SYSTEMS AND METHODS FOR PROVIDING A RF TRANSACTION DEVICE FOR USE IN A PRIVATE LABEL TRANSACTION

Field of Invention

The present invention generally relates to payment systems, and more particularly, to systems and methods for a transaction device including multiple data sets associated with various distinct transaction accounts.

Background of the Invention

Some financial transaction devices, such as credit cards and loyalty program cards, are capable of accessing information related to multiple accounts. For example, a credit card may be able to access membership data associated with both a credit card account and a wholesale purchase club account. These financial transaction devices may generally include one or more applications for selecting and then securely utilizing a sub-set of specified account information. However, the systems associated with these cards typically delegate the loading of these applications and management of the related data sets to third parties on behalf of both the issuer of the device and "application tenants" residing on the issuer's financial transaction devices. Managing data associated with a credit card via the issuer/third party may involve time consuming steps such as requesting permission to manage data, conforming to data standard formats, and implementing changes. Thus, traditional solutions for managing multiple application tenants are disadvantageous in that the traditional solutions leave a disproportional burden on the issuer and/or the delegated third party in terms of managing accounts on a financial transaction device.

Another disadvantage is that, in general, the financial transaction devices, which are capable of accessing information related to multiple accounts, are typically designed to access only those multiple accounts managed by the same issuer. For example, the same issuer provides both the credit card and the wholesale purchase club account to the user. As such, the issuer providing both accounts generally establishes its own application tenant storage format and management protocol related to the accounts. The established format and protocol is ordinarily different from any format or protocol used by other unrelated issuers, which provides the issuer increased control over access to the account data. Because of the differing unique protocols/formats amongst issuers, multiple issuers typically provide a transaction device corresponding to an account offered by the issuer, where the

data for accessing the account is stored in that issuer's protocol/format. Thus, a user wishing to access multiple accounts managed by different issuers, must ordinarily carry at least one transaction device per issuer. Carrying multiple transaction devices can be inconvenient in that the devices may be more easily misplaced, lost or stolen preventing the user from accessing the account.

Another disadvantage of the above conventional methods of managing multiple accounts, which is related to the different issuer formats/protocols, is that, since conventional financial transaction devices typically only store application tenant information related to one issuer, the information may not be recognized by the transaction processing system managed by a second issuer distinct from the first. That is, the user of the financial transaction device typically is only able to use the financial transaction device at locations identified by the issuer or acquirer of the transaction card. The financial transaction device may not be used at any other locations, since the locations not identified by the issuer will not recognize the application tenant information which is typically stored on the device in an issuer determined format. As such, in order to access multiple accounts managed by different issuers using different formats/protocols, the user must typically carry multiple cards, as noted above.

In addition to the above, the conventional multiple account management systems have another disadvantage in that data contained on the financial transaction devices may not be easily updated. That is, traditional financial transaction devices are only "readable" devices, and not "writeable" devices, where the data on the device may be read from the device but not written to the device. More particularly, once the financial device is issued to the user, the data often may not be modified. Instead, where information contained on the device is to be modified, a new physical consumer device (*e.g.*, transaction device) often needs to be issued. That is, the information stored on the financial transaction device is typically not permitted to be changed without issuer involvement. The issuer may be involved, for example, by verifying compatibility of proposed new or updated information, checking conformance of the data to the issuer's standard formatting and size guidelines, and implementing the changes. Thus, additional burdens are often placed on the issuer where it is desired to add unique data sets to a financial transaction device, or to update the data stored thereon.

As such, storing sufficient data on a single financial transaction device, which permits a user of the single device to complete transactions using multiple transaction

accounts issued by different distinct issuers, does not exist. A need exists for a single financial transaction device, which stores multiple independent data sets provided by multiple distinct issuers irrespective of the format/protocol of the various issuers.

Summary of the Invention

In one exemplary embodiment of the present invention, a system and method is provided for a Radio Frequency operable transaction device for storing multiple distinct data sets of different formats on the RF transaction device. The method includes the steps of: enrolling a first and second data set owner in a multiple account system on a single transaction device program; receiving at a read/write device a data set corresponding to a single device user from at least one of the first and second data set owners; receiving, from the read/write device, at least a first distinct data of a first format at the RF transaction device, wherein the first data set is owned by a first owner; receiving, from the read/write device, at least a second distinct data set of a second format at the RF transaction device, wherein the second data set is owned by a second owner, and wherein the first format is different from the second format; storing the first data set and the second data set on the RF transaction device in distinct fashion and in accordance with the first and second format respectively, where the first data set and the second data set are unique one from the other.

In another example, a RF transaction device comprises a data set management system for facilitating the storage of more than one data set stored on the transaction device, the RF transaction device comprising at least one data storage area configured to store a first distinct data set of a first format and a second distinct data set of a second format different from the first format. The first data set is associated with a first data set owner (*e.g.*, first issuer) and the first data set is configured to be stored on the RF transaction device independent of a second data set (*e.g.*, second issuer); and, the second data set is associated with the second owner and the second data set is configured to be stored on the RF transaction device independent of the first data set, wherein the first data set and the second data set are stored in accordance with the first and second format, respectively.

In yet another exemplary embodiment of the present invention, a data management system comprises: a RF transaction device associated with a first data set of a first format and a second data set of a second format, wherein the RF transaction device is configured to facilitate loading of the first data set without involvement of the second data set owner. The data management system may further comprise a read/write device configured to

communicate with the RF transaction device for providing the first and second data sets to the transaction device. The read/write device may be stand-alone, or the device may be connected to a transaction processing network. The read/write device may be used to load the issuer-owned data onto the transaction device in accordance with a data set owner-defined protocol.

In still another exemplary embodiment, the invention secures authorization from a data set owner prior to loading the data on the RF transaction device database. Once authorization is given, the issuer may be "enrolled" in a transaction device multiple account management system, the associated data owned by the enrolled issuer may then be loaded on the transaction device. The data may be loaded in a format recognizable by a merchant system or by a system maintained by the data set owner. Thus, when the transaction device is presented to complete a transaction, the data may be transferred to the issuer in an issuer-recognized format, reducing the need to carry multiple transaction devices for each issuer. That is, the issuer receives the data in a data set owner recognized format and may process the accompanying transaction under the data set owner previously established business as usual protocols. In this way, the data set owner is permitted to manage its issuer-provided program at the owner location, irrespective of the management of other programs provided by other distinct issuers enrolled in the multiple account management system.

In yet another exemplary embodiment of the invention, a radio frequency operable transaction device includes a database for storing a plurality of distinct data sets. The distinct data sets may be owned by the same or different data set owners. Moreover, the distinct data sets may be associated with one of a calling card, private label card or traditional loyalty, credit or debit card. Where the radio frequency transaction device stores a data set associated with a private label account, the transaction device may used to complete a private label transaction on a private label transaction completion system or internal network substantially maintained by the private label transaction account provider. Similarly, where the radio frequency transaction device stores a data set associated with a calling card account, the transaction device may used to complete a calling card call on a private label transaction completion system. Further still, where the radio frequency transaction device stores a data set associated with a traditional credit or debit account, the transaction device may used to complete a transaction on any conventional transaction completion system.

Brief Description of the Drawings

A more complete understanding of the present invention may be derived by referring to the detailed description and claims when considered in connection with the Figures, wherein like reference numbers refer to similar elements throughout the Figures, and:

FIG. 1 illustrates a general overview of an exemplary method for loading distinct data sets on a RF transaction device in accordance with an exemplary embodiment of the present invention;

FIG. 2 illustrates a block diagram overview of an exemplary system for loading distinct data sets on a RF transaction device in accordance with an exemplary embodiment of the present invention;

FIG. 3 illustrates a more detailed exemplary method for loading distinct data sets on a RF transaction device in accordance with an exemplary embodiment of the present invention;

FIG. 4 illustrates an exemplary data set management method for adding data sets in accordance with an exemplary embodiment of the present invention;

FIG. 5 illustrates an exemplary method for user self-management of data sets in accordance with an exemplary embodiment of the present invention;

FIG. 6 illustrates an exemplary method for issuer management of data sets in accordance with the present invention;

FIG. 7 illustrates an exemplary data set selection method for use in completing a transaction;

FIG. 8 illustrates an exemplary calling card transaction system for use in completing a calling card transaction in accordance with the present invention;

FIG. 9 illustrates a block diagram of exemplary functional block components of an exemplary RFID calling card fob for use in completing a calling card transaction in accordance with exemplary embodiments of the present invention;

FIG. 10 illustrates a block diagram of exemplary functional block components of an exemplary RFID reader for use in completing a calling card transaction in accordance with exemplary embodiments of the present invention;

FIGS. 11-13 illustrate an exemplary method for completing a RFID calling card transaction in accordance with exemplary embodiments of the present invention;

FIG. 14 is an exemplary representation of calling card data stored in a calling card validation database in accordance with exemplary embodiments of the present invention;

FIG. 15 is an exemplary private label transaction processing system which may be used with exemplary embodiments of the present invention; and

FIG. 16 illustrates and exemplary method for processing a private label transaction in accordance with the present invention.

Detailed Description of Exemplary Embodiments

While the exemplary embodiments herein are described in sufficient detail to enable those skilled in the art to practice the invention, it should be understood that other embodiments may be realized and that logical and mechanical changes may be made without departing from the spirit and scope of the invention. Thus, the following detailed description is presented for purposes of illustration only and not of limitation.

The present invention provides a system and method for a RF transaction device configured to receive multiple data sets (*e.g.*, "application tenants") of differing formats, wherein the data sets are associated with a plurality of distinct transaction account issuers. In this context, an "application tenant" may include all or any portion of any data sets, which are substantially correlated to an account issuer, which the issuer may additionally use to substantially identify an instrument user or related account. For example, where the account issuer provides application tenant information, the application tenant may include, *inter alia*, a membership identifier associated with a user enrolled in an issuer-provided transaction account program, and all related subsets of data stored on the transaction device. Where multiple application tenants are referred to herein, each tenant may constitute its own distinct data set, independent of any other application tenant data sets. For example, each application tenant may include a unique membership identifier and all associated subsets of data. Alternatively, an application tenant may include a membership identifier and an application for processing all data owned by an issuer. Thus, the data set or subset may include the processing application. Moreover, differing formats, as discussed herein, include differences in all or any portion of the formats. As such, "application tenant" and "distinct data set," and data set "owner" and account "issuer" may be used interchangeably herein.

In addition, it should be noted that although the present invention is described with respect to a financial transaction device, the invention is not so limited. The invention is suitable for any instrument capable of storing distinct data sets, which may be provided by multiple distinct account issuers where the distinct data sets may be formatted one different

from another. The account may be, for example, a loyalty, debit, credit, incentive, direct debit, savings, financial, membership account or the like. While the information provided by the account issuers may be described as being "owned" by the issuers, the issuers or their designees may simply be a manager of the account.

The present invention may be described herein in terms of functional block components, optional selections and/or various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware and/or software components configured to perform the specified functions. For example, the present invention may employ various integrated circuit components (*e.g.*, memory elements, processing elements, logic elements, look-up tables, and/or the like), which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the present invention may be implemented with any programming or scripting language such as C, C++, Java, COBOL, assembler, PERL, Visual Basic, SQL Stored Procedures, extensible markup language (XML), with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and/or the like.

As used herein, the terms "user," "end user," consumer," "customer" or "participant" may be used interchangeably with each other, and each shall mean any person, entity, machine, hardware, software and/or business. Furthermore, the terms "business" or "merchant" may be used interchangeably with each other and shall mean any person, entity, machine, hardware, software or business. Further still, the merchant may be any person, entity, software and/or hardware that is a provider, broker and/or any other entity in the distribution chain of goods or services. For example, the merchant may be a ticket/event agency (*e.g.*, Ticketmaster, Telecharge, Clear Channel, brokers, agents).

The systems and/or components of the systems discussed herein may also include one or more host servers or other computing systems including a processor configured to process digital data, a memory coupled to the processor for storing digital data, an input digitizer coupled to the processor for inputting digital data, an application program stored in the memory and accessible by the processor for directing processing of digital data by the processor, a display coupled to the processor and memory for displaying information derived from digital data processed by the processor and a plurality of databases, the

databases including client data, merchant data, financial institution data and/or like data that could be used in association with the present invention. The user computer and other systems described herein can be in a home or business environment with access to a network. In an exemplary embodiment, access is through the Internet through a commercially available web-browser software package.

Communication between various elements of the present invention is accomplished through any suitable communication means, such as, for example, a telephone network, intranet, Internet, point-of-interaction device (point-of-sale device, personal digital assistant, cellular phone, kiosk, etc.), online communications, off-line communications, wireless communications, and/or the like. One skilled in the art may also appreciate that, for security reasons, any databases, systems, or components of the present invention may consist of any combination of databases or components at a single location or at multiple locations, wherein each database or system includes any of various suitable security features, such as firewalls, access codes, encryption, decryption, compression, decompression, and/or the like.

