A hybrid terminal device includes a payment card reader and a smart phone and is configured to facilitate financial transactions. The payment card reader is configured to extract identification information from payment cards for use in facilitating the transactions. The hybrid terminal also obtains cardholder contact information and, based on the cardholder contact information, initiates transmission of a transaction notification related to a completed financial transaction, such as a financial transaction whose completion was facilitated by using the hybrid terminal device.
SYSTEM AND METHOD FOR PROVIDING PAPERLESS TRANSACTIONS

CROSS-REFERENCE TO RELATED APPLICATION


BACKGROUND

Technical Field

The present disclosure relates to systems, methods and articles for providing paperless transactions.

Description of the Related-Art

Credit and debit card financial transactions may occur using a payment acceptance device coupled to a plain-old-telephone system (POTS). The card is read by the payment acceptance device, which contacts a financial institution through the POTS to obtain authorization for the transaction.

BRIEF SUMMARY

In an embodiment, a hybrid terminal device comprises: a smart phone; and a payment card terminal communicatively and moveably coupled to the smart phone and configured to read payment cards, wherein the hybrid terminal includes one or more processors configured to implement at least one manager module and the at least one manager module is configured to respond to an indication of a completed financial transaction involving a cardholder by selectively initiating transmission of a transaction notification based on contact information associated with the cardholder. In an embodiment, the smart phone is configured to communicatively couple the hybrid terminal device to one or more remote servers to facilitate performance of at least one of real-time and on-line financial transactions involving use of the payment card terminal. In
an embodiment, the at least one manager module is configured to facilitate invoicing related to financial transactions. In an embodiment, the at least one manager module comprises: an electronic point-of-sale manager; and a sales application manager. In an embodiment, the contact information includes cardholder preference information and the transmission is initiated in accordance with the cardholder preference information. In an embodiment, the at least one manager module is configured to, in response to the indication: determine whether the contact information is stored on the hybrid terminal device; and when it is determined the contact information is stored by the hybrid terminal device, initiate transmission of the transaction notification based on the contact information stored by the hybrid terminal device. In an embodiment, the at least one manager module is configured to initiate a request for the contact information. In an embodiment, the request for the contact information is a request to a remote server. In an embodiment, the request for the contact information includes a payment card long number (PAN) extracted from a payment card by the payment card terminal. In an embodiment, the hybrid terminal further comprises a display, wherein the request for the contact information is displayed on the display. In an embodiment, the contact information includes a phone number and the transaction notification comprises a text message to the phone number. In an embodiment, the at least one manager module is configured to associate the phone number with the transaction. In an embodiment, the transaction notification comprises a short-message-service (SMS) text. In an embodiment, the contact information includes an email address and the transaction notification comprises an email message. In an embodiment, the payment card terminal is configured to extract a payment card long number (PAN) from a payment card. In an embodiment, the at least one manager module is configured to initiate retrieval of the contact information based on the extracted PAN. In an embodiment, the at least one manager module is configured to cause the hybrid terminal to facilitate a cardholder performing at least one of: providing the contact information; correcting the contact information; and confirming the contact
information. In an embodiment, the at least one manager module is configured to generate a passcode associated with the completed financial transaction and the transaction notification includes the passcode. In an embodiment, a system comprises one or more servers configured to provide financial transaction related services, and a hybrid terminal device as described herein.

In an embodiment, a method comprises: extracting cardholder identification information from a payment card using a card reader of a hybrid terminal device; and responding to an indication of a completed financial transaction associated with the payment card by: obtaining cardholder contact information; and initiating transmission of a transaction notification based on the obtained cardholder contact information, the initiating being performed by a smart phone module of the hybrid terminal device. In an embodiment, the obtaining cardholder contact information comprises retrieving cardholder contact information associated with the extracted cardholder identification information. In an embodiment, the retrieving cardholder contact information comprises retrieving cardholder contact information stored by the hybrid terminal device. In an embodiment, the retrieving cardholder contact information comprises requesting cardholder contact information from one or more remote servers. In an embodiment, the obtaining cardholder contact information comprises requesting information via a user interface of the hybrid terminal device. In an embodiment, the requesting information via the user interface includes at least one of: requesting entry of contact information; requesting correction of contact information; and requesting verification of contact information. In an embodiment, the cardholder contact information comprises a phone number. In an embodiment, the method comprises associating the phone number with the completed financial transaction. In an embodiment, the transaction notification comprises one or more short-message-service (SMS) messages. In an embodiment, the method comprises providing the cardholder with one or more documents associated with the completed financial transaction. In an embodiment, the one or more documents include at least one of an invoice and a receipt. In an embodiment,
the completed financial transaction is performed using the hybrid terminal
device. In an embodiment, the cardholder contact information includes
cardholder preference information and the transmission is initiated in
accordance with the cardholder preference information. In an embodiment, the
extracting cardholder identification information includes extracting a payment
card long number (PAN) from the payment card. In an embodiment, the
method comprises generating a passcode associated with the completed
financial transaction, wherein the transaction notification includes the passcode.
In an embodiment, the method further comprises retrieving information
associated with the completed financial transaction based on the passcode. In
an embodiment, a hybrid terminal device is configured to perform one or more
of the methods described herein. In an embodiment, a system comprises one
or more servers configured to facilitate completion of financial transactions and
a hybrid terminal device configured to communicatively couple to the one or
more servers, wherein the system is configured to perform one or more of the
methods described herein. In an embodiment, a non-transitory computer-
readable medium's contents cause a hybrid terminal device to perform one or
more of the methods described herein.

In an embodiment, a hybrid terminal device comprises: means for
extracting cardholder identification information from a payment card; and
means for responding to an indication of a completed financial transaction
associated with the payment card by: obtaining cardholder contact information;
and initiating transmission of a transaction notification based on the obtained
cardholder contact information. In an embodiment, the means for extracting
comprises a payment card reader of the hybrid terminal. In an embodiment, the
means for responding comprises a smart phone module of the hybrid terminal.

In an embodiment, a method comprises allowing a provider of
goods or services such as a merchant (generally referred to herein as an
acceptor) or a customer of such a provider (generally referred to herein as a
card holder) to conduct financial transactions.
In an embodiment, a hybrid terminal device that is part smart phone and part credit card terminal facilitates attended face-to-face transactions. In an embodiment, the hybrid terminal device is communicatively coupled with remote servers to manage and carry out payment transactions with online and/or real time verification. In an embodiment, hybrid device and server side elements/functionality support invoicing aspects of payment transaction sequences. In an embodiment, a conventional dedicated card terminal unit may be employed. In an embodiment, online (for example, web-based) card payment transactions may be employed.

In an embodiment, a method recognizes a card holder through a credit card terminal, hybrid device, secure communication, etc., and obtains or retrieves a phone number associated with the card holder. In an embodiment, the method provides the card holder with an opportunity to provide, correct or verify the phone number associated with the card holder. In an embodiment, the method comprises associating the phone number associated with the card holder with a transaction. In an embodiment, the phone number associated with the card holder is a mobile phone number. In an embodiment, the mobile phone number associated with the card holder is a number of a mobile phone present at a transaction site. In an embodiment, the method comprises providing notification of the transaction and/or completion of the transaction to the card holder. In an embodiment, the notification is through one or more SMS messages. In an embodiment, an SMS message is sent substantially simultaneous with the transaction. In an embodiment, the method comprises providing the cardholder with an online receipt, invoice and/or other documents associated with the transaction. In an embodiment, the method comprises providing the merchant with an opportunity to personalize the receipt, invoice and/or other documents associated with the transaction. In an embodiment, the method comprises selecting a transaction template from a plurality of transaction templates based on one or more characteristics of a transaction, populating the selected template with data related to the transaction, and generating appropriate electronic messages and/or documents pertaining to the
transaction, such as one or more SMS messages, emails, invoices, etc., or combinations thereof.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S)

Figure 1 shows an embodiment of a hybrid terminal device from several perspectives.

