



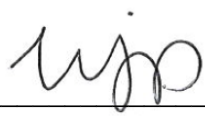
City of New York, State of New York, County of New York

I, Jacqueline Yorke, hereby certify that the document “**5 JP2001-306806**” is, to the best of my knowledge and belief, a true and accurate translation from Japanese into English.

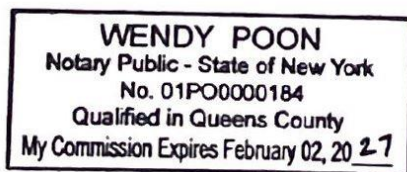


Jacqueline Yorke

Sworn to before me this
November 28, 2023



Signature, Notary Public



Stamp, Notary Public

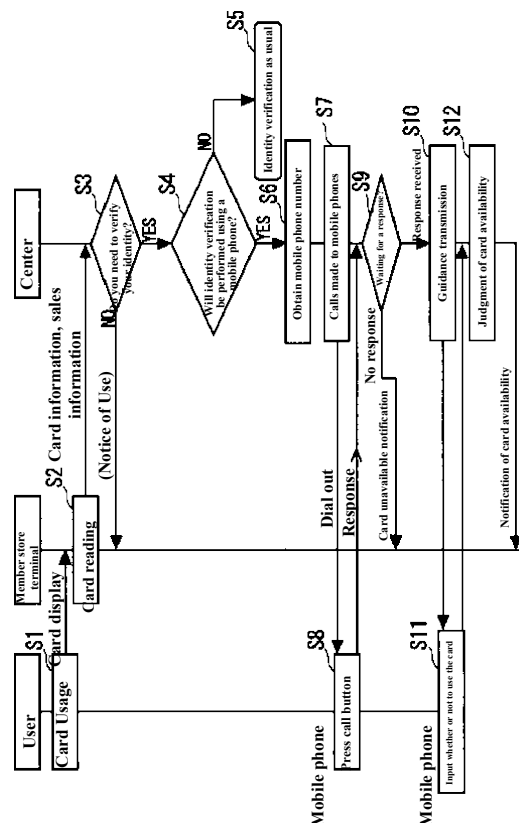
(51) Int.Cl. ⁷ G06F 17/60		Identification codes		FI		Theme Code (Reference)		
		234		G06F	17/60	234A	5B049	
		232				232	5B055	
		242				242		
		414				414		
				Request for Yes review	Number of Claims 30	OL	(21 pages in total)	
(21) Application number Japanese Unexamined Patent Application No. 2000-118673 (P2000 - 118673) (22) Date of application April 19, 2000 (4/19/2000)				(71) Applicant	000004237 NEC Corporation 5-7-1 Shiba, Minato-ku, Tokyo			
				(72) Inventor	Shinichi Kobayashi NEC Corporation, Minato-ku, Tokyo			5-7-1 Shiba,
				(74) Agents	100080816 Patent attorney: Asamichi Kato			
				F term (reference) 5B049 BB11 EE23 GG00 5B055 EE15 HA12 HB07 JJ03 KK05				

(54) [Title of Invention] Method and system for preventing unauthorized card use and recording media

(57) [Summary]

[Problem to be solved] To provide a method and system that can confirm the user's identity when the user uses a card and prevent unauthorized use by a third party.

[Means for solving the problems] When confirming that a card user using a card at a member store has the card, the card company center that received the card number read at the member store terminal will search for the phone number of the mobile communication terminal of the aforementioned user that is registered in advance in the database of the aforementioned center and send it to the mobile communication terminal of the aforementioned card user, and if it is entered from the mobile wireless terminal of the aforementioned user that the card can be used, the use of the aforementioned card will be allowed as if the identity has been confirmed.



[Scope of Claims]

[Claim 1] A method for preventing unauthorized use of a card characterized in that, in confirming that a card user who uses a card at a member store is the member who possesses the card, at a center that receives a card number read by the member store terminal and sent from the member store terminal, based on the card number, search for a mobile communication terminal telephone number of a cardholder that is registered in advance in the storage means of the center, call a mobile communication terminal of a telephone number corresponding to the card number, and allow the use of the card when the mobile communication terminal enters that the card can be used.

[Claim 2] A method for preventing unauthorized use of a card according to Claim 1, characterized in that, when the mobile communication terminal does not respond to the call and when the mobile communication terminal responds to the call enters the fact that card cannot be used, the center determines that identity verification cannot be performed and notifies the member store side that the card cannot be used.

[Claim 3] A method for preventing unauthorized use of a card characterized in that, in confirming that a card user using a card at a member store has the card, at a center that receives a card number read at the member store terminal and sent from the member store terminal, based on the card number, a mobile communication terminal of a cardholder pre-registered in the storage means of the center is called to a mobile communication terminal of a telephone number corresponding to the card number, and when a password is entered from the mobile communication terminal, at the center that receives the password, the password received is matched with a password of a member corresponding to the card number pre-registered in the storage means of the center, and the card is allowed to be used if these passwords are matched.

[Claim 4] A method for preventing unauthorized use of a card according to Claim 3, characterized in that if the called mobile communication terminal does not respond, and the password entered from the called mobile communication terminal does not match the password of a member corresponding to the card number registered in advance in the storage means of the center, it is determined that identity verification is not possible, and the member store is notified that the card is not usable.

[Claim 5] The present invention for preventing unauthorized use of a card is characterized by comprising a four steps in which the center side, which is communicatively connected to member store terminals and manages cards, has a database that stores and holds the telephone numbers of mobile communication terminals owned by the members as personal information of the members, in correspondence with the member's card numbers. When a user uses a card at a member store, the center receives the card number read by the member store terminal, and based on the card number, a first step is to search the database and obtain a telephone number corresponding to the card number; a second step is to make a call from the center to the mobile communication terminal of the obtained telephone number; upon receiving the incoming call from the center to the communication terminal, the user

inputs information corresponding to whether the card can be used from the operation unit of the mobile communication terminal, and the center side allows the card to be used from the mobile communication terminal. If information corresponding to "Acceptable" is received, the identity of the cardholder is confirmed, and a third step is to transmit a notification from the center to the member store terminal that the card can be used. If the called mobile communication terminal does not respond, and if the called mobile communication terminal inputs information that the card cannot be used and the center receives the information that the card cannot be used, a fourth step is to transmit a notification to the member store terminal that the card cannot be used.

[Claim 6] The present invention for preventing unauthorized use of a card is characterized in that the center side, which is connected to the member store terminal and manages the card, associates it with the member's card number and stores it as the member's personal information. A database is provided to store and hold telephone numbers and passwords of mobile communication terminals owned by the members, and when a user uses a card at a member store, the center receives the card number read by the member store terminal. Now, the first step is to search the database based on the card number and obtain a telephone number corresponding to the card number, and the second step is to make a call from the center to the mobile communication terminal of the obtained telephone number; upon receiving the incoming call from the center to the communication terminal, the user makes a call to the mobile communication terminal. When the center side receives the password transmitted from the mobile communication terminal, it compares the received password with the password of the member corresponding to the card number registered in advance in the database, and determines the password. The third step is to compare the card number with the member's password corresponding to the card number, and if the passwords match, the center authorizes the use of the card. If the called mobile communication terminal does not respond, and if the password input from the called mobile communication terminal does not match the password of the member corresponding to the card number registered in advance in the database, the fourth step is to determine that the center cannot confirm the identity and notifying the member store that the card cannot be used.

[Claim 7] A method for preventing unauthorized use of a card according to Claim 6, characterized in that, instead of entering a password from the mobile communication terminal, the user enters a password from the member store terminal, and the entered password is transmitted to the center side via a communication line, and the password is sent to the center side via the communication line, wherein the password is authenticated.

[Claim 8] A method for preventing unauthorized use of a card according to Claim 5, characterized in that a fingerprint input means is provided on the member store terminal side, the user's fingerprint information is input from the fingerprint input

means, and the input fingerprint information is transmitted to the center side via a communication line, the center verifies the identity by comparing the fingerprint information with fingerprint information registered in the database in association with the card number.

[Claim 9] A method for preventing unauthorized use of a card characterized in that, in order to confirm that the card user who uses the card at a member store is the member who owns the card, the center that receives the card number read by the member store terminal and transmitted from the member store terminal checks the card number. Based on the number, search the email address of the card member pre-registered in the storage means of the center and send an email asking whether or not the card can be used. If the user receives a reply email from the mobile communication terminal indicating that the card can be used, permitting the user to use the card.

[Claim 10] A method for preventing unauthorized use of a card characterized in that a device that is communicatively connected to a member store terminal and prevents unauthorized use of a card at the member store, which corresponds to the member's card number and serves as the member's personal information; a storage means provided to store and hold the telephone number of a mobile communication terminal owned by the member, and when the card user uses the card at a member store, the information transmitted from the member store terminal is based on the card number; a means for searching a storage means and acquiring a telephone number corresponding to the card number; a means for automatically making a call to a mobile communication terminal having the acquired telephone number; and a means for responding to an incoming call to the mobile communication terminal, and when the user inputs information indicating that the card can be used from the operation unit of the mobile communication terminal, the input information is received via a wireless communication line and telephone network, and a notification to the effect that the card can be used is sent to the member; a means for transmitting information to a store terminal, and when the mobile communication terminal does not respond, the user inputs information indicating that the card cannot be used from the mobile communication terminal, and the information is transmitted to a wireless communication line and telephone; and a means for transmitting a notification to the member store terminal that the card cannot be used when the card is received via a network.

[Claim 11] A method for preventing unauthorized use of a card characterized in that a device that is communicatively connected to a member store terminal and prevents unauthorized use of a card at the member store, which corresponds to the member's card number and serves as the member's personal information; a storage means provided for storing and retaining a telephone number of a mobile communication terminal owned by the member and a password of the member, and when a card user uses the card at a member store, a means for searching the storage means based on the

card number among information transmitted from the member store terminal and acquiring a telephone number corresponding to the card number; a means for automatically making a call to the mobile communication terminal having the acquired telephone number, and when the password transmitted via the communication line and telephone network is received, the password is compared with the password registered in the storage means in association with the card number, and if the passwords match, the card can be used; a means for transmitting a notification to the member store terminal to the effect that the card cannot be used if the passwords do not match.

[Claim 12] A method for preventing unauthorized use of a card characterized in that a device that is communicatively connected to a member store terminal and prevents unauthorized use of a card at the member store, which corresponds to the member's card number and serves as the member's personal information; a storage means provided to store an email address for a mobile communication terminal owned by the member, and when the card user uses the card at a member store, based on the card number among the information transmitted from the member store terminal, a means for searching the storage means and acquiring an email address corresponding to the card number; a means for automatically sending an email to the obtained email address inquiring whether or not the card can be used, and if the mobile communication terminal retrieves the email sent from the center, and the mobile communication terminal replies with an email indicating that the card can be used, a notification to the effect that the card can be used is sent to the member store terminal; a means for transmitting a notification to the effect that the card cannot be used to the member store terminal when the user replies an email indicating that the card cannot be used from the mobile communication terminal.

