit cards, debit cards or store cards. In another embodiment of the invention, other methods to register a payment option  
5 with a DW account without using a payment card may include funds transfer, linking to a bank account, cash deposit at a registered merchant and so on. These options may be useful for consumers who do not have valid payment cards. For ease of understanding, embodiments of the invention are described by way of reference to credit cards only, though it will be understood that the invention is applicable to other  
10 payment instruments such as debit cards, prepaid cards and so on, whether manifested in physical form, or as virtual cards which exist only in electronic form.

A user may be required to opt-in to allow electronic payment requests to be initiated by a user through an SMS message or through another messaging platform. This may  
15 be presented as an option to the user when they first register for a DW account or by accessing the DW account settings and enabling this option. In certain embodiments, the user may be required to verify their telephone number for security purposes. In one example of a mobile verification process, the DW provider system 14 generates a one time password (OTP) and sends it as part of the contents of a SMS message to  
20 the telephone number associated with the DW account. The mobile device 12 receives the OTP as part of the contents of the SMS. The user would then be prompted to enter the received OTP and the DW provider system 14 verifies and enables the option if the received OTP matches the issued OTP.

25 The user, upon enabling the SMS payment function on their DW account, may be prompted to provide a telephone number to be associated with future electronic payment requests initiated by SMS messages. Enhanced security measures may include the DW provider system 14 transmitting a one time password (OTP) as an SMS message to the mobile device 12 associated with the telephone number and  
30 requiring the user to enter the received OTP to authenticate the telephone number.

The system 10, in at least some embodiments, is capable of processing electronic payment requests initiated by SMS message for a multitude of payment types such as bill payments, auction payments, retail payments and etc. Such payments are  
35 typically associated with a particular merchant. A merchant offering SMS payment

transaction services may register with a DW provider and be entered into the database 716 of the DW provider system 14. Upon completion of the merchant's registration, the DW provider may provide the merchant with a unique merchant ID and a prescribed text format which would be provided to their customers to initiate an SMS payment transaction. In some embodiments, the merchant may specify the prescribed text format. The text format specification may be stored in database 716 and associated with the unique merchant ID, such that incoming payment requests received by DW provider system 14 may be processed according to the text format specification in order to generate payment authorisation request messages which are interpretable by the components of authorisation system 18.

### ***Processing an Electronic Payment Request***

Exemplary steps 300 performed by the components of system 10 for processing an electronic payment request are hereafter described with reference to Figure 4. At step 302, upon selection of the SMS icon on the "Home" graphical user interface (GUI) of the mobile device 12, the mobile device 12 generates for display 202 the contents of a user's text input entered either by means of a physical keyboard, numpad or onscreen keyboard. On receipt of user instruction to send an SMS message, the mobile device 12 retrieves the user input representing electronic payment request information represented by alphanumeric characters and sends it in the form of a SMS message with transceiver 212 to a messaging gateway system (in this instance an SMS gateway), which may validate the message prior to forwarding it to the DW provider system 14. The sender information, including the telephone number associated with the mobile device 12, may also be transmitted as part of the SMS message to the DW provider system 14.

Figure 7a, 7b and 7c shows an exemplary embodiment of the invention in practice. As one of ordinary skill in the art will appreciate, many variations, for example in the form and structure of the electronic payment parameters, are possible without departing from the scope of the invention.

Figure 7a shows an item that a merchant has made available as part of an auction to place a bid. It includes information needed to initiate an electronic payment request using an SMS message. This auction may be live, aired on a TV shopping channel or

through an auction website on the Internet. Figure 7a provides the following information:

- (a) a product description 602;
- 5 (b) a product ID 604;
- (c) a current bidding price 606;
- (d) a merchant ID 608; and
- (e) an order ID 610.

10 In this example, the item up for auction is a television which is available for a bidding price of \$2,000. A customer who is interested in placing a bid on this item would be able to do so by sending an SMS message (assuming they have registered for a DW account as described in the previous section).

15 Figure 7b shows an illustration of an embodiment of a mobile device 12 that has generated for display 202, an SMS message 652 sent by a DW account holder to place a bid on the exemplary item 602. The exemplary SMS message 652 contains 5 words separated by single spaces as shown in in Figure 7b which correspond to the information in Figure 7a as follows:

20

- (a) first word is the order ID 610;
- (b) second and third words are the merchant ID 608;
- (c) fourth word is the product ID 604; and
- (d) fifth word is the last four digits of primary account number (PAN).