Figure 2 is a functional block diagram of an embodiment of an environment suitable for providing transaction services according to at least one illustrated embodiment.

Figure 3 is a functional block diagram of an embodiment of a system to handling financial transactions.

Figures 4A and 4B are a flow chart illustrating an embodiment of a method of providing post-transaction-authorization services.

Figure 5 illustrates an embodiment of a method of determining whether cardholder information is available to an embodiment of a transaction processing system.

Figure 6 illustrates an embodiment of a method of facilitating retrieval of a receipt or invoice for a transaction by a cardholder.

Figure 7 illustrates an embodiment of a method of responding to a cardholder request to retrieve an invoice.

Figure 8 illustrates an embodiment of a method of a cardholder creating an account on an invoice server.

Figure 9 illustrates an embodiment of a method of a cardholder accessing an account on an invoice server.

Figure 10 illustrates an embodiment of a method of adding a card to an existing cardholder account.

Figure 11 illustrates an embodiment of a method of personalizing a receipt or invoice.

Figure 12 illustrates an embodiment of a method of personalizing a receipt or invoice.
Figure 13 illustrates an embodiment of a method of personalizing a receipt or invoice.

Figure 14 illustrates an embodiment of a method of selecting an appropriate template for a transaction and populating the selected template.

Figure 15 shows an embodiment of a method of generating an invoice at an EPOS and forwarding the invoice as part of transaction data.

Figure 16 illustrates an embodiment of a method of selecting an invoice template.

Figure 17 illustrates an embodiment of a method of generating an invoice containing online content.

DETAILED DESCRIPTION

In the following description, certain details are set forth in order to provide a thorough understanding of various embodiments of devices, systems, methods and articles. However, one of skill in the art will understand that other embodiments may be practiced without these details. In other instances, well-known structures and methods associated with, for example, mobile devices such as smart phones, card readers, point-of-sale systems, computing systems, virtual computing systems, telecommunication networks, web browsers, web servers, etc., have not been shown or described in detail in some figures to avoid unnecessarily obscuring descriptions of the embodiments.

Unless the context requires otherwise, throughout the specification and claims which follow, the word "comprise" and variations thereof, such as "comprising," and "comprises," are to be construed in an open, inclusive sense, that is, as "including, but not limited to."

Reference throughout this specification to "one embodiment," or "an embodiment" means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment. Thus, the appearances of the phrases "in one embodiment," or "in an embodiment" in various places throughout this specification are not
necessarily referring to the same embodiment, or to all embodiments. Furthermore, the particular features, structures, or characteristics may be combined in any suitable manner in one or more embodiments to obtain further embodiments.

The headings are provided for convenience only, and do not interpret the scope or meaning of this disclosure.

The sizes and relative positions of elements in the drawings are not necessarily drawn to scale. For example, the shapes of various elements and angles are not drawn to scale, and some of these elements are enlarged and positioned to improve drawing legibility. Further, the particular shapes of the elements as drawn are not necessarily intended to convey any information regarding the actual shape of particular elements, and have been selected solely for ease of recognition in the drawings.

Embodiments of systems and methods in which electronic devices such as credit card terminals employ short-message-service (SMS) payment notifications and email and web-based delivery of receipts and customer invoices are described herein.

Figure 1 shows various perspective views of an embodiment of a hybrid terminal device (SP/PED) 100 that includes smart phone and electronic point-of-sale functionality. As illustrated, the hybrid terminal device SP/PED 100 is part smart phone 102 and part credit card terminal 104. As discussed in more detail herein, embodiments of the hybrid terminal device SP/PED 100 are configured to communicatively couple to remote servers to facilitate face-to-face financial transactions with online and real time verification. As illustrated, the hybrid terminal device 100 comprises a two-part body with the parts moveably coupled together. As illustrated, a hinge 106 is employed to moveably couple the two-part body together. Other mechanical coupling systems may be employed. In some embodiments, one part of the two-part body may comprise a smart phone (SP) 102 and the other part may comprise a credit card terminal (PED) 104. In another example, one part may comprise a card reader and another part may comprise a computing and
telecommunications system. In some embodiments, the hybrid terminal device SP/PED 100 may comprise a one part main body.

The following discussion provides a brief, general description of a suitable computing environment in which the embodiments described herein may be implemented. Although not required, various embodiments will be described in the general context of computer-executable instructions, such as program application modules, objects, or macros being executed by one or more electronic devices, such as a smart phone, a credit card terminal, a hybrid smart phone/point-of-sale system, a personal computer, a server, etc., and various combinations thereof. Those skilled in the relevant art will appreciate that various embodiments can be practiced with other computing system configurations, including other handheld devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, networked personal computers (PCs), minicomputers, mainframe computers, virtual systems, and the like. Various embodiments can be practiced in distributed computing environments where tasks or modules are performed by remote processing devices, which are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

Figure 2 shows an embodiment of an environment 200 that may be employed to facilitate financial transactions as described herein. The environment 200 includes a computing system 10. For example, the computing system 10 may be configured as a smart phone, a point-of-sale terminal, a hybrid smart phone/point-of-sale terminal (See SP/PED 100 of Figure 1), a host server, such as a financial transactions server, a communications server, etc. The computing system 10 may, for example, be operated by a business providing goods or services to a consumer (commonly referred to as an acceptor), by a consumer purchasing goods or services from a business (commonly referred to as a cardholder), by a vendor, such as a financial institution, a communication service provider (for example, a financial institution or financial transaction service provider, a telecom service provider, an Internet
service provider), etc. The computing system 10 may take the form of any of
the variety of types discussed above, which may run a networking client, for
example a server, a Web browser, etc. The computing system 10 comprises a
processor unit 12, a system memory 14 and a system bus 16 that couples
various system components including the system memory 14 to the processing
unit 12. The processing unit 12 may be any logical processing unit, such as
one or more central processing units (CPUs), digital signal processors (DSPs),
application-specific integrated circuits (ASIC), etc. Unless described otherwise,
the construction and operation of the various blocks shown in Figure 2 are of
conventional design. As a result, such blocks need not be described in further
detail herein, as they will be understood by those skilled in the relevant art.

The system bus 16 can employ any known bus structures or
architectures, including a memory bus with memory controller, a peripheral bus,
and/or a local bus. The system memory 14 includes read-only memory
("ROM") 18 and random access memory ("RAM") 20. A basic input/output
system ("BIOS") 22, which can form part of the ROM 18, contains basic
routines that help transfer information between elements within the computing
system 10, such as during startup.

The computing system 10 also includes one or more optional
spinning media memories such as a hard disk drive 24 for reading from and
writing to a hard disk 25, and an optical disk drive 26 and a magnetic disk drive
28 for reading from and writing to removable optical disks 30 and magnetic
disks 32, respectively. The optical disk 30 can be a CD-ROM, while the
magnetic disk 32 can be a magnetic floppy disk or diskette. The hard disk drive
24, optical disk drive 26 and magnetic disk drive 28 communicate with the
processing unit 12 via the bus 16. The hard disk drive 24, optical disk drive 26
and magnetic disk drive 28 may include interfaces or controllers coupled
between such drives and the bus 16, as is known by those skilled in the
relevant art, for example via an IDE (Integrated Drive Electronics) interface.
The drives 24, 26 and 28, and their associated computer-readable media,
provide nonvolatile storage of computer-readable instructions, data structures,
program modules and other data for the computing system 10. Although the
depicted computing system 10 employs hard disk 25, optical disk 30 and
magnetic disk 32, those skilled in the relevant art will appreciate that other
types of spinning media memory computer-readable media may be employed,
such as, digital video disks (DVD), Bernoulli cartridges, etc. Those skilled in the
relevant art will also appreciate that other types of computer-readable media
that can store data accessible by a computer may be employed, for example,
non-spinning media memories such as magnetic cassettes, flash memory
cards, RAMs, ROMs, smart cards, etc.

