CARD BLOCKING SYSTEM AND PROCESS

TECHNICAL FIELD

[0001] The present invention relates to a card blocking system and process for preventing transactions from being conducted on selected payment cards via a user identifier of the card holder.

BACKGROUND

[0002] The use of electronic payment services has increased dramatically in recent decades. In particular, credit and debit card-based payment services have become integrated into everyday life due to their ability to allow a customer to complete purchases via the electronic transfer of funds to a merchant's account. Card-based payments offer many advantages over cash payments, including that the customer can provide a merchant with a payment in any currency without needing to transport physical denominations or having to manually perform conversions from one currency type to another, while retaining the efficiency of a cash exchange. The popularity of card based payment services has increased the importance of ensuring that control can be exercised over the use of a payment card issued to a card holder, such as to secure the funds of the card holder's corresponding payment account.

[0003] Despite the convenience of these payment technologies, there remains room for improvement. It is desired to provide a user identifier payment card blocking system and process that alleviate one or more difficulties of the prior art, or to at least provide a useful alternative.

SUMMARY

[0004] In a first aspect, there is provided a payment card blocking system including an authentication server device, the authentication server device including:

a database configured to store:

user data of a user, including data representing a unique user identification (UID) code and corresponding identification credentials of the user, said unique identification code uniquely identifying the user among all other users of the system, wherein said unique UID code is assigned by an external authority to the user;

payment card data representing one or more payment cards of the user, each payment card being linked to a card entity and issued by an issuing financial institution; and

a memory configured to store program instructions for execution by at least one computer processor to:

receive UID card block initiation data representing the initiation of a card blocking operation to prevent future payment transactions from being conducted with any one of the one or more payment cards of the user;

process the UID card block initiation data to:

i) authenticate the user based on the user data; and;

ii) generate, based on the payment card data, candidate card data representing one or more candidate payment cards of the user for which a card blocking operation can be performed; and

transmit the candidate card data to a payment device, such that selected ones of the one or more of the candidate payment cards are each blocked by the corresponding one or more issuing financial institutions.

[0005] In a second aspect, there is provided a process for blocking a payment card, including:

receiving, at an authentication server device, user identification (UID) card block initiation data representing the initiation of a card blocking operation to prevent future payment transactions from being conducted with any one of one or more payment cards of a user, each payment card being linked to a card entity and issued by an issuing financial institution;

processing, at the authentication server device, the UID card block initiation data to:

i) authenticate the user based on user data of the authentication server device, the user data including a UID code and corresponding

identification credentials of the user, said UID code uniquely identifying the user among all other users of the system, wherein said unique UID code is assigned by an external authority to the user; and

ii) generating candidate card data representing one or more candidate payment cards of the user for which a card blocking operation can be performed, the candidate card data being generated based on payment card data of the authentication server device, said payment card data representing the one or more payment cards of the user; and

transmitting, by the authentication server device, the candidate card data to a payment device, such that selected ones of the one or more of the candidate payment cards are each blocked by the corresponding one or more issuing financial institutions.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Some embodiments of the present invention are hereinafter described, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a block diagram of a card blocking system in accordance with some embodiments of the present invention;

Figure 2 is a block diagram of a computing device within the card blocking system;

Figure 3 is a flow diagram of a process for performing user identifier based payment card blocking in accordance with some embodiments of the present invention;

Figure 4 is a flow diagram for performing user and payment card registration of the process for performing payment card blocking in accordance with some embodiments of the present invention;

Figure 5 is a flow diagram for the initiation of a user identifier card blocking operation of the process for performing payment card blocking in accordance with some embodiments of the present invention;

Figure 6 is a flow diagram for selecting one or more payment cards of the process for performing payment card blocking in accordance with some embodiments of the present invention; and

Figure 7 is a flow diagram for executing a block in respect of a selected payment card of the process for performing payment card blocking in accordance with some embodiments of the present invention.

DETAILED DESCRIPTION

Overview

[0007] The inventors have identified some specific shortcomings with existing payment card technologies. The ubiquitous use of card-based payment services by merchants and consumers has lead to payment cards becoming a replacement for physical currency denominations for many individuals. These services allow the transfer of funds from a payment account of the card holder to a corresponding account of the merchant using only information stored on, or within, the payment card, including the payment card number, expiry date, card holder name and card verification code (CVC) or similar. The result is that the security of a particular payment account of a card holder is dependent on: i) physically ensuring that the card remains in the possession of the card holder, or an authorised party; and ii) preventing the card information from being compromised via exposure to an unauthorised third party.

[0008] As a result of the popularity of card based payment services, many individuals carry payment cards on their person while conducting everyday activities. Consequently, payment cards are frequently lost, misplaced or stolen resulting in the unauthorised appropriation of funds from the card holder's associated payment account. Furthermore, even when a payment card remains physically secured, the card details needed to conduct a transaction may still be exposed. Such exposure can, for example, occur due to phishing attacks which trick the card holder into unknowingly providing their information to a malicious third party. Alternatively, the card details can be compromised during a breach of security experienced by a trusted third party who stores the card details with the

permission of the card holder (e.g. a service provider to whom the card holder provides subscription information to including the details of a payment card).

[0009] The prevalence of card-based payment services, and the relative ease with which the card details required to perform transactions can be compromised, has lead to the implementation of 'blocking' measures by issuing financial institutions that issue the respective cards. Specifically, on the unauthorised exposure of the details of a payment card, or as a preventative step in the case of the loss of the physical card, the issuing financial institution enforces a block on the card preventing the card from being used to transact the corresponding payment account.