25

For a successful electronic payment request, the SMS message should follow a pre-defined form of electronic payment request parameters to ensure that the DW provider system 14, authorization system 18 and merchant server 16 are able to process the contents of the SMS message and complete the transaction successfully.

30

The expected structure and form of the electronic payment request parameters are stored on the DW database 716. The DW database 716 is a computer readable data storage that may be associated with a cloud server accessible by communication network 20. The DW database 716 may have various sets of parameters which may  
35 be associated with a unique identifier. This may be associated with the order ID 610

or identity of the messaging gateway system, for example. In another embodiment, the five words are separated by another delimiter character or combination of characters, such as a comma, colon or semi-colon.

5 At step 304, the SMS parser module 140 of the DW provider system 14 receives the contents of the SMS and the associated telephone number of the mobile device 12. The DW provider system 14 then executes, for example, process 400 (as shown in Figure 5), wherein the SMS contents are parsed to identify electronic payment request parameters. At step 401, the DW provider system 14 retrieves the expected  
10 electronic payment parameters from DW database 716. At step 402, the string representing the contents of the SMS message is checked to determine whether it contains any special characters, e.g. non-alphanumeric characters (other than allowable delimiter characters such as space, colon or semi-colon, for example). If there are no special characters, step 404 is performed, whereby the string is split into  
15 words by using a single horizontal whitespace character (i.e. space) as a delimiter.

At step 406, the total number of words in the split string are added and checked to determine whether it matches an expected total number of words (from retrieved expected electronic payment parameters) as defined by the DW provider system 14 or  
20 merchant system 16. In the example of Figures 5, 7a and 7b, this is five words.

At step 408, the first word in the split string is checked if it matches a keyword, order ID, as defined by a list accessed from the DW database 716. The order ID provides information about the payment type. For example, the order ID 610 in Figure 7a is  
25 "BID" whereby the order is for placing a bid for an auction payment. In another example, the order ID may be "BUY" which may be used to purchase an item.

In certain embodiments, further security checks on the order ID may be performed. At step 410, if further security checks are to be performed, step 414 is performed.  
30 This may include checking the order ID to determine if it has been enabled for an access control list (ACL). If the keyword is associated to an ACL, a permission list is retrieved whereby the DW account associated with the telephone number is checked against the list to ensure appropriate permissions have been granted to carry out the order type as defined by the keyword. Another example includes retrieving and

checking the total number of arguments associated with the order ID and matching it against an expected total number of arguments.

At step 416, the second and third words in the split string are checked if it matches  
5 merchant information as defined by a list of merchants and associated merchant keywords accessed from the DW database 716. In another embodiment, the string may be a single substring, or any number of strings. If there is a match, the associated merchant information is retrieved from the DW database 716.

10 At step 420, the fifth word of the split string is checked if the characters are numbers as they should represent a primary account number (PAN) nominated to be used for the transaction.

If all the checks result in an affirmative, the SMS contents is verified to be in correct  
15 form in step 422, otherwise in step 424, the SMS contents are deemed to be in incorrect form.

At step 306 in Figure 4, the telephone number of the sender of the SMS message is matched against the telephone numbers registered to all the digital wallet accounts in  
20 the DW database 716. Once a DW account has been identified to have the same telephone number, the DW account information (e.g., a wallet identifier) is retrieved from the DW database 716 by the DW provider system 14. The DW provider system 14 then executes process 500 as shown in Figure 6, for example, to authenticate the DW account and user.

25

At step 502, the fifth word in the split string from step 404 is retrieved representing the PAN number nominated by the user to be used in this electronic payment request. The PAN may be the actual PAN displayed on the card (for a physical card), but in some embodiments, may be a surrogate value (token) which has the same format as  
30 the actual PAN, and stands in for the PAN when being transmitted to the authorization system 18, as an added security measure. At step 504, the PAN registered to the DW account is retrieved from the DW database 716. If the PAN nominated in the SMS message has a total string length which is less than 16 characters, the PAN registered to the DW account is trimmed or truncated from the left to match the length of the  
35 PAN nominated in the SMS message. Additionally, if there are multiple PANs

registered to the DW account, the following step is executed for each of the PANs. At step 506, the PAN nominated in the SMS message is compared against the PAN registered to the DW account to determine if they are an exact match. If there are multiple exact matches of the PAN, the DW provider system 14 generates an SMS message including the matched PANs requesting the user to respond indicating the preferred PAN to be used for this transaction. The SMS message is sent to the telephone number associated with the digital wallet account and the DW provider system 14 waits until it receives an SMS message from said telephone number.