Program modules can be stored in the system memory 14, such
as an operating system 34 (for example, Windows™, Android™, etc), one or
more application programs 36, other programs or modules 38, and program
data 40. The system memory 14 also includes a server 41 for permitting the
computing system 10 to exchange data with sources such as Websites of the
Internet, corporate intranets, or other networks, as well as other server
applications on server computers. The server 41 may be markup language
based, such as hypertext markup language (HTML), and operate with markup
languages that use syntactically delimited characters added to the data of a
document to represent the structure of the document, etc.

While shown in Figure 2 as being stored in the system memory
14, the operating system 34, application programs 36, other program modules
38, program data 40 and server 41 can be stored on the hard disk 25 of the
hard disk drive 24, the optical disk 30 and the optical disk drive 26, the
magnetic disk 32 of the magnetic disk drive 28 and/or other memory such as a
flash drive, etc. A user can enter commands and information to the computing
system 10 through input devices such as a keypad or keyboard 42 and a
pointing device such as a mouse 44. Other input devices can include a
microphone, joystick, game pad, scanner, touch screen, card reader, chip
reader, etc. These and other input devices as illustrated are connected to the
processing unit 12 through an interface 46 such as a serial port interface that
couples to the bus 16, although other interfaces such as a parallel port, a game
port or a universal serial bus (USB) can be used. A display or monitor 48 or
other display devices may be coupled to the bus 16 via video interface 50, such
as a video adapter. The computing system 10 can include other output devices
such as speakers, printers, etc.

The computing system 10 can operate in a networked
environment using logical connections to one or more repositories 6 and/or
other computing systems 8a-8n. The computer system 10 may employ any
known means of communications, such as through a local area network (LAN)
52 or a wide area network (WAN), a telecommunications network or the Internet
54. Such networking environments are well known and may include, for
example, any type of telecommunications network or other network, such as
CDMA, OFDMA, GSM, WiMAX, VoIP, WiFi, Internet Protocol, various IEEE
standard protocols, etc.

When used in a LAN networking environment, the computing
system 10 may be coupled to the LAN 52 through an adapter or network
interface 56 (communicatively linked to the bus 16). When used in a WAN
networking environment, the computing system 10 often includes a device,
such as a modem 57, a mobile phone communication module or other device
for establishing communications over the WAN/Internet 54. As illustrated, a
modem 57 is shown in Figure 2 as communicatively linked between the
interface 46 and the WAN/Internet/Telecommunications network 54. In a
networked environment, program modules, application programs, or data, or
portions thereof, can be stored in a server computer (for example, another
configured computing system similar to the computing system 10). Those
skilled in the relevant art will readily recognize that the network connections
shown in Figure 2 are only some examples of establishing communication
links between computers and/or other systems and devices 60, and other links
may be used, including wireless links.

The computing system 10 may include one or more interfaces
such as slot 58 to allow the addition of devices either internally or externally to
the computing system 10. For example, suitable interfaces may include ISA
(Industry Standard Architecture), IDE, PCI (Personal Computer Interface) and/or AGP (Advance Graphics Processor) slot connectors for option cards, serial and/or parallel ports, USB ports (Universal Serial Bus), audio input/output (I/O) and MIDI/joystick connectors, slots for memory, credit card readers, scanners, bar code readers, RFID readers, etc., collectively referenced as 60.

The term computer-readable medium as used herein refers to any medium that participates in providing instructions to processor unit 12 for execution. Such a medium may take many forms, including but not limited to, non-volatile media, and volatile media. Non-volatile media includes, for example, hard, optical or magnetic disks 25, 30, 32, respectively. Volatile media includes dynamic memory, such as system memory 14.

Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, or any other magnetic medium, a CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, a PROM, and EPROM, a FLASH-EPROM, any other memory chip or cartridge, as described hereinafter, or any other medium from which a computer can read.

Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to processor unit 12 for execution. For example, the instructions may initially be carried on a magnetic disk of a remote computer. The remote computer can load the instructions into its dynamic memory and send the instructions over a telephone line using a modem. A modem 57 local to computer system 10 can receive the data on the telephone line and use an infrared transmitter to convert the data to an infrared signal. An infrared detector coupled to the system bus 16 can receive the data carried in the infrared signal and place the data on system bus 16. The system bus 16 carries the data to system memory 14, from which processor unit 12 retrieves and executes the instructions. The instructions received by system memory 14 may optionally be stored on storage device either before or after execution by processor unit 12.
The repository 6 may be a permanent storage medium for data. The repository 6 may be specific to each end user, or shared between some or all end users. For example, different financial services vendors (for example, banks or bank exchanges, VISA, Mastercard) may have separate repositories or may share repositories. The repository 6 (only one illustrated) may run on the same computing system as an application accessing the repository, or on another computing system accessible over the network 52, 54.

Embodiments of the computing system 10 of Figure 2 may not include all of the illustrated components of the computing system 10, may contain additional components not shown in Figure 10, and may not be configured as shown in Figure 10. For example, a computing system 10 configured as hybrid smart phone/point-of-sale system (see Figure 3), may not include an optical disk drive and may include one or more application specific integrated circuits or digital signal processors (not shown) to perform one or more of the functions of the hybrid smart phone/point-of-sale system. In another example, a hybrid smart phone/point of sale system may include one or more telecommunications modules to handle call processing, such as CDMA, OFDMA, GSM, etc., call processing.

Figure 3 is a functional block diagram of an embodiment of a system 300 for handling financial transactions. The system 300 includes a hybrid smart phone/point-of-sale device (SP/PED) 302 and one or more servers 304, which may typically be remote from the SP/PED 302. A provider of goods or services (an acceptor) may use the SP/PED 302 in communication with the one or more servers 304 to conduct financial transactions with a customer (a cardholder) or vendor. For example, a customer may purchase goods from the provider and pay for the goods by presenting a credit card to the provider. As discussed in more detail below, the provider may use the SP/PED 302 in communication with the one or more servers 304 to process the payment and provide notifications, invoices, etc., to the customer. In another example, a customer may return an item and the provider may use the SP/PED 302 to process a credit to the customer. Processing of the transaction may include
online and/or real time verification of the transaction. The SP/PED 302 may comprise one or more configured computing systems, such as an embodiment of the computing system 10 of Figure 2. Similarly, the one or more servers 304 may comprise one or more configured computing systems, such as an embodiment of the computing system 10 of Figure 2.

As illustrated, the SP/PED 302 comprises a smart phone module 306 and a point-of-sale module, credit card terminal, etc. (PED) 308 communicatively coupled together through an interface 307, which as illustrated is serial interface such as a USB interface, an RS232 interface, etc., exchanging messages in, for example, an ISO 8583 financial transaction card message format.

As illustrated, the smart phone module 306 comprises an operating system 310 (for example, a Windows™ or Android™ operating system), and application modules 312 (for example, in a system memory, see system memory 14 of Figure 2). As illustrated, the application modules include a sales application manager, an electronic-point-of-sale manager, and a serial device driver, which may, for example, control the serial interface 307.

As illustrated, the PED module 308 comprises an operating system 314 shown with drivers and configured to support for example, EMV L1 smart card reader standards and devices, such as the Financial Application Specification for SCF Compliant EMV Terminals (SEPA-FAST) standards. Other standards may be employed and supported. The PED module 308 as illustrated also includes an EMV L1 Kernel 316, configured to manage and/or perform various functions associated with financial transactions, such as language selection, personal identification number (PIN) prompting, payment card long number (PAN) reading, PIN and/or PAN verifying, encoding, encryption, decryption, transmitting, authorizing, etc. The PED module 308 includes a card applications module 318 configured to manage card applications and a communications manager 320 configured to manage communications between the PED module 308 and cards or other payment devices and between the PED module 308 and the smart phone module 306.
The PED module 308 includes an update manager 322 configured to manage and/or perform updates, for example updates to the operating system, drivers, kernels, card applications and communications manager. As illustrated the PED module comprises a module or reader interface 324 configured to read data from chips, such as smart micro chips on credit cards or RFID devices, and a module or reader interface 326 configured to read magnetic data, for example data stored in a magnetic strip on a credit card. The interface or module 326 may comprise a slot into which a credit card may be inserted, a slot through which a credit card may be swiped, etc. As illustrated, a card 328 with a smart chip is being read using the interface 324 and a card 330 with a magnetic strip is being read using interface 326. In some embodiments, a single module or reader interface may perform the functionality of the illustrated reader interfaces 324, 326. In some embodiments, all or part of the server functions (for example, the payment gateway) may be incorporated into or performed by the SP/PED 302. In some embodiments the interface 324 may be configured to wirelessly read the card 328.