[0010] Conventionally, card blocking requires that the card holder notify the issuing financial institution of the security breach with respect to the particular payment card, such as by telephone conversation. An operator of the issuing financial institution then manually operates a card management system, or equivalent, to block any future transactions from being performed with the card. This approach has several disadvantages. First, the requirement of interacting with the operator to effect the card block is often inconvenient and time consuming. The card holder typically must wait in a phone queue and subsequently provide information during a voice conversation, including information needed to verify their identity (such as address and/or a response to a 'challenge' question) and the details of the card to be blocked. When requesting a card block, the card holder is typically stressed (i.e. due to the potential loss of funds in the case that the card for which the block is requested is transacted by an unauthorised party) and participating in lengthy conventional blocking processes is undesirable.

[0011] Second, often a plurality of cards of the card holder will be simultaneously compromised (e.g. when the card holder's wallet is stolen). If the compromised cards are each issued by more than one issuing financial institution, then the card holder will need to engage in a conventional blocking process with each individual issuer in order to block the respective payment cards. This is extremely time consuming and increases the likelihood that a corresponding payment account of the card holder will be compromised (i.e. where the block of a particular

compromised card could not be executed before the unauthorised party transacts the account).

[0012] The described embodiments of the present invention include a user identification ("UID") based card blocking system and process for allowing a card holder (referred to herein as a "user" of the UID blocking system) to prevent future transactions from being performed with one or more payment cards, each issued by a corresponding issuing financial institution (referred to as an "issuer") and associated with a particular card entity (such as MasterCard) by the use of a unique user identification code (UID Code) and corresponding identification credentials. Specifically, payment cards of a user are registered with a UID card authentication system in association with the UID code and identification credentials of the user, where the UID code and identification credentials are independent of the issuer and the card entity of a particular payment card. The UID code of the user can be in the form of an existing number, or identifier, that is assigned to the user by an external authority, such as for example a social security number or passport number. Following registration of one or more payment cards, the user can interact with a payment device enabled by any type of financial institution, such as an Automatic Teller Machine (ATM), to initiate blocking of the UID of one or more of their registered payment cards.

[0013] The payment device interacts with a UID authentication server device, via an acquirer system, and is configured to receive the UID code and identification credentials from the user. The user can select one or more registered payment cards for which a blocking operation is to be performed directly from the payment device, irrespective of the issuer of, and/or the card entity linked to, each selected payment card. The blocked card numbers are then transmitted to respective issuers.

[0014] The UID card based blocking system stores and processes identification credentials of users of the system in order to authenticate a card block operation initiated by a user. In some embodiments, the identification credentials include biometric identifiers of the user, such as for example features extracted from a finger print, retina or facial scan of the user. In other embodiments, the

identification credentials can include an alphanumeric value provided by the user in the form of a Personal Identification Number (PIN) or One-Time Passcode (OTP).

[0015] In the described embodiments, an acquirer system facilitates communication between the payment device and the authentication server. Specifically, the acquirer receives registered card data from the authentication server representing the cards of the user for which UID based blocking can be performed following verification of the UID and ID credentials of the user. The forwarding of this data to the payment device allows the user to select one or more payment cards for the corresponding issuer(s) to block. The selection is processed by the acquirer and is forwarded to the UID block processing device of the nominated card entity. In the described embodiments, the nominated card entity processes data corresponding to each selected payment card for which UID blocking is to be performed, involving the generation of data representing a request to block each selected payment card according to the card entity that is associated with the card. In other embodiments, the UID block processing device is implemented by the acquirer, and data representing requests for UID based blocking of a particular selected payment card are forwarded directly to the card entity associated with the card. In further embodiments, it is possible for the user to block a selected payment card(s) using ATMs via the UID block processing device or any processing device which can be configured to identify the cardholder.

[0016] In the described embodiments, a UID card block request in respect of a particular payment card is authenticated by the corresponding issuer prior to a block being placed on the card. Authentication involves the processing, by one or more devices of the issuer, of a blocking token in the form of a cryptographically generated identifier representing the payment card uniquely within the issuer. The blocking token is generated by the issuer at the time of registration of the particular payment card with the UID card blocking system and is provided by the authentication server, following successful authentication of the user's UID code and identification credentials, for the purpose of authenticating a block request in respect of the particular card (as resulting from the user conducting a UID based card block operation).

[0017] The UID authentication server maintains data representing the status of each registered payment card (i.e. as 'blocked' or 'active'), and the issuer is configured to transmit update data to the authentication server indicating a change of the status of one or more registered payment cards. In some embodiments, the set of cards presented to the user as selectable for a UID blocking operation are determined dynamically based on the status of each card of the user at the time of initiation. For example, coloured indicators can be used to indicate the status. The UID blocking system can also be configured to notify the user when a blocking operation is performed by the corresponding issuer for a selected payment card, or when such an operation could not be performed.

