CARD VERIFICATION SYSTEM

[TECHNICAL FIELD]

[0001] The present invention relates to a card verification system.

[BACKGROUND ART]

[0002] In recent years, card settlements using credit cards, electronic money cards, debit cards, and the likes have been increased. With the increase of card settlements, however, damage caused by skimming has also been increased. Particularly, in the case of credit cards, since credit approval is given, damage is less likely to be detected unless the credit limit is exceeded. The damage may be often found only after the credit card statement sent at a later date is checked.

[0003] [Patent Document No. 1] Japanese Unexamined Patent Application Publication (Translation of PCT Application) No. 2002-508550

[Patent Document No. 2] Japanese Unexamined Patent Application Publication (Translation of PCT Application) No. 2002-537619

[DISCLOSURE OF THE INVENTION]

[PROBLEM TO BE SOLVED BY THE INVENTION]

[0004] If the skimming damage is noticed at the time when the statement is checked and if the damage is reported to the police thereafter, there will be some period of time after the use of a fraudulent card until the start of investigation. Accordingly,

the salesperson's memory will be faded, and the security camera footage may be often erased. Therefore, more effective investigation methods are currently required in order to reduce skimming crimes. Even though card information is skimmed, if a fraudulent card created based on the skimmed card information can be made unavailable, the card company or the cardholder will not sustain any actual damage. Accordingly, an authentication method other than a PIN number or other authentication methods vulnerable to skimming is required.

[0005] The present invention has been made in view of such a situation, and a purpose thereof is to provide a technique for reducing damage caused by card skimming.

[MEANS TO SOLVE THE PROBLEM]

[0006] A card verification system of an embodiment of the present invention includes: a card/mobile terminal relation information storage unit that stores card information for a settlement and mobile terminal information related to the card information; an authentication request receiving unit that receives an authentication request from the settlement system that has received a settlement request from a card reading terminal device; a mobile terminal information retrieval unit that retrieves, from the card/mobile terminal relation information storage unit, mobile terminal information related to the card information include in the authentication request received from the settlement system; a check request notification unit that notifies the mobile terminal device of a check request, based on the retrieved mobile terminal

information; a check result receiving unit that receives a check result including acceptance or un-acceptance of the settlement from the mobile terminal device, based on an operation of a user of the mobile terminal device; an authentication unit that decides whether or not the settlement according to the authentication request is authenticated, based on the received check result; and an authentication result notification unit that notifies the settlement system of an authentication result based on a check result of the authentication unit.

[0007] Another embodiment of the present invention is also a card verification system. This system includes: a fraudulence detection-use card information storage unit that stores card information indicating that the next use is regarded as illegal use; and an illegal use information notification unit that notifies, when card information about which a reference is made by a settlement system that has received a settlement request from a card reading terminal device is identical with card information registered in the fraudulence detection-use card information storage unit, a given information system of card illegal use information including the place where a fraudulent card was used.

[0008] Optional combinations of the aforementioned constituting elements, and implementations of the present invention in the form of methods, apparatuses, systems, recording media, and computer programs may also be practiced as additional modes of the present invention.

[ADVANTAGE OF THE INVENTION]

[0012] According to the present invention, damage caused by card skimming can be reduced.

[BRIEF DESCRIPTION OF THE DRAWINGS]

[0013] Fig. 1 is a block diagram that shows a configuration of a card settlement system according to a first embodiment of the present invention;

Fig. 2 is a block diagram that shows a configuration of a card reading terminal device shown in Fig. 1;

Fig. 3 is a block diagram that shows a configuration of a settlement system shown in Fig. 1;

Fig. 4 is a block diagram that shows a configuration of a card verification system shown in Fig. 1;

Fig. 5 is a diagram that shows an example of a card information /mobile terminal information relation table provided in a card/mobile terminal relation information storage unit shown in Fig. 4;

Fig. 6 is a block diagram that shows a configuration of a mobile terminal device shown in Fig. 1;

Fig. 7 is a diagram that shows an example of a settlement check screen displayed in the mobile terminal device;

Fig. 8 is a flowchart that shows a procedure of processing performed in the card settlement system according to the first embodiment;

Fig. 9 is a diagram that shows an example of a card information /mobile terminal information relation table provided in a card/mobile terminal relation information storage unit according

to a first modification of the first embodiment;

Fig. 10 is a diagram that shows an example of a card information /mobile terminal information relation table provided in a card/mobile terminal relation information storage unit according to a second modification of the first embodiment;

Fig. 11 is a block diagram that shows a configuration of a card settlement system according to a second embodiment of the present invention;

Fig. 12 is a block diagram that shows a configuration of a settlement system according to the second embodiment;

Fig. 13 is a diagram that shows an example of an affiliated shop information table provided in an affiliated shop information storage unit of the settlement system according to the second embodiment;

Fig. 14 is a block diagram that shows a configuration of a card verification system according to the second embodiment;

Fig. 15 is a diagram that shows an example of a detection information table provided in a detection-use card information storage unit of the card verification system according to the second embodiment;

Figs.16A-9D are diagrams that each show an example of a message displayed on a display unit of the card reading terminal device;

Fig. 17 is a flowchart that shows a procedure of processing performed in the card settlement system according to the second embodiment; and

Fig. 18 is a block diagram that shows a configuration of a card verification system dedicated to criminal investigation using a fraudulence detection card.

[BEST MODE FOR CARRYING OUT THE INVENTION]

[0011] In recent years, damage to credit cards caused by skimming has been widespread. Because the card is in hand, the victim notices the skimming damage only after receiving a credit card statement. Accordingly, unlike pickpocketing or robberies, skimming is noticed after a delay. Also, it is extremely difficult for the victim to identify the place where the damage was caused.

[0012] Major methods of skimming crimes are as follows: installing a skimming device on an automatic teller machine (ATM) to read card information, and stealing passwords using a miniature camera or a dummy numeric keypad; and having a staff member of a restaurant or a hotel illegally steal card information while the staff member handles a card.

[0013] Credit card authentication is generally performed by allowing the user to sign or to enter a password. However, the signature or password is often stolen concurrently with the skimming of card information. Now, in the embodiments of the present invention as described following, a new credit card authentication method is proposed.

