Activities for Security of ATM-BankIT

Ryoko Tsutsui Kazuhiro Kondou

Services provided by financial institutions are diversifying due to the advancement of network technologies in recent years, raising the level of convenience fordepositors. However, there has also been an increase in the number of crimes that outsmart technologies used in such services.

Incidents are on the rise involving counterfeit or stolen cards at ATMs resulting in the withdrawal of entire savings from accounts, which raises the level of interest for security as a preventative measure for crime.

This paper describes the security environment required for ATMs and also introduces activities relating to ATM-BankIT, which was announced in March 2005.

Crime surrounding ATMs

The status of damage thus far, according to a survey conducted by the Financial Service Agency, is shown below. **Figure 1** and **Figure 2** illustrate how the damage caused by counterfeit cards has been increasing since 2003[1)]. The following are the main methods used for the unauthorized drawing of funds from ATMs that have so far been detected:

- The perpetrator glances at the depositor as he or she operates the ATM before stealing the cards from the bag or wallet of the depositor by purse snatching or other means and the funds are drawn out during the time it takes the depositor to notify the police.
- Cash cards, along with items that reveal the personal information of the victims, such as a driver's license, are stolen through break ins and the funds are drawn out by determining the personal identification numbers using an analogy from the date of birth or the telephone numbers described on the stolen items.
- Cards are prepared with the data obtained by scanning the cards of other people, which are then used to draw funds from ATMs.

On many of these occasions the depositors were completely unaware of when the cards or data were stolen and in some cases such incidents were not discovered until the depositor verified his or her account balance at the bank.

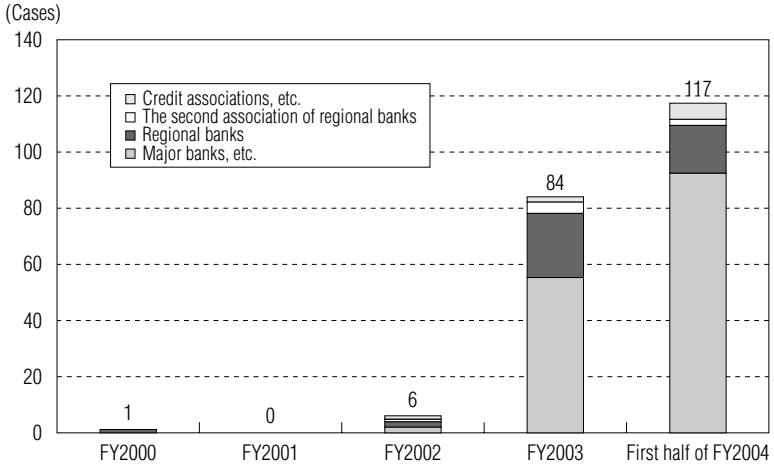

Fig. 1 Transition of number of incidents due to counterfeit cards

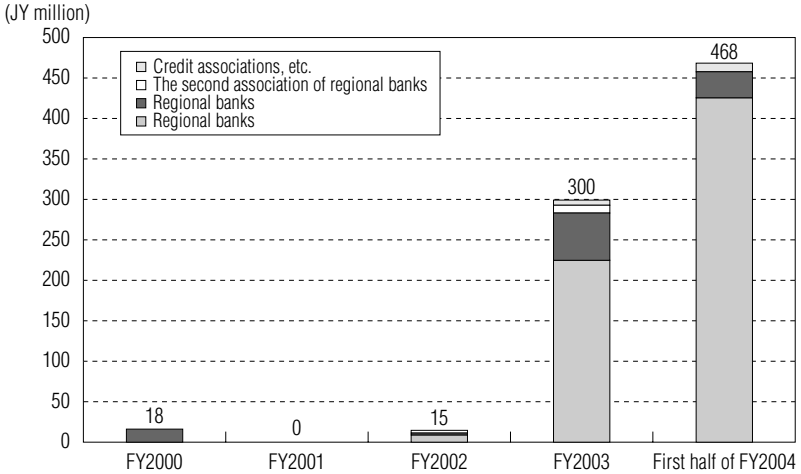

Fig. 2 Transition of amount of damage due to counterfeit cards

Activities undertaken by financial industry

Activities implemented by the Japanese Bankers Association, once they became aware of these examples, include the following.