[0018] The UID based card blocking system, and process described herein therefore advantageously provides a platform for blocking one or more payment cards of a user that:

- provides the user with flexibility over the process for initiating the blocking of a payment card, since a request to block the card can be submitted to the issuer using a payment device, such as an ATM, without requiring direct contact between the user and the issuer (e.g. a telephone call);
- provides convenience during the blocking process by utilising a user identifier code comprising information which is likely to be already possessed by the user and that is regulated by an external authority, and identification credentials which are intrinsic to the user (e.g. biometric identifiers) or easy to remember (e.g. a PIN code); and
- provides an efficient means for simultaneously requesting the blocking of multiple payment card irrespective of the issuer of, and the card entity linked to, each payment card while maintaining the integrity of the card blocking process by the use of security token information exchanged between a UID system authentication server and a device of the issuer of each respective payment card.

System

[0019] As shown in Figure 1, a payment card blocking system 100 includes an authentication server 120 in communication with devices of an acquirer 112 of a corresponding payment device 104. The authentication server 120 is connected to the acquirer 112 devices via communications network 117. The communications

network 117 can be a local or wide area network, or a combination of a plurality of different local or wide area sub-networks. The user 102 operates the payment device 104 in order to make a payment transaction with a payment card, and/or to initiate a user identifier (UID) based card blocking operation in respect of one or more payment cards. In the described embodiments, the payment device 104 is an automatic teller machine (ATM) configured to communicate with the acquirer 112 directly via a secure local network. In other embodiments, the payment device 104 can be configured to communicate with the acquirer 112 via a wide area network in the form of communications network 117, or another similar network.

[0020] The payment device 104 includes a reader 108 configured to read a payment card of the user 102 in order to identify corresponding payment card data, and a terminal 106 configured to verify the authority of the user 102 to: i) make a payment with a payment card; and/or ii) initiate a UID card block operation, via interactive user interface (UI) elements rendered on a display and corresponding input means allowing the user 102 to make selections from items represented by the UI elements. The terminal 106 includes a numerical keypad, or similar input device, configured to accept number, symbol and/or character input from user 102 (e.g. as required to enter a PIN or OTP code).

[0021] In the described embodiments, the payment cards of the user 102 are standard financial magnetic stripe cards in accordance with the ISO/IEC 7813 international standard. Each payment card stores payment card data including: the cardholder name; an indication of the primary account number (PAN) of a payment account of the cardholder; the expiration date of the card; a service code; and a discretionary data value, such as a PIN verification key indicator, a PIN verification value, a card verification value (CVV) or a card verification code (CVC).

[0022] The payment device 104 also includes a scanner 110 configured to obtain biometric identification credentials from the user 102. In some embodiments, scanner 110 is a digital imaging device that captures images of a finger, hand, and/or retina of the user 102 analyses the image(s) to produce biometric data representing features of the respective biometric(s) for the user 102. In other embodiments, the scanner 110 includes an audio capturing device configured to

record samples of the voice of the user 102, and to analyse the voice samples in order to produce biometric data representing speaker identification and/or verification features.

[0023] Each payment card of the user 102 is linked to one of a plurality of card entities, such as card entity 114 having a transaction server 116 configured to process transactions made with the one or more linked payment cards. The authentication server 120 communicates with one or more devices of an issuer 140 of the payment card for which a UID card block operation can be performed. The authentication server 120 communicates with the issuer 140 for the purpose of registering user 102 with the payment card blocking system 100, and for registering one or more payment cards of the user 102, as issued by issuer 140, such that the user 102 can initiate a UID card block operation in respect of one or more of these registered payment cards.

[0024] The authentication server 120 includes a communications module 121 for transmitting and receiving data, a logic module 122 for controlling the processing of data by the authentication server device 120, and a verification module 124 configured to verify the identity of the user 102 when the user initiates a UID card block operation. In the described embodiments, the identity of the user 102 is represented by a UID code, which is a unique value assigned to the user 102 by an external authority. For example, the UID code can be a social security number, or passport number is assigned to the user 102 by government agency of the country in which they reside. The verification module 124 processes the UID code in conjunction with identification credentials of the user 102 which can be in the form of a biometric feature (as discussed above), and/or a PIN or OTP code.

[0025] The authentication server 120 includes a database 125 comprising a user table 127 and a card table 129. User table 127 stores user data for each user of the payment card blocking system 100, the user data including a UID code uniquely identifying the user among all other users of the system 100. In the described embodiments, the user data also includes the full name, address, and contact phone number of the user.

[0026] In an alternative embodiment (as indicated by dotted lines), the database 125 is communicatively coupled to the card entity 114 instead of being included with the authentication server 120. In such an embodiment, after successful authentication by the card entity 114, the card entity 114 will transmit the card numbers corresponding to the UID to the authentication server 120 and the card entity 114 carried out requisite processing before transmitting the card details to respective issuers 140. The issuer 140 indicates the blocked cards and will notify the card entity 114 to the database 125. Once the update is carried out, the card entity 114 then transmits an acknowledgement to the issuer 140 confirming the successful blocking of the card(s).

[0027] Card table 129 stores payment card data representing each payment card registered with the payment card blocking system 100, and in association with a registered user of the system. The payment card data includes: the UID of the user associated with the payment card; an identifier of the card entity linked to the payment card; an identifier of the issuer of the payment card; and a blocking token that, when processed by the issuer of the payment card, indicates the authenticity of a card blocking request in respect of the payment card.

[0028] In some embodiments, the issuer identifier is an interbank card association (ICA) number. In other embodiments, the issuer is identified via a local data identifier value which is subsequently mapped to corresponding ICA values to during the card blocking operation. In some embodiments, the payment card data stored by card table 129 also includes card status data in the form of a status flag indicating whether the payment card is in an 'active' state such that transactions can be conducted with the payment card, or in a 'blocked' state where transactions are prevented from being conducted with the card.