[0014] Fig. 1 is a block diagram that shows a configuration of a card settlement system 1 according to a first embodiment of the present invention. In the card settlement system 1 according to the first embodiment, a settlement system 20, a card verification

system 10, a card reading terminal device 30, and a mobile terminal device 40 are used. The card verification system 10, card reading terminal device 30, and mobile terminal device 40 are connected to one another via a network 2. The network 2 represents a communication channel, and the communication medium or protocol thereof is not limited; however, a high-security communication protocol, such as SSL communication, should be desirably used.

[0015] The card reading terminal device 30 is a terminal device provided with a function to read information on a card 3 presented or inserted by a cardholder. For example, the card reading terminal device 30 may be a cash register connected to a card reader, an ATM, a handy terminal, or a tablet terminal with a card reader provided externally. In the description of the first embodiment, it is mainly assumed to be a cash register connected to a card reader. With this type of the card reading terminal device 30, a salesperson receives a card 3 from a customer and inserts the card 3 into the card reader, so that the card information is transferred into the cash register.

[0016] Fig. 2 is a block diagram that shows a configuration of the card reading terminal device 30 shown in Fig. 1. The card reading terminal device 30 comprises a control unit 31, a memory unit 32, a communication unit 33, a display unit 34, an operation unit 35, a card reading unit 36, and a printing unit 37. Card information read by the card reading unit 36 from a card 3 is output to the control unit 31. The control unit 31 connects to the network 2 via the communication unit 33 and notifies the settlement system

20 of a settlement request. The control unit 31 conveys the settlement request at least including the card information read by the card reading unit 36 and affiliated shop information retrieved from the memory unit 32.

[0017] Fig. 3 is a block diagram that shows a configuration of the settlement system 20 shown in Fig. 1. The settlement system 20 is provided in a data center of a card company or of a system operation company commissioned by a card company. The settlement system 20 generally consists of multiple servers. Also, the settlement system 20 may be constituted by servers installed in multiple locations connected by cloud computing.

[0018] The settlement system 20 comprises a control unit 21, a memory unit 22, a communication unit 23, a display unit 24, an operation unit 25, and an issuing unit 26. The control unit 21 includes a settlement request receiving unit 211, a card validity judgment unit 212, an authentication request notification unit 213, an authentication result receiving unit 214, and a settlement judgment result notification unit 215. Fig. 3 only shows the functional blocks of the control unit 21 related to the processes featured in the first embodiment. The functions of the control unit 21 can be implemented by cooperation between hardware resources and software resources or only by hardware resources. As hardware resources, processors, ROMs, RAMs, LSIs, or the likes can be employed. As software resources, operating systems, applications, and other programs can be employed. The memory unit 22 may be constituted by an HDD or SSD, for example, and includes

a card information storage unit 221 and an affiliated shop information storage unit 222. Fig. 3 also only shows the functional blocks of the memory unit 22 related to the processes featured in the first embodiment.

[0019] Fig. 4 is a block diagram that shows a configuration of the card verification system 10 shown in Fig. 1. The card verification system 10 may be possessed by another entity instead of a card company or by a card company itself. The card verification system 10 is also provided in a data center of the owner or of a system operation company commissioned by the owner. The card verification system 10 generally consists of multiple servers. Also, the settlement system 20 and card verification system 10 may be unified and integrally operated.

[0020] The card verification system 10 comprises a control unit 11, a memory unit 12, a communication unit 13, a display unit 14, and an operation unit 15. The control unit 11 includes an authentication request receiving unit 111, a mobile terminal information retrieval unit 112, a check request notification unit 113, a check result receiving unit 114, an authentication unit 115, and an authentication result notification unit 116. Fig. 4 also only shows the functional blocks of the control unit 11 related to the processes featured in the first embodiment. The functions of the control unit 11 can be implemented by cooperation between hardware resources and software resources or only by hardware resources. The memory unit 12 may be constituted by an HDD or SSD, for example, and includes a card/mobile terminal

relation information storage unit 121. Fig. 4 also only shows the functional blocks of the memory unit 12 related to the processes featured in the first embodiment.

[0021] Fig. 5 is a diagram that shows an example of a card information/mobile terminal information relation table 121a provided in a card/mobile terminal relation information storage unit 121 shown in Fig. 4. Specific description will be provided later.

[0022] Fig. 6 is a block diagram that shows a configuration of the mobile terminal device 40 shown in Fig. 1. The mobile terminal device 40 is a terminal device carried by a holder of a card 3. For the mobile terminal device 40, a smartphone, a feature phone, a tablet, a portable music player, or a portable game device may be used, for example. Since a communication function is required in the first embodiment, when a tablet, a portable music player, or a portable game device is used, such a device needs to be used with a SIM card inserted thereto or while being connected to an access point of a wireless LAN.

[0023] The mobile terminal device 40 comprises a control unit 41, a memory unit 42, a communication unit 43, an antenna 43a, a display unit 44, an operation unit 45, an imaging unit 46, and a GPS receiving unit 47. In the following, a procedure according to the first embodiment will be described referring to Figs 1-6.

[0024] The settlement request receiving unit 211 of the settlement system 20 receives a settlement request from the card reading terminal device 30 via the network 2. The card validity

judgment unit 212 judges the validity of the card information included in the settlement request. Specifically, the card validity judgment unit 212 reads the card information on the used card 3 from the card information storage unit 221, and checks whether or not the expiration date of the used card 3 has been reached, whether or not the credit limit of the used card 3 has been exceeded and so on. When the used card 3 is not valid, the settlement judgment result notification unit 215 notifies the card reading terminal device 30 of rejection of the settlement. When the used card 3 is valid, the authentication request notification unit 213 notifies the card verification system 10 of the authentication request for the received settlement request via the network 2. The authentication request includes at least the card information included in the received settlement request from the card reading terminal device 30.

[0025] The authentication request receiving unit 111 of the card verification system 10 receives the authentication request from the settlement system 20. The mobile terminal information retrieval unit 112 retrieves, from the card/mobile terminal relation information storage unit 121, the information on the mobile terminal device 40 related to the card information based on the card information included in the authentication request.