At step 508, the associated DW account is checked if the feature to initiate electronic payment requests through a SMS message has been enabled. In certain embodiments, enhanced security measures may be necessary and a user authentication step may be required. At step 510, the optional user authentication is performed and may include one or more of the following:

- (a) an automated phone call to the telephone number associated with the DW account holder; and
- (b) an automated request for the digital wallet account holder to reply with one or more of the following:
  - (i) a personal identification number (PIN);
  - (ii) a one time password (OTP);
  - (iii) a token generated passcode;
  - (iv) a password;
  - (v) an answer to a security question; and
  - (vi) the card validation code (CVC2) associated with the payment card.

The DW provider system 14 can be used with payment cards including credit cards, debit cards, store cards, etc. For ease of description, the DW provider system 14 is below described by way of reference to credit cards only. However, DW provider system 14 and the system 10 can be used with any suitable payment card.

At step 512, if the authentication steps 506, 508 and 510 are successful, the DW account and user is deemed to be authenticated. Otherwise, at step 514, the authentication is deemed to have failed.

At step 308 in Figure 4, upon receipt of a successful authentication, the transaction processor 144 of the DW provider system 14 generates and sends to the authorization system 18, an electronic payment request including the following:

5

- (a) PAN associated with the digital wallet account;
- (b) optionally, digital wallet account information; and
- (c) payment information including:
  - (i) merchant identifier;
  - (ii) transaction type;
  - (iii) transaction information; and
  - (iv) total transaction amount.

10

At step 310, the authorization system 18 receives the electronic payment request to determine if the transaction is approved. Exemplary embodiments of the authorization system 18 as well as the various entities that may be included in the system were described in detail in the section above. For example, the authorization system 18 will approve or deny the transaction based on the issuer's response to the payment request. The issuer's response may be determined based on a check of the account associated with the PAN has sufficient funds or credit and may also include fraud detection steps (e.g. checking if the transaction amount is above a certain threshold or if the originating source appears "unusual"). If the issuer approves the transaction, the authorization system 18 authorizes the electronic payment request and issues message data representing the approved payment transaction status and associated transaction information to the merchant server 16.

20

25

At step 312, the merchant server 16 receives message data representing the approved payment transaction status and associated transaction information. At step 314, the order processor 162 processes the order in accordance with the received transaction information. The order processor 162 retrieves order information associated with the order ID 610 and determines the type of order to be placed. The order processor 162 then matches the product ID 604 with a product in its product database 160. For example, if the first word in the split string was a keyword "BID", the order to be processed by the merchant 16 would be to place a bid on product ID 604 for an auction that is in process. In this embodiment, if the merchant accepts the

30

35

bid, a pre-auth (i.e. hold on the funds) is placed and the transaction is completed once the auction is concluded. If a new bid is placed and is accepted, the previous pre-auth is cancelled and a new pre-auth is placed.

- 5 At step 316, if the merchant server 16 has successfully processed the order, the merchant server 16 sends data representing successful completion of order placement to the DW provider system 14.

At step 320, the DW provider system 14 receives data representing a successful  
10 transaction and the SMS parser module 140 generates and sends an SMS message with the contents indicating the transaction details and status to the telephone number associated with the DW account. At step 322, the mobile device 12 associated with the telephone number receives the SMS and generates for display 202 the SMS message. For example, Figure 7c shows an embodiment of the mobile device  
15 12 generating on display 202 an exemplary SMS message 654 received from the DW provider system 14 indicating that the electronic payment request was successful and that the user has successfully placed a bid of \$2,000 for the item.

Many modifications will be apparent to those skilled in the art without departing from  
20 the scope of the present invention. For example, other embodiments of the invention may be to purchase an item (whether on an online shopping channel or at a physical store), to pay a bill or even transfer funds (whether to a merchant or to a private account). Additionally, the structure and form of the contents of the SMS (electronic payment parameters) may differ.