[0029] Card blocking requests for particular payment cards, as resulting from a UID card blocking operation initiated by the user 102 via the authentication server 120, are processed by a UID blocking engine 142 of the corresponding issuer 140. The UID blocking engine 142 includes a request handler module 144 which processes issuer block request data and invokes verification 146 and card block control 150 modules to perform card blocking according to the processes described

herein. The UID blocking engine 142 also includes a token generation module 148 configured to generate blocking token data for a payment card. In the described embodiments, the UID blocking engine 142 is a software application, or routine, executing on one or more devices of the issuer 140. The UID blocking engine 142 interacts with existing issuer devices, including a transaction processing device 160 for the purpose of obtaining data from a payment card database 164 containing information of the payment cards issued by the issuer 140, and from a transaction database 162 containing information of corresponding payment transactions conducted with these payment cards.

[0030] In some embodiments, UID blocking engine 142 is configured to send updates to the authentication server 120 with respect to the status of a particular payment card of the user 102, such as to indicate whether the issue has successfully enforced a block preventing future transactions from being performed with the payment card. The updater module 126 of the authentication server 120 is configured to process update information, and to modify any status data of the payment card that is stored within card table 129.

[0031] In the described embodiments, the acquirer 112 is configured to facilitate the exchange of data relating to the initiation of UID card blocking operations between the payment device 104 and the authentication server 120 (i.e. during initiation), and between the payment device 104 and the card entity 114 (i.e. during a request for blocking of specific selected cards). Card entity 114 is a particular card entity of the plurality of card entities that may be associated with each payment card (referred to as the "nominated card entity") and includes a UID block processing server 118 configured to receive UID block request data from acquirer 112, and to process this data in accordance with the processes described herein.

[0032] In the described embodiments of the payment card blocking system 100, the authentication server 120, card entity devices (including the transaction server 116 and the UID block processing server 118), acquirer 112 devices, and issuer 140 devices (including the transaction processing device 160 and the computing device(s) on which the UID blocking engine 142 is executed) are computer

systems 200 such as, for example, an Intel IA-32 based computer system, as shown in Figure 2, and the process 300 executed by the system 200 is implemented as programming instructions of one or more software modules 202 stored on non-volatile (e.g., hard disk or solid-state drive) storage 204 associated with the computer system. However, it will be apparent that at least parts of the aforementioned processes could alternatively be implemented as one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) and/or as configuration data of one or more field programmable gate arrays (FPGAs), for example.

[0033] Each system 200 includes random access memory (RAM) 206, at least one processor 208, and interfaces 210, 212, 214, all interconnected by a bus 216. The interfaces include a network interface connector (NIC) 212 which connects the system 200 to a communications network 116, such as the Internet.

[0034] Each system 200 also includes an operating system 224 such as Linux or Microsoft Windows, and a number of software modules 226 to 230, including web server software 226 such as Apache, available at http://www.apache.org, scripting language support 228 such as PHP, available at http://www.php.net, or Microsoft ASP, and structured query language (SQL) support 230 such as MySQL, available from http://www.mysql.com, which allows data to be stored in and retrieved from an SQL database 232.

[0035] In the described embodiments, the database 125, payment card database 164, and transaction database 162 are databases 232 implemented using SQL and are accessed by a database management system (DBMS) of the respective authentication server 120 and transaction processing 160 devices. The databases 232 can be operated by the one or more software modules 202 implementing the process 300. In other embodiments, each of the databases may be implemented on a separate computing device, or across multiple computing devices according to one or more techniques for the distributed processing and storage of data.

User and Card Registration

[0036] With reference to Figure 3, the blocking of a payment card by system 100 proceeds according to a process 300 involving the steps of registration 302, card blocking 304 (including the sub-processes of initiation 303, selection of payment cards for blocking 305, and execution of the card block 307) and notification 308. Figure 4 illustrates the registration process 302 involving the configuration of the payment card blocking system 100 for use by user 102. The registration process involves receiving, by the authentication server 120, user registration data (i.e. at step 402) representing a request to register user 102 with the payment card blocking system 100.

[0037] In the described embodiments, user registration request data is generated by the issuer 140 when the user 102 elects to enable UID based card blocking functionality with one or more of their payment cards issued by the issuer 140. More than one issuer 140 can also be notified. The enabling of the UID based card blocking functionality can be performed by the user 102 via a remote interface of the issuer 140, such as for example an Internet Banking Service (IBS). In other embodiments, the user data and corresponding payment card data can be received from the user 102 directly via a user registration portal that is remotely accessible to the user 102 over a wide area network (such as the Internet).

[0038] The user registration data includes: the first name, last name, address, and contact phone number of user 102; and the UID code assigned to the user by the relevant authority, and corresponding identification credentials that, when presented to the authentication server 120 in conjunction with the UID code, will authenticate the user 102 allowing the initiation of a card blocking operation for one or more registered payment cards. In some embodiments, the user can specify a preference for the form of the identification credentials to be used by the payment card blocking system 100. For example, the IBS of issuer 140 may allow the user 102 to select a PIN code as the identification credentials as an alternative, or in addition, to fingerprint feature data (which may be possessed by the issuer 140 as an existing means of authenticating payment transactions). In other embodiments, the UID card blocking functionality may be enabled via the automatic transmission of user registration data from issuer 140 to authentication server 120 without active input from user 102.