[0026] The card/mobile terminal relation information storage unit 121 stores the information of the card 3 and the information of the mobile terminal device 40 related to each other. In the example shown in Fig. 5, the card number, the expiration date,

the cardholder's name, and the security code are stored as the information on the card 3. These card information are the information provided from the card company using services provided by the card verification system 10 in advance.

[0027] In the example shown in Fig. 5, the mobile terminal type, the notification method, the telephone number, and the email address are stored as the information on the mobile terminal device 40. These mobile terminal information are the information provided from the card company using services provided by the card verification system 10 in advance. The card company allows a card user to register the mobile terminal information used for the authentication, when the card company contracts with the card user.

[0028] Many card users select a smartphone or a feature phone as the mobile terminal device 40 to be registered. The email, the short message service (SMS), or the voice guidance can be used as the notification method to the mobile terminal device 40 at the time of the authentication. When the email or the short message service is used, the push notification services provided by telecommunications carriers or OS vendors can be used. The use of the push notification services allows the display unit 44 to display a settlement check screen, even when the corresponding application is not running in the mobile terminal device 40 as long as the mobile terminal device 40 is powered on.

[0029] A user not familiar with handling the mobile terminal device 40 should use the voice guidance. When the voice guidance is used, there is an incoming call to the mobile terminal device

40 at the time of the authentication, and the user should choose a number in the operation unit 45 along the automated voice guidance.

[0030] The check request notification unit 113 of the card verification system 10 notifies the mobile terminal device 40 of a check request, based on the information on the mobile terminal device 40 retrieved by the mobile terminal information retrieval unit 112. For example, the check request notification unit 113 sends the telephone number of the mobile terminal device 40 to an OS vendor, and requests the push notification to the mobile terminal device 40. Upon reception of the check request according to a card verification from the card verification system 10, the control unit 41 of the mobile terminal device 40 displays a settlement check screen.

[0031] Fig. 7 is a diagram that shows an example of a settlement check screen 44a displayed in the mobile terminal device 40. The product name, the settlement amount, the OK key 44b, and the NG key 44c are displayed in the settlement check screen 44a shown in Fig. 7. When a user hands a card to a salesperson at the register as payment of the price, the settlement check screen 44a is displayed in the mobile terminal device 40 held by himself/herself. The user checks the contents in the settlement check screen 44a, and pushes the OK key 44b or the NG key 44c. In this example, it is assumed to be a touch panel display where the display unit 44 and the operation unit 45 are integrated. When the feature phone is used, the user inputs an intention to approve or to reject using physical keys provided on the operation unit 45.

[0032] Based on the user's operation to the operation unit 45, the control unit 41 notifies the card verification system 10 of a check result including user's acceptance or rejection of the settlement via the network 2. The check result receiving unit 114 of the card verification system 10 receives the check result from the mobile terminal device 40. The authentication unit 115 decides whether or not the settlement according to an authentication request is authenticated, based on the received check result. In the simplest design, when the check result from the mobile terminal device 40 is acceptance, the authentication unit 115 judges that the authentication is successful. When the check result is rejection, the authentication unit 115 judges that the authentication is unsuccessful. The authentication result notification unit 116 notifies the settlement system 20 of an authentication result.

[0033] The authentication result receiving unit 214 of the settlement system 20 receives the authentication result from the card verification system 10. The settlement judgment result notification unit 215 notifies the card reading terminal device 30 of the authentication result received from the card verification system 10 via the network 2. The control unit 31 of the card reading terminal device 30 allows the display unit 34 to display the authentication result.

[0034] Fig. 8 is a flowchart that shows a procedure of processing performed in the card settlement system 1 according to the first embodiment. Upon insertion of a card 3, the card

reading unit 36 of the card reading terminal device 30 reads the card information (S30), and the control unit 31 then notifies the settlement system 20 of a settlement request including the card information thus read (S31).

[0035] Accordingly, the card validity judgment unit 212 judges whether or not the card information included in the settlement request is valid (S20). If the card information is invalid (N at S20), the settlement judgment result notification unit 215 will notify the card reading terminal device 30 of rejection of the settlement (S24). If the card information is valid (Y at S20), the authentication request notification unit 213 will notify the card verification system 10 of an authentication request (S21).

[0036] Accordingly, the mobile terminal information retrieval unit 112 of the card verification system 10 retrieves, from the card/mobile terminal relation information storage unit 121, mobile terminal information related to the card information according to the authentication request (S10). Based on the mobile terminal information, the check request notification unit 113 notifies the registered mobile terminal device 40 of a check request (S11).

[0037] Upon reception of the check request, the control unit 41 of the mobile terminal device 40 allows the display unit 44 to display a settlement check screen (S40). Thereafter, the control unit 41 of the mobile terminal device 40 receives, via the operation unit 45, the user’s operation for acceptance or rejection of the settlement (S41) and notifies the card

verification system 10 of a check result in which the user's operation is reflected (S42).

[0038] Accordingly, the authentication result notification unit 116 of the card verification system 10 notifies the settlement system 20 of an authentication result based on the check result (S12). If the authentication is successful (Y at S22), the settlement judgment result notification unit 215 of the settlement system 20 will notify the card reading terminal device 30 of acceptance of the settlement (S23). If the authentication is unsuccessful (N at S22), the settlement judgment result notification unit 215 will notify the card reading terminal device 30 of rejection of the settlement (S24).

[0039] As stated above, according to the first embodiment, Even though card information is skimmed, if the registered mobile terminal device 40 is not stolen, it is basically possible to prevent illegal use. Even though the email address of the telephone number is leaked, if the registered mobile terminal device 40 is in hand of the cardholder, the cardholder notices illegal use at a time when the skimmed card information is used illegally. Therefore, skimming damages can be reduced.

[0040] Many users always carry the mobile terminal device 40. Therefore, the cardholder's convenience is hardly decreased. It can reduce the time and effort itself of users rather than to sign or to enter PIN number. Users only need to touch once on the screen. Also, if the authentication method according to the first embodiment is adopted, it can be expected to reduce skimming damages.