25

Throughout this specification, unless the context requires otherwise, the word "comprise", and variations such as "comprises" and "comprising", will be understood to imply the inclusion of a stated integer or step or group of integers or steps but not the exclusion of any other integer or step or group of integers or steps.

30

The reference to any prior art in this specification is not, and should not be taken as, an acknowledgment or any form of suggestion that the prior art forms part of the common general knowledge.

Claims Defining the Invention

1. A digital wallet provider system for processing electronic payment requests, the system including a server with one or more computer processors in communication  
5 with non-transitory computer readable data storage which are configured to:
- (a) receive electronic payment request message data, with an associated telephone number, for initiating an electronic payment request;
  - (b) parse the message data to identify electronic payment request parameters;
  - 10 (c) use the associated telephone number to identify a digital wallet account stored in said data storage;
  - (d) retrieve payment information from the digital wallet account;
  - (e) authenticate said payment information, wherein the step of authenticating payment information includes the following steps:  
15 (e1) retrieving digital wallet account information associated with the telephone number associated with the electronic payment request message data from data storage;
  - (e2) retrieving a primary account number (PAN) associated with the digital wallet account information; and
  - 20 (e3) checking if the PAN associated with the digital wallet account information matches a predefined word associated with payment credentials of the electronic payment request parameters;
  - (f) send an electronic payment request to an authorization server;
  - 25 (g) receive data representing an electronic payment request approval status; and
  - (h) send message data representing the electronic payment request approval status.
- 30 2. The system claimed in claim 1, wherein the step of parsing the message data to identify electronic payment request parameters includes the following steps:
- (a) splitting the string into multiple words by a delimiter;
  - (b) checking that the split string has a total number of words that matches an expected number;

- (c) checking that a predefined word associated with an order type in the split string matches a keyword from a list of predefined keywords retrieved from data storage;
- 5 (d) checking that a predefined word or words associated with identifying a merchant in the split string matches a list of merchants retrieved from data storage; and
- (e) checking that the characters in a predefined word associated with payment credentials are numbers.

10 3. The system claimed in claim 1 or claim 2, wherein the step of authenticating payment information includes checking if the digital wallet account has enabled the feature of initiating electronic payment requests via message data.

15 4. The system claimed in any one of claims 1 to 3, wherein the step of checking if the PAN associated with the digital wallet account information matches the predefined word associated with payment credentials of the electronic payment request includes:

- (a) if the length of the predefined word is less than the length of the PAN, truncating the PAN from the left to match the number of characters in the predefined word of the parsed message data; and/or
- 20 (b) if there are multiple payment cards associated with the digital wallet account;
  - (i) generating message data including any PANs that were an exact match with the predefined word;
  - (ii) sending the generated message data to the mobile device associated with the digital wallet account; and
  - 25 (iii) receiving subsequent message data from the mobile device indicating the PAN to be used for the electronic payment request.

30 5. The system claimed in any one of claims 1 to 4, wherein the step of receiving the electronic payment request message data includes receiving the following:

- (a) contents of the message data from a mobile device; and
- (b) a telephone number associated with the mobile device.

6. The system claimed in any one of claims 1 to 5, wherein the step of authenticating payment information includes a user authentication step including one or more of the following:
- 5 (a) an automated phone call to the mobile device associated with the digital wallet account holder; and
  - (b) an automated request for one or more of the following:
    - (i) a personal identification number (PIN);
    - (ii) a one time password (OTP);
    - (iii) a token generated passcode;
    - 10 (iv) a password;
    - (v) an answer to a security question; and
    - (vi) the card validation code (CVC2) associated with the payment card.
- 15 7. The system claimed in any one of claims 1 to 6 wherein the electronic payment request includes one or more of the following:
- (a) digital wallet account information including an associated PAN;
  - (b) a merchant identifier; and
  - (c) a total transaction amount.
- 20 8. The system claimed in any one of claims 1 to 7, wherein the PAN is secured by means of tokenisation and/or encryption.
9. The system claimed in any one of claims 1 to 8, wherein if any of the steps are
- 25 unsuccessful, the digital wallet provider:
- (a) generates message data indicating that the electronic payment request was unsuccessful; and
  - (b) sends the message data to the telephone number associated with the digital wallet account.
- 30 10. The system claimed in any one of claims 1 to 9, wherein the message data is any one of the following:
- (a) a short message service (SMS) message;
  - (b) a multimedia messaging service (MMS) message; and
  - 35 (c) a message sent using an instant messaging service.