[Claim 13] A method for preventing unauthorized use of a card characterized in that a card unauthorized use prevention system in a card authorization system including a member store terminal equipped with a card reading device, and a center communicatively connected to the member store terminal to manage cards, wherein the center reads a member's card information; correspondingly, a database provided that stores and holds the telephone number of the mobile communication terminal owned by the member as the member's personal information, and when the card user uses the card at the member store, the database is sent from the member store terminal; a means for searching the database based on the card number to obtain a telephone number corresponding to the card number; a means for automatically calling the obtained telephone number to the mobile communication terminal; a means for transmitting guidance information to the mobile communication terminal instructing the user to input whether or not a card can be used when the user goes off-hook after receiving an incoming call notification to the mobile communication terminal, and when the member inputs information indicating that the card can be used from the

operation unit of the mobile communication terminal, the member receives the card usage information via a wireless communication line and telephone network, and sends a notification that the card can be used to the member; a means for transmitting a notification that the mobile communication terminal does not respond to a call from the center; and a means for the user to operate the mobile communication terminal, and when information indicating that the card cannot be used is input from the department and the card cannot be used is received via a wireless communication line and a telephone network; and a means for controlling to send a notification to the effect that the card cannot be used to the member store terminal.

[Claim 14] A method for preventing unauthorized use of a card characterized in that a card unauthorized use prevention system in a card authorization system including a member store terminal equipped with a card reading device, and a center communicatively connected to the member store terminal to manage cards, wherein the center reads a member's card information; correspondingly, a database provided that stores and holds the telephone number of the mobile communication terminal owned by the member as the member's personal information, and when the card user uses the card at the member store, the database is sent from the member store terminal; a means for searching the database based on the card number to obtain a telephone number corresponding to the card number; a means for automatically calling the mobile communication terminal having the acquired telephone number; a means for transmitting guidance information to the mobile communication terminal instructing the user to input a password when the user goes off-hook after receiving an incoming call notification to the mobile communication terminal, and when a password is input from the operation unit of a mobile communication terminal, the password transmitted via a wireless communication line and a telephone network is received, the database is referred to from the password, and the password is registered corresponding to the card number; a means for transmitting a notification to the member store terminal that the card can be used if the passwords match as a result of the verification; a means for the mobile communication terminal to respond to a call from the center, and a means for controlling to send a notification to the effect that the card cannot be used to the member store terminal when there is no response and when the passwords do not match as a result of the password verification.

[Claim 15] A method for preventing unauthorized use of a card characterized in that a card unauthorized use prevention system in a card authorization system including a member store terminal equipped with a card reading device, and a center communicatively connected to the member store terminal to manage cards, wherein the center reads a member's card information; correspondingly, a database provided to store and hold email addresses for mobile communication terminals for members who own mobile communication terminals equipped with email sending/receiving functions as the member's

personal information, and card users can access member stores; a means for searching the database based on the card number among the information sent from the member store terminal when using the card to obtain an email address corresponding to the card number; a means for automatically sending an email inquiring as to whether the card can be used, and If the user retrieves the email sent from the center using the mobile communication terminal and replies with an email from the mobile communication terminal indicating that the card can be used, a notification to the effect that the card can be used is sent to the member; a means for transmitting to a store terminal, and if there is no response from the mobile communication terminal, or if an email indicating that the card cannot be used is returned from the mobile communication terminal, a notification to the effect that the card cannot be used is sent to the store terminal; and a means for controlling transmission to a member store terminal.

[Claim 16] A method for preventing unauthorized use of a card according to any one of Claims 13 to 15 characterized in that the database includes an area for recording whether or not identity verification is performed by calling a mobile communication terminal when using a card, and the setting of whether or not identity verification is performed by calling a mobile communication terminal is freely changed.

[Claim 17] A method for preventing unauthorized use of a card according to Claim 13 or 14 characterized in that a fingerprint input device is connected to the member store terminal and inputs fingerprint information, and the fingerprint information of the user is input from the fingerprint input device, and the input fingerprint information is transmitted from the member store terminal to the communication line. The fingerprint information is sent to the center via the above, and the center stores the fingerprint information in the database. Identity verification is performed by comparing fingerprint information registered in association with the card number.

[Claim 18] A method for preventing unauthorized use of a card according to Claim 14 characterized in that the member store terminal is provided with a password input means, and instead of inputting a password from the mobile communication terminal, the user inputs a password from the password input means of the member store terminal, and the input password is used for communication. The password is sent to the center via a line, and the center receives the password, refers to the database from the password, and compares it with the password registered corresponding to the card number.

[Claim 19] A method for preventing unauthorized use of a card characterized in that a database that is communicatively connected to a member store terminal equipped with a card reading device and that stores and maintains the telephone number of the mobile communication terminal as the member's personal information in correspondence with the member's card number at a card management center, which is equipped with: (a) when a card user uses a card at a member store, a process of searching the database based on the card number among the information sent from the member store

terminal and obtaining a telephone number corresponding to the card number; (b) a process of automatically calling the mobile communication terminal having the acquired telephone number; (c) when the user goes off-hook after receiving an incoming call notification to the mobile communication terminal, a means for transmitting guidance information to the mobile communication terminal instructing the user to input whether or not the card can be used; and (d) when the user inputs information indicating that the card can be used from the operation unit of the mobile communication terminal, the user receives the card usage information via a wireless communication line and telephone network, and receives a message indicating that the card can be used. A notification is sent to the member store terminal, and on the other hand, when the user inputs information indicating that the card cannot be used from the operation unit of the mobile communication terminal, the information is transmitted via the wireless communication line and telephone network and send a notification to the member store terminal to the effect that the card cannot be used in response to the request, and record a program for causing each of the processes (a) to (d) above to be executed on the computer of the center.

[Claim 20] A method for preventing unauthorized use of a card characterized in that a database that is communicatively connected to a member store terminal equipped with a card reading device and that stores and maintains the telephone number of the mobile communication terminal as the member's personal information in correspondence with the member's card number at a card management center, which equipped with: (a) when a card user uses a card at a member store, a process of searching the database based on the card number among the information sent from the member store terminal and obtaining a telephone number corresponding to the card number; (b) a process of automatically calling the mobile communication terminal having the obtained telephone number; (c) a process of using the card when the user goes off-hook after receiving an incoming call notification to the mobile communication terminal; and (d) when the user inputs information indicating that the card can be used from the operation unit of the mobile communication terminal, the card usage information is received via a wireless communication line and a telephone network, and a notification to the effect that the card can be used is sent to the member store terminal, while the user receives the information from the operation unit of the mobile communication terminal. When entering information indicating that the card cannot be used, the information is received via a wireless communication line and telephone network, and a recording medium have recorded thereon a program for causing a computer at the center to execute each of the processes (a) to (d), including the process of transmitting a notification that the card cannot be used to the member store terminal.

[Claim 21] A method for preventing unauthorized use of a card characterized in that at a center that is communicatively connected to a member store terminal equipped with a card reading device and manages the card, a mobile communication

terminal equipped with an email sending and receiving function is associated with the member's card number as the member's personal information, which is equipped with a database that remembers and maintains member email addresses: (a) a process of acquiring the email address corresponding to the card number when a card user uses a card at a member store, the database is searched based on the card number among the information sent from the member store terminal; (b) a process of automatically sending an email to the email address inquiring whether the card can be used; and (c) the user retrieves the email sent from the center with the mobile communication terminal, and when the communication terminal replies with an email indicating that the card can be used, a notification to the effect that the card can be used is sent to the member store terminal, and on the other hand, if the user replies from the mobile communication terminal with an email indicating that the card cannot be used, a notification to the effect that the card cannot be used is sent, and a recording medium have recorded thereon a program for causing a computer at the center to execute each of the processes (a) to (c), including the process for transmitting to the member store terminal.

[Claim 22] A recording medium according to any one of Claims 19 to 21 characterized in that the user's fingerprint information input from a fingerprint input device connected to the member store terminal is transmitted from the member store terminal to the center side via a communication line, and the center side reads the fingerprint information, and a recording medium is used to store a program for causing a computer at the center to execute a process of verifying the identity of the person by comparing the fingerprint information registered in the database in association with the card number.

[Detailed description of invention]

[0001]

[Technical field to which the invention pertains] The present invention relates to a method and system for preventing unauthorized use of cards, and in particular to a method, system, and recording medium suitable for preventing unauthorized use of cards such as credit cards used by card members for product payment, financing, etc.

[0002]

[Prior art] Credit cards are widely used as the third currency after cash and checks, and credit card businesses are currently used in a wide variety of industries, including credit sales, banking, retail, and oil. Also, there are currently proposals to standardize (unify) credit cards, cash cards, and debit cards.

[0003] When using a credit card, a card member presents his or her credit card to a member store, has the member store's terminal (card authorization terminal) read the credit card, and the terminal receives credit card information, sales details, etc. The information is transmitted online via a communication line to a host computer at the card management center of the card company, and authorization is performed as necessary, such as checking the creditworthiness of the credit card.

[0004] If there is no problem with the above authorization result and the card can be used, the card user completes a series of product purchase procedures using the card by filling in the signature in the designated area on the usage statement slip. The price for the product is paid by a credit card company, etc., and later, the price is debited from the user's bank account along with a predetermined fee.

[0005]

[Problems to be solved by the invention] By the way, as long as a credit card is genuine, it can be used fraudulently by someone other than the cardholder, and members whose credit card is used without permission due to loss or theft will suffer a loss. Furthermore, even if a counterfeit credit card is used, if authorization is passed, the counterfeit credit card can be used for fraudulent purchases, loans, etc., resulting in losses for the card company.

[0006] As a security control against unauthorized use of these cards, the following steps are typically taken to confirm the identity of the user when using the card.

[0007] In other words, if a credit card company detects that a card user uses a credit card to purchase products exceeding a predetermined amount, a representative from the credit card company will contact the member store by phone, and when a card user answers the phone at a member store, a staff member asks a number of questions based on the member's personal information to confirm the card user's identity. This question is usually a question that only the user himself or herself can answer immediately and naturally, such as the user's work phone number.

[0008] If the card user is able to correctly respond to the questions asked by the person in charge, it is confirmed that the card user is the member holding the card, and as a result, the use of the card (payment by card) is permitted.

[0009] However, when a card user purchases a product, it can be said that it is inefficient in terms of man-hours for a credit card company representative to ask card users questions to verify their identity over the phone while looking at member information and the like.