Therefore, it is likely that the premiums paid to insurance companies from card companies are lowered. The card companies return the amount to points of the cardholders. Therefore, if the authentication method is used, the incentives that the point return rate is increased can be given to users. In this case, it can be expected that cardholders positively accept the authentication method.

[0041] In the following, a first modification of the first embodiment will be described. In the above example, it is assumed that a cardholder and a holder of the registered mobile terminal device 40 are identical. However, it is not necessary that the both are identical. For example, a cardholder is a wife and a holder of the registered mobile terminal device 40 is the husband. Also, the other way is acceptable. Also, it is allowed that a cardholder is elderly or underage and a holder of the registered mobile terminal device 40 is the protector (e.g. child, parent, or guardian). Also, it is allowed that the information on a plurality of mobile terminal devices 40 is related to information on one card 3.

[0042] Fig. 9 is a diagram that shows an example of a card information/mobile terminal information relation table 121b provided in a card/mobile terminal relation information storage unit 121 according to a first modification of the first embodiment. In the card information/mobile terminal information relation table 121b shown in Fig. 9, two pieces of information on two mobile terminal devices 40 is related to information on one card 3 in the data

of management number 00000001.

[0043] In the first modification, when the information on the card 3 included in the authentication request from the settlement system 20 is related to the information on a plurality of mobile terminal devices 40, the check request notification unit 113 of the card verification system 10 notifies each of the plurality of mobile terminal devices 40 of a check request. When the check results from all of the plurality of mobile terminal devices 40 received by the check result receiving unit 114 are acceptance, the authentication unit 115 judges that the authentication is successful. When the check results from at least one of the plurality of mobile terminal devices 40 are non-acceptance, the authentication unit 115 judges that the authentication is failure.

[0044] According to the first modification, if the registered plurality of mobile terminal devices 40 are not stolen, it is basically possible to prevent illegal use of cards 3. Therefore, it is possible to further enhance security. Also, it is possible to flexibly incorporate rules on handling cards within a family into the system.

[0045] Fig. 10 is a diagram that shows an example of a card information/mobile terminal information relation table 121c provided in a card/mobile terminal relation information storage unit 121 according to a second modification of the first embodiment. In the second modification, the usable regions of the card 3 are included in the card information. Since the card information is electronic data, the card information is easily spread all over

the world via the internet. There, the country where the card information is skimmed and the country where the card is used illegally are often not identical. A cardholder registers in advance in the card company the countries where the card 3 is used. Also, the usable region is not limited to a unit of country, and may be a unit (e.g. the EU) larger than country or may be a unit (e.g. Tokyo) smaller than country.

[0046] In the second modification, when the region where the card 3 is used included in the authentication request received from the settlement system 20 is different from the usable region of the card registered in the card/mobile terminal relation information storage unit 121, the authentication unit 115 of the card verification system 10 judges that the authentication is failure. In the second modification, it is preferable that the check request notification unit 113 notifies the mobile terminal device 40 of a check request including the region where the card 3 is used.

[0047] Thus, according to the second modification, the risk that the skimmed card information is used illegally abroad can be reduced. Also, it is also possible that a region where the child uses the card 3 is limited in the living region

[0048] In the third modification, whether or not the authentication method is used is separated according to a settlement amount. When the settlement amount included in the settlement request from the card reading terminal device 30 is equal to or higher than the set amount (e.g. 10,000 yen), the

authentication request notification unit 213 notifies the card verification system 10 of an authentication request. When the settlement amount is equal lower than the set amount, the authentication request notification unit 213 does not notify. When the settlement amount is equal lower than the set amount, a user selects the authentication method to sign or to enter a password as previously or no authentication.

[0049] In the third modification, it is possible to balance between the secure security and the convenience. In particular, in the first modification, since a plurality of user approvals is required, it is assumed the card settlement is impossible by not gain all user approvals in period of time. In contrast, in the third modification, in the case of small settlement, the conventional authentication method is used. In this case, it is possible to ensure the convenience.

[0050] In the fourth modification, location information generated by the GPS receiving unit 47 is used in addition to user's operation to the operation unit 45 of the mobile terminal device 40 for acceptance or rejection of a settlement. The GPS receiving unit 47 receives radio waves form satellites, and identities the latitude/longitude of the mobile terminal device 40 to generate the location information. The control unit 41 notifies the card verification system 10 of the location information generated by The GPS receiving unit 47 in addition to a check result including user acceptance or rejection of a settlement.

[0051] The authentication unit 115 of the card verification

system 10 judges whether or not that the location information of the affiliated shop where the card 3 is used and the location information received from the mobile terminal device 40 are practically identical with each other. When user's check result is acceptance and the location information are identical with, the card verification system 10 judges that the authentication is successful. When the condition is not satisfied, the card verification system 10 judges that the authentication is unsuccessful. Also, in the fourth modification, the location information of the affiliated shop is included in an authentication request from the settlement system 20.

[0052] Thus, according to the fourth modification, it cannot be authenticated only by stealing the email address the mobile terminal device 40 and by intercepting the confirmation email, it is possible to further enhance security. Also, without requiring user's operation to for acceptance or rejection of a settlement, when the location information of the affiliated shop and the location information of the mobile terminal device 40 are only practically identical with each other only, the card verification system 10 may judge that the authentication is successful. Since user's operation is not required, the convenience is improved. In particular, in the case of small settlement, the authentication method is effective. When the settlement amount is equal to or higher than the set amount (e.g. 10,000 yen), the settlement check method based on user's operation should be adopted. When the settlement amount is lower

than the set amount, the check method based on comparing location information should be adopted.