The systems may be suitably coupled to the network via data links. A variety of conventional communications media and protocols may be used for data links. For example, a connection to an Internet Service Provider (ISP) over the local loop as is typically used in connection with standard modem communication, cable modem, Dish networks, ISDN, Digital Subscriber Line (DSL), or various wireless communication methods. The merchant system might also reside within a local area network (LAN) that interfaces to the network via a leased line (T1, D3, etc.). Such communication methods are well known in the art and are covered in a variety of standard texts. *See, e.g.*, Gilbert Held, "Understanding Data Communications" (1996), hereby incorporated by reference.

The computing units may be connected with each other via a data communications network. The network may be a public network and assumed to be insecure and open to eavesdroppers. In the illustrated implementation, the network may be embodied as the Internet. In this context, the computers may or may not be connected to the Internet at all times. For instance, the customer computer may employ a modem to occasionally connect to the Internet, whereas the bank-computing center might maintain a permanent connection to the Internet. Specific information related to the protocols, standards, and application software utilized in connection with the Internet may not be discussed herein. For further information regarding such details, see, for example, Dilip Naik, "Internet Standards and

Protocols" (1998); "Java 2 Complete," various authors (Sybex 1999); Deborah Ray and Eric Ray, "Mastering HTML 4.0" (1997); Loshin, "TCP/IP Clearly Explained" (1997). All of these texts are hereby incorporated by reference.

It may be appreciated that many applications of the present invention could be formulated. One skilled in the art may appreciate that a network may include any system for exchanging data or transacting business, such as the Internet, an intranet, an extranet, WAN, LAN, satellite communications, and/or the like. It is noted that the network may be implemented as other types of networks, such as an interactive television (ITV) network. The networked components may interact via Web Services technologies, including, but not limited to SOAP, UDDI and WSDL. The user may interact with the system via any input device such as a keyboard, mouse, kiosk, personal digital assistant, handheld computer (*e.g.*, Palm Pilot®), cellular phone and/or the like. Similarly, the invention could be used in conjunction with any type of personal computer, network computer, workstation, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, Solaris, MVS or the like. Moreover, although the invention is frequently described herein as being implemented with TCP/IP communications protocols, it may be readily understood that the invention could also be implemented using IPX, Appletalk, IP-6, NetBIOS, OSI or any number of existing or future protocols. Moreover, the present invention contemplates the use, sale or distribution of any goods, services or information over any network having similar functionality described herein.

In accordance with various embodiments of the invention, the Internet Information Server, Microsoft Transaction Server, and Microsoft SQL Server, are used in conjunction with the Microsoft operating system, Microsoft NT web server software, a Microsoft SQL database system, and a Microsoft Commerce Server. Additionally, components such as Access or SQL Server, Oracle, Sybase, Informix MySQL, Interbase, etc., may be used to provide an ADO-compliant database management system. The term "webpage" as it is used herein is not meant to limit the type of documents and applications that might be used to interact with the user. For example, a typical website might include, in addition to standard HTML documents, various forms, Java applets, Javascript, active server pages (ASP), common gateway interface scripts (CGI), extensible markup language (XML), dynamic HTML, cascading style sheets (CSS), helper applications, plug-ins, and/or the like.

The financial transaction device (*e.g.*, smart card, magnetic stripe card, bar code card, optical card, biometric device, radio frequency card or transponder, or pervasive device (a traditionally non-computerized device that is embedded with a computing unit such as a watch, kitchen appliance, cell phone, jewelry, wallets and purses, clothing including coats and hats, glasses and/or the like)) may communicate to the merchant information from one or more data sets associated with the financial transaction device. In one example, membership data and credit card data associated with an account or card may be transmitted using any conventional protocol for transmission and/or retrieval of information from an account or associated transaction card (*e.g.*, credit, debit, loyalty, etc.). In one exemplary embodiment, the transaction device may be configured to communicate via RF signals. As such, the data contained on the instrument may be communicated via radio frequency signals.

A financial transaction device may include one or more physical devices used in carrying out various financial transactions. For example, a financial transaction device may include a rewards card, charge card, credit card, debit card, prepaid card, telephone card, smart card, magnetic stripe card, radio frequency card/transponder and/or the like. In yet another exemplary embodiment of the present invention, a financial transaction device may be an electronic coupon, voucher, and/or other such instrument.

The financial transaction device in accordance with this invention may be used to pay for acquisitions, obtain access, provide identification, pay an amount, receive payment, redeem reward points and/or the like. In the radio frequency ("RF") embodiments of the transaction device, instrument-to-instrument transactions may also be performed. See, for example, Sony's "Near Field Communication" ("NFC") emerging standard, which is touted as operating on 13.56 MHz and allowing the transfer of any kind of data between NFC enabled devices and across a distance of up to twenty centimeters. See also, Bluetooth chaotic network configurations; described in more detail at:

http://www.palowireless.com/infotooth/whatis.asp

which is incorporated herein by reference. Furthermore, data on a first RF device may be transmitted directly or indirectly to another RF device to create a copy of all or part of the original device.

Furthermore, financial transaction device as described herein may be associated with various applications, which allow the financial transaction devices to participate in various programs, such as, for example, loyalty programs. A loyalty program may include one or

more loyalty accounts. Exemplary loyalty programs include frequent flyer miles, on-line points earned from viewing or purchasing products or websites on-line and programs associated with diner's cards, credit cards, debit cards, hotel cards, and/or the like. Generally, the user is both the owner of the transaction card account and the participant in the loyalty program; however, this association is not necessary. For example, a participant in a loyalty program may gift loyalty points to a user who pays for a purchase with his own transaction account, but uses the gifted loyalty points instead of paying the monetary value.

For more information on loyalty systems, transaction systems, and electronic commerce systems, see, for example, U.S. Utility Patent Application Serial No. 10/304,251, filed on November 26, 2002, by inventors Antonucci, et al., and entitled "System and Method for Transfer of Loyalty Points"; U.S. Continuation-In-Part Patent Application Serial No. 10/378,456, filed on March 3, 2003, by inventors Antonucci, et al., and entitled "System and Method for the Real-Time Transfer of Loyalty Points Between Accounts"; U.S. Patent Application Serial No. 09/836,213, filed on April 17, 2001, by inventors Voltmer, et al., and entitled "System And Method For Networked Loyalty Program"; U.S. Continuation-In-Part Patent Application Serial No. 10/027,984, filed on December 20, 2001, by inventors Ariff, et al., and entitled "System And Method For Networked Loyalty Program"; U.S. Continuation-In-Part Patent Application Serial No. 10/010,947, filed on November 6, 2001, by inventors Haines, et al., and entitled "System And Method For Networked Loyalty Program"; U.S. Continuation-In-Part Patent Application Serial No. 10/084,744, filed on February 26, 2002, by inventors Bishop, et al., and entitled "System And Method For Securing Data Through A PDA Portal"; the Shop AMEX™ system as disclosed in Serial No. 60/230,190, filed September 5, 2000; the Loyalty As Currency™ and Loyalty Rewards Systems disclosed in Serial No. 60/197,296, filed on April 14, 2000, Serial No. 60/200,492, filed April 28, 2000, Serial No. 60/201,114, filed May 2, 2000; a digital wallet system disclosed in U.S. Serial No. 09/652,899, filed August 31, 2000; a stored value card as disclosed in Serial No. 09/241,188, filed on February 1, 1999; a system for facilitating transactions using secondary transaction numbers disclosed in Serial No. 09/800,461, filed on March 7, 2001, and also in related provisional applications Serial No. 60/187,620, filed March 7, 2000, Serial No. 60/200,625, filed April 28, 2000, and Serial No. 60/213,323, filed May 22, 2000, all of which are herein incorporated by reference. Other examples of online loyalty systems are disclosed in Netcentives U.S. Patent No. 5,774,870, issued on June 30, 1998, and U.S.

Patent No. 6,009,412, issued on December 29, 1999, both of which are hereby incorporated by reference.

Further still, a "code," "account", "account number," "identifier," "loyalty number" or "membership identifier," as used herein, includes any device, code, or other identifier/indicia suitably configured to allow the consumer to interact or communicate with the system, such as, for example, authorization/access code, personal identification number (PIN), Internet code, other identification code, and/or the like that is optionally located on a rewards card, charge card, credit card, debit card, prepaid card, telephone card, smart card, magnetic stripe card, bar code card, radio frequency card and/or the like. The account number may be distributed and stored in any form of plastic, electronic, magnetic, radio frequency, audio and/or optical device capable of transmitting or downloading data from itself to a second device. A customer account number may be, for example, a sixteen-digit credit card number, although each credit provider has its own numbering system, such as the fifteen-digit numbering system used by an exemplary loyalty system. Each company's credit card numbers comply with that company's standardized format such that the company using a sixteen-digit format may generally use four spaced sets of numbers, as represented by the number "0000 0000 0000 0000." The first five to seven digits are reserved for processing purposes and identify the issuing bank, card type and etc. In this example, the last sixteenth digit is used as a sum check for the sixteen-digit number. The intermediary eight-to-ten digits are used to uniquely identify the customer. In addition, loyalty account numbers of various types may be used.

Further yet, the "transaction information" in accordance with this invention may include the nature or amount of transaction, as well as, a merchant, user, and/or issuer identifier, security codes, or routing numbers, and the like. In various exemplary embodiments of the present invention, one or more transaction accounts may be used to satisfy or complete a transaction. For example, the transaction may be only partially completed using the transaction account(s) correlating to the application tenant information stored on the transaction device with the balance of the transaction being completed using other sources. Cash may be used to complete part of a transaction and the transaction account associated with a user and the transaction device, may be used to satisfy the balance of the transaction. Alternatively, the user may identify which transaction account, or combination of transaction accounts, stored on the transaction device the user desires to

complete the transaction. Any known or new methods and/or systems configured to manipulate the transaction account in accordance with the invention may be used.

In various exemplary embodiments, the financial transaction device may be embodied in form factors other than, for example, a card-like structure. As already mentioned, the financial transaction device may comprise an RF transponder, a SpeedPass®, store discount card, or other similar device. Furthermore, the financial transaction device may be physically configured to have any decorative or fanciful shape including key chains, jewelry and/or the like. The financial transaction device may furthermore be associated with coupons. A typical RF device which may be used by the present invention is disclosed in U.S. Application Serial No. 10/192,488, entitled "System And Method For Payment Using Radio Frequency Identification In Contact And Contactless Transactions," and its progeny, which are all commonly assigned, and which are all incorporated herein by reference.

As used herein, the term "data set" may include any set of information and/or the like which may be used, for example, in completing a transaction. For example, data sets may include information related to credit cards, debit cards, membership clubs, loyalty programs, speed pass accounts, rental car memberships, frequent flyer programs, coupons, tickets and/or the like. This information may include membership identifiers, account number(s), personal information, balances, past transaction details, account issuer routing number, cookies, identifiers, security codes, and/or any other information. The data set may additionally include an issuer defined management process for determining which subsets of data are to be provided to an issuer or merchant. In some instances, a data set may be associated with one or more account numbers corresponding to accounts maintained by the account issuer. A data set may contain any type of information stored in digital format. For example, a data set may include account numbers, programs/applications, scripts, cookies, instruments for accessing other data sets, and/or any other information.

Various information and data are described herein as being "stored." In this context, "stored" may mean that the information is kept on a database. In accordance with the invention, a database may be any type of database, such as relational, hierarchical, object-oriented, and/or the like. Common database products that may be used to implement the databases include DB2 by IBM (White Plains, New York), any of the database products available from Oracle Corporation (Redwood Shores, California), Microsoft Access or MSSQL by Microsoft Corporation (Redmond, Washington), or any other database product. A database may be organized in any suitable manner, including as data tables or lookup

tables. Association of certain data may be accomplished through any data association technique known and/or practiced in the art. For example, the association may be accomplished either manually or automatically. Automatic association techniques may include, for example, a database search, a database merge, GREP, AGREP, SQL, and/or the like. The association step may be accomplished by a database merge function, for example, using a "key field" in each of the manufacturer and retailer data tables. A "key field" partitions the database according to the high-level class of objects defined by the key field. For example, a certain class may be designated as a key field in both the first data table and the second data table, and the two data tables may then be merged on the basis of the class data in the key field. In this embodiment, the data corresponding to the key field in each of the merged data tables may be the same. However, data tables having similar, though not identical, data in the key fields may also be merged by using AGREP, for example.

Although the same owner may own all data sets associated with a particular financial transaction device, it is contemplated that in general, some of the data sets stored on the financial transaction device have different owners. Furthermore, the storage of data sets is configured to facilitate independent storage and management of the data sets on the financial transaction device. Further still, the data sets may be stored in distinct differing formats provided by the distinct issuer or data set owner (also called "issuer," herein). The owners of data sets may include different individuals, entities, businesses, corporations, software, hardware, and/or the like. However, one skilled in the art will appreciate that the owners may also include different divisions or affiliates of the same corporation or entity.