- Established extremely difficult to counterfeit standard specifications for IC cash cards.
- Raised awareness of depositors regarding their handling of cash cards and personal identification numbers (2003 to 2004).
- Compensation rules determined for damages incurred due to counterfeit cash cards (October 2005).

It was decided that financial institutions will compensate the full amount of damages if there is no fault by the depositor who becomes a victim of a crime with regards to the management of cash cards and personal identification numbers[2), 3)].

Furthermore, the Center for Financial Industry Information Systems again announced in April 2005 their security standard for financial information systems as a strategy to prevent such crimes.

The Financial Service Agency also recommended in their "Final Report by the Study Group on Counterfeit Cash Card Problems" of June 2005 regarding financial information systems, which include ATMs among others[4)]. In response to these financial institutions have been implementing the following types of countermeasures:

- Introduced the use of IC cash cards (from 2002).
- Set up service for individuals to set withdrawal limit (from 2002).
- Lowered withdrawal limit amounts.
- Set up service to allow depositors themselves to set time periods and locations for withdrawing funds at ATMs (from 2005).
- Started verification of identification through biometric authentication (from 2004).
- Introduced an abnormal transaction detection system.

Activities undertaken for ATM-BankIT

The development of ATM-BankIT (**Photo 1**), announced by Oki Electric in March2005, was conducted based on four product concepts.

a. Raised security levels

Security functions were substantiated (details to be described later) from the standpoint of crime prevention strategies and enhanced monitoring of crime.

b. Raised reliability levels and reduced operating costs

The reliability of equipment has been dramatically improved and unattended operation over a long period has been achieved. Furthermore, the banknote stacker capacity has been increased to a larger volume, contributing to a reduction in guarded cash delivery costs.

Photo 1 ATM-BankIT

c. Comfortable operability

Guidance for operations is provided by light display functions. Furthermore, the concept of a universal design has been adopted in consideration for the usability of physically challenged and elderly persons.

d. Expandability and multifunctionality

The installation of dedicated units was performed in order to make it possible to offer services that are linked with non-contact IC cards and mobile phones, which are assumed to be utilized in a variety of circumstances in the lives of consumers.

Increasing the level of security in particular, was the area in which most efforts were made with regards to ATM-BankIT. Specific details of the activities undertaken are shown below.

(1) Strategies for preventing crime

a. Prevention of card counterfeiting

- **IC cash cards**

Standard functions of ATM-BankIT hardware support IC cash cards. It is possible to prevent the counterfeiting of cards with IC cash cards, because they offer a higher tamper resistance in comparison with conventional magnetic cards, which makes it difficult for counterfeiters to skim data from the card or to write unauthorized data on the card.

- **Masking of account numbers on transaction receipts**

Since it is believed that there are ways by which cards are counterfeited by deducing the data information on the cash cards from the receipts issued by ATMs, a portion of the information indicated on receipts is masked so that the entire data will not be revealed.

b. Raised level of elaborate authentication

- **Biometric authentication**

It is possible to use biometric authentication technology in place of conventional personal identification numbers, as a means of user authentication with ATM-BankIT. Three methods of biometric authentication are available, including the palm vein authentication (**Photo 2**), finger vein authentication and iris authentication. Selections can be made with these methods according to the needs of the bank.

Authentication is conducted using the biometric data of the depositor that is pre-registered on the IC cash card and verified against data obtained from the scanning of a hand, finger or eye held to the sensor when ATMs are used. In general, the false detection rate of biometric authentication technology is extremely low at 0.01% or less, making the unauthorized drawing of funds with stolen cards extremely difficult in comparison with using a personal identification number that can be guessed.

Photo 2 Image of authentication using palm vein sensor

c. Strategy for preventing theft of personal identification numbers

- **Field of light control film**

A special light control film is installed on the display screen of ATMs to restrict the field of view of the screen to prevent unauthorized persons from glancing at the entry contents (particularly the personal identification number) from the rear or sides.

- **Rear verification mirror**

Mirrors with a wide 90-degree field of view are installed at the front of ATMs, making it possible for users operating the ATMs to verify whether suspicious persons are behind them. Deterrent effects against criminals are also expected.