[0039] The user registration data is received by communications module 121 of the authentication server 120 and is transmitted to the logic module 122 for processing. At step 404, the logic module 122 invokes the verification module 124 to verify the received user registration data. In some embodiments, the verification process involves verifying the UID code with the name, address and/or other information of the user 102 as conducted by a system of the authority assigning the UID code. Verification module 124 is invoked to check the validity of the user registration data by comparing the UID code to corresponding codes represented by data stored in the user table 127 of database 125 (i.e. to ensure that the UID code of the registration request is unique among all presently registered users of the system 100). The verification process of step 404 is successful if the UID code of the user registration data is confirmed to match to the UID code assigned to user 102 by the external authority, and if the code does not correspond to the UID code of a presently registered user.

[0040] At step 406, user table 127 is updated with the user registration data, including the UID code and identification credentials of user 102. In some embodiments, the authentication server 120 is configured to only store the UID code and identification credentials of the user 102 such that the name, address, contact phone and other information of user 102 is discarded after verification at step 404. Following the storage of the user registration data in user table 127, user 102 is registered with the payment card blocking system 100.

[0041] At step 408, the authentication server 120 receives card registration data representing a request to register one or more payment cards issued to the user 102 by issuer 140. The card registration data includes, for each payment card, an identifier of the card entity linked to the payment card, an identifier of the issuer, and a blocking token that, when processed by the issuer, indicates the authenticity of a card blocking request in respect of the payment card. The card registration data also includes the UID code of the user 102 which is used to associate each payment card with the user 102 within the authentication server 120.

[0042] The card registration data is generated by the UID blocking engine 142, involving the extraction of corresponding card number, UID code, card entity identifier, and card status data values from the payment card database 164 of the transaction processing device 160. The blocking token data is generated by the token generation module 148 and a time prior to card registration. In the described embodiments, the blocking token is in the form of a string generated by the application of the asymmetric RSA encryption algorithm to the card number, and using a particular private key of the issuer 140. The skilled addressee will appreciate that other methods for generating a cryptographically secure blocking token for the payment card can be used without departing from the scope of the described invention. The card registration data is transmitted to authentication server 120 by the request handler module 144 of the UID blocking engine 142 executing on the issuer devices.

[0043] At step 410, the logic module 122 updates the card table 129 to store card data corresponding to the received card registration data for each payment card of user 102. Completion of this process results in the successful registration of each aforementioned payment card with the payment card blocking system 100, such that the user 102 can initiate a UID based card block operation and subsequently select one or more of the registered payment cards to be blocked, as described herein below. In described embodiments, a payment card is associated with a single user within the payment card blocking system 100 even if the issuer 140 considers that the payment card is jointly owned (such as, for example, in the case of a payment card corresponding to a payment account jointly held by a multiple individuals). In other embodiments, payment cards may be registered to more than one user of the system 100 such that a UID card block operation can be performed on the card by any one of these users.

Card Blocking

[0044] With respect to Figure 3, following the registration process of step 302, the card blocking process of step 304 requests blocking of one or more payment cards of the user 102, such that future transactions are prevented from being performed with those cards. Specifically, card blocking process 304 involves the sub processes of initiating UID based card blocking with the authentication server 120 (i.e. at step 303), the subsequent selection of one or more payment cards to be blocked

from a set of candidate payment cards of the user 102 that are eligible for UID based card blocking (i.e. at step 305), and the execution of the card block operations by the corresponding issuers (i.e. at step 307).

[0045] The authentication server 120 configured to perform a card blocking process including the steps of:

receiving UID card block initiation data representing the initiation of a card blocking operation to prevent future payment transactions from being conducted with any one of one or more payment cards of a user, each payment card being linked to a card entity and issued by an issuing financial institution;

processing the UID card block initiation data to:

i) authenticate the user 102 based on user data of the authentication server device, the user data including a UID code and corresponding identification credentials of the user, said UID code uniquely identifying the user among all other users of the system; and

ii) generating candidate card data representing one or more candidate payment cards of the user 102 for which a card blocking operation can be performed, the candidate card data being generated based on payment card data stored in a database of the authentication server device, said payment card data representing the one or more payment cards of the user 102; and

transmitting the candidate card data to a payment device 104, such that selected ones of the one or more of the candidate payment cards are each blocked by the corresponding one or more issuing financial institutions.

[0046] Figure 5 illustrates the card blocking initiation process (i.e. step 303) performed by the authentication server 120. The user 102 operates terminal 106 of the payment device 104 to commence the process. For example, the user 102 may be presented with a UI element option (such as a "BLOCK CARDS" button) on the display of the terminal 106. The user 102 enters their UID code (the "supplied UID code") into the terminal 106 via an input device such as a number pad. The payment device 104 presents the user 102 with a notification via the user interface indicating that identification credentials are required. The user 102 provides their identification credentials (the "supplied ID credentials") by operating the input

device of the terminal 106 (such as the number pad in the case of a PIN or OTP code), or the scanner 110 which is configured to obtain biometric data from the user 102 and generate corresponding data representing ID credentials of the appropriate form (as discussed above).