[0053] In the following, a second embodiment will be described. In the first embodiment, it is focused to block the illegal use based on the skimmed card information. In the second embodiment, it is focused to reduce skimming crime itself by detecting skimming crime. Skimming crime is difficult to detect and hence is a crime of which the criminal is difficult to arrest. The type of such a criminal group is called “hit and away” type, and the criminal group operates while moving from place to place; accordingly, even if damage can be promptly detected, arresting the criminal will be difficult. Also, such a criminal group forms a hierarchy with the leader at the top, the role of stealing card information, and the role of actually using a fraudulent card, called withdrawers, at the bottom; accordingly, even if a withdrawer at the bottom can be caught, it will be difficult to reach the leader. Therefore, through conventional police stakeouts or detection of skimming devices, it is difficult to eliminate the skimming crimes. There will be described, as the second embodiment, a card settlement system 1 for enabling a new investigation method effective for detection of skimming crimes.

[0054] Fig. 11 is a block diagram that shows a configuration of a card settlement system 1 according to the second embodiment of the present invention. The card settlement system 1 according to the second embodiment also works in cooperation with a police information system 50. Further, the card settlement system 1 works

in cooperation with a security camera 60 installed in an affiliated shop, as needed.

[0055] Fig. 12 is a block diagram that shows a configuration of a settlement system 20 according to the second embodiment. The control unit 21 of the settlement system 20 according to the second embodiment is constructed by adding a detection-use card information generating unit 216, a detection-use card information notification unit 217, an affiliated shop information notification unit 218, and an instruction transfer unit 219 to the functional blocks of the control unit 21 of the settlement system 20 according to the first embodiment shown in Fig. 3.

[0056] Fig. 13 is a diagram that shows an example of an affiliated shop information table 222a provided in an affiliated shop information storage unit 222 of the settlement system 20 according to the second embodiment. Specific description will be provided later.

[0057] Fig. 14 is a block diagram that shows a configuration of a card verification system 10 according to the second embodiment. The control unit 11 of the card verification system 10 according to the second embodiment is constructed by adding a detection-use card information receiving unit 117, a detection-use card information comparison unit 118, an affiliated shop information acquisition unit 119, an illegal use information notification unit 1110, a card preservation instruction issuing unit 1111, a message generating unit 1112, a message display instruction issuing unit 1113, and a video preservation instruction issuing unit 1114 to

the functional blocks of the control unit 11 of the card verification system 10 according to the first embodiment shown in Fig. 5. Also, the memory unit 12 of the card verification system 10 according to the second embodiment is constructed by adding a detection-use card information storage unit 122 to the functional blocks of the memory unit 12 of the card verification system 10 according to the first embodiment shown in Fig. 5.

[0058] Fig. 15 is a diagram that shows an example of a detection information table 122a provided in a detection-use card information storage unit 122 of the card verification system 10 according to the second embodiment. In the following, a procedure according to the second embodiment will be described referring to Figs 11-15. A description duplicated with that in the first embodiment will be omitted as appropriate.

[0059] The investigative authorities request a card company to issue a card used to detect fraudulence. Accordingly, the card company creates, for example, a card of which the first use is regarded as normal use and of which the second or later use is regarded as illegal use (hereinafter, such a card will be referred to as a one-time card). The one-time card has the same appearance as a normal card but contains different card information. The detection-use card information generating unit 216 of the settlement system 20 generates card information for fraudulence detection according to the request from the investigative authorities and transmits the card information to the issuing unit 26. Accordingly, the issuing unit 26 issues a fraudulence

detection card containing the card information. In the card information storage unit 221, information of a fraudulence detection card having the same data structure as information of a normal card is registered. The detection-use card information notification unit 217 then notifies the card verification system 10 of the information of the fraudulence detection card.

[0060] The detection-use card information receiving unit 117 of the card verification system 10 receives the card information from the card verification system 10 and registers the card information in the detection-use card information storage unit 122. As shown in Fig. 15, detection-use card information includes a valid flag in addition to the items of normal card information. The valid flag is set to “0 (non-active)” when the detection-use card is in a normal use mode and is set to “1 (active)” when the detection-use card is in a detection mode. In the state where a card has not been used since the issuance of the card, the valid flag is set to “0”. Once a one-time card is used, the valid flag is changed from “0” to “1”. Card information in which the valid flag is “1” corresponds to card information indicating that the next use of the card will be regarded as illegal use.

[0061] After the card is used in multiple card reading terminal devices 30 to be investigated, the mode may be switched from the normal use mode to the detection mode. When a card reading terminal device 30 assumed to be used for skimming cannot be identified, a trap is sometimes set by allowing a number of card reading terminal devices 30 to read card information of a detection-use card. In

this case, after the card information is read by multiple card reading terminal devices 30, the mode may be switched from the normal use mode to the detection mode.

[0062] In the following, it will be assumed as an example that a different one-time card is used for each card reading terminal device 30 to be investigated. In this case, the place where skimming occurred can be uniquely identified. The issued one-time cards are distributed to investigators of the investigative authorities. By identifying a shop or an ATM mutually used by multiple skimming victims, the investigative authorities can identify a candidate of shops and ATMs with a strong possibility of being used for skimming. There is also a case where a candidate of shops and ATMs with a strong possibility of being used for skimming can be identified based on information provided by a citizen or an insider.

[0063] An investigator uses a one-time card at a shop or an ATM with a strong possibility of being used for skimming. Namely, the investigator allows a card reading terminal device 30 to be investigated to read the card information of the one-time card. The settlement request receiving unit 211 of the settlement system 20 receives from the card reading terminal device 30 a settlement request including the card information of the one-time card. The card validity judgment unit 212 then judges the validity of the card information included in the settlement request. In the card information storage unit 221, card information of a one-time card is also registered in a data structure same as that of normal card

information. Accordingly, the card validity judgment unit 212 judges the card information of the one-time card to be valid.

[0064] The authentication request notification unit 213 notifies the card verification system 10 of an authentication request including the card information of the one-time card. Accordingly, the authentication request receiving unit 111 of the card verification system 10 receives the authentication request from the settlement system 20. The detection-use card information comparison unit 118 then compares the card information with detection-use card information stored in the detection-use card information storage unit 122. When it is card information of a one-time card, there is card information identical therewith in the detection-use card information storage unit 122.