[0010] Since the number of credit card transactions is expected to increase dramatically in the future, it is desirable to automate and save labor in the identity verification work performed by credit card companies without reducing the accuracy of identity verification.

[0011] Furthermore, the conventional identity verification process described above does not allow card users to suspect themselves until their identity is confirmed by the credit card company or sales staff at member stores. This could lead to the user feeling that the card is being used, and there is a possibility that the card user may be offended. As a result, sufficient customer satisfaction (CS) may not be provided, and sales promotion activities may have the opposite effect.

[0012] Therefore, the present invention has been made in view of the above problems, and its main purpose is to provide a method, device, system, and recording medium that facilitate the work of confirming on the center side that a card user is the member holding the card and prevent unauthorized use by a

third party.

[0013] Another objective of the present invention is to provide methods, devices, systems, and recording media that contribute to sales promotion activities while maintaining high security while preventing the increase in development costs and capital investment and reducing the burden on member stores and card companies in order to prevent card fraud.

[0014]

[Means for solving the problems] In order to confirm that the card user using the card at the member store is the member who possesses the card, the present invention permits the use of the card at a center that receives the card number read by the member store terminal and sent from the member store terminal, based on the card number, to search for the phone number of the mobile communication terminal of the card holder that is registered in advance in the storage means of the center, to call the mobile communication terminal of the phone number corresponding to the card number, and when the said mobile communication terminal enters the fact that the card can be used.

[0015] In the present invention, if the called mobile communication terminal does not respond or if the card cannot be used from the called mobile communication terminal is input, it is determined that the identity cannot be confirmed, and the member store side is notified that the use of the card is not permitted.

[0016] In the present invention, a password may preferably be entered from the mobile communication terminal of the card user, and the password may be compared with a password registered in the storage device of the center to allow the use of the card if the password matches.

[0017] Furthermore, in the present invention, a password may be entered from a member store terminal, or a fingerprint of a card user may be entered, and the fingerprint information may be verified at the center by comparing it with the characteristic information registered in the database. And as will be apparent from the following description, the above objectives are similarly achieved by the invention described in each claim of the claims.

[0018]

[Embodiments of the present invention] The embodiments of the present invention are described below. In a preferred embodiment of the present invention, an authorization database installed at a card company center that is communicatively connected to member store terminals is stored as personal information of card members in correspondence with card numbers (card IDs), and the telephone number of a mobile communication terminal such as a mobile phone or a PHS (Personal Handy Phone System) terminal owned by the card member is registered.

[0019] During the card creation procedure, the user enters the telephone number of the mobile communication terminal owned by the user as necessary information on the application form when creating the card. As a result of the examination of the application by the card company, if card issuance is

approved for the user, this telephone number is registered in the card company's database as member personal information in association with a card number (ID) for uniquely identifying the issued card. The password on the application form is also linked to the card number (ID) and registered in the database. If there is a change in the telephone number of the mobile communication terminal held by the cardholder, the cardholder shall notify the card company to that effect, and the contents of the center database shall be updated.

[0020] In addition, in order to prevent unauthorized use of the card, it shall be possible to select whether to perform identity verification processing by calling the mobile communication terminal at the time of card creation, and after the card creation, it may be possible to change the setting of whether to perform identity verification processing by calling the mobile communication terminal. If identity verification is not performed by calling the mobile communication terminal when using the card, identity verification will be performed using the conventional procedure. For this reason, members who do not possess mobile communication terminals can use the card.

[0021] When a user uses a card at a member store, the center uses the card number from among the information sent from the member store terminal to the center to confirm the identity of the user by calling the mobile communication terminal from the database. If the mode is set to confirm the identity by calling a mobile communication terminal when using the card, the database is searched for the telephone number corresponding to the card number.

[0022] At the center, a call will be made to the searched phone number. In this case, preferably, the retrieved telephone number (outgoing telephone number) is set in an automatic dialing device to automatically call the mobile communication terminal.

[0023] When a user goes off-hook (i.e. presses the call button) after receiving an incoming call notification (ringing or vibrating) to the mobile communication terminal owned by the user, a notification is sent to the mobile communication terminal via voice guidance or text display, asking it to respond as to whether or not the card can be used.

[0024] When a user enters card-usable information from the operation unit of the mobile communication terminal, the center that receives this determines that identity verification has been performed, and sends a card-usable notification to the member store.

[0025] On the other hand, the mobile communication terminal does not respond to the call from the center to the mobile communication terminal, and if necessary, if the call still cannot be established even after a predetermined retry, the member store is notified that the card cannot be used.

[0026] In addition, when the user inputs information that the card cannot be used from the operation unit of the mobile communication terminal, the center that receives this information sends a notification that the card cannot be used to the member store terminal.

[0027] For example, if a third party steals a card of a card

holder and uses it illegally, or uses a counterfeit card, the card holder can recognize that someone other than he or she is using his or her card illegally by receiving a call from the card company's center, and enters the card non-usable information from the mobile communication terminal to inform the center.

[0028] In one embodiment of the present invention, the information input from the mobile communication terminal indicating that the card can be used may be a code specified by guidance notified by the mobile communication terminal.

[0029] In other words, in this embodiment, the card user has a mobile communication terminal with a previously registered telephone number when using the card in accordance with the contract (card usage rules), and the card user responded to a call from the center to the mobile communication terminal, and entered the card usage, so it is assumed that the user's identity has been verified. The card member selects the mobile phone identity verification mode after understanding that the card member will use the mobile phone to verify his or her identity when using the card to pay for products exceeding a specified amount, such as in the contract at the time of card creation. Furthermore, since many people own mobile phones today, it can be said that there is almost no burden on users for owning a mobile phone.

[0030] In order to further increase security, when a user goes off-hook after receiving a notification of an incoming call to a mobile communication terminal, the user is prompted to enter the password by voice guidance or text display on the mobile communication terminal. A notification is sent to the terminal, and the user who recognizes the notification enters a password of a predetermined number of digits from the mobile communication terminal. This password may be sent to the center, and the center may verify the user's identity by comparing it with a password registered in a database.

[0031] Furthermore, in another embodiment of the present invention, instead of inputting a password from a mobile communication terminal, a password may be input from a member store terminal, and the password may be transmitted to the center side via a communication line. In this case as well, security can be improved by combining the system with a system that sends a call to a mobile communication terminal and receives a response to verify the identity of the person when using the card.

[0032] Furthermore, in another embodiment of the present invention, the member store terminal is provided with a fingerprint input means, the user's fingerprint information is input from the fingerprint input means, and the input fingerprint information is transmitted via a communication line. The fingerprint information may be transmitted to the center side and checked against fingerprint information registered in the database corresponding to the card number to confirm the identity. Currently, devices have been developed that perform authentication by fingerprint comparison instead of entering a user ID and password when logging into a computer, and since the time required for fingerprint comparison is also shortened, it can be said to be effective for identity verification.

[0033] Furthermore, in another embodiment of the present invention, in order to confirm that the card user who uses the card at the member store is the member who owns the card, a card number transmitted from the member store terminal is received. Based on the card number, the center searches the card member's email address pre-registered in the center's database and sends an email asking whether the card can be used, and the user activates the email sending and receiving function. If a reply email indicating that the card can be used is received from a mobile communication terminal equipped with the card, the card may be permitted to be used.

[0034] In the embodiment described above, even if the card user is the actual card user, when using the card, if the call to the mobile communication terminal owned by the card member is not successful and the identity cannot be confirmed, the conventional method is used. Since the identity verification work will be performed through the processing procedure, no inconvenience (occurrence of a situation such as the card becoming unusable) on the user side will occur due to the introduction and operation of the system of the present invention.

[0035] In one embodiment of the present invention, a center that is communicatively connected to a member store terminal equipped with a card reading device and manages cards stores information in the member's possession as the member's personal information in correspondence with the member's card number. It is equipped with a database that stores and maintains the telephone numbers and passwords of mobile communication terminals in possession, and (a) when a card user uses a card at a member store, a process of searching the database based on the card number among the information sent from the member store terminal to obtain a telephone number corresponding to the card number; (b) a process of automatically calling the mobile communication terminal having the obtained telephone number; (c) a process of automatically calling the mobile communication terminal with the obtained telephone number; a process of transmitting guidance information to the mobile communication terminal instructing the user to input whether the card can be used; and (d) when the user inputs the card usage permission from the mobile communication terminal, the card usage information is received via a wireless communication line and a telephone network, and a notification to the effect that the card can be used is sent to the member store terminal. On the other hand, when the user inputs information that the card cannot be used from the mobile communication terminal, a process of receiving the card unusable information via a wireless communication line and a telephone network and transmitting a notification to the member store terminal that the card cannot be used is executed. Each of the processes (a) to (d) above is realized by executing a program on a computer at the center.

[0036] In another embodiment of the present invention, a center that is communicatively connected to a member store terminal equipped with a card reading device and manages cards stores information about the member as the member's personal information in correspondence with the member's

card number. It is equipped with a database that stores and maintains the telephone numbers and passwords of mobile communication terminals in possession, and (a) when a user uses a card at a member store, based on the card number among the information sent from the member store terminal, a process of searching the database to obtain a telephone number corresponding to the card number; (b) a process of automatically calling the mobile communication terminal having the acquired telephone number; (c) a process of transmitting guidance information to the mobile communication terminal instructing the user to input a password when the user goes off-hook after receiving an incoming call notification to the mobile communication terminal; and (d) when the user inputs a password from the operation unit of the mobile communication terminal, the password transmitted via the wireless communication line and telephone network is received, the database is referred to from the password, and the card number is entered. The card is compared with the correspondingly registered password, and if they match, a notification to the effect that the card can be used is sent to the member store terminal, and if the passwords do not match, a process of transmitting a notification to the effect that the card cannot be used to the member store terminal is executed. Each of the processes (a) to (d) above is realized by executing a program on a computer at the center.

[0037] In yet another embodiment of the present invention, a center that is communicatively connected to a member store terminal equipped with a card reading device and manages cards sends an email message as the member's personal information in correspondence with the member's card number. It is equipped with a database that stores and retains the email addresses of members who own mobile communication terminals equipped with sending and receiving functions, and (a) when a card user uses a card at a member store, the database is searched based on the card number among the information sent from the member store terminal, and the email address corresponding to the card number is obtained; (b) a process of automatically sending an email to the email address inquiring about whether or not the card can be used; and (c) if the user retrieves the email sent from the center with the mobile communication terminal and replies with an email from the mobile communication terminal indicating that the card can be used, a notification to the effect that the card can be used is sent to the member store. On the other hand, if the user returns an email indicating that the card cannot be used from the mobile communication terminal, a process of transmitting a notification to the effect that the card cannot be used is executed to the member store terminal. Each of the processes (a) to (c) above is realized by executing a program on a computer at the center.