- **Scrambled display of personal identification number entry keys**

The ten key arrangements used for entering personal identification numbers on ATM screens are randomly rearranged and displayed for each transaction. Even with the implementation of a field of view limiting filter, there is a potential danger of having personal identification numbers deciphered through the observation of finger movements alone. The application to display entry keys in a scrambled arrangement was prepared for that reason.

- **Personal identification number modification function on ATMs**

Since personal identification numbers can be guessed or obtained by glancing at displays, it is desirable to set numbers that are unlikely to be guessed as well as by periodically changing the number. For this reason personal identification numbers can now be changed on the screen of ATMs.

- **Raising awareness at ATMs**

Messages are displayed on the screens of ATMs to promote caution for setting personal identification numbers that are difficult to guess.

Of all the depositors who became victims of crime, 45.2% were using numbers that were based on their date of birth, phone numbers or addresses1, implying that personal identification numbers may have been guessed, based on the aforementioned personal information.

Periodical verification of the account balance and changing the personal identification numbers on the screen are urged for this reason. Alternatively, cautionary messages can be displayed each time a transaction is performed with depositors who are using personal identification numbers that are easily guessed, such as those that match their date of birth.

- **Encrypting pin pads**

It is also possible to install encrypting pin pads as dedicated keys for entering personal identification numbers. Analysis of personal identification numbers from the details of communications with host computers is prevented, since encryption is performed inside the unit of the pin pad.

d. Strategies to prevent criminal withdrawal of large sums

- **Modification function for withdrawal limits**

It is possible for depositors themselves to change the withdrawal limits using the screens of ATMs. If the withdrawal limit is large the entire balance of an account can be withdrawn before a depositor becomes aware of the damage, however, it is possible to lower the withdrawal limit to the level of normal withdrawals. Since it is necessary to carry out procedures at tellers to raise the withdrawal limit, it is not possible for third parties to misuse the modification function of ATMs.

(2) Monitoring functions

a. Monitoring functions of ATMs

- **Customer cameras**

It is possible to obtain an image of a person operating an ATM each time a transaction is performed by using the customer camera installed at the front of an ATM. This is

combined with a search function that handles multiple conditions, making it possible to acquire evidence material that could be used after an incident, particularly when a transaction is made using a stolen or counterfeit card.

- **Image monitoring system**

The images taken by monitoring cameras installed inside branches are recorded on large capacity hard disk drives in image-monitoring servers at the center via DVR. The system offers superior search characteristics since it is possible the data can be centrally managed on the single media of a hard disk drive. It is, therefore, possible to provide a rapid response when transaction problems or crimes occur. Furthermore, by linking up with ATMs, it is possible to equip the system with a function to obtain images at the same time a transaction takes place. In addition, it is possible to detect and automatically monitor suspicious persons and suspicious objects through the dynamic object analysis of images taken by monitoring cameras.

(3) Around the clock customer response

Oki Electric is offering comprehensive services, such as accepting consignments for ATM monitoring operations, through an affiliated company specializing in the operation of ATMs (Japan Business Operations Co., Ltd.). Timely customer responses are made possible by outsourcing the work through the consignment of operations to a company specializing in these operations. When a depositor becomes aware of an irregularity with regards to their account balance, it is possible to receive a relevant notification immediately so they can invalidate the cash card to prevent extensive damage from occurring.

References

1) Financial Services Agency, Overview of Results from Fact Finding Survey on Problems of Counterfeit Cash Cards, February 2005.
2) Japanese Bankers Association, Amendment on Draft Proposal for Card Regulations, October 2005.
3) Japanese Bankers Association, Consensus on Protection of Depositors Regarding Counterfeit and Stolen Cash Cards, October 2005.
4) Financial Services Agency, Final Report by the Study Group on Counterfeit Cash Card Problems, June 2005.

Authors

Ryoko Tsutsui: System Hardware Company, System Hardware Development Div., System Design Dept.-2, ATM SE Team.

Kazuhiro Kondou: System Hardware Company, System Hardware Development Div., System Design Dept.-2, ATM SE Team, Team Leader.