[0047] In some embodiments, the user 102 can operate the terminal 106 to specify the form of the supplied ID credentials for the purpose of initiating the UID based card blocking. For example the user 102 can choose between entering ID credentials in the form of a biometric feature and/or as a PIN or OTP code. In the described embodiments, OTP codes are provided to registered users of the payment card blocking system 100 by a UID blocking service provider system, such as for example by an electronic message (e.g. SMS or email) or by the use of a physical authenticator device configured to generate codes in the form of pseudo random sequences. The OTP code generation process performed by the UID blocking service provider system is synchronised with the authentication server 120 such that data of the user table 127 is updated to contain the valid OTP for each registered user.

[0048] The supplied UID code and ID credentials are transmitted from the payment device 104 to the authentication server 120 via acquirer 112 within UID block initiation data. At step 502, the UID block initiation data is received by the communications module 121 of the authentication server 120. The communications module 121 transmits the UID block initiation data to the logic module 122 for processing, and at step 504 verification module 124 is invoked to verify the data. Verification involves accessing the user table 127 of database 125 to search for the supplied UID code in the UID field of the user data of each registered user.

[0049] If the supplied UID code matches to the UID code of corresponding user data in the user table 127, the verification module 124 compares the supplied ID credentials to the ID credentials of the user data. The degree of matching required between the supplied ID credentials and the credentials stored within user data entries of the user table 127 can vary based on the form of these credentials. Specifically, positive verification may occur when the supplied ID credentials differ

from the stored ID credentials by less than a predetermined threshold amount. For example, when the ID credentials are in the form of fingerprint features, a classification or pattern matching score is calculated between the supplied feature data and the stored feature data, and positive verification is considered to occur if the matching score equals or exceeds some predetermined value (e.g. 95%). However, for other forms of the identification credentials an exact match between the supplied and stored ID credentials data is necessary (e.g. where the credentials are in the form of a PIN code).

[0050] Following positive verification of the supplied UID code and ID credentials data, the authentication server 120 generates candidate payment card data representing one or more candidate payment cards for the UID based card blocking (i.e. at step 506). Logic module 122 accesses the card table 129 of database 125 and retrieves card data corresponding to each registered payment card of user 102. Candidate payment card data is generated by concatenating the card data of each of the payment cards of user 102 that are eligible to be blocked by the UID based blocking processes described herein (referred to as the "candidate" payment cards).

[0051] In the described embodiments, the candidate payment cards of user 102 include each payment card registered with the payment card blocking system 100 in respect of the user 102, and regardless of whether the payment card is presently active or blocked. In other embodiments, the set of candidate payment cards are determined based on the payment card data of table 129. For example, cards with card status data indicating that they are presently in a blocked state may be excluded from the set of candidate payment cards provided to the user 102 (such as to avoid the redundancy associated with requesting a block for an already blocked payment card) or the cards in the blocked state are not selectable by the user 102.

[0052] At step 508, the communications module 121 of authentication server 120 transmits the candidate card data to the acquirer 112, which is configured to forward this data to the payment device 104. The user 102 operates the terminal 106 to select one or more payment cards for which blocking is to be performed

from the set of candidate payment cards. Figure 6 illustrates the card selection sub process 305 of the card blocking process 304 performed by the payment card blocking system 100. At step 602, the candidate card data is received by the payment device 104. Terminal 106 processes the candidate card data and displays interactive elements on the UI that are operable by the user 102 for the purpose of selecting one or more of the candidate payment cards for blocking.

[0053] At step 604, the payment device 104 generates UID block request data representing a request for the corresponding issuer of each selected payment card to block the card. In the described embodiments, the UID block request data includes the card data of each selected payment card. In some embodiments, the UID block request data also contains information relating to the payment device 104 and/or the request, such as for example the time at which the request was made or an identifier of the payment device 104. The payment device 104 is configured to transmit the UID block request data to the acquirer 112. Transmission can be subject to confirmation, by the user 102, of the blocking operations in respect of the selected cards (e.g. where the user activates a "CONFIRM TO BLOCK SELECTED CARDS" button, or similar UI element).

[0054] The acquirer 112 receives the UID block request data from the payment device 104, and forwards the data to a UID block processing server 118. The UID block request data is processed by the UID block processing server 118, involving:

processing, for each selected payment card, the corresponding card data of the UID block request data to determine the card entity linked to the card (i.e. at step 606);

generating, for each particular card entity determined to be linked to at least one selected payment card, card entity block request data including the card data of each selected payment card linked to that card entity (i.e. at step 607); and

transmitting the card entity block request data to a device of each particular card entity.

[0055] Specifically, the UID block processing server 118 groups the payment card data of selected payment cards that are linked to the same card entity, and generates card entity block request data for the card entity including the

corresponding grouped payment card data. In the described embodiments, the UID block processing server 118 is implemented as one or more computing devices of the nominated card entity 114 and is configured to receive the generated UID block request data from the acquirer 112. The card entity linked to each selected payment card is identified by a card entity identifier field of the corresponding card data, as included within the UID block request data. The UID block processing server 118 maps the card entity identifier to a location of the corresponding device on an internal network connecting each card entity.

[0056] In other embodiments the UID block processing server 118 is a device of the acquirer 112, such that the generation of card entity block request data at step 607 is performed by the acquirer 112 and is subsequently transmitted to one or more card entities for processing.

[0057] At step 608, issuer block request data is generated representing a request for an issuer (such as issuer 140) to perform card blocking for one or more selected payment cards of the user 102. The issuer block request data is generated by one or more devices of the card entity linked to the selected payment cards (the "linked card entity", which may or may not be the nominated card entity 114). For example, in the case where the card entity 114 is the linked card entity, a device of card entity 114 concatenates the payment card data of selected payment cards that are issued by the same issuer and generates issuer block request data including the concatenated payment card data.