[0038] In the above embodiment, the present invention can be implemented by reading and executing the program from a recording medium (FD (floppy (registered) disk), CD-ROM, DVD (digital versatile disk), HDD (hard disk medium), magnetic tape, semiconductor memory, etc.) that records a program to be executed by a center computer, or by

downloading and installing the program from a remote server device, etc., to a center computer via a communication medium. [0039]

[Example] In order to describe the above-described embodiments of the present invention in further detail, examples of the present invention will be described with reference to the drawings.

[0040] FIG. 1 is a diagram showing a system configuration of an embodiment of the present invention. Referring to FIG. 1, one embodiment of the present invention includes a member store terminal 2 equipped with a credit card reading device, and a credit card company center 1 connected to the member store terminal 2 via a communication line 3 to manage cards. The credit card company center 1, which is connected to the member store terminal 2, is connected, for example, by a dedicated communication line 3, but in addition to a ground network such as a public network, it may be connected by a satellite communication line, etc. Note that although one member store terminal 2 is shown in FIG. 1 for simplicity, a plurality of member store terminals 2 are normally connected to the center 1. As the member store terminal 2 equipped with a credit card reading device, a terminal with a well-known configuration is used, and in this embodiment, the existing terminals at member stores are used as they are.

[0041] A summary of the processing operation of an embodiment of the present invention is as follows.

[0042] When the user 7 uses the card to pay for products purchased at a member store, the user 7 hands the card 8 of the member store to a clerk (not shown) at the member store, and the card information is read by the member store terminal 2. The card information and sales information are transmitted from the member store terminal 2 to the center 1 via the communication line 3.

[0043] The center 1 searches for the pre-registered phone number of the user's mobile phone from the card number sent from the member store terminal 2, and makes a call to the user's mobile phone 6.

[0044] A call from the center 1 arrives at the mobile phone 6 of the user 7 via the telephone network 4 and a wireless base station 5 that manages the zone of the mobile phone 6. When the user responds to the incoming call notification on the mobile phone 6 and connects to the call, and inputs from the mobile phone 6 that the card can be used, the card is allowed to be used.

[0045] Although a mobile phone will be described as an example of a mobile communication terminal owned by a user, it is of course possible to use a PHS (Personal Handy-Phone System) terminal (simple mobile phone).

[0046] FIG. 2 is a diagram showing an example of the configuration of the center 1 in an embodiment of the present invention. It should be noted that FIG. 2 only shows the components of the center 1 related to the card fraud prevention function, which is the main part of the present invention, and other components are omitted.

[0047] Referring to FIG. 2, the center 1 in one embodiment of the present invention that associates each member with a card

number (ID) and stores the member's mobile phone number includes: a database 12 in which passwords etc. are registered; a communication line interface 18 that provides an interface for transmitting and receiving data via a communication line 3 between the member store terminal 2, and a card sent from the member store terminal 2; a card number acquisition unit 10 that receives card information from a communication line interface 18 that receives card information transmitted from the member store terminal 2 and acquires a card number; a card number acquisition unit 10 that receives card information and acquires a card number; an identity verification necessity determination unit 11 that searches a database 12 based on the card number and checks whether the mode is set to perform identity verification using a mobile phone from the record data corresponding to the card number; a mobile phone number acquisition unit 13 that acquires a phone number corresponding to the card number from the database 12 and a telephone terminal interface 15; a telephone call/response control unit 14 that automatically makes a call to the card user's mobile phone based on the phone number passed from the mobile phone number acquisition unit 13, and manages responses from the card user's mobile phone, guidance transmission, etc.; a card usage permission determination unit 16 that determines whether the card can be used based on input information from the operation unit of the card user's mobile phone 6, and the determination result of the card usage permission determination unit 16 is transmitted via the communication line interface 18; and a card usage permission notification unit 17 that transmits the information to the member store terminal 2. The processing and functions of each of the above-mentioned parts in the center 1 are realized by program control executed on a computer in the center 1. Note that the communication line 3 may be a telephone network.

[0048] When the mobile phone 6 responds to a call from the center 1 to the mobile phone 6 (see FIG. 1) and information indicating that the card can be used is input, the information that the card can be used is received via the telephone network 4. Based on the information from the telephone call/response control unit 14, the card usage permission determination unit 16 determines that the card can be used.

[0049] On the other hand, if information indicating that the card cannot be used is input from the mobile phone 6, or, if the mobile phone 6 does not respond to a call to the mobile phone 6 (including out of service area, power off, etc.), the card usage permission determining unit 16 sets the card usage to be disabled. The telephone call/response control unit 14 has a timeout management function for receiving an incoming response to a call from the mobile phone 6.

[0050] In addition, when creating a card, the user must indicate on the application form whether or not to use a mobile phone to verify their identity, and if they wish to use a mobile phone to verify their identity, the telephone number and password of the mobile phone possessed by the user are recorded in the database 12, and the telephone number of the mobile phone and, if necessary, the password are also associated with the card

number (ID) and registered in the database 12.

[0051] Cardholders who already have a card can receive the service of the system according to the invention by simply notifying the card company of the mobile phone number owned by the cardholder, and there is no need to issue a new card, etc.

[0052] FIG. 3 is a diagram schematically showing an example of the configuration of the database 12 that manages card members in an embodiment of the present invention. Referring to FIG. 3, in addition to the card number (identification information) and personal information such as the card member's name, gender, age, and address, each entry includes information on whether or not to use a mobile phone to verify the identity of the member when using the card, the phone number of the member's mobile phone if the member's identity is verified using the mobile phone, and password information. The database 12 also includes card usage history information and various information for checking creditworthiness, but these pieces of information are omitted because they are not directly related to the subject matter of the present invention.

[0053] FIG. 4 is a diagram for explaining the processing flow of the user 7 (mobile phone 6), member store terminal 2, and center 1 in one embodiment of the present invention. The operation of one embodiment of the present invention will be described with reference to FIGS. 1 to 4.

[0054] When the user 7 uses a card at a member store (step S1), the member store terminal 2 reads the card (step S2), and card information and sales information are transmitted to the center 1.

[0055] The center 1 receives information from the member store terminal 2, and if, for example, the amount to be used is low and identity verification is not required, the center 1 notifies that the card can be used and performs the card payment process as usual (NO in step S3).

[0056] On the other hand, in the case of paying a large amount by card, the center 1 refers to the database 12 and checks whether the mode is set to perform identity verification using a mobile phone when using the card based on the card number (step S4). If the mode is not set to perform identity verification using a mobile phone, the person in charge at Center 1 calls the user to the telephone set up at the member store and performs identity verification, etc., as usual (step S5).

[0057] When set to a mode in which identity verification is performed by a mobile phone, the phone number of the mobile phone registered corresponding to the card number is searched and obtained from database 12 (step S6), and the phone number of the mobile phone is automatically dialed (step S7).

[0058] If the user presses the call button (off-hook) in response to the ringing, etc., of the mobile phone 6 (step S8), the center 1 receives this response ("response received" in step S9) and sends guidance (step S10). The guidance may be audio or text information. For example, in the case of voice guidance, guidance information such as "Thank you for using our credit card. If the card can be used for the current transaction, please enter permission to use it". The storage and transmission

control of this guidance information is performed by the telephone call and response control unit 16 and the telephone terminal interface 15.

[0059] This guidance information may include store information of the member store where the card is used. If the card user is someone other than the cardholder, the cardholder can recognize from this guidance information that the card has been fraudulently used and the location thereof.

[0060] The user enters the card acceptability input (number and #, etc. agreed with the card company) from the mobile phone 6 (Step S11). The input information indicating whether the card can be used or not may be a number determined at the time of card creation (for example, 1 for usable and 0 for unusable), or a predetermined operation button.

[0061] The center 1 judges the card usage permission information transmitted from the mobile phone 6, determines whether the card can be used (step S12), and notifies the member store terminal 2 of the determination result of the usage permission.

[0062] By the way, for users who have used this system many times and are already accustomed to inputting whether or not a card can be used using a mobile phone, and who do not need notification of detailed guidance, the guidance information may be simplified or omitted. Whether guidance is necessary or unnecessary for each member is registered and managed as appropriate for each member in the database 12 of the center 1.

[0063] When the user 7 enters information on whether the card can be used from mobile phone 6, a notification that the identity of the customer has been confirmed (a notification that the card can be used) is sent to the member store terminal 2, and payment can be made using the card. In other words, the user signs the detailed slip and completes the product purchase process using the card.

[0064] On the other hand, as a result of waiting for an incoming call response in step S9 of FIG. 4, if there is no response from the mobile phone 6 due to a timeout or the like (including cases where the call cannot be made due to out of service area, power off, etc.), the center 1 notifies the subscriber terminal 2 that the card cannot be used.

[0065] In one embodiment of the invention, if the user is the cardholder and the user is not carrying a mobile phone at the time of using the card or is unable to respond due to a dead battery, etc., the card can be used after the card company has verified the customer's identity using the conventional method via the member store's telephone or the like. In addition, in the above embodiment, an explanation was given of a configuration in which an automatic call is made to the phone number of a mobile phone retrieved from the card number, but an operator etc. can manually call the phone number of the mobile phone retrieved from the card number. Of course, the present invention can also be applied to business operations in which calls are made to a mobile phone.

[0066] Next, a second embodiment of the present invention will be described. In the second embodiment of the present invention, the card user inputs a password from the mobile

phone 6 in response to a call made from the center 1 to the mobile phone 6 for identity verification. In the second embodiment of the present invention, the basic configuration of the system is similar to that shown in FIG. 1.

[0067] FIG. 5 is a diagram showing the configuration of the center 1 in the second embodiment of the present invention. Referring to FIG. 5, in the second embodiment of the present invention, the card usage permission determination unit 16 of the first embodiment is replaced with a password authentication unit 19. In the second embodiment of the invention, The identity verification necessity determination unit 10, the identity verification necessity determination unit 11, the mobile phone number acquisition unit 13, and the telephone call/response control unit 14 are basically the same as those of the first embodiment. The processing and functions of each of the above-mentioned parts in the center 1 are realized by program control executed on a computer in the center 1.

[0068] In a second embodiment of the present invention, the card company center 1, which received the card number read at the member store terminal 2, automatically dials the phone number of the user's mobile phone 6, and when a predetermined number of digits of the password is entered from the mobile phone 6, the telephone terminal interface 15, which received the password as a PB (push button) signal from the telephone network 4, supplies the received password (converted to a text code) to the password authentication unit 19 via the telephone call and response control unit 14.

[0069] The password authentication unit 19 compares the received password with the password registered in the database 12 corresponding to the card number, and if they match, it is determined that the user's identity has been verified and that the card can be used.