As discussed above, many issuers of existing financial transaction devices utilize predetermined formats for account numbers, data and/or applications stored in association with the financial transaction device. Similarly, the data storage media associated with these financial transaction devices is typically configured to accommodate specific predetermined data formats. Thus, since the data format associated with a first issuer is often different from a data format of a second issuer, storage of multiple distinct data of differing formats on a single device provides complications for conventional systems. This is true since, each issuer typically maintains an account processing system that uses a processing protocol different from other issuers, and the information stored on the transaction card relative to the issuer must be formatted accordingly. As such, to ensure the security and integrity of the issuer-owned data, the loading of data on a transaction device is typically performed by an issuer or a third-party provider who typically uploads all related and similarly formatted data

sets onto the transaction device. However, since the third party may typically only be authorized by the issuer to load issuer-owned data of similar format onto an issuer-provided transaction device, including differently formatted data sets on a single transaction device by the third party is often not permitted. More particularly, independent owners of data sets are often reluctant to conform their data set formats to a "standard format" because of the security advantages of maintaining a separate, distinct, often secreted format.

In contrast, and in accordance with an exemplary embodiment of the present invention, the format of the information stored in the present invention may vary from one data set to another. That is, the present invention permits the data to be stored on the financial transaction device in any format, and more particularly, in any format recognizable by the data owner/transaction device issuer. Thus, as noted, each data set may be used for a very wide variety of purposes including storage of applications, raw data, cookies, coupons, membership data, account balances, loyalty information, and/or the like.

In accordance with one aspect of the present invention, any suitable data storage technique may be utilized to store data without a standard format. Data sets may be stored using any suitable technique, including, for example, storing individual files using an ISO/IEC 7816-4 file structure; implementing a domain whereby a dedicated file is selected that exposes one or more elementary files containing one or more data sets; using data sets stored in individual files using a hierarchical filing system; data sets stored as records in a single file (including compression, SQL accessible, hashed via one or more keys, numeric, alphabetical by first tuple, etc.); block of binary (BLOB); stored as ungrouped data elements encoded using ISO/IEC 7816-6 data elements; stored as ungrouped data elements encoded using ISO/IEC Abstract Syntax Notation (ASN.1) as in ISO/IEC 8824 and 8825; and/or other proprietary techniques that may include fractal compression methods, image compression methods, etc.

In one exemplary embodiment, the ability to store a wide variety of information in different formats is facilitated by storing the information as a Block of Binary (BLOB). Thus, any binary information can be stored in a storage space associated with a data set. As discussed above, the binary information may be stored on the financial transaction device or external to but affiliated with the financial transaction device. The BLOB method may store data sets as ungrouped data elements formatted as a block of binary via a fixed memory offset using either fixed storage allocation, circular queue techniques, or best practices with respect to memory management (*e.g.*, paged memory, memory recently used, etc.). By

using BLOB methods, the ability to store various data sets that have different formats facilitates the storage of data associated with the financial transaction device by multiple and unrelated owners of the data sets. For example, a first data set which may be stored may be provided by a first issuer, a second data set which may be stored may be provided by an unrelated second issuer, and yet a third data set which may be stored, may be provided by a third issuer unrelated to the first and second issuers. Each of these three exemplary data sets may contain different information that is stored using different data storage formats and/or techniques. Further, each data set may contain subsets of data, which also may be distinct from other subsets.

Even further, the invention contemplates the use of a self-service user interaction device. In this context, the self-service user interaction device may be any device suitable for interacting with a transaction device, and receiving information from the transaction device user and providing the information to a merchant, account issuer, account manager, data set owner, merchant point-of-sale, and the like. For example, the self-service user interaction device may be a stand-alone read write device, self-service Kiosk, merchant point-of-sale, read/write device, and the like. In one example, the self-service user interaction device may be configured to communicate information to and from the transaction device and to manipulate the data sets stored thereon. The self-service interaction device may be in communication with the various components of the invention using any communications protocol.

In general, systems and methods disclosed herein are configured to facilitate the loading of multiple distinct data sets onto a RF transaction device. With reference to **FIG. 1**, an exemplary method 100 according to the present invention is shown. Method 100 may include, for example, issuing a RF transaction device to a user (step 110), enrolling multiple data set owners in a multiple account transaction device program (step 112), presenting the transaction device (step 114), and loading distinct data sets onto the transaction device, where the data sets may be owned by unrelated account issuers (step 116). Once the data is appropriately loaded (step 120), the RF transaction device user may present the RF transaction device to a merchant system for completion of a transaction (step 122).

The system may be further configured such that, during an exemplary transaction, data sets associated with the financial transaction device may be managed. For example, the user may be prompted (*e.g.*, on a screen, by electronic voice, by a store clerk, by a signal

and/or the like) as to the possibility of adding, for example, a loyalty account to the same financial transaction device and the user may also be presented with terms and/or conditions in a similar or different manner. The user may be prompted at any time during the transaction, but the user may be prompted at the completion of the transaction. If the user accepts the invitation to add data to the financial transaction device, a new data set may be added (step 116). If the data is to be added, the stand-alone device may be configured to provide any account information (*e.g.*, account identifier, security code, data owner routing number, etc.) to the transaction device for storage thereon. The stand-alone may locate an appropriate database location on transaction device for storing the added data. The stand-alone device facilitates storage of the data in a distinct location on the transaction device database, where the data is stored independently of any other data. In an exemplary embodiment, the data is added to a database location on the transaction device, which is reserved for independently storing all data owned by a particular data set owner. Alternatively, the data may be stored in a distinct location on the transaction device, which is a separate location than is used to store any other data set. Further still, the data set is stored in accordance with any storage protocol permitting the data to be stored and retrieved independently of other data.

The adding of the data may be verified by the issuer prior to making the modifications. The issuer may verify the data by, for example, running a verifying protocol for determining if the information is properly stored or formatted. If verified, all databases containing the data set to be updated or a mirror image of the data set to be updated are modified in accordance with the user or issuer-provided instructions, and/or the issuer defined data storage protocol or format.

In one exemplary embodiment, multiple account issuers may be enrolled in a multiple account management program using a financial transaction device in accordance with the invention (step 112). For example, permission for adding account issuer owned data may be obtained from the data set owner. The data set owner may then be requested to provide account information to be stored on a transaction device. The data set owner may then provide account information relative to a distinct user account for loading onto the transaction device in accordance with the present invention. The issuers may be enrolled prior to issuance of the instrument or the issuers may be enrolled after issuance. By enrolling in the management program, the issuer may provide authorization for including the issuer-owned data on the financial transaction device. The issuer-owned data may be

included (*e.g.*, added) on the transaction device using a stand-alone interaction device, merchant system, or user personal computer interface upon presentment of the transaction device to the stand-alone interaction device 290 (step 114). The stand-alone interaction device may add the issuer-owned data while preserving a format recognizable by an issuer account management system. For example, the stand-alone device may identify an appropriate header or trailer associated with the data and adds the data accordingly. The stand-alone may add the data using any adding instruction or protocol as provided by the data set owner so that the resulting added data is stored in a format recognizable by the data set owner system. In this way, the stand-alone device may add the data while maintaining the data set owner's format. Alternatively, the interaction device may store the issuer-owned data on the transaction device in any format, provided that the issuer-owned data is provided to the issuer system (or to merchant system) in an issuer system (or merchant system) recognizable format.

It should be noted, that the financial transaction device may be issued with or without one or more data sets stored thereon. The financial transaction device may be issued using various techniques and practices now known or hereinafter developed wherein an instrument is prepared (*e.g.*, embossed and/or loaded with data) and made available to a user for effecting transactions. Although the present invention may contemplate adding data sets (step 120) before issuing a financial transaction device (step 110), in various exemplary embodiments, by way of illustration, the data sets are described herein as being added (step 120) after issuance (step 110).

At any time after issuance (step 110) of the financial transaction device, or when the data is successfully added (step 116), the financial transaction device may be used in a commercial transaction. In one exemplary embodiment of the present invention, a user communicates with a merchant, indicates a desire to participate in an issuer-provided consumer program. The user may communicate with the merchant by, for example, presenting the transaction device to the merchant and indicting a desire to complete a transaction. The user may indicate his desire to complete a transaction using any conventional process used by the merchant. The user may further indicate that the user wishes to complete the transaction using the financial transaction device.

During completion of the transaction, the user may present the financial transaction device to a merchant system (step 122). The financial transaction device is configured to

communicate with the merchant, using any conventional method for facilitating a transaction over a network.

As stated above, in various embodiments of the present invention, the data can be stored without regard to a common format. However, in one exemplary embodiment of the present invention, the data set (*e.g.*, BLOB) may be annotated in a standard manner when provided for manipulating the data onto the financial transaction device. The annotation may comprise a short header, trailer, or other appropriate indicator related to each data set that is configured to convey information useful in managing the various data sets. For example, the annotation may be called a "condition header," "header," "trailer," or "status," herein, and may comprise an indication of the status of the data set or may include an identifier correlated to a specific issuer or owner of the data. In one example, the first three bytes of each data set BLOB may be configured or configurable to indicate the status of that particular data set (*e.g.*, ADD, LOADED, INITIALIZED, READY, BLOCKED, ACTIVE, INACTIVE). Subsequent bytes of data may be used to indicate for example, the identity of the issuer, user, transaction/membership account identifier, or the like. The use condition annotations are further discussed herein.

The data set annotation may also be used for other types of status information as well as various other purposes. For example, the data set annotation may include security information establishing access levels. The access levels may, for example, be configured to permit only certain individuals, levels of employees, companies, or other entities to access data sets, or to permit access to specific data sets based on the transaction, merchant, issuer, user or the like. Furthermore, the security information may restrict/permit only certain actions such as accessing data sets. In one example, the data set annotation indicates that only the data set owner or the user are permitted to access or add a data set, various identified merchants are permitted to access the data set for reading, and others are altogether excluded from accessing the data set. However, other access restriction parameters may also be used allowing various entities to access a data set with various permission levels as appropriate.

The data, including the header or trailer may be received from a data set owner via any communication method described herein. The header or trailer may be appended to a data set to be modified, added or deleted, to indicate the action to be taken relative to the data set. The data set owner may provide the to a stand-alone interaction device configured to add the data in accordance with the header or trailer. As such, in one exemplary

embodiment, the header or trailer is not stored on the transaction device along with the associated issuer-owned data but instead the appropriate action may be taken by providing to the transaction device user at the stand-alone device, the appropriate option for the action to be taken. However, the present invention contemplates a data storage arrangement wherein the header or trailer, or header or trailer history, of the data is stored on the transaction device in relation to the appropriate data.

In various exemplary embodiments, the step of adding data sets may be repeated. For example, first, second, and additional data sets may be added (step 120) to the financial transaction device in any order. In one exemplary embodiment of the present invention, the first data set is owned by a first data set owner (*i.e.*, first issuer) and the second data set is owned by a second data set owner (*i.e.*, second issuer).

For example, permission for adding account issuer owned data may be obtained from the data set owner. The data set owner may then be requested to provide account information to be stored on a transaction device. The data set owner may then provide account information relative to a distinct user account for loading onto the transaction device in accordance with the present invention. The issuers may be enrolled prior to issuance of the instrument or the issuers may be enrolled after issuance. By enrolling in the management program, the issuer may provide authorization for including the issuer-owned data on the financial transaction device. The issuer-owned data may be included (*e.g.*, added, deleted, modified, augmented, etc.) on the transaction device using a stand-alone interaction device, merchant system, or user personal computer interface upon presentment of the transaction device to the stand-alone interaction device 290 (step 114). The stand-alone interaction device may manipulate the issuer-owned data while preserving a format recognizable by an issuer account management system. For example, the stand-alone device may identify the appropriate header or trailer associated with the data and add, delete or modify the data accordingly. The stand-alone may manipulate the data using any manipulation instruction or protocol as provided by the data set owner so that the resulting manipulated data is in a format recognizable by the data set owner system. In this way, the stand-alone device may manipulate the data while maintaining the data set owner's format. Alternatively, the interaction device may store the issuer-owned data on the transaction device in any format, provided that the issuer-owned data is provided to the issuer system (or to merchant system) in an issuer system (or merchant system) recognizable format.

It should be noted, that the financial transaction device may be issued with or without one or more data sets stored thereon. The financial transaction device may be issued using various techniques and practices now known or hereinafter developed wherein an instrument is prepared (*e.g.*, embossed and/or loaded with data) and made available to a user for effecting transactions. Although the present invention may contemplate adding data sets (step 120) before issuing a financial transaction device (step 110), in various exemplary embodiments, by way of illustration, the data sets are described herein as being added (step 116) after issuance (step 110).