Figures 4A and 4B are a flow diagram of an embodiment of a method 400 of providing post-transaction authorization services. For convenience, the method 400 will be described with reference to the embodiment of a system 300 of Figure 3. The method 400 may be performed by embodiments other than the system 300 of Figure 3. At act 402, the method is started following completion of a basic transaction payment flow. For example, after a cardholder has had their card read by a reader (for example, reader 324 or 326 of Figure 3), has authenticated the card (for example, by entering their PIN into a keypad on the SP/PED device 302) and has authorized a payment to be taken from an account, for example, from the PAN associated with the card. The method 400 proceeds from act 402 to act 404.

At act 404, the method 400 determines whether information related to the PAN of the card is available. For example, the SP/PED 402 may determine whether a notification preference, and phone number, email address, etc., associated with the notification preference is stored. For example, The
SP/PED 402 may determine whether information related to the PAN is stored locally on the SP/PED, or is stored remotely.

When it is determined at act 404 that information related to the PAN is available, the method proceeds from act 404 to act 406, where a notification preference information associated with the PAN is retrieved and/or analyzed to determine the notification preference.

When it is determined at act 406 that the notification preference is to always send an SMS to a mobile phone number, the method 400 proceeds from act 406 to act 408. At act 408, a message pertaining to the transaction is generated, for example by the SP/PED 302. The message may contain a transaction amount, a merchant name, and a notice that the confirmation has been sent. In some embodiments, this message may appear on a display of the SP/PED 302. The method proceeds from act 408 to act 410, where the SP/PED 302 causes an SMS message 410A to be generated and sent to the cardholder’s phone number, for example, to the cardholder’s mobile phone through a carrier server. As illustrated, the message includes the carrier name, a date and/or time, an indication of the source of the message (for example, the acceptor or a vendor of the acceptor such as a financial institution, a summary of the transaction, and instructions for how to download a full receipt. The method 400 proceeds from act 410/410A to act 412, where the cardholder is prompted to return the SP/PED to the acceptor. As illustrated, the method 400 proceeds from act 412 to act 414, where a signal that the transaction is complete, such as a beep, is generated, and to act 416, where information, for example in the form of a message, is presented to the acceptor.

When it is determined at act 406 that the notification preference is to always send an email, the method 400 proceeds from act 406 to act 418. At act 418, an email message is generated and sent to a stored email address. The message or a similar message may also be displayed on a display of the SP/PED 302. The method proceeds from act 418 to act 412, which is described above.
When it is determined at act 406 that the notification preference is to ask first, then send an SMS if desired, the method 400 proceeds from act 406 to act 420. At act 420, the SP/PED 302 displays an indication that the transaction has been approved and may display summary information pertaining to the transaction. As illustrated, the cardholder and/or acceptor also is prompted to indicate whether a receipt should be sent to a phone number, such as a mobile phone number. If the cardholder and/or acceptor indicates yes, for example by pressing an OK key, the method proceeds from act 420 to act 422. If the cardholder and/or acceptor indicates no, for example by hitting cancel or by failing to respond within a set time period, the method may terminate or proceed to act 412. At act 422 a message is displayed on the SP/PED 302 indicating a receipt is being sent to a stored phone number (for example, a stored mobile number). The method 400 proceeds from act 422 to act 410.

When it is not determined at act 404 that information associated with the PAN of the card is available, the method 400 proceeds from act 404 to act 424. At act 424, the SP/PED 302 displays an indication that the transaction has been approved and may display summary information pertaining to the transaction. As illustrated, the cardholder and/or acceptor also is prompted to indicate whether a receipt should be sent to a phone number, such as a mobile phone number. If the cardholder and/or acceptor indicates yes, for example by pressing an OK key, the method proceeds from act 424 to act 426. If the cardholder and/or acceptor indicates no, for example by hitting cancel or by failing to respond within a set time period, the method may terminate or proceed to act 412.

At act 426, the cardholder and/or acceptor is prompted to enter a phone number and to press OK when the phone number is entered. The method proceeds from act 426 to act 428. At act 428, the cardholder and/or acceptor is asked to confirm the phone number, for example by pressing OK. The method 400 proceeds from act 428 to act 430. At act 430, a message is
displayed, for example on the SP/PED 302, indicating a receipt is being sent to the phone number. The method 400 proceeds from act 430 to act 410.

Embodiments of methods of processing transactions may contain additional acts not shown in Figures 4A and 4B, may not contain all of the acts shown in Figures 4A and 4B, may perform acts shown in Figures 4A and 4B in various orders, and may be modified in various respects. For example, additional time-out routines may be employed. For example, if at act 428 a cardholder and/or acceptor fails to confirm a phone number within a threshold time period, the method may terminate or proceed to act 412. In another example, if at act 428 a cardholder and/or acceptor indicates a phone number is not correct, the method may return to act 426 so the number may be reentered. In another example, a cardholder and/or acceptor may be prompted before an email message is sent to an email address (similar to act 420).

In another example, other methods for obtaining a cardholder phone number may be employed. For example, a cardholder may be requested to enter a code that can be used to uniquely associate the transaction with a phone number. The cardholder may be asked to dial a phone number and speak the code or enter the code via dial tone keys (DTMK) using either the cardholder's phone or the SP/PED 302. In another example, the cardholder may be asked to send an SMS with a selection of digits from the payment card, for example, the last four digits, to a provided phone number. The system 300 may be configured to manage a pool of such numbers so that conflicts are avoided (for example, to avoid assigning two cards with the same last four numbers to a same provided number). The combination of the provided phone number to be called and the selection of digits to be entered may be used to confirm that the cardholder phone is the correct phone to which to send an SMS message confirming the transaction. Similarly, voice calls to a provided number where the digits are spoken out or entered via dial tone keys (DTMK) may be employed to authorize the sending of an SMS transaction receipt to a mobile phone number. In another example, the cardholder may be given a phone number to call within an allocated time window during which a
request for an SMS transaction receipt remain valid, which may typically be a short time window, such as for example, five minutes. The system 300 may manage a pool of provided phone numbers and use the provided phone number and allocated time window to identify the corresponding transaction and send an SMS transaction receipt.

Figure 5 illustrates an embodiment of a method 500 of determining whether cardholder information is available to an embodiment of a transaction processing system. For convenience, the method 500 will be described with reference to the embodiment of a system 300 of Figure 3. The method 500 may be performed by embodiments other than the system 300 of Figure 3. The method 500 may be incorporated into other methods, such as the method 400 of Figures 4A and 4B. For example, act 404 of Figure 4A may perform an embodiment of the method 500 of Figure 5.

At act 1 of Figure 5, the EPOS manager of the system 300 requests the PAN of the cardholder's card. At act 2 of Figure 5, the card reader (for example reader 324 or 326 of Figure 3) returns the PAN to the EPOS manager. At act 3 of Figure 5, the EPOS manager checks a local cardholder database stored on the SP-PED 302 to determine whether the PAN is recognized. If the PAN is recognized (for example, in the local database), contact information is retrieved from the local data base at act 4 of Figure 5. As illustrated, "cardholder_contact_info" is returned, which may be a record containing the cardholder's name, email address, mobile phone number, and/or other contact information. If the PAN is not recognized locally, at act 5 of Figure 5, the EPOS manager communicates with a remote cardholder account gateway, such as a server.