[0070] On the other hand, if the passwords do not match, the password authentication unit 19 transmits guidance such as inputting a predetermined number of retries to the mobile phone 6 via the telephone call/response control unit 14, and the password input and verification process are performed again. If the passwords still do not match even after retry the entry, it is determined that the card cannot be used. Based on the determination result of the password authentication unit 19, the card usage permission notification unit 17 notifies the member store terminal 2 whether the card can be used or not.

[0071] FIG. 6 is a diagram for explaining the processing flow of the user 7 (mobile phone 6), the member store terminal 2, and the center 1 in the second embodiment of the present invention. In FIG. 6, description of the same processing as in FIG. 4 will be omitted, and differences will be described below.

[0072] When the center 1 makes a call to the mobile phone 6 (step S7) and the mobile phone 6 is on-hook and a response is received, the center 1 transmits guidance information regarding password input to the mobile phone 6 (step S10). The user enters a password (for example, a 4-digit number) from the operation section of the mobile phone 6, and the password is sent to the center 1. The password authentication unit 19 verifies the password (step S14), and if the authentication is OK (step S15), the center 1 notifies the member terminal 2 that the

card can be used.

[0073] If the password does not match even after a predetermined number of retry attempts, the password authentication unit 19 determines that the password authentication is NG (not possible) (NO in step S15), and a notification that the card cannot be used is notified to the member store terminal 2.

[0074] As described above, in the second embodiment of the present invention, when the user 7 receives an incoming call notification on the mobile phone 6 and goes off-hook, the user 7 is prompted to enter the password by voice guidance or text display on the mobile phone. A notification is sent to the telephone 6, and the user who recognizes the notification enters a password of a predetermined number of digits from the mobile phone 6. This password is sent to the center 1, and the center 1 stores this password in the database 12. The user's identity is verified by comparing the user's password with the password registered in the , improving security.

[0075] In addition, in each of the above embodiments, as the member store terminal, it is possible to use an existing terminal as it is, which prevents an increase in development costs and an increase in the burden on the member store when implementing the present invention.

[0076] The present invention can be modified in various ways other than the above embodiments. As an example of a modification, a third embodiment of the present invention will be described. The third embodiment of the present invention is a modification of the second embodiment of the present invention, in which the user is authenticated using a password input from the member store terminal. FIG. 7 is a diagram for explaining a third embodiment of the present invention.

[0077] Referring to FIG. 7, when the user 7 uses the card, the process from receiving the card information obtained from the card reader of the member store terminal 2 at the center 1 to calling the mobile phone 6 of the user 7 is the same as in the previous embodiment. When the user 7 answers the incoming call to the mobile phone 6 and inputs that the card can be used, a first stage of identity verification is performed, and at this point, the call connection between the center 1 and the mobile phone 6 is disconnected.

[0078] Then, the user 7 inputs his or her own password from the password input unit 21 such as the keyboard or numeric keypad of the member store terminal 2. The password information is sent to the center 1 and checked against passwords registered in the database 12.

[0079] Next, a fourth embodiment of the present invention will be described. In the fourth embodiment of the present invention, the user's identity is authenticated by comparing fingerprint information registered in advance at the center 1 at the time of card creation or the like. FIG. 8 is a diagram for explaining a fourth embodiment of the present invention.

[0080] When using the card, the user 7 places a predetermined finger on the fingerprint input device 22 and inputs a fingerprint instead of inputting a password as in the third embodiment. The predetermined feature information is

extracted within the fingerprint input device 22 from the fingerprint information (image information) input from the fingerprint input device 22, and the extracted feature information is transmitted to the center 1, and is stored in the database 12 of the center 1. The card number is compared with the characteristic information of the fingerprint registered as personal information to confirm the identity of the individual. It should be noted that an image input device is provided as the fingerprint input device 22, and image information of the fingerprint acquired by the image input device is transmitted to the center 1. The center 1 may perform a fingerprint matching process based on the received fingerprint image information.

[0081] When the amount of payment using a credit card or the like is large, security management is improved by using a combination of mobile phone calls, fingerprint verification, etc.

[0082] Next, a fifth embodiment of the present invention will be described. FIG. 9 is a diagram showing the configuration of a fifth embodiment of the present invention. Referring to FIG. 9, in a fifth embodiment of the present invention, if a cardholder has a mobile phone or PHS terminal equipped with an email function, the center 1 will send an email asking whether or not the card can be used to confirm the cardholder's identity. If the user sees this email and sends a reply email to the center 1, the user will be permitted to use the card.

[0083] Referring to FIG. 9, the mobile phone 6 accesses a server (a mail server such as an SMTP (Simple Mail Transfer Protocol) server and a POP server, a DNS server) 51 and the Internet 9 via a wireless base station 5. Note that in the wireless packet service, the wireless base station 5 is connected to the Internet via a packet control device, gateway, and router (not shown)..

[0084] In order to confirm that the user 7 who uses the card 8 at a member store is the member who owns the card, the center 1 receives the card number sent from the member store terminal 2. Based on the card number, the email address of the cardholder registered in advance in the database of the center 1 is searched, and an email containing an inquiry as to whether or not the card can be used is sent to the email address.

[0085] The user 7 retrieves the received mail from a mail server (not shown) using a mobile phone 6 equipped with an email sending/receiving function, and if the card can be used, sends a reply mail to the center 1 to that effect. When the center 1 receives a reply email from the mobile phone 6, the card is permitted to be used.

[0086] On the other hand, if someone other than the cardholder uses the member's card fraudulently, the cardholder learns of this fact from the email retrieved from the mobile phone 6 and sends a reply email to the center 1 stating that the card cannot be used. When the center 1 receives a reply mail from the mobile phone 6 indicating that the card cannot be used, it notifies the member store that the card cannot be used. In addition, in the event that an email cannot be sent to the member's registered email address, or if a reply email is not returned to the center, the member store will be notified that the card cannot be used. In this case, the conventional identification procedures described above are performed.

[0087] FIG. 10 is a diagram showing the configuration of a center according to a fifth embodiment of the present invention. Referring to FIG. 10, the center 1 comprises an email address acquisition unit 23, an email transmission/reception unit 24, and an Internet protocol communication unit 25 that interfaces with the Internet 9, which differs from the structure of the embodiment shown in FIG. 2.

[0088] In addition, the database 12 stores and holds the email addresses of members who have mobile communication terminals with sending and receiving functions.

[0089] Based on the card number, the email address acquisition unit 23 searches and acquires an email address corresponding to the card number from the database 12.

[0090] The mail transmission/reception unit 24 automatically sends an email inquiring about whether or not the card can be used to the email address acquired by the email address acquisition unit 23, and also manages the reception of reply emails.

[0091] The card usage determination unit 16 determines whether the email sent by the email transmission/reception unit 24 is correctly sent to the destination, and when a reply mail is received from the destination (the user's mobile phone 6), it is determined whether the content allows the card to be used or not.

[0092] When an email indicating that the card can be used is returned from the mobile phone 6, the card usage permission notification unit 17 sends a notification that the card can be used to the member store terminal 2. On the other hand, if the user replies with an email indicating that the card cannot be used from the mobile phone 6, or if the reply email cannot be received within a predetermined time, a notification to the effect that the card cannot be used is sent to the member store terminal 2. In this embodiment as well, the processing and functions of the above-mentioned units in the center 1 are realized by program control executed on the computer in the center 1.

[0093] In addition, when entering a password on a mobile communication terminal equipped with a simple browser function and capable of accessing servers and the Internet, by accessing the website of the center 1 from the mobile communication terminal side (entering the user ID and password), the center 1 side may recognize this access and perform identity verification.

[0094] Furthermore, in the above embodiment, although the use of credit cards has been explained as an example, the term "card" in this specification is not limited to credit cards issued and managed by credit card companies, it can be applied to any membership card that allows you to purchase products at member stores and receive financing.

[0095] In addition, the configuration of the center shown in the drawings is an example of its functional configuration, and the present invention is not limited to the configuration of the above embodiment. It goes without saying that the present invention includes various changes and modifications that can be made by those skilled in the art within the scope of each

claim of the present invention.

[0096]

[Effects of the present invention] As explained above, according to the present invention, the following effects are achieved.

[0097] The first effect of the present invention is that when a user uses a card, the user's mobile communication terminal is called from the telephone number of the member's mobile communication terminal registered in advance at the center side. By configuring the system to confirm whether or not the card can be used, it is possible to save labor in verifying the identity of the user, and prevent unauthorized use of the card while suppressing increases in development costs and capital investment.

[0098] The second effect of the present invention is that by appropriately using a combination of input of whether or not a card can be used, password input, and fingerprint information that characterizes an individual from a mobile communication terminal, which means that it is possible to construct a system that excludes unauthorized use depending on the desired security level.

[Brief Description of Drawings]

FIG. 1 is a diagram schematically showing a system configuration of a first embodiment of the present invention.

FIG. 2 is a diagram showing the configuration of a center in the first embodiment of the present invention.

FIG. 3 is a diagram schematically showing an example of a center database in the first embodiment of the present invention.

FIG. 4 is a diagram for explaining the processing flow of the first embodiment of the present invention.

FIG. 5 is a diagram showing the configuration of a center according to a second embodiment of the present invention.

FIG. 6 is a diagram for explaining the processing flow of a second embodiment of the present invention.

FIG. 7 is a diagram schematically showing a system

configuration of a third embodiment of the present invention.

FIG. 8 is a diagram schematically showing a system configuration of a fourth embodiment of the present invention.

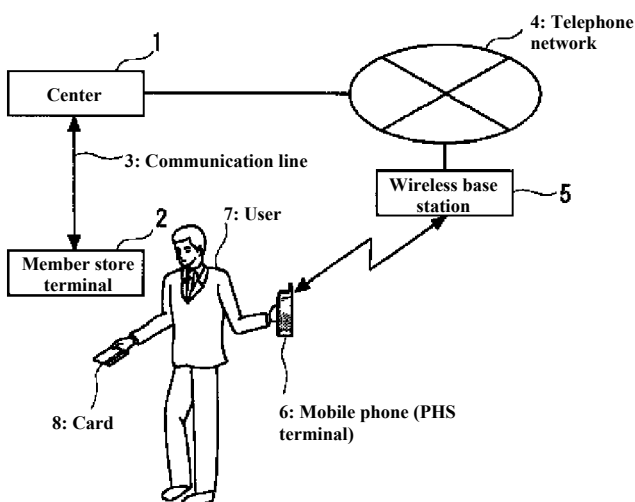
FIG. 9 is a diagram schematically showing a system configuration of a fifth embodiment of the present invention.

FIG. 10 is a diagram showing the configuration of a center according to a fifth embodiment of the present invention.