It should be noted, that the RF transaction device may be issued with or without one or more data sets stored thereon. The RF transaction device may be issued using various techniques and practices now known or hereinafter developed wherein a device is prepared (*e.g.*, embossed and/or loaded with data) and made available to a user for effecting transactions. Although the present invention may contemplate loading data sets onto the transaction device (step 120) before or during issuance of a RF transaction device (step 110), in various exemplary embodiments, by way of illustration, the data sets are described herein as being loaded after issuance.

At any time after issuance (step 110) of the financial transaction device, the financial transaction device may be used in a commercial transaction. In one exemplary embodiment of the present invention, a user communicates with a merchant, indicates a desire to participate in an issuer-provided consumer program. The user may communicate with the merchant by, for example, presenting the transaction device to the merchant and indicting a desire to complete a transaction. The user may indicate his desire to complete a transaction using any conventional process used by the merchant. The user may further indicate that the user wishes to complete the transaction using the financial transaction device.

During completion of the transaction, the user may present the financial transaction device to a merchant system. The financial transaction device is configured to communicate with the merchant, using any conventional method for facilitating a transaction over a network.

The RF transaction device (*e.g.*, smart card, magnetic stripe card, bar code card, optical card, biometric device, radio frequency card or transponder and/or the like) may communicate, to the merchant, information from one or more data sets associated with the RF transaction device. In one example, membership data and credit card data associated with an account or card may be transmitted using any conventional protocol for transmission

and/or retrieval of information from an account or associated transaction card (*e.g.*, credit, debit, loyalty, etc.). In one exemplary embodiment, the transaction device may be configured to communicate via RF signals. As such, the data contained on the device may be communicated via radio frequency signals.

With reference now to **FIG. 2**, in one exemplary embodiment of the present invention, a multiple data set transaction device system ("management system") 200 comprises, for example, a merchant system 220, various issuer systems 230, and a RF transaction device 240. Management system 200 may further be accessed by a user 201 on a user computer 250 or via a transaction device such as, for example, kiosk 270, stand-alone interaction device 290, automated teller, or the like. In these examples, communications between user computer 250 or kiosk 270 and merchant system 220 or issuer systems 230 may take place via, for example, a network 260. In various embodiments, merchant system 220, user computer 250 and/or kiosk 270 are configured to communicate with RF transaction device 240. For example, communication with the RF transaction device 240 may be facilitated by a read/write device 280, such as a merchant point-of-sale, merchant RFID reader, computer interface, or the like, configured to receive information provided by the RF transaction device 240.

In general, merchant system 220 is configured to interact with a user 201 attempting to complete a transaction, and to communicate transaction data to one or more of issuer systems 230. Issuer systems 230 are configured to interact with RF transaction device 240 to receive and/or exchange data facilitating a transaction. Merchant system 220 may be operated, controlled and/or facilitated by any merchant that accepts payment via a transaction device. Merchant system 220 is configured to facilitate interaction with user 201, which may be any person, entity, software and/or hardware. The user 201 may communicate with the merchant in person (*e.g.*, at the box office), or electronically (*e.g.*, from a user computer 250 via network 260). During the interaction, the merchant may offer goods and/or services to the user 201. The merchant may also offer the user 201 the option of completing the transaction using a RF transaction device 240. Merchant system 220 may include a computer system 222 that may offer the option via a suitable website, web pages or other Internet-based graphical user interface that is accessible by users. The term "webpage" as it is used herein is not meant to limit the type of documents and applications that might be used to interact with the user. Any type of user interface wherein the user may be provided options for adding data to the transaction device may be used.

Each user 201 may be equipped with a computing system to facilitate online commerce transactions. For example, the user 201 may have a computing unit in the form of a personal computer (*e.g.*, user computer 250), although other types of computing units may be used including laptops, notebooks, hand held computers, set-top boxes, and/or the like. The merchant system 220 may have a computing unit 222 implemented in the form of a computer-server, although other implementations are possible. The issuer systems 230 may have a computing center such as a mainframe computer. However, the issuer computing center may be implemented in other forms, such as a mini-computer, a PC server, a network set of computers, or the like.

Issuer systems 230 may be configured to manipulate a transaction account associated with the corresponding issuer-owned data stored on the transaction device 240 (or database 282, discussed below) in accordance with a related transaction. For example, the issuer systems 230 may receive "transaction information" and manipulate an account status or balance in accordance with the information received. In accordance with the transaction amount, the issuer systems 230 may, for example, diminish a value available for completing a transaction associated with the account, or the issuer systems 230 may alter the information relative to the account user (*e.g.*, demographics, personal information, etc.).

It should be noted that issuer systems 230 may also be configured to interact with RF transaction device 240, directly or indirectly via stand-alone interaction device 290, to individually provide data sets for loading on RF transaction device 240. In some embodiments, the data sets may be provided to the stand-alone device 290 via network 260 for storing on RF transaction device 240 when the transaction device is presented. In other embodiments, issuer systems 230 may store data set information within their own systems, which may communicate with the RF transaction device via user computer 250, kiosk 270, or merchant system 220. In the embodiments described, the issuer systems 230 may be configured to push the data set to the RF transaction device 240, via the stand-alone interaction device 240 or the merchant system 220, kiosk 270, interaction device 290 or computer 250 which may be configured to pull such information from the issuer systems 230.

In addition, the data may be loaded onto the transaction device 240 using, for example, a stand-alone interaction device 290 configured to communicate with at least one of the issuer systems 230 which may or may not be configured to communicate with a merchant system 220. The interaction device 290 may communicate with the issuer systems

230 using any of the aforementioned communication protocols, techniques and data links. The communication between the stand-alone interaction device 290 and the issuer systems 230 may be facilitated by a network 260. In an exemplary embodiment, the network 260 may be secure against unauthorized eavesdropping.

The functionality provided by the issuer systems 230 may be provided to user interface 250 via a network, such as for example, the Internet. In this embodiment, the user 201 would locate an issuer system 230 using the interface 250 and an appropriate UDDI and WSDL. Once an issuer system 230 is located, the user 201 may initiate an issuer-provided service or product using SOAP and WSDL. In this embodiment a central web server (not shown, but between 230 and 250), would host a website that would provide access from the user computer 250 to the services of the issuer systems 230.

Interaction device 290 may provide instructions to the issuer systems 230 for requesting receipt of issuer-owned data, such as for example, account data, user member identification data, member demographic data, or the like, which the issuer wishes to store on the financial transaction device 240. The interaction device 290 may communicate with the issuer systems 230 using an issuer recognizable communications protocol, language, methods of communication and the like, for providing and receiving data. In one exemplary embodiment, issuer-owned data is received by the interaction device 290 from issuer systems 230, and stored onto the financial transaction device 240. The data may be stored or manipulated in accordance with the issuer-provided instructions, protocol, storage format, header or trailers received by the interaction device from issuer systems 230. The issuer-owned data may be stored on the financial transaction device 240 in any format recognizable by a merchant system 220, and further recognizable by issuer systems 230. In one exemplary embodiment, the issuer-owned data is stored using an issuer system 230 format which may be later formatted in merchant system 220 recognizable protocol when provided to the merchant system 220. In one embodiment, the issuer-owned information is stored on the financial transaction device 240 in the identical format with which it was provided by the issuer systems 230. In that regard, interaction device 290 may be any device configured to receive issuer-owned data from an issuer system 230, and write the data to a database, such as, for example, a database on instrument 240 or database 282. Further, as described more fully below, the issuer-owned information may also be provided by the issuer systems 230 to a remote database 282 where the information is stored such that it mirrors the corresponding information stored on the transaction device 240.

As noted, in accordance with the invention, a transaction device is provided which permits the storage and presentment of at least one of a plurality of data sets for completing a transaction. In one exemplary embodiment, the interaction device 290 may be configured to add the issuer-owned data to the transaction device when the transaction device 240 is initially configured, prior to providing the transaction device 240 to the user 201. The interaction device 290 may additionally be configured to add additional distinct data sets owned by other distinct issuers on the transaction device 240 when the transaction device 240 is next presented, for example, to the stand-alone interaction device 290. In this regard, the interaction device 290 may receive from multiple distinct issuer systems 230, via the network 260, the issuer-provided protocol/instructions and additionally may load the additional distinct data sets on the transaction device 240 in real-time, substantially real-time, or in a batch processing mode. The additions may be provided to the interaction device 290 for storage and later use when the transaction device 240 is next presented. Alternatively, the interaction device 290 may be configured to retrieve the instructions from the issuer systems 230 when the transaction device 240 is next presented to interaction device 290, on a random basis, during a predetermined time period (*e.g.*, every presentment for the next three days), at predetermined intervals (*e.g.*, every third presentment) and/or the like. Similarly, any of the devices discussed herein may communicate or exchange data at similar time periods or intervals. Further, where other devices, such as, for example, a kiosk 270, merchant point-of-interaction device, or the like, are likewise configured to add the issuer data on transaction device 240, the invention contemplates that the real-time or substantially real-time adding of the above distinct data sets in similar manner as is described with the interaction device 290.

Alternatively, the device to which the transaction device 240 may be presented may not be equipped for adding the data to the transaction device 240. For example, merchant system 220 may be any conventional merchant system which communicates to an issuer system 230, and which permits a user 201 to complete a financial transaction, but which is not configured to add the issuer data contained on the transaction device 240. In general, conventional merchant systems are not configured to write or overwrite data included on the payment devices presented to the merchant system for processing. That is, the merchant system 220 may include little or no additional software to participate in an online transaction supported by network 260. Loading of the data sets on transaction device 240 may be performed independent of the operation of the merchant system 220 (*e.g.*, via issuer system

230 or interaction device 290). As such, the present invention may not include retrofitting of the merchant system 220, to accommodate system 200 operation. Thus, where the merchant system 220 is not configured to add the data on the transaction device 240, such additions of the data set may be made using the interaction device 290 or directly using an issuer system 230 as described above.

The merchant system 220, kiosk 270, interaction device 290, may include additional components or methods for permitting the transaction device user 201 to self-add the data onto the transaction device 240. In this case, the systems 220, 270, and 290 may include an additional user interface for use by the user 201 to identify the adding action to be taken. Where the systems 220, 270, and 290 are configured to communicate with the transaction device 240 and to add the data sets thereon, the additions may be completed or substantially completed in real-time or substantially real-time. For example, the user 201 may present the transaction device 240 to one of the systems 220, 270, or 290, provide instructions (*e.g.*, "ADD DATA SET") for adding the data on transaction device 240 to the system 220, 270, or 290, and system 220, 270, or 290 may add the data onto the transaction device 240 in real-time or substantially real-time, for example, prior to permitting the transaction device 240 to be used by the user 201 to complete a transaction. Alternatively, the instructions for adding data sets may be provided by the user 201 to the merchant system 220 or kiosk 270, and the merchant system 220 or kiosk 270 may further provide the instructions to the network 260 for use in later adding the data. For example, the instructions may be provided by system 220 or 270 to the issuer system 230 managed by the issuer owning the data to be added. The issuer system 230 may provide the data sets to be added to, for example, interaction device 290, for updating the transaction device 240 when next presented. In one exemplary embodiment, the instructions may be stored at the issuer system 230, until such time as the transaction device 240 is next presented to a device configured to add the data on the transaction device 240. Once presented, the data set may be provided to the device (*e.g.*, computer 250, interaction device 290, etc.) for storing the data set on the transaction device 240.

In another exemplary embodiment, the user 201 may self-manage the data sets by, for example, adding data sets using a conventional computer system 250, which may be in communication with the network 260. Computer system 250 may or may not be configured to interact with RF transaction device 240. Where the computer system 250 is not configured to interact with the transaction device 240, the user 201 may provide instructions

for adding data sets to the issuer system 230 for later use in adding data to the corresponding transaction device 240 data, for example, when the transaction device 240 is next presented in similar manner as described above. Where the computer 250 is configured to interact with the RF transaction device 240 to modify the data stored thereon, the user 201 may provide instructions to the computer 250 for adding the data on the RF transaction device in real-time or substantially real-time. Consequently, the computer 250 may receive adding instructions from the user 201 and perform the additions accordingly, and may add the data to the transaction device 240 in real-time or substantially real-time. The computer 250 may additionally be configured to receive authorization of the adding instructions from issuer system 230 prior to making the user 201 requested additions. The issuer system 230 may receive the user 201 instructions and verify whether the identified additions of data sets are available to the user 201 or if the identified data sets are valid. If the identified additions and data sets are authorized, the issuer system 230 may add the data to a transaction device database including a distinct data storage area associated with the issuer system 230. Any management of the data sets discussed herein may include authorizations, restrictions or levels of access as is known in the art.

In one exemplary method of self-management, a user 201 logs onto a website via user computer 250, or onto a stand-alone device, such as, for example, interaction device 290 or kiosk 270, and selects an option for adding data sets on a RF transaction device 240. The additions or requested additions may be transmitted to the transaction device 240 via a reader/writer device 280 configured to communicate the data to transaction device 240. In this context, the reader/writer device 280 may be any conventional transaction device reader or writer.