[0058] The issuer of each selected payment card is identified by the value of the issuer ID field of the corresponding payment card data, as included in the card entity block request data. The card entity 114 maps each issuer identifier to a corresponding device of the issuer, such as for example the device executing the UI blocking engine 142 in the case of issuer 140. At step 610, the issuer block request data is transmitted to issuer 140, and steps 608 and 610 are repeated for each issuer issuing one or more of the selected payment cards represented within the card entity block request data.

[0059] Figure 7 illustrates the sub process of executing a card block 307 in respect of a selected payment card. At step 702, the issuer block request data is received and a device of issuer 140. The request handler 144 extracts the payment card data of a selected payment card issued to the user 102 by issuer 140, and invokes verification module 146 to authenticate the block request in respect of the card (i.e. at step 704). In the described embodiments, the blocking token generated for each payment card prior to registration is stored in the payment card database of the transaction processing device 160. Authentication involves comparing the blocking token included in the payment card data received by issuer 140 (i.e. within the issuer block request data) to the corresponding blocking token stored in the payment card database 164 of the issuer 140. The blocking request for the payment card is authenticated if the respective tokens match, indicating that the corresponding blocking operation was initiated with, and subject to verification by, the authentication server 120 in accordance with the processes described herein above. In other embodiments, the blocking token of a particular payment card is dynamically regenerated by the UID blocking engine 142 via invocation of the token generation module 148 at the time of authenticating the block request.

[0060] Following successful authentication of the block request for a particular selected payment card issued by issuer 140, at step 706 card block controller 150 is invoked to execute the blocking operation for the payment card. Card block controller 150 generates blocking data interpretable by the transaction processing device 160 to prevent payment transactions from being conducted on the selected payment card, and updates the payment card data within the payment card database 164.

[0061] At step 708, the request handler module 144 generates UID card status update data to update the status of a selected payment card following the generation of blocking data for the card. The UID card status update data includes an indication of the card number, the updated card status as ‘blocked’ and the corresponding blocking token of the card. The UID blocking engine 142 transmits the card status update data to the authentication server 120. The UID card status update data is received by the communications module 121 and transmitted to the logic module 122 for processing.

[0062] The logic module 122 invokes the verification module 124 to authenticate the status update based on a comparison of the blocking token of the card status update data with the corresponding blocking token of the payment card data stored within card table 129. On successful verification, the logic module 122 updates the card table 129 to set the status of the selected payment card as 'blocked'. Steps 704 to 708 are repeated for each of the selected payment cards represented within the issuer block request data. In other embodiments, the UI blocking engine 142 can be configured to generate UID card status update data and transmit the data to the authentication server 120 in respect of any change to the state of a payment card that is registered with the payment card blocking system 100. For example, the UID card status update data may indicate that a particular payment card has become 'active' after being blocked previously, either as a result of operating the UID card blocking system 100 or otherwise.

Notification

[0063] With reference to Figure 3, the payment card blocking system 100 can be configured to notify the user 102 of the blocking of a particular payment card as a result of a UID blocking operation which nominated that card. At step 308, following the receipt of UID card status update data the authentication server 120 generates UID block notification data to indicate to the user 102 that the issuer 140 has executed a block preventing transactions from being conducted on one or more of the payment cards that were selected at step 307.

[0064] The UID block notification data can be a block notification message of a predetermined form, such as, for example, a UID card block notification SMS or email message. The communications module 121 transmits the UID block notification data to the user 102 via an appropriate protocol based on the form of the block notification message. In some embodiments, user 102 is notified of an unsuccessful request to block a selected payment card, such as when the payment card is already blocked by the issuer 140, or when the issuer 140 cannot block the selected payment card for any other reason.

[0065] The authentication server 120 can be configured to determine that the blocking request has failed if a corresponding UID card status update is not

received within a predetermined “timeout” period commencing from the time when the candidate card data is transmitted to the acquirer 112 (i.e. at step 508). On determination that the blocking of a particular selected payment card has failed, the authentication server 120 can be configured to generate, and subsequently transmit to user 102 via acquirer 112 and payment device 104, a corresponding block notification message indicating the failure of the blocking in respect of the associated UID blocking operation which nominated the card, in accordance with the notification processes described above.

[0066] Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention.

[0067] Throughout this specification, unless the context requires otherwise, the word "comprise", and variations such as "comprises" and "comprising", will be understood to imply the inclusion of a stated integer or step or group of integers or steps but not the exclusion of any other integer or step or group of integers or steps.

[0068] The reference in this specification to any prior publication (or information derived from it), or to any matter which is known, is not, and should not be taken as an acknowledgment or admission or any form of suggestion that that prior publication (or information derived from it) or known matter forms part of the common general knowledge in the field of endeavour to which this specification relates.