[0065] Accordingly, the detection-use card information comparison unit 118 retrieves the identical detection-use card information from the detection-use card information storage unit 122 and checks the valid flag therein. When the valid flag is “0”, the flag is changed to “1” and the information in the detection-use card information storage unit 122 is overwritten accordingly. After the valid flag is changed to “1”, normal authentication processing is performed for the authentication request. When the valid flag is “1”, in order to acquire detailed information of the affiliated shop, the affiliated shop information acquisition unit 119 notifies the settlement system 20 of an acquisition request for acquiring the affiliated shop information.

[0066] Accordingly, the affiliated shop information

notification unit 218 of the settlement system 20 retrieves the requested affiliated shop information from the affiliated shop information storage unit 222 and notifies the card verification system 10 thereof. In a second embodiment, as affiliated shop information, investigation information for facilitating detection of illegal use is also registered, in addition to the basic information including an address and a telephone number. In the example shown in Fig. 13, the type of the reader, whether or not a card return rejection function is provided, whether or not a message display function is provided, whether or not a security camera is installed, whether or not the security camera is connected to the network, and the investigative cooperation level are registered as the investigation information.

[0067] The readers fall roughly into two types: attended devices operated by users providing products or services; and unattended devices operated by cardholders themselves. A typical unattended device is an ATM. With a credit card with a caching function, by inserting the credit card into an ATM of a financial institute, a loan can be taken out up to a credit limit set by the card company. Namely, if the card information and PIN number of the credit card is leaked, there will be a risk of having money withdrawn.

[0068] The card return rejection function may be provided in a type of reader that holds the entire card or a large portion of the card to read the card information inside. For example, there are ATMs provided with a function to keep, when a fraudulent

card such as a forged card is inserted thereto, the inserted card inside so as not to return the card. A general swipe-type reader is not provided with such a card return rejection function.

[0069] The message display function is a function to display, on the display unit 34 of the card reading terminal device 30, information for a user providing a product or service. Since displaying a message for requesting investigative cooperation from a salesperson is basically considered, this function is provided for an attended device.

[0070] Whether or not there is a security camera 60 capturing images of the card reading terminal device 30 is registered. In addition, whether the security camera 60 is connected to the network 2 and remotely operable or is operated in a stand-alone mode is also registered.

[0071] The investigative cooperation level is set in advance for an affiliated shop by a card company or the investigative authorities together with the affiliated shop. There are five investigative cooperation levels in the description of the second embodiment, with “5” as the highest level and “1” as the lowest level. The level “5” is selected for an affiliated shop that actively helps investigation by prolonging a withdrawer’s stay at the register or holding a withdrawer, and the level “1” is selected for an affiliated shop that is reluctant to get involved in criminal investigation.

[0072] The affiliated shop information acquisition unit 119 in the settlement system 20 acquires affiliated shop information

from the card verification system 10. The illegal use information notification unit 1110 then notifies the police information system 50 via the network 2 of card illegal use information including the place where the fraudulent card was used, included in the affiliated shop information. For example, the illegal use information notification unit 1110 may notify the police information system 50 in the country where the fraudulent card was used. When the police information system 50 receives the card illegal use information from the card verification system 10, an investigator near the place where the fraudulent card was used is ordered to head for the site. For example, an investigator is informed of use of a fraudulent card by police radio by an investigation team of which the jurisdiction covers the place where the fraudulent card was used.

[0073] In some countries, a special organization other than the police may have investigation authority to detect card crimes. In this case, card illegal use information is conveyed to an information system in the organization. Alternatively, card illegal use information may be conveyed to an information system in a mass medium, such as a newspaper and a TV station. By allowing mass media to cover skimming crimes, raising public interest in skimming crimes can be expected.

[0074] When the affiliated shop information indicates that the card return rejection function is provided, the card preservation instruction issuing unit 1111 issues a fraudulent card preservation instruction for ordering that the card 3 inserted

into the card reading unit 36 of the card reading terminal device 30 be kept inside the card reading unit 36. The fraudulent card preservation instruction is then transmitted to the settlement system 20, and the instruction transfer unit 219 in the settlement system 20 notifies the card reading terminal device 30 of the fraudulent card preservation instruction. When the card reading terminal device 30 cannot directly control the card reading terminal device 30, an information system in the financial institute in which the card reading terminal device 30 is provided is requested to preserve the card 3 inserted into the card reading unit 36. Since the illegally used card 3 may have fingerprints of a withdrawer or another member of the criminal group left thereon, preserving the illegally used card will be preservation of evidence.

[0075] When the affiliated shop information indicates that a security camera is installed and the security camera is connected to the network, the video preservation instruction issuing unit 1114 issues a video preservation instruction for ordering that video data captured by the security camera 60 be preserved. The video preservation instruction is then transmitted to the settlement system 20, and the instruction transfer unit 219 in the settlement system 20 notifies a control system for the security camera 60 of the video preservation instruction. Since video images from the security camera 60 are generally erased after a retention period, preservation of at least video images captured at the date and time when the card was illegally used is requested.

The video preservation instruction may include a message for requesting submission of video images capturing a user who has illegally used the card to the investigative authorities.

[0076] When the security camera 60 is a type of camera of which the image quality including the resolution and frame rate can be adjusted by setting, the video preservation instruction issuing unit 1114 may instruct the control system for the security camera 60 to increase the image quality.

[0077] When the affiliated shop information indicates that the message display function is provided, the message generating unit 1112 generates a message to be displayed on the display unit 34 of the card reading terminal device 30. The message generating unit 1112 generates a message based on the investigative cooperation level, whether or not a security camera is installed, and whether or not the security camera is connected to the network, which are included in the affiliated shop information, and also based on the investigation policy of the police.

[0078] Figs. 16A–16D are diagrams that each show an example of a message displayed on the display unit 34 of the card reading terminal device 30. Fig.16A shows an example of a message for the case where the investigative cooperation level is “5” and a hardened security guard, for example, is allocated within the shop. When a stand-alone security camera 60 is installed, an alerting message, such as “Do not erase the camera footage”, may be added. Video images stored in the memory of the stand-alone security camera 60 are overwritten in a short period of time (in a day, for example)

in order to save the memory. Accordingly, it is preferable to display such an alerting message for preservation of video images from the security camera 60.