At act 6 of Figure 5, the remote gateway determines whether a remote card holder database recognizes the PAN (for example, stores contact information pertaining to the PAN). If the remote gateway recognizes the PAN, contact information is retrieved from the remote database at act 7 of Figure 5 and the remote gateway returns the contact information to the EPOS manager.
at act 12 of Figure 5. As illustrated, this is done by returning a cardholder_contact_info record as described above.

If the PAN is not recognized by the remote cardholder database, the method 500 proceeds to act 8 of Figure 5. At act 8 of Figure 5, an Issuer Identification Number (UN) is extracted from the PAN and an Issuer Identification Database is checked to determine whether the issuer will release cardholder contact information on request, for example if there is an agreement with the issuer that cardholder contact information will be released upon request. The UN is usually the first six digits of the PAN. At act 9, the Issuer Identification Database returns an indication to the Remote Cardholder Account Gateway of whether the issuer will provide contact information upon request. When it is determined that the Issuer will release cardholder contact information upon request, the Remote Cardholder Account Gateway requests cardholder contact information from the Issuing Bank Gateway at act 10 of Figure 5, and the Issuing Bank Gateway returns the cardholder contact information to the Remote Cardholder Gateway at act 11 of Figure 5. As illustrated, this is done by returning a cardholder_contact_info record as described above. At act 12 of Figure 5, the Remote Cardholder Account Gateway returns cardholder contact information to the EPOS manager of the SP/DEP 302. As illustrated, this is done by returning a cardholder_contact_info record as described above.

Embodiments of methods of obtaining cardholder contact information may contain additional acts not shown in Figure 5, may not contain all of the acts shown in Figure 5, may perform acts shown in Figure 5 in various orders, and may be modified in various respects. For example, when no local database is maintained, an embodiment may omit acts 3 and 4 of Figure 5.

Figure 6 illustrates an embodiment of a method 600 of facilitating retrieval of a receipt or invoice for a transaction by a cardholder. In the illustrated embodiment, the cardholder may access the system in an ad-hoc fashion and is not required to have or create an account to access the information. For convenience, Figure 6 will be described with respect to the EPOS manager of the SP/PED 302 of Figure 3. The method 600 may be
performed by embodiments other than the system 300 of Figure 3. The method 600 may be incorporated into other methods, such as the method 400 of Figures 4A and 4B.

At act 1 of Figure 6, an EPOS manager (for example, the EPOS manager of the embodiment of Figure 3) provides a cardholder with a passcode. For example, the passcode may be displayed on the SP/PED 302 (for writing down or memorization), or may be included in an SMS or email summary receipt, etc., sent to the cardholder. The passcode is a unique id for the transaction generated by the EPOS. The passcode may be provided to the cardholder by displaying the passcode through an EPOS user interface. The cardholder or acceptor may memorize or write down the passcode. The passcode may be provided to the cardholder in an SMS message. While a passcode may be difficult to guess, it is not necessary that the passcode be globally unique, and the passcode may be generated by the local EPOS.

At act 2 of Figure 6, the EPOS manager sends the passcode and associated transaction data to a payment gateway, such as the payment gateway illustrated in Figure 3. The transaction data may be an object that contains payment core data elements such as the card PAN and expiration date, as well as additional data that may be known to the EPOS, such as a description of the items purchased. At act 3 of Figure 6, the payment gateway causes the passcode and associated transaction data to be stored in an invoice server. In some embodiments, the object may contain the passcode. The invoice server may generate an invoice based on the transaction data.

At act 4 of Figure 6, a cardholder opens an invoice server homepage, for example, using a web browser. At act 5 of Figure 6, the cardholder enters the passcode. At act 6 of Figure 6, the web server provides the passcode to the invoice server. If one or more matches are found, at act 7 of Figure 6, the invoice server provides web server with a list of matching invoices (e.g., a list of invoices in the invoice server that are possible matches to the passcode, as illustrated invoicejist) and initiates a request for associated authentication data (authenticationDataReqd, as illustrated). The
authentication data is a set of additional data that can be used to authenticate the cardholder. This data could include the full PAN, a specified subset thereof, the card expiration date, an authentication code appearing on the card, etc. There may be more than one match for a passcode because multiple local EPOS managers generate the passcodes. Thus, the authentication data may also be used to select the appropriate transaction invoice to be generated. For example, if two or more hits for a passcode are found to exist on an invoice server, additional data may serve (or be requested) to differentiate the correct invoice. For example, the fifth or sixth digit to a PAN may be requested if this digit is unique to each potential match.

At act 8 of Figure 6, the cardholder is requested to provide the authentication data requested by the invoice server. If the cardholder provides the requested information at act 8a, the method 600 proceeds to act 9 of Figure 6.

At act 9 of Figure 6, the web server forwards the passcode and any requested authentication data provided by the cardholder to the invoice server. If the authentication data is validated, at act 10 the invoice server provides an indication that the cardholder has been authenticated (as illustrated, cardholderValid) and an invoice ID to the web server. The invoice ID is unique to an invoice associated with the transaction. At act 11 of Figure 6, the web server requests the invoice associated with the invoice ID from the invoice server. At act 12, the invoice server provides the invoice associated with the invoice ID to the web server. At act 13, the web server displays the invoice to the cardholder.

Embodiments of methods of retrieving invoices may contain additional acts not shown in Figure 6, may not contain all of the acts shown in Figure 6, may perform acts shown in Figure 6 in various orders, and may be modified in various respects. For example, if a passcode is unique to a particular transaction or other-non-transaction related verification methods are employed, one or more of the authentication steps may be omitted. In another
example, the invoice server may wait for a request and/or completion of an authentication process to generate an invoice.

Figure 7 illustrates an embodiment of a method 700 of processing a request for an invoice before related transaction data has been provided to an invoice server. For example, an SP/PED or other payment terminal may accept transactions in an off-line mode, and subsequently upload the transaction data to the invoice server. For convenience, Figure 7 will be described with respect to the system of Figure 3. The method 700 may be performed by embodiments other than the system 300 of Figure 3. The method 700 may be incorporated into other methods, such as the method 600 of Figure 6.

At act 1 of Figure 7, an EPOS manager (for example, the EPOS manager of the embodiment of Figure 3) provides a cardholder with a passcode. For example, the passcode may be displayed on the SP/PED 302 (for writing down or memorization), or may be included in an SMS or email summary receipt, etc., sent to the cardholder. The passcode may be a unique id for the transaction generated by the EPOS.

At act 2 of Figure 7, a cardholder opens an invoice server homepage, for example, using a web browser. At act 3 of Figure 7, the cardholder enters the passcode (for example, in response to a prompt or in a field of a browser page). At act 4 of Figure 7, the web server provides the passcode to the invoice server. At act 5 of Figure 7, the invoice server indicates there is no match. This could be due to an incorrect passcode being entered by the cardholder, but as illustrated it is due to the fact that the transaction data and associated passcode have not yet been provided to the invoice server by the EPOS.

At act 6 of Figure 7, the web server notifies the cardholder that there is no matching invoice yet available and invites the cardholder to provide an email address or phone number to receive a notification when an invoice is available. At act 7 of Figure 7, the cardholder provides an email address (or a phone number), etc. At act 8 of Figure 7, the web server requests the invoice server to provide a notice when a transaction associated with the passcode is
received. At act 9 of Figure 7, the EPOS has gone on line and sends the passcode and associated transaction information to the payment gateway. At act 10 of Figure 7, the payment gateway causes the invoice server to store the passcode and associated transaction information in the invoice server. At act 11 of Figure 7, the invoice server causes a notification to be sent to the cardholder that the invoice is now available, for example to an email address provided by the cardholder.

Embodiments of methods of processing requests for invoices may contain additional acts not shown in Figure 7, may not contain all of the acts shown in Figure 7, may perform acts shown in Figure 7 in various orders, and may be modified in various respects. For example, as discussed above with respect to Figure 6, false matches may sometime occur due to duplicate passcodes. In this case, authentication may be attempted before the cardholder is provided with an opportunity to request a notice. In another example, the method 700 may be modified to retrieve the contact information from the transaction data if a notification request is received.