As noted, in some exemplary embodiments of invention, authorization may be obtained from issuer systems 230 prior to adding, deleting or manipulating the data on transaction device 240. Authorization may be obtained by requesting the authorization during the process of adding the data sets to the transaction device 240. Authorization may be given where the user 201 provides appropriate security information, which is verified by the issuer system 230. The security information may be, for example, a security code granting access to the issuer-owned data on the transaction device 240. For example, a point-of-sale machine may be configured to allow the input of a code, or an answer to a prompt, which is provided to and verified by issuer system 230. Once verified the addition of data requested may be made to the data contained on the RF transaction device.

It should be noted that the authorization code may be used to permit the user 201 to select which issuer-provided data to utilize for completion of a transaction. For example, a point-of-interaction device (POI) device may be programmed to search the RF transaction device for a data set containing a particular club membership data set, or to locate all available data sets for providing to a user 201 display available data sets to the user 201, thereby permitting the user 201 to select which data set to use to complete a transaction. If no data set is found, the POI device may alert the user 201 or prompt the merchant to alert the user 201 of the possibility of adding issuer-owned data to the RF transaction device. A positive response to this alert may cause the POI device to add an issuer data set to the transaction device. Additional security on the transaction device 240 may prevent access to certain data by any parties discussed herein.

It is noted that the user 201 may already be a member of a membership program managed by an issuer system 230 in which case the associated user 201 membership data may be assigned to user 201 for inclusion on transaction device 240. As such, the user 201 may be permitted to add the membership data set to the transaction device 240. Alternatively, the user 201 may become a member by selecting to add the membership information to the RF transaction device, using the interactive device 290. In some embodiments, changes made to the data sets stored on the transaction device 240 may be updated to the RF transaction device 240 in real-time or substantially real-time, where the interactive device 290 is in communication with the transaction device 240. The changes may also be completed the next time the user 201 presents the RF transaction device 240 to a stand-alone interaction device 290 or to a kiosk 270, merchant system 220, or the like.

In another exemplary embodiment of the present invention, merchant system 220, kiosk 270, and/or user computer 250 may be configured to interact with RF transaction device 240 via a read/write device 280. Read/write device 280 may be any device configured to communicate with RF transaction device 240. In one embodiment, read/write device 280 is configured to read and write to RF transaction device 240. For example, read/write device 280 may be a point-of-interaction magnetic card reader/writer. In another example, where the transaction device includes a RF transmitter/receiver for communicating with system 200, read/write device 280 may include a mating transponder configured to receive and transmit issuer-owned data. Read/write device 280 may be configured to select data sets for use by a merchant using any suitable selection technique including but not

limited to proprietary commands or command sequences or use of ISO/IEC 7816-4 application selection sequences (*e.g.*, GET command).

Managing of the data sets (step 116) as used herein may include adding the data sets to the transaction device 240 database. More particularly, **FIG. 3** illustrates a general overview of an exemplary data set management method 300 comprising the steps of: loading a data set (step 310), initializing a data set (step 320), and verifying availability of data set (step 330). In this manner, a data set may be added to a RF transaction device, initialized and verified for usage in the completion of a transaction. Furthermore, the ability to update, modify, replace and/or delete a data set may be subject to security requirements.

In one embodiment exemplifying self-management of the transaction device database, the various processes may include a user 201 facilitating the input of information into a data management system 200 to cause the data set to be loaded. The information may be inputted via keypad, magnetic stripe, smart card, electronic pointer, touchpad and/or the like, into a user computer 250, POS terminal, kiosk 270, ATM terminal and/or directly into the merchant system 220 via a similar terminal or computer associated with merchant server 222. The information may be transmitted via any network 260 discussed herein to merchant system 220 or issuer systems 230. In another embodiment, the merchant may enter the information into an issuer system 230 on behalf of the user 201. This may occur, for example, when the user 201 and/or issuer system 230 authorizes the management of data sets on RF transaction device 240 over a telephone and the service representative inputs the information. In this embodiment, the transaction device 240 may be updated at the next presentment opportunity.

Any suitable procedures may be utilized to determine whether a data set is currently ready for use and available (step 330). In one example, when a financial transaction device 240 is presented, the availability of the data set is verified by checking whether the data set has been corrupted or blocked (step 332), or deleted (step 333). For example, the data set may be checked to determine if the data set has been accessed or altered without permission ("corrupted") or if the data set exists or has been removed from the transaction device 240 ("deleted"). The check may be performed using any suitable protocol or comparing data. If the answer to these questions is no, then the data set is available and ready for use (step 334). If the data is corrupted or blocked, subroutines may be used to attempt to retry reading the data (step 336). If the data set is marked deleted or removable, subroutines will prevent access to the data set (step 335) and remove the data set (step 340). For example, a suitable

subroutine may place a DELETE "marker" on the data set, which prevents the data from being transmitted during completion of a transaction. The data set may then be marked for deletion and deleted from the transaction device 240 at the next presentment of the device. In similar manner, where the data set is corrupted, a CORRUPTED marker may be appended to the data set and the data set is prevented from being transmitted during completion of a transaction. The marker may be a header or trailer as discussed herein.

Various methods may be used to add a data set to a financial transaction device 240 or to replace a data set on a financial transaction device 240. **FIG. 4** illustrates an exemplary method 400 of adding a data set to a financial transaction device 240, including the general steps of presenting the financial transaction device (step 410), verifying the addition of the data set to the financial transaction device (step 420), placing the data set in a temporary holding area (step 430), and adding the data set (step 440).

More particularly, the user 201 presents the financial transaction device 240 (step 410) to a device 280 configured to communicate with device 240. The user 201 may present financial transaction device 240 at a point-of-purchase or to an interaction device 240 or kiosk 270. For example, the user 201 may wave the RF transaction device 240 in front of a POI machine in a retail store, which is configured to receive data from the device 240. Alternatively, the user 201 may present the financial transaction device 240 at a self-service location such as a kiosk 270 in a mall. Moreover, the user 201 may present the financial transaction device 240 to a peripheral device associated with a personal computer, or the like.

The user 201 is then given the opportunity to add a data set to the transaction device 240. For example, device 280 may detect the absence of a particular data set on the transaction device by searching the transaction device 240 databases and comparing the existing data sets to the data set to be added. If the data set to be added is not found on the database, the user 201 may be prompted to confirm the addition of this data set to the instrument (step 420). The user may be prompted via an interactive user interface displaying the option to add the data set. In one example, when a user 201 presents a financial transaction device 240 to a merchant, the card reader detects the absence of a loyalty data set and provides a message on a display to the user 201 or the store clerk indicating that the loyalty data set can be added if desired. The user 201 may answer in the negative and complete the purchase using typical transaction methods (step 425). Alternatively, if user 201 provides an affirmative response, the algorithm may prepare a data

set for communication with the financial transaction device 240 (step 430). The process may determine whether the data set (or information that could be used to create the data set) exists in some form or on some device other than on the financial transaction device 240 (step 432). Determining whether a data set exists may involve querying an issuer system 230, database 282, or the like. For example, the issuer system 230 may compare the data set to other data sets the issuer system 230 has assigned to a particular user 201. If the data set is not assigned to a particular user, then issuer system may determine that the data set is available for adding to the transaction device 240. Determining whether a data set exists may also take place when a store clerk verbally asks (or a screen prompts) the user 201 to present another card containing the information. For example, the data set may exist on a movie rental card and stored in magnetic stripe form, bar code, and/or the like.

If the data set exists in an accessible form, the data set may be captured (step 436). In this example, the user 201 may present the movie rental card and the data read from the movie rental card may then be stored in a data set associated with the financial transaction device 240. For example, the user 201 may desire to add a shopping loyalty card to the user's 201 financial transaction device 240. The user 201 may swipe, scan or otherwise present the loyalty card such that the data set from the loyalty card is captured. The system may be further configured such that the merchant, kiosk 270, or computer system may access an issuer system 230 to obtain information for creating the data set. Thus, if a user 201 does not have the movie rental card on the user's 201 person, the system 230 may prompt the clerk to request identifying/security information and to access the user's 201 account and therefore facilitate adding a movie rental data set associated with the user's 201 transaction device 240. Any other suitable methods of capturing data sets may also be used.

If the data set does not exist, a new data set may be created (step 434) for inclusion on the transaction device 240. Creation of the data set may, for example, involve filling out an application, providing name and address, creating an account, and/or the like. In either event, the pre-existing or newly created data set is temporarily held in a storage area (*e.g.*, database 282, local memory or the like) for transfer to the transaction device 240 (step 438). Additional data sets may be prepared for transmittal to transaction device 240 (step 439).

In this exemplary embodiment, the transaction device 240 is presented again to read/write device 280 (step 442). Read/write device 280 is configured to attempt to transfer the data set(s) to the transaction device 240 (step 444). For example, existing read/write device 280 may be configured with software and/or hardware upgrades to transmit data to

the transaction device 240. In one exemplary embodiment, if the data sets were not transferred correctly, the process may try the transfer again. In another exemplary embodiment, data sets are added one at a time or altogether. Thus, a user 201 may pass a card through a card reader/writer one or more times during the addition process. The transaction may be completed (step 425) using the new data set or another selected method of payment. The same steps may be used in a self-service embodiment, however, in one embodiment, no financial transaction takes place along with the addition of data sets. It should also be noted that under appropriate circumstances, a user 201 could add data sets at a point-of-purchase without actually completing a purchase.

In various exemplary embodiments, the user 201 and/or the owner of the data set may manage the data set (*i.e.*, steps 432-439) in advance of presenting the transaction device 240. For example, a user 201 on user computer 250 may choose to add or delete data sets via a website configured for management of data sets. In another example, an issuer system 230 may add functionality to an account and may desire to update the data set associated with that account. In either example, data sets that have been prepared in advance may be ready for transmission upon presentment of the transaction device 240. The transmission of the data sets may be transparent to the user 201. For example, the user 201 may present the transaction device 240 (step 442) to complete a purchase and the waiting data sets may automatically be added to the user's 201 card (step 440).

As noted, the data associated with the transaction device 240 may be modified by the user 201 and/or by the issuer system 230. **FIGS. 5** and **6** respectively, depict exemplary methods for user 201 and issuer system 230 data management. For example, with respect to user 201 self-management method 500, the issuer system 230 may provide the user 201 with a transaction device 240 (step 502). The transaction device 240 may be provided with pre-stored issuer-owned data, or the device may be configured to permit the user 201 to add the data at a later date. The user 201 may then present the transaction device 240 to read/write device 280 for initiating the self-management process (step 504). The read/write device 280 may then read the data on the transaction device 240, and provide the data to an interaction device 290 for displaying to the user 201 (step 506). Alternatively, the interaction device 290 may provide the user 201 a list of available data to be added to the transaction device 240.

The user 201 may then be permitted to identify which data the user 201 wishes to add (step 508). Identification of the data may include providing the data with a trailer or

header indicating the adding action to be taken. The header and an indicator of the data to be added may then be provided to the issuer system 230 (step 510) for verification as to whether such desired additions are available to the user 201 (step 512). If the desired additions are not available, the additions will not be made and the user 201 is notified accordingly (step 514). The user 201 may then be permitted to identify whether other data is to be added (step 516). If so (step 508), the interaction device 290 may provide a request for adding to the issuer system 230 (step 510) and the verification process is repeated.

Alternatively, where the issuer system 230 verifies that the additions of distinct data sets may be made (step 512), the interaction device 290 may provide instructions to the interaction device 290 to the appropriate data on the transaction device 240 (step 518). The user 201 may then be permitted to select other data sets to add (step 516), in similar manner as was described above. Where the addition of data sets is complete, the user 201 may then present the transaction device 240 to a merchant for use in completing a transaction.

FIG. 6 depicts an exemplary method 600 wherein the issuer system 230 manages the data contained on the transaction device 240. For example, the issuer may identify on the issuer system 230 which data sets are to be added to the transaction device database (step 602). The device 240 may be provided with pre-stored issuer-owned data, or the instrument 240 may be configured to permit the user 201 to add the data at a later date. The user 201 may the present the transaction device 240 to read/write device 280 for initiating the self-management process (step 604). The read/write device 280 may then read the data on the transaction device 240, and provide the data to an interaction device 290 for displaying to the user 201 (step 606). Alternatively, the interaction device 290 may provide the user 201 a list of available data to be added to the instrument 240.

In addition, the issuer system 230 may query as to whether the issuer system 230 is in possession of the transaction device 240 for making the additions to the data set on the transaction device 240 in real-time or substantially real-time (step 608). If so, the additions are made accordingly (step 610) and the transaction device 240 may then be authorized for use in completing a transaction using the distinct data set added (step 612).