[0079] Fig. 16B shows an example of a message for the case where the investigative cooperation level is “4” or “5”. When a hardened security guard, for example, is not allocated within the shop, even if the investigative cooperation level is “5”, the message of Fig. 16B is selected instead of the message of Fig. 16A. After checking the message of Fig. 16B, the salesperson tries to gain time by requesting the user to fill in a personal information form, for example. Gaining time enables an investigator to get closer to the shop.

[0080] There may be an investigation policy of tracking a withdrawer so as to apprehend the withdrawer making contact with an upper member, rather than holding the withdrawer in the shop. In the case of this investigation policy, even if the investigative cooperation level is “5” and a hardened security guard is allocated within the shop, the message of Fig. 16B is selected instead of the message of Fig. 16A. This investigation method is effective especially when an investigator has been staking out the shop.

[0081] Fig. 16C shows an example of a message for the case where the investigative cooperation level is “2” or “3”. The message requests a salesperson to call the police without requesting a large burden on the salesperson. Shortly after a withdrawer left the shop, the salesperson who has dealt with the withdrawer vividly remembers the looks and clothes of the

withdrawer or the direction in which the withdrawer fled. Also, upon display of the message, the salesperson will observe the customer more carefully. The call from the salesperson helps the investigative authorities to accurately and promptly acquire information on the withdrawer, which can be used for the initial investigation.

[0082] Fig. 16D shows an example of a message for the case where the investigative cooperation level is “1” or “2”. In the case of an affiliated shop that is negative about investigative cooperation, the shop is requested to reject settlement for use of a fraudulent card. When the investigative cooperation level is “2” and a stand-alone security camera 60 is installed, preservation of video images from the security camera 60 may be requested.

[0083] The message display instruction issuing unit 1113 of the card verification system 10 issues a message display instruction for instructing the display unit 34 of the card reading terminal device 30 to display a message generated by the message generating unit 1112. The message display instruction is then transmitted to the settlement system 20, and the instruction transfer unit 219 in the settlement system 20 notifies the card reading terminal device 30 of the message display instruction.

[0084] Fig. 17 is a flowchart that shows a procedure of processing performed in the card settlement system 1 according to the second embodiment. Upon insertion of a card 3 for fraudulence detection, the card reading unit 36 in the card reading

terminal device 30 reads the card information (S30), and the control unit 31 then notifies the settlement system 20 of a settlement request including the card information thus read (S31).

[0085] Accordingly, the card validity judgment unit 212 judges whether or not the card information included in the settlement request is valid (S20). If the card information is invalid (N at S20), the process will skip to the step S24 in Fig. 8. If the card information is valid (Y at S20), the authentication request notification unit 213 will notify the card verification system 10 of an authentication request (S21).

[0086] Accordingly, the detection-use card information comparison unit 118 of the card verification system 10 makes a comparison to determine whether or not there is a piece of card information registered in the detection-use card information storage unit 122 that is identical with the card information for which the authentication request has been transmitted from the settlement system 20 (S13). If there is no identical card information (N at S13), the process will skip to the step S10 in Fig. 8. If there is identical card information (Y at S13), the valid flag of the identical card information is checked (S14). When the valid flag is “0” (N at S14), the detection-use card information comparison unit 118 changes the valid flag from “0” to “1” (S15). Thereafter, the process will skip to the step S10 in Fig. 8.

[0087] When the valid flag is “1” (Y at S14), the affiliated shop information acquisition unit 119 notifies the settlement

system 20 of an acquisition request for acquiring the affiliated shop information (S16). Upon reception of the acquisition request, the affiliated shop information notification unit 218 in the settlement system 20 retrieves the corresponding affiliated shop information from the affiliated shop information storage unit 222 and notifies the card verification system 10 thereof (S25). Accordingly, the affiliated shop information acquisition unit 119 in the card verification system 10 acquires the affiliated shop information thus conveyed by the settlement system 20 (S17).

[0088] The illegal use information notification unit 1110 notifies the police information system 50 of card illegal use information including an address included in the acquired affiliated shop information (S18). An instruction issuing unit issues an instruction for initiating processing to be performed in the affiliated shop when fraudulence is detected (S19), and the instruction transfer unit 219 of the settlement system 20 transfers the issued instruction to at least one of the card reading terminal device 30, an information system in the shop, and an information system for the security camera 60 (S26).

[0089] In the second embodiment described above, when a one-time card of which the valid flag is active is used, it can be regarded as deliberate illegal use. The withdrawer who knows the circumstances can be arrested on the spot. Even if a person has asked another person, who does not know the circumstances, to use the card, the person who has asked the another person will be an indirect perpetrator. Conventionally, at the time when a

withdrawer uses a fraudulent card, the victim generally has not noticed the skimming damage and hence has not filed a damage report yet. Accordingly, it has been legally difficult to arrest the withdrawer on the spot, even though the withdrawer's behavior seemed to be suspicious.

[0090] A one-time card has the same appearance as a normal card and can be normally used when the valid flag thereof is non-active. Accordingly, a person who has illegally obtained the card information and PIN number of the one-time card uses them without noticing that they are the card information and PIN number prepared for fraudulence detection.

[0091] In the second embodiment, investigation can be promptly initiated after an illegal use, so that the evidence can be preserved and a witness's memory will be reliable. In addition, if the withdrawer can be tracked, reaching an upper member of the criminal group can also be expected.

[0092] Also, if such an investigation method becomes widely known, a restraining effect on use of fraudulent cards can be expected. There have been an increasing number of cases where a person conspiring to use a fraudulent card purchases skimmed card information and PIN number through the Internet so as to make a fraudulent card. In this case, since the person who skimmed the card and the person who used the fraudulent card are less connected to each other, arresting the both persons is difficult.

[0093] However, if persons who are to use fraudulent cards feel the risk of being arrested at the time of use of the fraudulent

cards, an increasing number of the persons will be discouraged from causing a crime. Accordingly, it is expected that the demand for skimmed card information will be decreased, and the sales of skimmed card information of a seller will also be decreased. With such a mechanism, it can be expected that the number of skimming crimes will be gradually decreased.