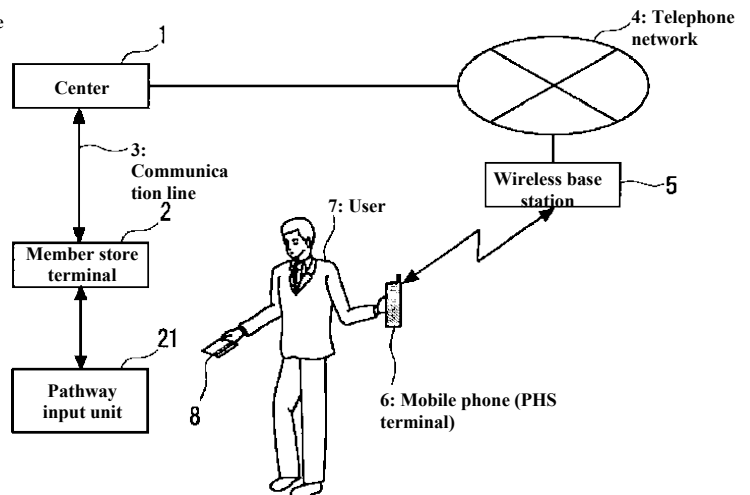
[Reference Signs List]

- 1 Center
- 2 Member store terminals
- 3 Communication lines
- 4 Telephone networks
- 5 Wireless base stations
- 6 Mobile communication terminals (mobile phones, PHS terminals)
- 7 Users
- 8 Cards (credit cards)
- 9 Internet
- 10 Card number acquisition unit
- 11 Identity verification necessity determination unit
- 12 Database
- 13 Mobile phone number acquisition unit
- 14 Telephone call/response control unit
- 15 Telephone terminal interface
- 16 Card usage determination unit
- 17 Card usage permission notification unit
- 18 Communication line interface
- 19 Password authentication unit
- 21 Password input unit
- 22 Fingerprint input device
- 23 Email address acquisition unit
- 24 Email transmission/reception unit
- 25 Internet protocol communication unit

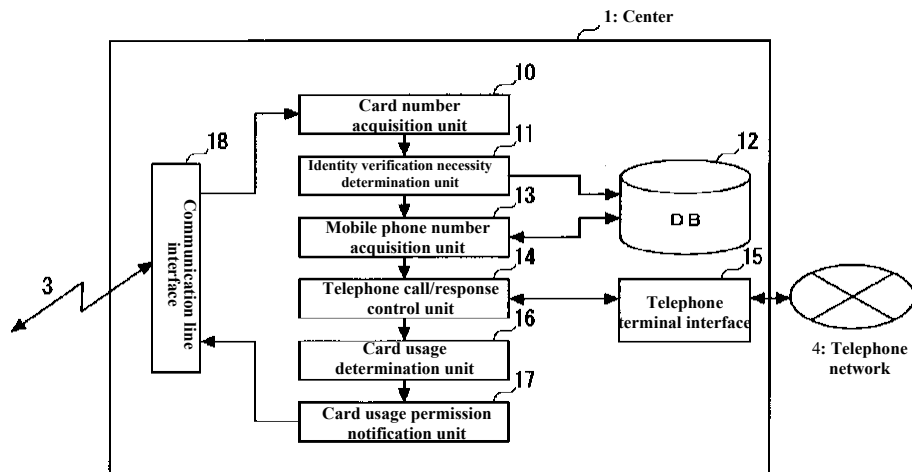
[FIG. 1]



[FIG. 7]



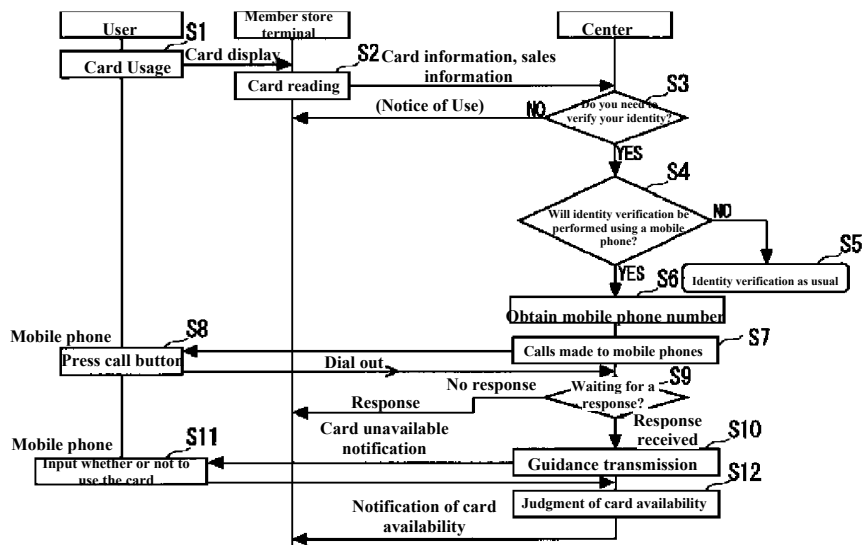
[FIG. 2]



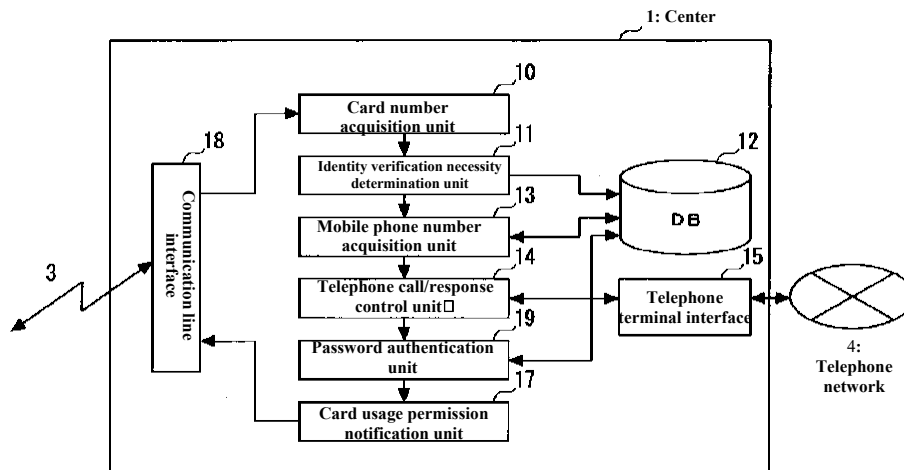
[FIG. 3]

Card Number (ID)	Name	Age	Gender	Address	Place of work	Presence or absence of identity verification by mobile phone	Mobile phone number	Password
100XXXXX	Ichiro Patent	35	Male	C	A	YES	090-abcc-cddd	KJMN
201YYYYY	Japanese Hanako	40	Female	D	B	NO		QPRS

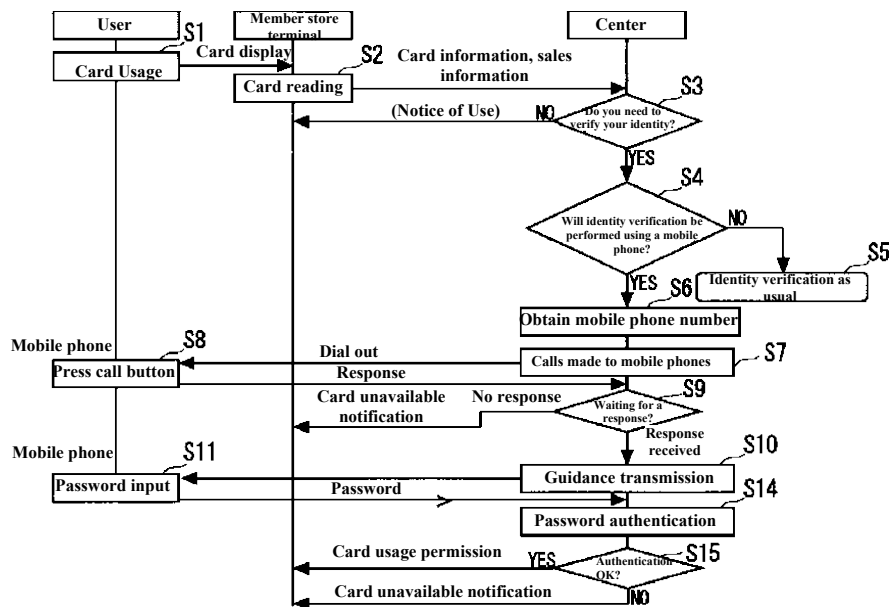
[FIG. 4]



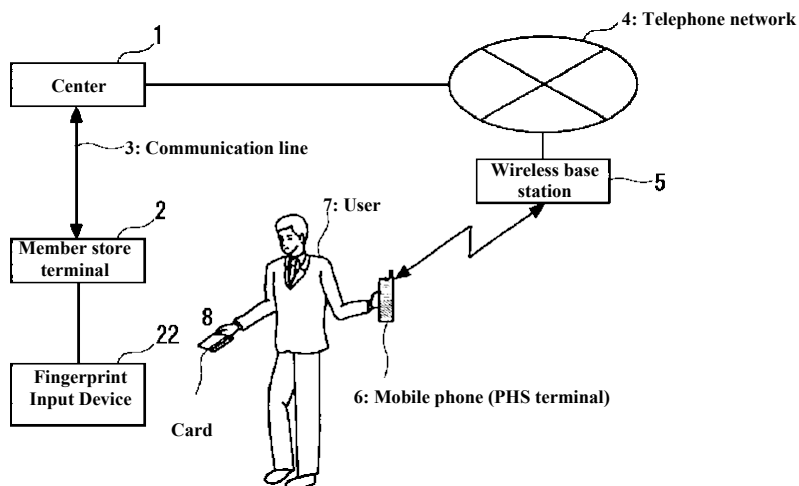
[FIG. 5]



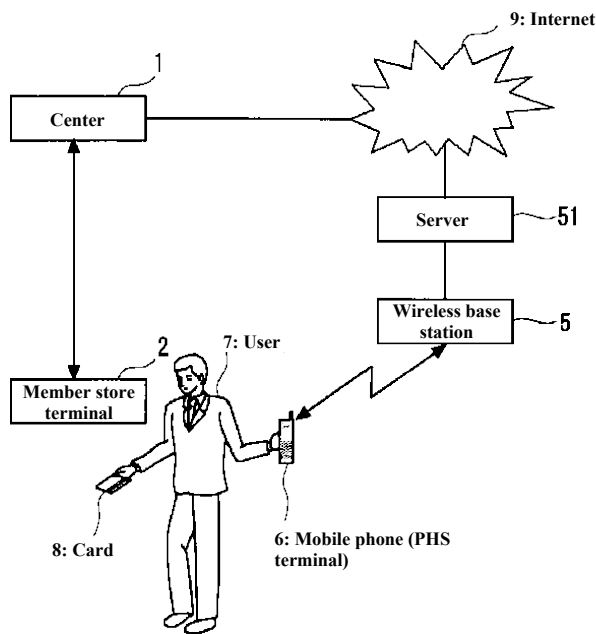
[FIG. 6]