Where the issuer system 230 is not in possession of the transaction device 240 at the time the issuer determines that the addition of the distinct data sets on the transaction device 240 are to be made (step 608), the distinct data sets to be added may be made on the issuer system 230 (step 604), and may be placed in queue on the issuer system 230, for uploading to the transaction device 240 when it is next presented to the issuer system 230 or to an

appropriate read/write device 280 (step 614). When the transaction device 240 is presented thusly (step 616), the issuer system 230 may be notified that the transaction device 240 is available for adding the identified distinct data sets, and the issuer system 230 may then provide the instructions for addition (*e.g.*, modified data including headers) to the appropriate read/write device 280 for adding the data sets to the transaction device 240 (step 618). The transaction device 240 may then be provided to the user 201 for use in completing a transaction (step 612).

As noted, the transaction device 240 may include multiple data sets which correspond to distinct issuer systems 230, and which may be used to complete a transaction. The user 201 may be permitted to choose which data set to use for transaction completion. **FIG. 7** illustrates an exemplary method by which the user 201 may choose which of the data sets to use to complete a transaction. For example, the user 201 may present the transaction device 240 to a merchant system for use in completing a transaction (step 702). The merchant system 220 may then read the data stored on the transaction device 240 and report to the user 201 all distinct data sets which may be used to complete a transaction (step 704). The user 201 may then select the appropriate data set (step 706) and the transaction is completed accordingly (step 708).

It should be noted that completion of a transaction may be performed under any business as usual standard employed by the merchant and/or issuer system 230. For example, the merchant server 222 may be configured to communicate transaction data to the appropriate issuer system 230, in real-time or substantially real-time, or by using batch processing at the end of each day. Any suitable means for delivering the transaction data to the issuer systems 230 may be used. In one exemplary embodiment of the present invention, the transaction data may be delivered to the issuer system 230 via a network 260. The issuer system 230 may receive the transaction information and process the transaction under issuer defined protocol independent of any other protocol used by other issuers to process a transaction. The issuer system 230 may receive the transaction data then provide the merchant with the appropriate satisfaction for the transaction.

In another exemplary embodiment, transaction device 240 may include calling card account numbers associated with a calling card account provided by a telephone local or long distance carrier. A "calling card," as used herein, allows a calling card user 201 (*e.g.*, subscriber) to place toll calls while away from the home or office without having to bill the call to a third party or to continually insert coins into a public telephone. A typical calling

card enables a user to dial a directory number of a called party and a calling card number to place a call. The "calling card" may also include the use of an account number to access any other service such as, for example, cable television service, pay per view content, fax service, internet access via an internet phone and the like. The account may also include account numbers from disparate service providers such as, for example, utility accounts, such that the fob may be used at the merchant to purchase and bill to that account. For example, a solar power device provider may enter into an agreement with a power company to allow customers to bill their device purchases to the power company.

Upon validation of the dialed calling card number by a host services system (HSS), a connection between the caller and the called party is established. The calling card subscriber is requested to subsequently pay for the telephone call (and all other calls placed during a predetermined period) upon receiving an itemized calling card bill.

Referring to **FIGS. 8-10**, with continued reference to **FIG. 1**, an exemplary embodiment of a telecommunications calling card network 800 in which the present invention may be practiced is shown. Particularly, an exemplary telecommunications network 800 may include a host services system 802 configured to sequentially decrementing a validated calling card account during a telephone call, a billing system 820, rating database 830, calling card validation database 840, updating system 850, customer service switch 860, validator 880, inter-exchange network 890, local exchange carrier (LEC) network 895, and a radio frequency identification reader 801 in communication with a telephone call initiating system 843.

The operator services system 802 may comprise a main processor 804. Main processor 804 may facilitate the administration of system-wide control functions. The system-wide control functions may be interconnected, via system data link 805, to switch interface 806. Switch interface 806 serves as an interface between the system and other networks. A dual-tone multi-frequency (DTMF) receiver 810 may be interconnected to processor 804 by data link 803. The DTMF receiver 810 may be responsible for the reception and processing of a caller's dialed input. Card recognition database 812 communicates with processor 804 over data link 809. The database 812 may store a list of calling card vendor identifications. An internal database 814 may be accessed by the processor 804 via data link 811 for obtaining announcement protocols and generating billing data for transmittal to billing system 820. Internal database 814 may be in further communication with updating system 850 via a data link 817. Updating system 850 may

update the internal database 814 via link 817. Attendant position 816 may allow a human operator to serve as an interface between a caller and HSS 802, if necessary.

Calling card data is retrieved by the HSS 802 from calling card validation database 840 over signaling link 841, where the calling card validation database may be included in a calling card issue system 230. In an exemplary embodiment, calling card data includes remaining balance information, which may be related to a calling card account number provided to a calling card financial transaction device 240 using the methods described herein. In this context, the application tenant may be a calling card number, calling card account number, or the like. The issuer systems 230 may include any number of conventional calling card carriers, such as, AT&T, Cox Communication, Bell South, Qwest, or the like. The calling card carrier issuer system 230 may enroll in the multiple calling card accounts system 200 in accordance with the methods described herein. Further, distinct calling card account numbers may be stored on the transaction device 240 in a transaction device database as is described above.

Card validation database 840, according to an exemplary embodiment of the invention, may be updated by updating system 850 which accesses the validating database 840 by signaling link 851. Rate information is retrieved from rating database 830 via signaling link 831, and is used by HSS 802 to determine a maximum call duration for calls and the per minute decrement amount required for a particular call. Calling card customers 201 who experience problems with their calling cards may be forwarded to a customer representative posted at attendant position 816 of customer service switch 860 as known in the art. Periodically, calling card issuing companies or issuer systems 240 may add prepaid non-billed balances to a card account to promote calling card use. This promotional balance is entered at the discretion of the card company by the customer representative into customer service switch 860. Customer service switch 860 is interconnected to: HSS 802 via bi-directional trunk 863; inter-exchange carrier network 890 via bi-directional trunk 865; and updating system 850 via signaling link 861. Customer service switch 860 also has access to validator 880 via signaling link 881.

Inter-exchange carrier network 890 receives calling card calls from a switch in a LEC network, such as LEC network 895, over bi-directional trunk 897. Particularly, inter-exchange carrier network 890 is accessed when a caller served by LEC network phone line AAA (or BBB) dials a card company's toll-free access number, such as "1-866-123-4567". Once the call is received in inter-exchange carrier network 890, it is extended over trunk 893

to HSS switch interface 806. Alternatively, the caller may access switch interface 806 directly from LEC network 895, via trunk 898, by simply dialing "0" plus a directory number.

As such, once one or more calling card numbers is populated onto the transaction device 240, the user may seek call completion according to the system 800 and may seek authorization of the call request using any call carrier 230 business as usual standards.

System 800 may include a transaction device 240 (shown in **FIG. 9**) having a transponder 904 and a RFID reader 801 (shown in **FIG. 10**) in RF communication with transaction device 240. The transaction device 240 may be called a fob 240 herein. Although the present invention is described with respect to a fob 240, the invention is not to be so limited. Indeed, system 800 may include any fob 240 configured to communicate data for transaction completion. In one exemplary embodiment the fob 240 may be configured to communicate with a RFID reader 801 via RF communication. Typical form factors for the fob 240 may include, for example, a key ring, tag, card, cell phone, wristwatch or any such form capable of being presented for interrogation.

FIG. 9 illustrates a block diagram of the many functional blocks of an exemplary fob 240 in accordance with the present invention. Fob 240 may be a RFID fob 240 which may be presented by the user 201 to facilitate an exchange of funds or points, etc., for receipt of goods or services. As described herein, by way of example, the fob 240 may be a RFID fob which may be presented for facilitating payment for goods and/or services.

Fob 240 may include an antenna 902 for receiving an interrogation signal from RFID reader 801 via antenna 1006 (or alternatively, via external antenna 1005) shown in **FIG. 10**. Fob antenna 902 may be in communication with a transponder 904. In one exemplary embodiment, transponder 904 may be a 13.56 MHz transponder compliant with the ISO/IEC 14443 standard, and antenna 902 may be of the 13 MHz variety. The transponder 904 may be in communication with a transponder compatible modulator/demodulator 906 configured to receive the signal from transponder 904 and configured to modulate the signal into a format readable by any later connected circuitry. Further, modulator/demodulator 906 may be configured to format (*e.g.*, demodulate) a signal received from the later connected circuitry in a format compatible with transponder 904 for transmitting to RFID reader 801 via antenna 902. For example, where transponder 904 is of the 13.56 MHz variety, modulator/demodulator 906 may be ISO/IEC 14443-2 compliant.

Modulator/demodulator 906 may be coupled to a protocol/sequence controller 908 for facilitating control of the authentication of the signal provided by RFID reader 801, and for facilitating control of the sending of the fob 240 account number. In this regard, protocol/sequence controller 908 may be any suitable digital or logic driven circuitry capable of facilitating determination of the sequence of operation for the fob 240 inner-circuitry. For example, protocol/sequence controller 908 may be configured to determine whether the signal provided by the RFID reader 801 is authenticated, and thereby providing to the RFID reader 801 the account number stored on fob 240.

Protocol/sequence controller 908 may be further in communication with authentication circuitry 910 for facilitating authentication of the signal provided by RFID reader 801. Authentication circuitry may be further in communication with a non-volatile secure memory database 912. Secure memory database 912 may be any suitable elementary file system such as that defined by ISO/IEC 7816-4 or any other elementary file system allowing a lookup of data to be interpreted by the application on the chip. Database 912 may be any type of database, such as relational, hierarchical, object-oriented, and/or the like.

In addition, protocol/sequence controller 908 may be in communication with a database 914 for storing at least a fob 240 account data, and a unique fob 240 identification code. Protocol/sequence controller 908 may be configured to retrieve the account number from database 914 as desired. Database 914 may be of the same configuration as database 912 described above. The fob account data and/or unique fob identification code stored on database 914 may be encrypted prior to storage. Thus, where protocol/sequence controller 908 retrieves the account data, and or unique fob identification code from database 914, the account number may be encrypted when being provided to RFID reader 801. Further, the data stored on database 914 may include, for example, an unencrypted unique fob 240 identification code, a user identification, Track 1 and 2 data, as well as specific application applets.

Fob 240 may be configured to respond to multiple interrogation frequency transmissions provided by RFID reader 801. That is, RFID reader 801 may provide more than one RF interrogation signal. In this case, fob 240 may be configured to respond to the multiple frequencies by including in fob 240 one or more additional RF signal receiving/transmitting units 926. RF signal receiving/transmitting unit 926 may include an antenna 918 and transponder 920 where the antenna 918 and transponder 920 are compatible with at least one of the additional RF signals provided by RFID reader 801. For example, in

one exemplary embodiment, fob 240 may include a 134 kHz antenna 918 configured to communicate with a 134 kHz transponder 920. In this exemplary configuration, an ISO/IEC 14443-2 compliant modulator/demodulator may not be required. Instead, the 134 kHz transponder may be configured to communicate directly with the protocol/sequence controller 908 for transmission and receipt of authentication and account number signals as described above.

FIG. 10 illustrates an exemplary block diagram of a RFID reader 801 in accordance with an exemplary embodiment of the present invention. RFID reader 801 includes, for example, an antenna 1006 coupled to a RF module 1003 (*e.g.*, transponder 1002), which is further coupled to a control module 1004. In addition, RFID reader 801 may include an antenna 1005 positioned remotely from the RFID reader 801 and coupled to RFID reader 801 via a suitable cable 1120, or other wire or wireless connection.

RF module 1003 and antenna 1006 may be suitably configured to facilitate communication with fob 240. Where fob 240 is formatted to receive a signal at a particular RF frequency, RF module 1003 may be configured to provide an interrogation signal at that same frequency. For example, in one exemplary embodiment, fob 240 may be configured to respond to an interrogation signal of about 13.56 MHz. In this case, RFID antenna 1006 may be 13 MHz and may be configured to transmit an interrogation signal of about 13.56 MHz. That is, fob 240 may be configured to include a first and second RF module (*e.g.*, transponder) where the first module may operate using a 134 kHz frequency and the second RF module may operate using a 13.56 MHz frequency. The RFID reader 801 may include two receivers which may operate using the 134 kHz frequency, the 13.56 MHz frequency or both. When the reader 801 is operating at 134 kHz frequency, only operation with the 134 kHz module on the fob 240 may be possible. When the reader 801 is operating at the 13.56 MHz frequency, only operation with the 13.56 MHz module on the fob 240 may be possible. Where the reader 801 supports both a 134 kHz frequency and a 13.56 MHz RF module, the fob 240 may receive both signals from the reader 801. In this case, the fob 240 may be configured to prioritize selection of one or the other frequency and reject the remaining frequency. Alternatively, the reader 801 may receive signals at both frequencies from the fob upon interrogation. In this case, the reader 801 may be configured to prioritize selection of one or the other frequency and reject the remaining frequency.