11. A method for processing an electronic payment request performed by one or more computer processors of a digital wallet provider system executing instructions stored on non-transitory computer readable data storage that, when executed, cause  
5 the system to perform the steps of:

- (a) receiving electronic payment request message data, with an associated telephone number, for initiating an electronic payment request;
- (b) parsing the message data to identify electronic payment request parameters;
- 10 (c) using the associated telephone number to identify a digital wallet account stored in said data storage;
- (d) retrieving payment information from the digital wallet account;
- (e) authenticating said payment information, wherein the step of authenticating payment information includes the following steps:
  - 15 (e1) retrieving digital wallet account information associated with the telephone number associated with the electronic payment request message data from data storage;
  - (e2) retrieving a primary account number (PAN) associated with the digital wallet account information;
  - 20 (e3) checking if the PAN associated with the digital wallet account information matches a predefined word associated with payment credentials of the electronic payment request parameters;
- (f) sending an electronic payment request to an authorization server;
- 25 (g) receiving data representing an electronic payment request approval status; and
- (h) sending message data representing the electronic payment request approval status.

30 12. The method claimed in claim 11, wherein the step of parsing the message data to identify electronic payment request parameters includes the following steps:

- (a) splitting the string into multiple words by a delimiter;
- (b) checking that the split string has a total number of words that matches an expected number;

- (c) checking that a predefined word associated with an order type in the split string matches a keyword from a list of predefined keywords retrieved from data storage;
- (d) checking that a predefined word or words associated with identifying a merchant in the split string matches a list of merchants retrieved from data storage; and
- (e) checking that the characters in a predefined word associated with payment credentials are numbers.

13. The method claimed in claim 11 or claim 12, wherein the step of authenticating payment information includes checking if the digital wallet account has enabled the feature of initiating electronic payment requests via message data.

14. The method claimed in any one of claims 11 to 13, wherein the step of checking if the PAN associated with the digital wallet account information matches the predefined word associated with payment credentials of the electronic payment request includes:

- (a) if the length of the predefined word is less than the length of the PAN, truncating the PAN from the left to match the number of characters in the predefined word of the parsed message data; and/or
- (b) if there are multiple payment cards associated with the digital wallet account;
  - (i) generating message data including any PANs that were an exact match with the predefined word;
  - (ii) sending the generated message data to the mobile device associated with the digital wallet account; and
  - (iii) receiving subsequent message data from the mobile device indicating the PAN to be used for the electronic payment request.

15. The method claimed in any one of claims 11 to 14, wherein the step of receiving the electronic payment request message data includes receiving the following:

- (a) contents of the message data from a mobile device; and
- (b) a telephone number associated with the mobile device.

16. The method claimed in any one of claims 11 to 15, wherein the step of authenticating payment information includes a user authentication step including one or more of the following:
- 5 (a) an automated phone call to the mobile device associated with the digital wallet account holder; and
  - (b) an automated request for one or more of the following:
    - (i) a personal identification number (PIN);
    - (ii) a one time password (OTP);
    - (iii) a token generated passcode;
    - 10 (iv) a password;
    - (v) an answer to a security question; and
    - (vi) the card validation code (CVC2) associated with the payment card.
- 15 17. The method claimed in any one of claims 11 to 16 wherein the electronic payment request includes one or more of the following:
- (a) digital wallet account information including an associated PAN;
  - (b) a merchant identifier; and
  - (c) a total transaction amount.
- 20 18. The method claimed in any one of claims 11 to 17, wherein the PAN is secured by means of tokenisation and/or encryption.
19. The method claimed in any one of claims 11 to 18, wherein if any of the steps
- 25 are unsuccessful, the digital wallet provider:
- (a) generates message data indicating that the electronic payment request was unsuccessful; and
  - (b) sends the message data to the telephone number associated with the digital wallet account.
- 30 20. The method claimed in any one of claims 11 to 19, wherein the message data is any one of the following:
- (a) a short message service (SMS) message;
  - (b) a multimedia messaging service (MMS) message; and
  - 35 (c) a message sent using an instant messaging service.