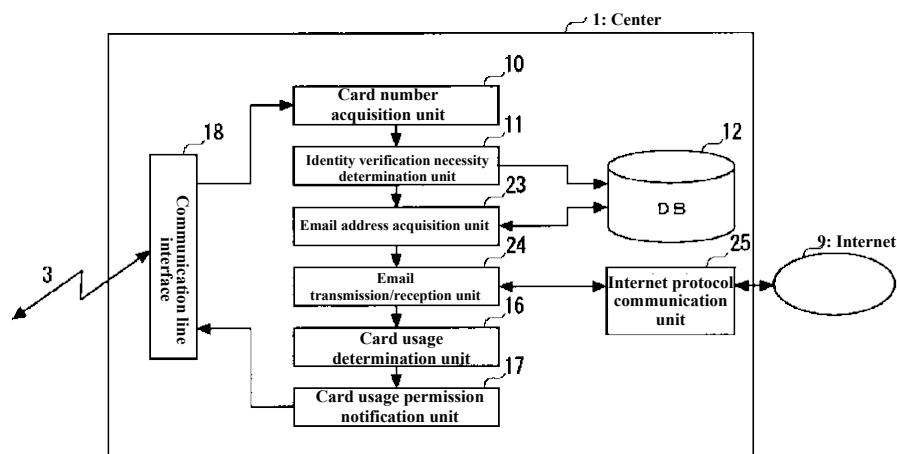
[FIG. 8]



[FIG. 9]



[FIG. 10]



[Procedural amendment]

[Submission Date] December 25, 2000 (12/25/2000)

[Procedural amendment 1]

[Name of document subject to amendment] Specification

[Name of items subject to amendment] Scope of claims

[Correction method] Changed

[Correction Content]

[Scope of Claims]

[Claim 1] A method for preventing unauthorized use of a card characterized in that, in confirming that a card user who uses a card at a member store is the member who possesses the card, at a center that receives a card number read by the member store terminal and sent from the member store terminal, based on the card number, search for a mobile communication terminal telephone number of a cardholder that is registered in advance in the storage means of the center, call a mobile communication terminal of a telephone number corresponding to the card

number, and allow the use of the card when the mobile communication terminal enters that the card can be used.

[Claim 2] A method for preventing unauthorized use of a card according to Claim 1, characterized in that, when the mobile communication terminal does not respond to the call and when the mobile communication terminal responds to the call enters the fact that card cannot be used, the center determines that identity verification cannot be performed and notifies the member store side that the card cannot be used.

[Claim 3] A method for preventing unauthorized use of a card characterized in that, in confirming that a card user using a card at a member store has the card, at a center that receives a card number read at the member store terminal and sent from the member store terminal, based on the card number, a mobile communication terminal of a cardholder pre-registered in the storage means of the center is called to a mobile

communication terminal of a telephone number corresponding to the card number, and when a password is entered from the mobile communication terminal, at the center that receives the password, the password received is matched with a password of a member corresponding to the card number pre-registered in the storage means of the center, and the card is allowed to be used if these passwords are matched.

[Claim 4] A method for preventing unauthorized use of a card according to Claim 3, characterized in that if the called mobile communication terminal does not respond, and the password entered from the called mobile communication terminal does not match the password of a member corresponding to the card number registered in advance in the storage means of the center, it is determined that identity verification is not possible, and the member store is notified that the card is not usable.

[Claim 5] The present invention for preventing unauthorized use of a card is characterized by comprising a four steps in which the center side, which is communicatively connected to member store terminals and manages cards, has a database that stores and holds the telephone numbers of mobile communication terminals owned by the members as personal information of the members, in correspondence with the member's card numbers. When a user uses a card at a member store, the center receives the card number read by the member store terminal, and based on the card number, a first step is to search the database and obtain a telephone number corresponding to the card number; a second step is to make a call from the center to the mobile communication terminal of the obtained telephone number; upon receiving the incoming call from the center to the communication terminal, the user inputs information corresponding to whether the card can be used from the operation unit of the mobile communication terminal, and the center side allows the card to be used from the mobile communication terminal. If information corresponding to "Acceptable" is received, the identity of the cardholder is confirmed, and a third step is to transmit a notification from the center to the member store terminal that the card can be used. If the called mobile communication terminal does not respond, and if the called mobile communication terminal inputs information that the card cannot be used and the center receives the information that the card cannot be used, a fourth step is to transmit a notification to the member store terminal that the card cannot be used.

[Claim 6] The present invention for preventing unauthorized use of a card is characterized by comprising a four steps in which the center side, which is communicatively connected to member store terminals and manages cards, has a database that stores and holds the telephone numbers of mobile communication terminals owned by the members as personal information of the members, in correspondence with the member's card numbers. When a user uses a card at a member store, the center receives the card number read by the member store terminal, and based on the card number, a first step is to search the database and obtain a telephone number corresponding to the card number; a second step is to make a

call from the center to the mobile communication terminal of the obtained telephone number. When the user inputs a password from the operation unit of the mobile communication terminal and the center receives the password transmitted from the mobile communication terminal, the received password is registered in the database in advance. A third step is to compare the card number with the member's password corresponding to the card number, and if the passwords match, the center allows the use of the card; and if the calling mobile communication terminal does not respond, and if the password entered from the called mobile communication terminal does not match the password of the member corresponding to the card number registered in advance in the database, the center cannot confirm the identity, and a fourth step is to notify the affiliated store that the card cannot be used.

[Claim 7] A method for preventing unauthorized use of a card according to Claim 6, characterized in that, instead of entering a password from the mobile communication terminal, the user enters a password from the member store terminal, and the entered password is transmitted to the center side via a communication line, and the password is sent to the center side via the communication line, wherein the password is authenticated.

[Claim 8] A method for preventing unauthorized use of a card according to Claim 5, characterized in that a fingerprint input means is provided on the member store terminal side, the user's fingerprint information is input from the fingerprint input means, and the input fingerprint information is transmitted to the center side via a communication line, the center verifies the identity by comparing the fingerprint information with fingerprint information registered in the database in association with the card number.

[Claim 9] A method for preventing unauthorized use of a card characterized in that, in order to confirm that the card user who uses the card at a member store is the member who owns the card, the center that receives the card number read by the member store terminal and transmitted from the member store terminal checks the card number. Based on the number, search the email address of the card member pre-registered in the storage means of the center and send an email asking whether or not the card can be used. If the user receives a reply email from the mobile communication terminal indicating that the card can be used, permitting the user to use the card.

[Claim 10] A method for preventing unauthorized use of a card characterized in that a device that is communicatively connected to a member store terminal and prevents unauthorized use of a card at the member store, which corresponds to the member's card number and serves as the member's personal information; a storage means provided to store and hold the telephone number of a mobile communication terminal owned by the member, and when the card user uses the card at a member store, the information transmitted from the member store terminal is based on the card number; a means for searching a storage means and acquiring a telephone number corresponding to the card number; a means

for automatically making a call to a mobile communication terminal having the acquired telephone number; and a means for responding to an incoming call to the mobile communication terminal, and when the user inputs information indicating that the card can be used from the operation unit of the mobile communication terminal, the input information is received via a wireless communication line and telephone network, and a notification to the effect that the card can be used is sent to the member; a means for transmitting information to a store terminal, and when the mobile communication terminal does not respond, the user inputs information indicating that the card cannot be used from the mobile communication terminal, and the information is transmitted to a wireless communication line and telephone; and a means for transmitting a notification to the member store terminal that the card cannot be used when the card is received via a network.

[Claim 11] A method for preventing unauthorized use of a card characterized in that a device that is communicatively connected to a member store terminal and prevents unauthorized use of a card at the member store, which corresponds to the member's card number and serves as the member's personal information; a storage means provided for storing and retaining a telephone number of a mobile communication terminal owned by the member and a password of the member, and when a card user uses the card at a member store, a means for searching the storage means based on the card number among information transmitted from the member store terminal and acquiring a telephone number corresponding to the card number; a means for automatically making a call to the mobile communication terminal having the acquired telephone number, and when the password transmitted via the communication line and telephone network is received, the password is compared with the password registered in the storage means in association with the card number, and if the passwords match, the card can be used; a means for transmitting a notification to the member store terminal to the effect that the card cannot be used if the passwords do not match.

[Claim 12] A method for preventing unauthorized use of a card characterized in that a device that is communicatively connected to a member store terminal and prevents unauthorized use of a card at the member store, which corresponds to the member's card number and serves as the member's personal information; a storage means provided to store an email address for a mobile communication terminal owned by the member, and when the card user uses the card at an member store, based on the card number among the information transmitted from the member store terminal, a means for searching the storage means and acquiring an email address corresponding to the card number; a means for automatically sending an email to the obtained email address inquiring whether or not the card can be used, and if the mobile

communication terminal retrieves the email sent from the center, and the mobile communication terminal replies with an email indicating that the card can be used, a notification to the effect that the card can be used is sent to the member store terminal; a means for transmitting a notification to the effect that the card cannot be used to the member store terminal when the user replies an email indicating that the card cannot be used from the mobile communication terminal.

[Claim 13] A method for preventing unauthorized use of a card characterized in that a card unauthorized use prevention system in a card authorization system including a member store terminal equipped with a card reading device, and a center communicatively connected to the member store terminal to manage cards, wherein the center reads a member's card information; correspondingly, a database provided that stores and holds the telephone number of the mobile communication terminal owned by the member as the member's personal information, and when the card user uses the card at the member store, the database is sent from the member store terminal; a means for searching the database based on the card number to obtain a telephone number corresponding to the card number; a means for automatically calling the obtained telephone number to the mobile communication terminal; a means for transmitting guidance information to the mobile communication terminal instructing the user to input whether or not a card can be used when the user goes off-hook after receiving an incoming call notification to the mobile communication terminal, and when the member inputs information indicating that the card can be used from the operation unit of the mobile communication terminal, the member receives the card usage information via a wireless communication line and telephone network, and sends a notification that the card can be used to the member; a means for transmitting a notification that the mobile communication terminal does not respond to a call from the center; and a means for the user to operate the mobile communication terminal, and when information indicating that the card cannot be used is input from the department and the card cannot be used is received via a wireless communication line and a telephone network; and a means for controlling to send a notification to the effect that the card cannot be used to the member store terminal.