Further, protocol/sequence controller 1014 may include an optional feedback function for notifying the user of the status of a particular transaction. For example, the

optional feedback may be in the form of an LED, LED screen and/or other visual display which is configured to light up or display a static, scrolling, flashing and/or other message and/or signal to inform the fob 240 user that the transaction is initiated (*e.g.*, fob is being interrogated), the fob is valid (*e.g.*, fob is authenticated), transaction is being processed, (*e.g.*, fob account number is being read by RFID reader) and/or the transaction is accepted or denied (*e.g.*, transaction approved or disapproved). Such an optional feedback may or may not be accompanied by an audible indicator (or may present the audible indicator singly) for informing the fob 240 user of the transaction status. The audible feedback may be a simple tone, multiple tones, musical indicator, and/or voice indicator configured to signify when the fob 240 is being interrogated, the transaction status, or the like.

RFID antenna 1006 may be in communication with a transponder 1002 for transmitting an interrogation signal and receiving at least one of an authentication request signal and/or an account data from fob 240. Transponder 1002 may be of similar description as transponder 114 of **FIG. 2**. In particular, transponder 1002 may be configured to send and/or receive RF signals in a format compatible with antenna 902 in similar manner as was described with respect to fob transponder 904. For example, where transponder 1002 is 13.56 MHz RF rated antenna 902 may be 13.56 MHz compatible. Similarly, where transponder 1002 is ISO/IEC 14443 rated, antenna 1006 may be ISO/IEC 14443 compatible.

RF module 1003 may include, for example, transponder 1002 in communication with authentication circuitry 1008 which may be in communication with a secure database 1010. Authentication circuitry 1008 and database 1010 may be of similar description and operation as described with respect to authentication circuitry 910 and secure memory database 914 of **FIG. 9**. For example, database 1010 may store data corresponding to the fob 240 which are authorized to transact business over system 800. Database 1010 may additionally store RFID reader 801 identifying information for providing to fob 240 for use in authenticating whether RFID reader 801 is authorized to be provided the fob account number stored on fob database 914.

Authentication circuitry 1008 may be of similar description and operation as authentication circuitry 910. That is, authentication circuitry 1008 may be configured to authenticate the signal provided by fob 240 in similar manner that authentication circuitry 910 may be configured to authenticate the signal provided by RFID reader 801. As is described more fully below, fob 240 and RFID reader 801 engage in mutual authentication.

In this context, "mutual authentication" may mean that operation of the system 800 may not take place until fob 240 authenticates the signal from RFID reader 801, and RFID reader 801 authenticates the signal from fob 240.

The RFID reader 801 may be configured to communicate using a RFID internal antenna 1006. Alternatively, RFID reader 801 may include an external antenna 1005 for communications with fob 240, where the external antenna 1005 may be made remote to the RFID reader 801 using a suitable cable and/or data link 821. RFID reader 801 may be further in communication with a telephonic device 843 via a data link 803. A suitable description for a transaction device or fob 240, and a RFID reader 801 may be found in U.S. Patent No. 10/192,488, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed on July 9, 2002, incorporated herein by reference in its entirety.

The call handling process begins when a user 201 presents the fob 240 containing the calling card data to a RFID reader 801 by, for example, placing the fob 240 in proximity to the reader 801. The reader 801 may interrogate the fob 240 and receive a calling card account number, which may be stored in the fob database 1010. The reader may receive the calling card number and forward the calling card number to the telecommunications device 843 in a device 843 recognizable format. The user 201 may further indicate the destination of his call by inputting a call directory number into a keypad located on the telecommunications device 843. The telecommunications device 843 may then forward the calling card number and the call directory number to the HSS for processing. With reference to **FIGS. 11-13**, HSS switch interface 806 receives the call from either inter-exchange carrier network 890 or LEC network 895 (step 200). HSS 802 prompts the caller for a calling card number by issuing a unique tone or an announcement from announcement database 808 to main processor 804 via link 807 (step 202). HSS 802 receives the calling card number in DTMF receiver 810 (step 204). Alternatively, if the caller is unable to provide the calling card number by dialing digits within a pre-determined time period, a human operator at attendant position 816 is connected to the caller by switch interface 806 so that the calling card number can be retrieved and extended to DTMF receiver 810. The process continues to step 206 in which HSS main processor 804 uses the calling card number it received from DTMF receiver 810 to access calling card recognition database 812. In decision step 208, HSS 802 determines whether the calling card number contains a valid vendor identification (*i.e.*, if the card number corresponds to a recognized vendor) in

the database. If the outcome of decision step 208 is a "NO" determination, the HSS 802 performs error handling, as is known in the art (step 209). If the outcome of decision step 208 is a "YES" determination, the process continues to step 210 in which HSS 802 sends a query to calling card validation database 840 over signaling link 841 to request calling card data associated with the card number. HSS 802 receives card data, including card product-type data and card information data, from calling card validation database 840 (step 212). If the card product-type data received from calling card validation database 840 indicates that the card is a permanent or "unlimited use" type card, the process continues in which rate information for the call is retrieved from rating database 830 (step 214). The call is connected to the called party at customer line BBB via trunk 896 (step 215). HSS 802 monitors the duration of the call, as is known in the art (step 216). Upon completion of the call (step 218), HSS 802 transmits billing data for the call to billing system 820 over data link 821 and processing ends in step 219. In this example, however, the card type data indicates that the card is a promotional card. Therefore, the process continues through connector "A" to **FIG. 12**.

In decision step 300, HSS 802 determines whether card information data received from validation database 840 indicates that the remaining balance of the promotional card has been depleted (*i.e.*, whether the remaining balance equals $0.00). If the outcome is a "YES" determination, the process continues in which determination is made as whether the card is an unlimited use card (step 301). For example, this situation would occur if the pre-established non-billed balance had been issued by a calling card company as a promotional "bonus" to a loyal permanent card user, and the card user has depleted the balance. If the outcome is a "YES" decision, the process returns to step 215. If, however, the outcome is a "NO" determination, the process continues in which HSS 802 issues a message from announcement database 808 which queries the caller to determine whether connection to a customer service representative to arrange for further use of the card is desired (step 302). HSS 802 waits for a predetermined time period for a response to the query (a dialed input received at DTMF facility 810) from the caller (step 304). HSS 802 determines whether a positive response was received from the caller (step 307). If the outcome is a "YES" determination, the process continues in which HSS 802 extends the call to customer service switch 860 over trunk 863 (step 309). HSS 802 disconnects the connection to the called party by dropping trunk 896 (step 311). Further processing continues through connector "B" to **FIG. 13**, described below. If the outcome of decision step 307 is a "NO"

determination, however, the process continues to step 308 in which HSS 802 disconnects the call and the process ends in step 310.

In this example, the remaining balance is not $0.00. Therefore, the outcome of decision step 300 is a "NO" determination, and the process continues in which HSS 802 accesses rating database 830, via signaling link 831, to determine the per minute billing rate to apply to this particular call (step 320). HSS processor 804 uses the billing rate and the remaining balance received from validation database 840 to calculate the maximum duration of the call (step 322). HSS 802 retrieves the announcement protocol from internal database 814 (step 324). In this call flow example, the announcement protocol includes: issuing a first announcement which informs the caller of the maximum call duration and balance depletion protocol; and issuing a second warning announcement prior to balance depletion which provides the caller with a customer service representative connection option. HSS announcement database 808 issues the first announcement, which states the maximum call duration and disconnection information (step 326). The process continues in which HSS switch interface 806 connects the caller served by line AAA to the called party served by line BBB LEC network 895 via trunk 896 (step 328). HSS 802 continues to monitor the duration of the call, and periodically updates calling card validation database 840 with a new remaining balance as the call continues (step 330). HSS 802 determines the remaining balance is approaching depletion (step 331). At some pre-determined remaining balance, (*e.g.*, a remaining balance which allows the call to continue for only 30 seconds) HSS 802 issues the second announcement which states amount of time remaining and instructions for further use of a calling card (step 332). In this example, the caller wishes to convert her promotional card into a permanent calling card. Therefore, in response to the query, the caller depresses a particular button on the phone. The process then returns to decision step 307.

FIG. 13 illustrates the steps performed in telecommunications network 800 after HSS 802 has determined that the caller desires connection to a customer service representative. Trunk 896 connection to the called party is dropped and the call is connected to customer service switch 860 via trunk 863 (step 400). A customer service representative receives the call from HSS 802 (step 402). The customer representative answers the call and obtains all necessary information from the caller who wishes to continue to use the calling card number associated with a promotional card (step 404). In this case, the caller wants to bill all future charges to her home telephone account corresponding to directory number

"602-123-4567". Accordingly, the customer representative obtains from the caller her current calling card number, home directory number and billing address. The customer representative verifies the validity of the directory number account by accessing validator 880, as is known in the art (step 406).

The customer representative accesses updating system 850 via customer service switch 860 using the caller's promotional calling card number (step 408). The customer representative enters card type data and card information data into customer service switch 860 via attendant position 862 (step 410). Customer service switch 860 transmits the new data to updating system 850 via signaling link 861 (step 412). Updating system 850 updates calling card validation database 840 via signaling link 851 (step 414). Customer services switch 860 receives an "update complete" message from updating system 850 (step 416). The process continues in which customer switch 860 sends a message to HSS 802 indicating that the calling card data update is complete (step 418). HSS 802 releases trunk 863 to customer service switch 860 and releases trunk connection 898 to the caller (step 420). The process ends in step 422.

FIG. 14 shows a representation of data stored in calling card validation database 840 with respect to three distinct calling cards. As shown in **FIG. 14**, calling card number "1" is card product-type "A". Accordingly, information stored for this particular calling card account requires remaining balance data which, in this case, is $0.00 as well as balance depletion protocol data which requires all calls made using calling card number "1" to be billed to an account associated with directory number "708-555-1234". Calling card number "2" relates to card product-type "B" which requires remaining balance and balance depletion protocol data. Calling card number "2" has a remaining balance of $5.00 which indicates that the user of this card may continue to place calls. Unlike calling card number "1", however, the balance depletion protocol associated with this particular calling card is to disconnect all calls upon depletion of the remaining balance. Calling card number "3" is a "C" product-type card. The card information data indicates that all calls made using calling card number "3" should be billed to an account associated with directory number "708-555-6457". There is no pre-established non-billed balance associated with calling card number "3". A complete understanding of the operation of a conventional telephone calling card system in accordance with the present invention may be found in U.S. Patent No. 5,864,609, issued January 26, 1999, to Cross, et al., which is herein incorporated by reference.

In another exemplary embodiment of the invention, a user may use the transaction device 240 in a system which may be partially or substantially maintained by a transaction account provider. The transaction account provider may be, for example, a department store (*e.g.*, Sears Department Store), a specialty store (*e.g.*, Radio Shack), or the like. As used herein, these account providers, which issue an account for use only with (or mainly with) the account provider and related companies, may be termed "private label" account providers, and the transaction account provided by these account providers may be termed a "private label account." The private label account providers may ordinarily use or maintain a transaction processing system which facilitates processing transactions associated with the private label account, without substantial use of third party account providers like American Express, MasterCard, Visa, Discover, or the like. In this instance the transaction system maintained by the private label account provider may be termed an internal private label transaction completion system, which may operate over an internal network. The internal network may be one that is substantially free of eavesdropping from third-party listeners.

FIG. 15 is an exemplary private label transaction account processing system 1500 which may be used in accordance with the present invention. Private label transaction system 1500 includes a transaction device 240, which may be in communication with a merchant POS 1502. Alternatively, the private label system 1500 may include a reader 801 in communication with the merchant POS 1502 and the transaction device 240. Merchant POS 1502 (or reader 801) may be in further communication with a private label merchant system 1504. In some exemplary embodiments, the merchant POS 1502 (or reader 801) may be in communication with the merchant system 1504 and the merchant system 1504 may be in communication with an account provider system 1514. The merchant POS 1502 (or reader 801) may be in communication with account provider system 1514 via an external network 1512. External network 1512 may be any data exchange system for transacting business such as the Internet, an extranet, WAN, LAN, satellite communications, or the like as described above.

The internal network 1506 may be of similar description as external network 1512 except that internal network 1506 may be substantially controlled by a merchant system 1504. The merchant system 1504 may provide its own private label account for conducting transactions only or mainly on the merchant system 1504. In another example, internal network 1506 may be any network substantially limited to connecting a plurality of private label merchant systems 1516 substantially maintained by the same or related private systems

which provide a private label account for conducting transactions only on the private label merchant systems 1504, 1516. In this instance, related private label transaction account providers 1516 may have similar functionality as system 1504. That is, each private label merchant system 1516 may be configured to receive a private label account number from transaction device 240 and process the transaction under the merchant system 1516 business as usual standards. In this exemplary embodiment, a transaction device 240 may be configured to complete a transaction on any one of systems 1504, 1516, where the systems 1504, 1516 are related or maintained by related private label account providers. For example, transaction device 240 may communicate and complete transactions on a system maintained by Sears Department Store and a private label system maintained by a Firestone tire seller.