Figure 8 illustrates an embodiment of a method 800 of a cardholder creating an account on an invoice server. For example, the cardholder may wish to view multiple invoices or access invoices after passcodes have expired. For convenience, Figure 8 will be described with respect to the system 300 of Figure 3. The method 800 may be performed by embodiments other than the system 300 of Figure 3. The method 800 may be incorporated into other methods, such as the method 600 of Figure 6.

At act 1 of Figure 8, a cardholder is invited by the web server to create an account for future invoice retrieval. For example, this may happen in an ad hoc manner during an invoice retrieval initiated by the cardholder (see Figures 6 and 7). At act 2 of Figure 8, the cardholder accepts the invitation. At act 3 of Figure 8, the web server asks the cardholder to provide an email address and/or id and to create a password. At act 4 of Figure 8, the cardholder provides the requested email address and/or id and creates a password. At act 5 of Figure 8, the web server sends an email to the
cardholder supplied email address with a verification URL. At act 6, the
cardholder loads the URL into a browser. At act 7 of Figure 8, the web server
creates an account and stores account information, such as the email address,
password and PAN, in a remote cardholder database. Note that the PAN may
already be known to the web server, for example if the account is created
during retrieval of an invoice.

Embodiments of methods of creating cardholder accounts may
contain additional acts not shown in Figure 8, may not contain all of the acts
shown in Figure 8, may perform acts shown in Figure 8 in various orders, and
may be modified in various respects. For example, if the invitation is issue in
response to a request for an invoice associated with a passcode which is not
yet available (see method 700 of Figure 7), the method 800 may include
requesting the PAN or information sufficient to determine the PAN from the
cardholder.

Figure 9 illustrates an embodiment of a method 900 of a
cardholder accessing an account on an invoice server. For convenience,
Figure 9 will be described with respect to the system 300 of Figure 3. The
method 900 may be performed by embodiments other than the system 300 of
Figure 3. The method 900 may be incorporated into other methods, such as
the method 600 of Figure 6.

At act 1 of Figure 9, a cardholder opens an invoice server
homepage with a browser. At act 2 of Figure 9, the cardholder is provided with
an opportunity to login to the cardholder’s account. At act 3 of Figure 9, the
cardholder enters login information, for example, an email address and/or ID
and a password. At act 4 of Figure 9, the web server requests authentication of
the account by accessing the remote cardholder database. At act 5 of Figure 9,
the remote cardholder database replies to the web server authenticating the
account. The authentication may include an account ID to facilitate requests for
further data about the account. At act 6, the web server requests the PAN(s)
associated with the cardholder from the remote cardholder database. For
example, more than one account may be linked to the cardholder. At act 7, the
remote cardholder database provides the PAN(s) to the web server. In some embodiments, instead of requesting PAN(s) and providing PAN(s) at acts 6 and 7 of Figure 9, alternative identifiers may be used to reduce the passing of secure PANs within the system. At act 8, the web server requests one or more invoices associated with the PAN(s) and/or alternative identifiers from the invoice server. At act 9, the invoice server returns the requested invoices.

Embodiments of methods of accessing cardholder accounts may contain additional acts not shown in Figure 9, may not contain all of the acts shown in Figure 9, may perform acts shown in Figure 9 in various orders, and may be modified in various respects. For example, as discussed above, the method 900 may be modified to use identifiers other than cardholder PAN(s).

Figure 10 illustrates an embodiment of a method 1000 of facilitating a cardholder associating additional cards with an invoice server account. For convenience, Figure 10 will be described with respect to the system 300 of Figure 3. The method 1000 may be performed by embodiments other than the system 300 of Figure 3. The method 1000 may be incorporated into other methods, such as the method 800 of Figure 8 or the method 900 of Figure 9.

At act 1 of Figure 10, the cardholder is invited by a web server to add a card to an existing cardholder account in the system. This may be done, for example, in an ad hoc manner when a cardholder requests an invoice. At act 2, the cardholder accepts the invitation. At act 3, the cardholder is asked by the web server to provide login information for an existing account. At act 4, the cardholder provides the requested information to the web server, which may include a valid email address and/or ID and password. At act 5, the web server causes the remote cardholder database to add the PAN for the new card to an existing account (for example, based on the email address and/or ID).

Embodiments of methods of adding cards to cardholder accounts may contain additional acts not shown in Figure 10, may not contain all of the acts shown in Figure 10, may perform acts shown in Figure 10 in various orders, and may be modified in various respects. For example, if the
cardholder is already signed on to an existing account when an invitation is issued, the method 1000 may be modified to omit acts 3 and 4 of Figure 10.

Figure 11 illustrates an embodiment of a method 1100 of personalizing a receipt or invoice provided to a cardholder. For convenience, Figure 11 will be described with respect to the system 300 of Figure 3. The method 1100 may be performed by embodiments other than the system 300 of Figure 3.

At act 1 of Figure 11, the acceptor uploads a new invoice template to an invoice server. The invoice server may be accessed via a web browser, for example. Invoice templates may be uploaded in various formats, such as Word™, PDF™, etc. At act 2 of Figure 11, the acceptor views the template using the browser and marks dynamic areas of the invoice, for example, areas that are likely to be changed based on transaction data, including standard fields such as transaction amount and optionally custom dynamic fields (for example, a business name or logo). Alternatively, the invoice server may be configured to automatically recognize markup already inserted into the uploaded template file that specifies dynamic data elements. At act 3 of Figure 11, the invoice server stores the invoice template in an invoice template storage for use in generating subsequent invoices associated with the acceptor.

Embodiments of methods of personalizing receipts or invoices may contain additional acts not shown in Figure 11, may not contain all of the acts shown in Figure 11, may perform acts shown in Figure 11 in various orders, and may be modified in various respects. For example, the embodiment of Figure 11 may be modified to personalize a receipt template instead of an invoice template.

Figure 12 illustrates an embodiment of a method 1200 in which an acceptor may select an invoice or receipt template from a list and personalize the selected template, for example for a particular transaction. At act 1, the acceptor accesses the invoice server via a web browser and selects a template from a list of templates. At act 2, the invoice server requests the selected template from an invoice template storage. At act 3, the requested template is
provided to the invoice server. At act 4, the acceptor modifies text in customizable text fields, for example, enters contact information for an acceptor’s business into selected fields. At act 5, the acceptor uploads media assets into the template (for example, logos or pictures). At act 6, the invoice server stores the customized template in the invoice template storage.

Embodiments of methods of personalizing receipts or invoices may contain additional acts not shown in Figure 12, may not contain all of the acts shown in Figure 12, may perform acts shown in Figure 12 in various orders, and may be modified in various respects. For example, the embodiment of Figure 12 may be modified to include associating the stored customized template with the acceptor for security and access control purposes.

Figure 13 illustrates an embodiment of a method 1300 in which an acceptor may select a default invoice and personalize the selected template. At act 1, the acceptor accesses the invoice server via a web browser and selects a default template, for example, from a list of templates. At act 2, the invoice server requests the selected template from an invoice template storage. At act 3, the requested template is provided to the invoice server. The response at act 3 as illustrated includes a record customizableFields identifying which fields in the template may be modified. At act 4, the invoice server queries an acceptor account server to obtain data for customizable fields in the template that may already be stored or available to the acceptor account server. For example, data such as the acceptor name, address, telephone number, etc., which typically would have been provided when the acceptor account was created. At act 5, the acceptor account server provides the available information and acceptor account data to the invoice server. At act 6, the invoice server incorporates the retrieved data into the default template and stores the customized template in the invoice template storage.

Embodiments of methods of personalizing receipts or invoices may contain additional acts not shown in Figure 13, may not contain all of the acts shown in Figure 13, may perform acts shown in Figure 13 in various
orders, and may be modified in various respects. For example, the embodiment of Figure 13 may be modified to allow the acceptor to review/modify the default template after it is populated with data retrieved from the acceptor account server.