[0094] The present invention has been described with reference to the embodiments. The embodiments are intended to be illustrative only, and it will be obvious to those skilled in the art that various modifications to a combination of constituting elements or processes could be developed and that such modifications also fall within the scope of the present invention.

[0095] In the second embodiment, there has been described the card settlement system 1 for enabling both an authentication method using the mobile terminal device 40 and criminal investigation using a card 3 for fraudulence detection. Alternatively, a card settlement system 1 dedicated to criminal investigation using a card 3 for fraudulence detection may be constructed.

[0096] Fig. 18 is a block diagram that shows a configuration of a card verification system 10 dedicated to criminal investigation using a card 3 for fraudulence detection. Compared to the card verification system 10 shown in Fig. 14, the mobile terminal information retrieval unit 112, check request notification unit 113, check result receiving unit 114, and authentication unit 115 can be omitted in the card verification

system 10 shown in Fig. 18. Also, instead of an authentication request, a reference request for requesting a reference regarding whether or not it is card information of a detection-use card is transmitted from the settlement system 20. Accordingly, a reference request receiving unit 111a and a reference result notification unit 116a are provided instead of the authentication request receiving unit 111 and authentication result notification unit 116.

[0097] In the above description, a card 3 is assumed to be a credit card, but it may also be a bank ATM card, an electronic money card, or a debit card. In particular, if the card verification system 1 according to the first embodiment is applied to an ATM card system and it is set so that a settlement confirmation notice is sent to the child's mobile terminal device 40, it can be effectively prevented that the remittance scam aimed at elderly people.

[DESCRIPTION OF THE REFERENCE NUMERALS]

[0098] 1 card settlement system, 2 network, 3 card, 10 card verification system, 11 control unit, 111 authentication request receiving unit, 111a reference request receiving unit, 112 mobile terminal information retrieval unit, 113 check request notification unit, 114 check result receiving unit, 115 authentication unit, 116 authentication result notification unit, 116a reference result notification unit, 117 detection-use card information receiving unit, 118 detection-use card information

comparison unit, 119 affiliated shop information acquisition unit, 1110 illegal use information notification unit, 1111 card preservation instruction issuing unit, 1112 message generating unit, 1113 message display instruction issuing unit, 1114 video preservation instruction issuing unit, 12 memory unit, 121 card/mobile terminal relation information storage unit, 122 detection-use card information storage unit, 20 settlement system, 21 control unit, 211 settlement request receiving unit, 212 card validity judgment unit, 213 authentication request notification unit, 214 authentication result receiving unit, 215 settlement judgment result notification unit, 216 detection-use card information generating unit, 217 detection-use card information notification unit, 218 affiliated shop information notification unit, 219 instruction transfer unit, 22 memory unit, 23 communication unit, 24 display unit, 25 operation unit, 26 issuing unit, 30 card reading terminal device, 31 control unit, 32 memory unit, 33 communication unit, 34 display unit, 35 operation unit, 36 card reading unit, 37 printing unit, 40 mobile terminal device, 41 control unit, 42 memory unit, 43 communication unit, 43a antenna, 44 display unit, 45 operation unit, 46 imaging unit, 47 GPS receiving unit, 50 police information system, 60 the security camera.

[INDUSTRIAL APPLICABILITY]

[0099] The present invention is applicable to a field of credit card settlement.

WHAT IS CLAIMED IS:

1. A card verification system, comprising:

a fraud detection-use card information storage unit that stores card information indicating, when the number of uses is a predetermined number or less, the use is regarded as normal use, and, when the number uses exceeds the predetermined number, the use is regarded as illegal use; and

an illegal use information notification unit that notifies a predetermined information system about illegal use of the card, the illegal use information including location of where the card was used, when a settlement system has received a settlement request from a card reading terminal device with card information identical to card information registered in the fraud detection-use card information storage unit and when the number of uses exceeds the predetermined number.

2. The card verification system of claim 1, wherein the predetermined number is one.

3. The card verification system of claim 1, wherein, when the number of uses is a predetermined number or less, the use is regarded as normal use, and, when the number uses exceeds the predetermined number, the use is regarded as illegal use, and the card information indicates that the card read by a card reading terminal device is to be investigated.

4. The card verification system of claim 1, wherein the card reading terminal device comprises a reading unit capable of keeping an inserted card inside, and

wherein the card verification system further comprises a card preservation instruction issuing unit that issues a fraudulent card preservation instruction for ordering that a card inserted into the reading unit be kept inside when card information, for which a request is made by a settlement system that has received a settlement request from the card reading terminal device, is identical with card information registered in the fraud detection-use card information storage unit and also when the number of uses exceeds the predetermined number.

5. The card verification system of claim 1, wherein the card reading terminal device comprises a display unit that displays information for a user providing a product or service, and

wherein the card verification system further comprises a message display instruction issuing unit that issues a message display instruction for instructing the display unit of the card reading terminal device to display a message for conveying illegal use when a settlement system has received a settlement request from the card reading terminal device with card information identical to card information registered in the fraud detection-use card information storage unit and when the number of uses exceeds the predetermined number.

6. The card verification system of claim 1, wherein:

a security camera capturing images of the card reading terminal device is installed; and

the card verification system further comprises a video preservation instruction issuing unit that issues a video preservation instruction for ordering that video data captured by the security camera be preserved when a settlement system has received a settlement request from the card reading terminal device with card information identical to card information registered in the fraud detection-use card information storage unit and when the number of uses exceeds the predetermined number.

7. A method for detecting illegal use of a card, comprising:

a first step of receiving an authentication request from a settlement system that has received a settlement request from a card reading terminal device that has read a card for which, when the number of uses is a predetermined number or less, the use is regarded as normal use, and, when the number uses exceeds the predetermined number, the use is regarded as illegal use;

a second step of determining whether or not information of the card is identical with card information registered in a fraud detection-use card information storage unit and whether or not the number of uses is the predetermined number or greater; and

a third step of notifying a predetermined information system, when the information of the card is identical with card information registered in the fraud detection-use card information storage unit

and when the number of uses is the predetermined number or greater, of card illegal use information including the place where a fraudulent card was used.