CLAIMS

1. A payment card blocking system including an authentication server device, the authentication server device including:

a database configured to store:

user data of a user, including data representing a unique user identification (UID) code and corresponding identification credentials of the user, said unique identification code uniquely identifying the user among all other users of the system, wherein said unique UID code is assigned by an external authority to the user;

payment card data representing one or more payment cards of the user, each payment card being linked to a card entity and issued by an issuing financial institution; and

a memory configured to store program instructions for execution by at least one computer processor to:

receive UID card block initiation data representing the initiation of a card blocking operation to prevent future payment transactions from being conducted with any one of the one or more payment cards of the user;

process the UID card block initiation data to:

i) authenticate the user based on the user data; and;

ii) generate, based on the payment card data, candidate card data representing one or more candidate payment cards of the user for which a card blocking operation can be performed; and

transmit the candidate card data to a payment device, such that selected ones of the one or more of the candidate payment cards are each blocked by the corresponding one or more issuing financial institutions.

2. The system of claim 1, wherein the payment card data of representing each said payment card includes:

the UID of the user;

an identifier of a card entity linked to the payment card;

an identifier of an issuing financial institution of the payment card; and

a blocking token that, when processed by the issuing financial institution of the payment card, indicates the authenticity of a card blocking request in respect of the payment card.

3. The system of claim 2, wherein the blocking token is either a cryptographically generated identifier representing the payment card uniquely to the issuing financial institution or generated by the encryption of the card number via an asymmetric encryption algorithm.

4. The system of any one of claims 1 to 3, wherein the identification credentials of the user includes any one or more of: a PIN code; an OTP code; and one or more biometric identifiers of the user.

5. The system of claim 4, wherein the biometric identifiers of the user include: a finger print; a retina feature pattern; or a facial feature pattern.

6. The system of any one of claims 1 to 5, wherein the authentication server device is configured to register the user by:
receiving user registration data including a specified UID code and identification credentials of the user;
verifying the received specified UID code and identification credentials of the user registration data; and
processing, on positive verification, the user registration data to generate the user data for the user.

7. The system of claim 6, wherein the user registration data includes name and contact information of the user.

8. The system of claim 6, wherein verification of the specified UID code and identification credentials includes providing the specified UID code and the name and contact information of the user to an external authority assigning the UID code to the user, and receiving an authentication response in respect of the identity of the user from said external authority.

9. The system of any one of claims 6 to 8, wherein the user registration data is received from a device of an issuer of a payment card of the user.

10. The system of any one of claims 6 to 9, wherein the authentication server device is further configured to:
receive card registration data to register a payment card of the user; and
process the received card registration data to generate payment card data in respect of the payment card.

11. The system of claim 10, wherein the card registration data includes:
an indication of the card number;
an indication of the UID code of the user;
an indication of the card entity linked to the payment card;
an indication of the issuing financial institution of the payment card;
a blocking token of the payment card that, when processed by the issuing financial institution of the payment card, indicates the authenticity of a card blocking request in respect of the payment card; and
card status data indicating whether the payment card is presently blocked by the corresponding issuing financial institution.

12. The system of claim 11, wherein the candidate payment cards are determined, at least in part, based on the card status data of each of the one or more payment cards of the user.

13. The system of any one of claims 1 to 12, wherein processing the UID card block initiation data to authenticate the user includes: comparing a supplied UID code and supplied identification credentials both of the UID card block initiation data to one or more UID codes and corresponding identification credentials of the user data.

14. The system of any one of claims 1 to 18, wherein the candidate payment card data is transmitted to the payment device via one or more devices of an acquirer of the payment device.

15. The system of claim 14, wherein the payment device is an Automatic Teller Machine (ATM), and where the user selects one or more of the candidate payment cards via interaction with the user interface elements displayed on a terminal of the ATM.

16. The system of either claim 14 or 15, wherein the payment device is configured to generate UID block request data corresponding to a request to block each of the one or more selected payment cards, said UID block request data including payment card data for each of the selected payment cards.

17. The system of claim 16, wherein the UID block request data is processed by a UID block processing device, the processing including:
processing, for each selected payment card, the corresponding card data of the UID block request data to determine the card entity linked to the card;
generating, for each particular card entity determined to be linked to at least one selected payment card, card entity block request data including the card data of each selected payment card linked to that card entity; and
transmitting the card entity block request data to a device each particular card entity.

18. The system of claim 17, wherein the UID block processing device is a device of a nominated card entity and is configured to receive the generated UID block request data from the acquirer.

19. The system of either claim 17 or 18, wherein the card entity block request data is processed by one or devices of the particular card entity to generate issuer block request data for each selected payment card, the issuer block request data representing a request for the issuing financial institution to perform a card blocking operation in respect of the selected payment card.

20. The system of any one of claims 1 to 19, wherein the authentication server is configured to receive UID block update data from a device of the issuing financial institution, said UID block update data indicating an update to the status of one or more of the selected candidate payment cards.

21. A process for blocking a payment card, including:
receiving, at an authentication server device, user identification (UID) card block initiation data representing the initiation of a card blocking operation to prevent future payment transactions from being conducted with any one of one or more payment cards of a user, each payment card being linked to a card entity and

issued by an issuing financial institution;

processing, at the authentication server device, the UID card block initiation data to:

i) authenticate the user based on user data of the authentication server device, the user data including a UID code and corresponding identification credentials of the user, said UID code uniquely identifying the user among all other users of the system, wherein said unique UID code is assigned by an external authority to the user; and

ii) generating candidate card data representing one or more candidate payment cards of the user for which a card blocking operation can be performed, the candidate card data being generated based on payment card data of the authentication server device, said payment card data representing the one or more payment cards of the user; and

transmitting, by the authentication server device, the candidate card data to a payment device, such that selected ones of the one or more of the candidate payment cards are each blocked by the corresponding one or more issuing financial institutions.