The transaction device 240, merchant POS 1502 and reader 801, may be of similar description as similar components as described above. As such, with brief reference to **FIGS. 8** and **9**, the transaction device 240 may include a database 914 which may be loaded or populated with a private label account identifier or account number in accordance with the method described in **FIG. 4**. The transaction device 240 may include a transponder 904 which may be configured to provide the private label account identifier to the merchant POS 1502 or reader 801 using any of the methods described herein. For example, the private label account identifier may be included in transaction device database 914 in any format recognized by the merchant system 1504, 1516, POS 1502, or reader 801. The private label account identifier may include particular numbers or other codes or headers to direct the transaction data to a particular private label system. As such, the transaction device 240 may be used at any POS or reader (even a third-party POS), but the transaction will be transmitted to the appropriate private label system via any communication system discussed herein.

In another example, the private label account number may be provided to the transaction device database 914 in ISO/IEC 7811 et al. magnetic stripe track 1 / track 2 format, which is ISO/IEC 7813 compliant. As such, the transaction device may provide the private label account number to the POS 1502 or reader 801 in the magnetic stripe format. That is, transaction device 240 may include a transponder 904 which may be configured to transmit the account identifier in track 1 / track 2 format.

The private label account identifier may be received by merchant system 1504 from the POS 1502 or reader 801 and provide the account identifier to a merchant system

processor 1508 for processing. The processor 1508 may be any computing system as described above for receiving an account number and completing a user transaction request. For example, the processor 1508 may receive a user transaction request, and determine whether the request is to be authorized by retrieving user private label account information stored on a private label database 1510, along with any other desired information from any other internal or third party database. The database 1510 may store a plurality of distinct private label account numbers correlated to a plurality of distinct users. The processor 1508 may receive the transaction request containing the private label account number from the POS 1502 and retrieve the account information (*e.g.*, user name, account balance, available transaction amount, etc.). The processor 1508 may compare the transaction request to the account information and determine whether the transaction should be authorized. The processor 1508 may use any method determined by the private label system 1504 for transaction authorization. The processor may also use inputted and/or stored biometric data or any other authentication information.

FIG. 16 is an exemplary processing method which is suitable for use in the present invention. The method may begin when a user presents a transaction device 240 for loading a private label data set into device secure database 914 (step 1602). The transaction device 240 may be initialized to communicate with and complete a transaction on private label merchant system 1504 (step 1604). The method may also include issuing the transaction device 240 with pre-loaded private label data. In one embodiment, the transaction device 240 may still need to be activated via a telephone system (*e.g.*, menu or voice response system) or website (*e.g.*, enter information. The transaction device 240 may include indicia of the private label entity by itself or in addition to other indicia. In another embodiment, the transaction device 240 may be configured to display indicia of a private label entity or allow the user to affix indicia to the device 240. Transaction device 240 may also display multiple indicia of various private label entities and be configured to allow the user to select a particular private label account to transmit to the reader. The system may also be configured to allow the user to select a particular private label account on the POS terminal such that, for example, the reader or POS may only transmit information related to the selected account.

The system and method may also be configured to enable a transaction device 240 to function in multiple modes, for example, as both a credit card and a separate service partner's membership card. The system provides back-end functionality that takes

advantage of cooperation between the multiple service providers. More particularly, the system provides methods for opening new accounts, methods for accomplishing transaction device replacement, methods for canceling a service partner membership, methods for canceling a primary party account, and methods for transferring an account to a different service partner account. The multiple-service transaction device enabled by the present invention may include any combination of membership information, a barcode, and a photo in addition to standard credit card information. A method for providing a multiple-service card may include, for example, receiving at a service partner an application for a multiple-service card from a consumer, wherein the application comprises fields which include credit application information for a particular transaction device and service partner information. The service partner information may be related at least in part to membership in the service partner establishment. The system reviews the application for fields which include service partner information, extracts the service partner information from the application for a multiple-service device. The system then communicates the service partner information to a service partner to determine if the service partner desires to provide access into the service partner establishment and to purchase goods and services from the service partner using the transaction device. The system then reviews the application for fields which include credit card application information, extracts credit application information from the application for a multiple-service card and communicates the credit card application information to a provider of credit services. The provider of credit services thereafter determines whether it desires to extend credit to the consumer; and if the provider of credit services desires to extend credit to the consumer, the system establishes an account associated with the consumer, initiating processing, statementing, billing, accounting, and servicing functions relating to the account and causing a multiple-service transaction device to be sent to the consumer, wherein the multiple-service transaction device is configured for providing a primary party's services and a service partner's services. For additional information related to the application process or the dual card feature, see U.S. Serial No. 09/764,688, filed on January 16, 2001, by inventors Fitzmaurice, et al., and titled "MULTIPLE-SERVICE CARD SYSTEM," which is hereby incorporated by reference.

After initializing the device, a user may then present the transaction device 240 to a private label merchant system 1504 for completing a user transaction request (step 1606). The transaction device 240 may provide the private label account identifier to the merchant POS 1502 (or reader 801) (step 1608), which may receive the account identifier and forward

the account identifier and merchant transaction request to the merchant system private label processor 1508 (step 1610). The account identifier may be transmitted via an internal network 1506.

The merchant system 1504 may include a private label database 1510 which may store account information relative to the account identifier received. The processor 1508 may receive the private label account identifier and correlate the account identifier to the related private label transaction account information stored on database 1510 (step 1612). The processor 1508 may then verify whether the transaction request should be authorized using any private label merchant system protocol (step 1614). For example, the processor 1508 may compare the value of the transaction request with the value available which is associated with the account identifier received and authorize the transaction to be completed if the transaction request is less than the value available. Otherwise, the processor 1508 may not authorize completion of the transaction.

The processor 1508 may also incorporate a private or third-party loyalty or incentive point system wherein loyalty points may be awarded to the user. The loyalty points may be stored within the database 1510 of transaction device 240 or may be stored within merchant system.

It should be appreciated that the particular implementations shown and described herein are illustrative of the invention and its best mode and are not intended to otherwise limit the scope of the present invention in any way. Indeed, for the sake of brevity, conventional data networking, application development and other functional aspects of the systems (and components of the individual operating components of the systems) may not be described in detail herein. It should be noted that many alternative or additional functional relationships or physical connections may be present in a practical data set management system.

As may be appreciated by one of ordinary skill in the art, the present invention may be embodied as a method, a data processing system, a device for data processing, and/or a computer program product. Accordingly, the present invention may take the form of an entirely software embodiment, an entirely hardware embodiment, or an embodiment combining aspects of both software and hardware. Furthermore, the present invention may take the form of a computer program product on a computer-readable storage medium having computer-readable program code means embodied in the storage medium. Any

suitable computer-readable storage medium may be utilized, including hard disks, CD-ROM, optical storage devices, magnetic storage devices, and/or the like.

These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means which implement the function specified in the flowchart block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions which execute on the computer or other programmable apparatus include steps for implementing the functions specified in the flowchart block or blocks.

In the foregoing specification, the invention has been described with reference to specific embodiments. However, it may be appreciated that various modifications and changes can be made without departing from the scope of the present invention. For example, the issuer may reserve all management of data stored on the transaction device, thereby prohibiting the user from modifying the issuer-owned data thereon. Further, each issuer system may have its own data management protocol, which necessarily does not interfere with or depend upon the data management protocol of other issuer systems. As such, the specification and figures are to be regarded in an illustrative manner applicable irrespective of the data processing protocol used by a data set owner, rather than a restrictive one, and all such modifications are intended to be included within the scope of the present invention. Accordingly, the scope of the invention should be determined by the appended claims and their legal equivalents, rather than by the examples given above. For example, the steps recited in any of the method or process claims may be executed in any order and are not limited to the order presented.

Benefits, other advantages, and solutions to problems have been described above with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as critical, required, or essential features or elements of any or all the claims. As used herein, the terms "comprises," "comprising," or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only

those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. Further, no element described herein is required for the practice of the invention unless expressly described as "essential" or "critical."

Claims

What is claimed is:

1. A method for facilitating a private label account transaction using data sets stored on a Radio Frequency operable transaction device, the method comprising the steps of:

providing a radio frequency transaction device responsive to a radio frequency interrogation signal, said transaction device including a database configured for storing a data set owned by a private label account provider;

facilitating adding to said database, said private label account provider owned data set and

wherein said transaction device is operable to provide said data set via radio frequency communication for completion of a private label transaction, and

wherein a portion of said data set facilitates the completion of a private label transaction.

2. A method of claim 1, including the step of providing said radio frequency transaction device operable to communicate with a RFID reader via said RF communications, said transaction device operable to communicate with said RFID reader in response to a RFID reader provided interrogation signal.

3. A method of claim 2, wherein said data set owned by a private label account provider comprises a private label account identifier.

4. A method according to claim 3, wherein said transaction device is operable to provide said private label account identifier to said RFID reader.

5. A method according to claim 4, wherein said RFID reader operable to receive said private label account identifier in magnetic stripe format.

6. The method of claim 1, wherein said data set is stored on said database in magnetic stripe format.

7. The method of claim 1, further comprising providing a private label transaction account associated with private label account identifier, said private label transaction account having a value associated with transaction account usage, and wherein said private label transaction results in a modification of said value of the private label transaction account.

8. The method of claim 1, wherein said facilitating adding to said database further comprises:

receiving at a service partner an application for a multiple-service transaction device from a consumer, said application comprising fields which include credit application information for a particular credit transaction device and service partner information, said service partner information related at least in part to membership in the service partner establishment;

reviewing said application for fields which include service partner information;

extracting said service partner information from said application for a multiple-service transaction device;

communicating said service partner information to a service partner to determine if said service partner desires to provide access into said service partner establishment and to purchase goods and services from said service partner using said particular credit transaction device;

reviewing said application for fields which include credit application information;

extracting said credit application information from said application for a multiple-service transaction device;

communicating said credit application information to a provider of credit services, said provider of credit services thereafter determining whether it desires to extend credit to the consumer; and

if said provider of credit services desires to extend credit to the consumer, establishing an account associated with said consumer, initiating processing, statementing, billing, accounting, and servicing functions relating to said account and causing a multiple-service transaction device to be sent to the consumer, wherein said multiple-service

transaction device is configured for providing a primary party's services and a service partner's services.

9. The method of claim 1, wherein a portion of said data set facilitates the completion of a private label transaction wherein the transaction includes one of issuing and redeeming loyalty points.

10. A system for a transaction device for storing a private label account identifier on a RF operable transaction device,

said RF transaction device comprising:

at least a first data storage area configured to store said private label account identifier,

said private label account identifier associated with a private label data set owner and said data storage area configured to store said private label account identifier in a format.

11. A system according to claim 10, wherein said format is magnetic stripe format.

12. A system for facilitating the management of a plurality of data sets stored on a RF operable transaction device,

said transaction device comprising:

at least one data storage area configured to store a first data set in a first format and a second data storage area configured to store a second data set in a second format different from said first format,

said first data set associated with a first owner and said data storage area configured to store said first data set in said first format independent of said second data set, and

said second data set associated with said second owner and said data storage area configured to store said second data set in said second format independent of said first data set, wherein said first data set is associated with one of a private label transaction account, and a calling card transaction account, and said second data set is

associated with one of a private label transaction account, calling card transaction account, and a credit card transaction account;

a remote database configured to store a exact duplicate representation of said first data storage area and said second data storage area; and

an interaction device configured to read and write data to said transaction device storage area, said interaction device configured to receive said first and second data sets from said remote data base, and to provide said first and second data sets to said transaction device database.

13. A system for a transaction device for storing a private label account identifier on a RF operable transaction device,

said RF transaction device embedded in a pervasive instrument comprising:

at least a first data storage area configured to store said private label account identifier,

said private label account identifier associated with a private label data set owner and said data storage area configured to store said private label account identifier in a format.

14. A system for facilitating the management of a plurality of data sets stored on a RF operable pervasive transaction device,

said pervasive transaction device comprising:

at least one data storage area configured to store a first data set in a first format and a second data storage area configured to store a second data set in a second format different from said first format,

said first data set associated with a first owner and said data storage area configured to store said first data set in said first format independent of said second data set, and,

said second data set associated with said second owner and said data storage area configured to store said second data set in said second format independent of said first data set, wherein said first data set is associated with one of a private label transaction account, and a calling card transaction account, and said second data set is associated with one of a private label transaction account, calling card transaction account, and a credit card transaction account;

a remote database configured to store a exact duplicate representation of said first data storage area and said second data storage area; and

an interaction device configured to read and write data to said transaction device storage area, said interaction device configured to receive said first and second data sets from said remote data base, and to provide said first and second data sets to said transaction device database.