Figure 14 illustrates an embodiment of a method 1400 of selecting an appropriate template for a transaction and populating the selected template. For example, a payment application on a hybrid device (see payment manager of SP/PED 302 of Figure 3) may enrich the payment transaction with additional metadata such as descriptions and images associated with components of the transaction. Thus, the payment application may select a template that is able to support the metadata provided. In another scenario, the acceptor may from time-to-time represent the interests of a third party (for example, the acceptor may be an independent agent subcontracted by a larger branded company). When the acceptor is accepting payments on behalf of the third party, the acceptor may indicate this to the hybrid device (see SP/PED 302 of Figure 3) which may cause a template to be selected and or populated based on information pertaining to the third party.

At act 1 of Figure 14, the invoice server requests transaction data associated with a transaction id from an EPOS manager of a hybrid device. At act 2, the EPOS manager provides the requested transaction data to the invoice server. The reply as illustrated also contains a transaction_invoice_preference field. For example, based on the type of transaction (for example, a purchase of a lottery ticket may specify a template including a graphical representation of a lottery ticket), an agent capacity of the acceptor, etc.

At act 3 of Figure 14, the invoice server requests the specified invoice template from the invoice template storage. The invoice template storage may store a collection of invoice templates, which may include system-wide invoice templates, custom invoice templates specific to one or more acceptors, invoice templates specific to third-party application providers (e.g., in the case of a transaction that was triggered by a third-party application), etc. At
act 4, the invoice template storage returns the requested invoice template. At act 5 of figure 14, the invoice server generates the invoice by inserting the available transaction data into the corresponding fields of the invoice template and producing output that can be displayed in a web browser (e.g., HTML), downloaded, printed (e.g., PDF), etc.

Embodiments of methods of personalizing receipts or invoices may contain additional acts not shown in Figure 14, may not contain all of the acts shown in Figure 14, may perform acts shown in Figure 14 in various orders, and may be modified in various respects. For example, the embodiment of Figure 14 may be modified to allow the acceptor to review/modify the invoice after it is generated.

Figure 15 shows an embodiment of a method 1500 of generating an invoice at the EPOS (see EPOS manager of SP/PED 302 of Figure 3) and forwarding the invoice as part of the transaction data. At act 1 of Figure 15, the EPOS driver forwards a transaction ID and an invoice template generated by a payment application of a hybrid device (see EPOS manager of SP/PED 302), which may or may not be populated with all the transaction data, to a transaction metadata manager. The invoice template may be a compatible template file (e.g., PDF) created or sourced by a payment application (see EPOS manager of SP/PED 302). The transaction metadata manager may be part of the application manager and/or a payment application manager of the SP/PED 302. At act 2, the transaction ID and invoice template are forwarded by the hybrid device to the invoice server. Embodiments of methods of personalizing receipts or invoices may contain additional acts not shown in Figure 15, may not contain all of the acts shown in Figure 15, may perform acts shown in Figure 15 in various orders, and may be modified in various respects. For example, the embodiment of Figure 15 may be modified to allow the acceptor to review/modify the invoice after it is generated and before it is forwarded to the invoice server. In another example, the invoice server may add additional transaction data to the invoice.
Figure 16 illustrates an embodiment of a method of selecting an invoice template. For example, when transaction data does not include a request for a specific invoice or is incompatible with a default template.

At act 1 of Figure 16, the invoice server requests transaction data from a hybrid device (see SP/PED 302 of Figure 3). At act 2 of Figure 16, the hybrid device provides the transaction data to the invoice server. At act 3, the invoice server requests a template that best matches the transaction data from the invoice template storage. The invoice template storage may be a server, and thus the invoice server or the invoice template storage may be configured to select the best match based on one or more characteristics of the transaction. As discussed elsewhere, the invoice template storage may store a collection of invoice templates, which may include system-wide invoice templates, custom invoice templates specific to one or more acceptors, invoice templates specific to third-party application providers (e.g., in the case of a transaction that was triggered by a third-party application), etc. At act 4, the invoice template storage provides the best match template to the invoice server. The invoice template style selected may be a best match based on data fields to be displayed in the invoice. For example, if the only data available is a amount, a time stamp and a subset of the digits of a PAN (e.g., the last four digits of the PAN), then a simple receipt template may be selected. In another example, if the data includes a rich line-by-line description of each item included in a purchase, a more complex invoice template featuring itemized billing may be selected. At act 5, the invoice server populates and generates the invoice, for example, as discussed above. Embodiments of methods of generating invoices may contain additional acts not shown in Figure 16, may not contain all of the acts shown in Figure 16, may perform acts shown in Figure 16 in various orders, and may be modified in various respects. For example, the embodiment of Figure 16 may be modified to allow the acceptor to review/modify the invoice after it is generated.

Figure 17 illustrates an embodiment of a method 1700 of generating an invoice containing information (for example, text or images or
dynamic content) pulled from web services. At act 1 of Figure 17, a cardholder requests an invoice from an invoice server. For example, a cardholder may access an invoice server via a web browser. At act 2 of Figure 17, the invoice server determines whether the invoice includes online content, and if so, requests the online content (for example, from another server). For invoices that have dynamic online content fields, the dynamic content may be fetched as the invoice is built. Optionally, some transaction data may be passed to the content server in the request (e.g., a type of item purchased). This feature may be used for a variety of purposes, such as retrieving special offers, coupon codes that can be presented to the cardholder on the invoice, to present specific information related to items on the invoice (e.g., warranty information), etc. At act 3 of Figure 17, the online content is provided to the invoice server. As illustrated, the online content includes dynamic content.

At act 4 of Figure 17, the retrieved online content is inserted into the invoice by the invoice server, for example, instead of placeholders. At act 5, the invoice server displays the invoice to the cardholder, for example, in a web page. Embodiments of methods of generating invoices may contain additional acts not shown in Figure 17, may not contain all of the acts shown in Figure 17, may perform acts shown in Figure 17 in various orders, and may be modified in various respects. For example, the embodiment of Figure 17 may be modified to insert default content in the event the online content is not available, to email a copy of the invoice to a cardholder, etc.

Some embodiments may take the form of or comprise computer program products. For example, according to one embodiment there is provided a computer readable medium comprising a computer program adapted to perform one or more of the methods or functions described above. The medium may be a physical storage medium such as for example a Read Only Memory (ROM) chip, or a disk such as a Digital Versatile Disk (DVD-ROM), Compact Disk (CD-ROM), a hard disk, a memory, a network, or a portable media article to be read by an appropriate drive or via an appropriate connection, including as encoded in one or more barcodes or other related
codes stored on one or more such computer-readable mediums and being readable by an appropriate reader device.

Furthermore, in some embodiments, some or all of the methods and/or functionality may be implemented or provided in other manners, such as at least partially in firmware and/or hardware, including, but not limited to, one or more application-specific integrated circuits (ASICs), digital signal processors, discrete circuitry, logic gates, standard integrated circuits, controllers (e.g., by executing appropriate instructions, and including microcontrollers and/or embedded controllers), field-programmable gate arrays (FPGAs), complex programmable logic devices (CPLDs), etc., as well as devices that employ RFID technology, and various combinations thereof. For example, embodiments of a hybrid smart phone/point-of-sale terminal may be implemented as discussed above (e.g., partially in hardware, partially with controllers executing instructions, etc.).

The various embodiments described above can be combined to provide further embodiments. Aspects of the embodiments can be modified, if necessary to employ concepts of the various patents, applications and publications to provide yet further embodiments.

These and other changes can be made to the embodiments in light of the above-detailed description. In general, in the following claims, the terms used should not be construed to limit the claims to the specific embodiments disclosed in the specification and the claims, but should be construed to include all possible embodiments along with the full scope of equivalents to which such claims are entitled. Accordingly, the claims are not limited by the disclosure.
CLAIMS

1. A hybrid terminal device, comprising:
   a smart phone; and
   a payment card terminal communicatively and moveably coupled to the smart phone and configured to read payment cards, wherein the hybrid terminal includes one or more processors configured to implement at least one manager module and the at least one manager module is configured to respond to an indication of a completed financial transaction involving a cardholder by selectively initiating transmission of a transaction notification based on contact information associated with the cardholder.