[Claim 14] A method for preventing unauthorized use of a card characterized in that a card unauthorized use prevention system in a card authorization system including a member store terminal equipped with a card reading device, and a center communicatively connected to the member store terminal to manage cards, wherein the center reads a member's card information; correspondingly, a database provided that stores and holds the telephone number of the mobile communication terminal owned by the member as the member's personal information, and when the card user uses the card at the member store, the database is sent from the member store

terminal; a means for searching the database based on the card number to obtain a telephone number corresponding to the card number; a means for automatically calling the mobile communication terminal having the acquired telephone number; a means for transmitting guidance information to the mobile communication terminal instructing the user to input a password when the user goes off-hook after receiving an incoming call notification to the mobile communication terminal, and when a password is input from the operation unit of a mobile communication terminal, the password transmitted via a wireless communication line and a telephone network is received, the database is referred to from the password, and the password is registered corresponding to the card number; a means for transmitting a notification to the member store terminal that the card can be used if the passwords match as a result of the verification; a means for the mobile communication terminal to respond to a call from the center, and a means for controlling to send a notification to the effect that the card cannot be used to the member store terminal when there is no response and when the passwords do not match as a result of the password verification.

[Claim 15] A method for preventing unauthorized use of a card characterized in that a card unauthorized use prevention system in a card authorization system including a member store terminal equipped with a card reading device, and a center communicatively connected to the member store terminal to manage cards, wherein the center reads a member's card information; correspondingly, a database provided to store and hold email addresses for mobile communication terminals for members who own mobile communication terminals equipped with email sending/receiving functions as the member's personal information, and card users can access member stores; a means for searching the database based on the card number among the information sent from the member store terminal when using the card to obtain an email address corresponding to the card number; a means for automatically sending an email inquiring as to whether the card can be used, and If the user retrieves the email sent from the center using the mobile communication terminal and replies with an email from the mobile communication terminal indicating that the card can be used, a notification to the effect that the card can be used is sent to the member; a means for transmitting to a store terminal, and if there is no response from the mobile communication terminal, or if an email indicating that the card cannot be used is returned from the mobile communication terminal, a notification to the effect that the card cannot be used is sent to the store terminal; and a means for controlling transmission to a member store terminal.

[Claim 16] A method for preventing unauthorized use of a card according to any one of Claims 13 to 15 characterized in that the database includes an area for recording whether or not identity verification is performed by calling a mobile communication terminal when using a card, and the setting of whether or not identity verification is performed by calling a

mobile communication terminal is freely changed.

[Claim 17] A method for preventing unauthorized use of a card according to Claim 13 or 14 characterized in that a fingerprint input device is connected to the member store terminal and inputs fingerprint information, and the fingerprint information of the user is input from the fingerprint input device, and the input fingerprint information is transmitted from the member store terminal to the communication line. The fingerprint information is sent to the center via the above, and the center stores the fingerprint information in the database. Identity verification is performed by comparing fingerprint information registered in association with the card number.

[Claim 18] A method for preventing unauthorized use of a card according to Claim 14 characterized in that the member store terminal is provided with a password input means, and instead of inputting a password from the mobile communication terminal, the user inputs a password from the password input means of the member store terminal, and the input password is used for communication. The password is sent to the center via a line, and the center receives the password, refers to the database from the password, and compares it with the password registered corresponding to the card number.

[Claim 19] A method for preventing unauthorized use of a card characterized in that a database that is communicatively connected to a member store terminal equipped with a card reading device and that stores and maintains the telephone number of the mobile communication terminal as the member's personal information in correspondence with the member's card number at a card management center, which equipped with: (a) when a card user uses a card at a member store, a process of searching the database based on the card number among the information sent from the member store terminal and obtaining a telephone number corresponding to the card number;

(b) a process of automatically calling the mobile communication terminal having the acquired telephone number;

(c) when the user goes off-hook after receiving an incoming call notification to the mobile communication terminal, a means for transmitting guidance information to the mobile communication terminal instructing the user to input whether or not the card can be used;

and (d) when the user inputs information indicating that the card can be used from the operation unit of the mobile communication terminal, the user receives the card usage information via a wireless communication line and telephone network, and receives a message indicating that the card can be used. A notification is sent to the member store terminal, and on the other hand, when the user inputs information indicating that the card cannot be used from the operation unit of the mobile communication terminal, the information that the card cannot be used is received via a wireless communication line and a telephone network, and a recording medium records a program for causing a computer at the center to execute each

of the processes (a) to (d), including the process of transmitting a notification to the member store terminal that the card cannot be used.

[Claim 20] A method for preventing unauthorized use of a card characterized in that a database that is communicatively connected to a member store terminal equipped with a card reading device and that stores and maintains the telephone number of the mobile communication terminal as the member's personal information in correspondence with the member's card number at a card management center, which equipped with:

(a) when a card user uses a card at a member store, a process of searching the database based on the card number among the information sent from the member store terminal and obtaining a telephone number corresponding to the card number;

(b) a process of automatically calling the mobile communication terminal having the acquired telephone number;

(c) a process of transmitting guidance information to the mobile communication terminal instructing the user to input a password when the user goes off-hook after receiving an incoming call notification to the mobile communication terminal;

and (d) When the user inputs a password from the operation unit of the mobile communication terminal, the user receives the password transmitted via the wireless communication line and telephone network, refers to the database based on the password, and the card number is compared with the registered password. As a result of the verification, if they match, a notification to the effect that the card can be used is sent to the member store terminal, and if the passwords do not match, a notification to the effect that the card cannot be used is sent to the member store terminal, and a recording medium to store a program for causing a computer at the center to execute each of the processes (a) to (d).

[Claim 21] A method for preventing unauthorized use of a card characterized in that at a center that is communicatively connected to a member store terminal equipped with a card reading device and manages the card, a mobile communication terminal equipped with an email sending and receiving function is associated with the member's card number as the member's personal information, which is equipped with a database that remembers and maintains member email addresses:

(a) a process of searching the database when a card user uses the card at a member store based on the card number among the information sent from the member store terminal to obtain the email address corresponding to the card number;

(b) a process of automatically sending an email to the email address inquiring whether the card can be used;

and (c) if the user retrieves the email sent from the center with the mobile communication terminal and replies with an email from the mobile communication terminal indicating that the card can be used, the user will receive a notification that the card can be used. On the other hand, if the user replies from the mobile communication terminal with an email indicating that

the card cannot be used, a notification to the effect that the card cannot be used is sent, and a recording medium have recorded thereon a program for causing a computer at the center to execute each of the processes (a) to (c), including the process for transmitting to the member store terminal.

[Claim 22] A recording medium according to any one of Claims 19 to 21 characterized in that the user's fingerprint information input from a fingerprint input device connected to the member store terminal is transmitted from the member store terminal to the center side via a communication line, and the center side reads the fingerprint information, and a recording medium is used to store a program for causing a computer at the center to execute a process of verifying the identity of the person by comparing the fingerprint information registered in the database in association with the card number.

[Claim 23] A method for preventing unauthorized use of a card characterized in that, based on the card number of the received information, the center receives the information sent from the member store terminal equipped with a device to read the card information of the card user who uses the card, and the telephone number of the cardholder's mobile communication terminal registered in advance in the storage means of the center is searched, and the mobile communication terminal having the telephone number corresponding to the card number is called.

[Claim 24] A method for preventing unauthorized use of a card characterized in that, based on the card number of the received information, the center receives the information sent from the member store terminal equipped with a device to read the card information of the card user who uses the card, and the email address of the cardholder's mobile communication terminal registered in advance in the storage means of the center is searched, and information for confirming card usage is notified by email to the mobile communication terminal of the email address.

[Claim 25] A card fraud prevention control device characterized in that a device that is communicatively connected to a member store terminal and prevents unauthorized use of a card at the member store, which corresponds to the member's card number and serves as the member's personal information; a storage means provided for storing and retaining a telephone number of a mobile communication terminal owned by the member, and when a card user uses the card at a member store, based on the card number among the information transmitted from the member store terminal; a means for searching the storage means and acquiring a telephone number corresponding to the card number; and a means for automatically calling the acquired telephone number to a mobile communication terminal.

[Claim 26] A card fraud prevention control device characterized in that a device that is communicatively connected to a member store terminal and prevents unauthorized use of a card at the member store, which corresponds to the member's card number and serves as the member's personal information; a storage means provided for

storing an email address for a mobile communication terminal owned by the member, and when the card user uses the card at an affiliated store, based on the card number among the information transmitted from the affiliated store terminal, a means for searching the storage means and acquiring an email address for a mobile communication terminal corresponding to the card number; and a means for automatically sending an e-mail containing card usage confirmation information to the obtained email address.

[Claim 27] A card fraud prevention control device characterized in that a card unauthorized use prevention system in a card authorization system including a member store terminal equipped with a card reading device and a center that is communicatively connected to the member store terminal and manages cards, wherein the center reads the member's card information; correspondingly, a database that stores and holds telephone numbers of mobile communication terminals owned by the members as personal information of the members, and when a card user uses the card at a member store, information transmitted from the member store terminal includes: a means for searching the database based on the card number and acquiring a telephone number corresponding to the card number; and a means for automatically calling the acquired telephone number to a mobile communication terminal.

[Claim 28] A card fraud prevention control device characterized in that a card unauthorized use prevention system in a card authorization system including a member store terminal equipped with a card reading device and a center that is communicatively connected to the member store terminal and manages cards, wherein the center reads the member's card information; correspondingly, a database that stores and holds e-mail addresses for mobile communication terminals for members who own mobile communication terminals equipped with email sending and receiving functions, as personal information of the members, in association with the member's card numbers; a means for searching the database based on the card number among the information transmitted from the member store terminal when using the card at the card number to obtain an email address for the mobile communication terminal corresponding to the card number; and a means for automatically sending an email containing card usage confirmation information to the obtained email address.

[Claim 29] A database that is communicatively connected to a member store terminal equipped with a card reading device and that stores and maintains the telephone number of the mobile communication terminal as the member's personal information in correspondence with the member's card number at a card management center, which is equipped with

(a) a process of searching the database when a card user uses a card at a member store based on the card number among the information sent from the member store terminal and obtaining a telephone number corresponding to the card number; and

(b) a recording medium recording a program for executing the processes of (a) and (b) above on the computer of the center, including the process of automatically calling the mobile communication terminal having the acquired telephone number.

[Claim 30] At a center that is communicatively connected to a member store terminal equipped with a card reading device and manages the card, a mobile communication terminal equipped with an email sending and receiving function is associated with the member's card number as the member's personal information, which is equipped with a database that remembers and maintains member email addresses;

(a) a process of searching the database to obtain an email address for a mobile communication terminal corresponding to the card number based on the card number among the information sent from the member store terminal when a card user uses a card at a member store; and

(b) a means for automatically sending an email for card usage confirmation to the email address; and a recording medium recording a program for causing a computer at the center to execute the processes in (a) and (b) above.