2. The hybrid terminal device of claim 1 wherein the smart phone is configured to communicatively couple the hybrid terminal device to one or more remote servers to facilitate performance of at least one of real-time and on-line financial transactions involving use of the payment card terminal.

3. The hybrid terminal device of claim 1 wherein the at least one manager module is configured to facilitate invoicing related to financial transactions.

4. The hybrid terminal device of claim 1 wherein the at least one manager module comprises:
   an electronic point-of-sale manager; and
   a sales application manager.

5. The hybrid terminal device of claim 1 wherein the contact information includes cardholder preference information and the transmission is initiated in accordance with the cardholder preference information.
6. The hybrid terminal device of claim 1 wherein the at least one manager module is configured to, in response to the indication:
   determine whether the contact information is stored on the hybrid terminal device; and
   when it is determined the contact information is stored by the hybrid terminal device, initiate transmission of the transaction notification based on the contact information stored by the hybrid terminal device.

7. The hybrid terminal device of claim 1 wherein the at least one manager module is configured to initiate a request for the contact information.

8. The hybrid terminal device of claim 7 wherein the request for the contact information is a request to a remote server.

9. The hybrid terminal device of claim 8 wherein the request for the contact information includes a payment card long number (PAN) extracted from a payment card by the payment card terminal.

10. The hybrid terminal of claim 7, further comprising:
    a display, wherein the request for the contact information is displayed on the display.

11. The hybrid terminal of claim 1 wherein the contact information includes a phone number and the transaction notification comprises a text message to the phone number.

12. The hybrid terminal of claim 11 wherein the at least one manager module is configured to associate the phone number with the transaction.
13. The hybrid terminal of claim 1 wherein the transaction notification comprises a short-message-service (SMS) text.

14. The hybrid terminal of claim 1 wherein the contact information includes an email address and the transaction notification comprises an email message.

15. The hybrid terminal of claim 1 wherein the payment card terminal is configured to extract a payment card long number (PAN) from a payment card.

16. The hybrid terminal of claim 15 wherein the at least one manager module is configured to initiate retrieval of the contact information based on the extracted PAN.

17. The hybrid terminal of claim 1 wherein the at least one manager module is configured to cause the hybrid terminal to facilitate a cardholder to performing at least one of:
   - providing the contact information;
   - correcting the contact information; and
   - confirming the contact information.

18. The hybrid terminal of claim 1 wherein the at least one manager module is configured to generate a passcode associated with the completed financial transaction and the transaction notification includes the passcode.

19. A method, comprising:
   - extracting cardholder identification information from a payment card using a card reader of a hybrid terminal device; and
responding to an indication of a completed financial transaction
associated with the payment card by:

- obtaining cardholder contact information; and
- initiating transmission of a transaction notification based on
the obtained cardholder contact information, the initiating being performed by a
smart phone module of the hybrid terminal device.

20. The method of claim 19 wherein the obtaining cardholder
contact information comprises retrieving cardholder contact information
associated with the extracted cardholder identification information.

21. The method of claim 20 wherein the retrieving cardholder
contact information comprises retrieving cardholder contact information stored
by the hybrid terminal device.

22. The method of claim 20 wherein the retrieving cardholder
contact information comprises requesting cardholder contact information from
one or more remote servers.

23. The method of claim 19 wherein the obtaining cardholder
contact information comprises requesting information via a user interface of the
hybrid terminal device.

24. The method of claim 19 wherein the requesting information
via the user interface includes at least one of:
- requesting entry of contact information;
- requesting correction of contact information; and
- requesting verification of contact information.

25. The method of claim 19 wherein the cardholder contact
information comprises a phone number.
26. The method of claim 24, comprising associating the phone number with the completed financial transaction.

27. The method of claim 19 wherein the transaction notification comprises one or more short-message-service (SMS) messages.

28. The method of claim 19, comprising providing the cardholder with one or more documents associated with the completed financial transaction.

29. The method of claim 28 wherein the one or more documents include at least one of an invoice and a receipt.

30. The method of claim 19 wherein the completed financial transaction is performed using the hybrid terminal device.

31. The method of claim 19 wherein the cardholder contact information includes cardholder preference information and the transmission is initiated in accordance with the cardholder preference information.

32. The method of claim 19 wherein the extracting cardholder identification information includes extracting a payment card long number (PAN) from the payment card.

33. The method of claim 19, further comprising generating a passcode associated with the completed financial transaction, wherein the transaction notification includes the passcode.

34. The method of claim 33, further comprising retrieving information associated with the completed financial transaction based on the passcode.
35. A hybrid terminal device configured to perform the method of any of claims 19 to 34.

36. A system, comprising:
one or more servers configured to facilitate completion of financial transactions; and
a hybrid terminal device configured to communicatively couple to the one or more servers, wherein the system is configured to perform the method of any of claims 19 to 34.

37. A system, comprising:
one or more servers configured to provide financial transaction related services; and
a hybrid terminal device according to any of claims 1 to 18.

38. A hybrid terminal device, comprising:
means for extracting cardholder identification information from a payment card; and
means for responding to an indication of a completed financial transaction associated with the payment card by:
   obtaining cardholder contact information; and
   initiating transmission of a transaction notification based on the obtained cardholder contact information.

39. The hybrid terminal device of claim 38 wherein the means for extracting comprises a payment card reader of the hybrid terminal.

40. The hybrid terminal device of claim 39 wherein the means for responding comprises a smart phone module of the hybrid terminal.
4.1. A non-transitory computer-readable medium whose contents cause a hybrid terminal device to perform a method according to any of claims 19 to 34.
FIG. 2
Send message to card holder’s mobile phone

410A
Carrier Name
04/17/2009

New Message from TrustedBrand
You paid £123.49 to Acme Inc with your VISA card ending 4480. To download a full receipt go to trustbrand.net and enter code 16192 when prompted.

412
Please return device to merchant.

414
Success Beep

416
Present result to acceptor

FIG. 4B
FIG. 7

Cardholder

1: Issue Passcode

EPOS

2: Opens invoice web server homepage with web browser

Payment Gateway

3: Cardholder enters passcode

Invoice Server

4: checkInvoice(passcode)

Web Server

5: reply(NULL)

6: Invite cardholder to enter email address in order to receive notification when invoice is available in system

7: Cardholder provides email address

8: notifyIfAvailable(passcode, email address)

9: sendTransaction(transactionData, passcode)

10: storeInvoice(transactionData, passcode)

11: Email sent to cardholder to notify that invoice is now available
1: Cardholder invited to create an account for future invoice retrieval

2: Cardholder accepts invitation

3: Ask cardholder to provide email address and create a password

4: Cardholder provides email address and creates a new password

5: Email sent to cardholder supplied email address with verification URL

6: Verification URL loaded in browser

7: `createAccount(emailAddress, password, PAN)`
Interaction: Adding PAN to existing account (Adding PAN to existing account)

1: Cardholder invited to add their card to an existing cardholder account in the system
2: Cardholder accepts invitation
3: Ask cardholder to provide login information for existing account
4: Cardholder provides valid email address and password
5: addPANToAccount(emailAddress, PAN)

(remote) Cardholder DB

Web Server

FIG. 10
Interaction between Accepting Account and Invoice Server

1: Choose preferred default template
2: Get template
3: Reply with customizable fields
4: Query with account data
5: Reply with account data
6: Store customizations

FIG. 13
FIG. 16
Interaction Dynamic web content in invoices

1: Request an invoice
2: [invoiceRequiresOnlineContent="TRUE"] getContent(contentURL, requiredTransactionData)
3: reply(dynamicContent)
4: insertIntoInvoice(dynamicContent)
5: display(invoice)

FIG. 17