Toward a cashless society in 2020!

Ensure the safety and security of credit card transactions

Credit cards are becoming more and more indispensable in our everyday lives, being used for online shopping or at a supermarket. However, identity card data breach and fraudulent credit card transactions are also increasing with the expansion of credit card use. How can the safety of transactions be ensured? Let's look at the problems and countermeasures.

Do not allow card holder data to be stolen!

In order to prevent card data breach, make sure not to store card data online and always comply with security standards.

Do not allow the use of counterfeit cards at stores!

Promote the introduction of IC credit cards, which are difficult to counterfeit, and reinforce the identification stage by making customers enter a PIN code at the store.

Do not allow the use of stolen credit card data on the Internet!

Counteract fraudulent use of credit card account number with new ways to identify cardholders.

The total number of credit cards issued in Japan as of 2015 is approximately 258.9 million. In addition to in-store payment, they are also used for e-commerce. In 2014, the usage increased by 10.7% from the previous year to approximately 46 trillion yen. However, cases of identity card data breach and fraudulent credit card transactions are also increasing rapidly. While other countries are taking strict security countermeasures, if Japan lags behind and becomes a "security hole," society here may even become a nest for card criminal fraud. There is an urgent need to implement countermeasures.

Envisaging the Tokyo 2020 Olympic and Paralympic Games, it is necessary to ensure the safety and security of credit card transactions, which have become a staple modern payment method, and realize a cashless society. In order to do so, multi-layered actions at each and every occasion of handling credit cards, such as the prevention of card data breach and the prohibition of fraudulent credit card transactions are necessary. If data such as card numbers and expiration dates are stolen, it will lead to fraudulent credit card transactions. Therefore, countermeasures taken by relevant business operators to prevent information leaks are essential. Recommended measures include stopping storage of card data at member merchants, which tend to have lax security, and compliance with PCI DSS, which is the international security standard.

IC cards are effective in preventing fraudulent credit card transactions at stores. It is difficult to counterfeit an IC credit card, and identification can be done by entering a PIN code at a store. On the other hand, the payment terminal at the store must be chip migration, and the introduction of POS terminals is lagging. To prevent fraudulent use of credit card account number on e-commerce, there are measures such as the use of a pre-registered password or identification process which asks the user to enter the security code shown on the back of the card which require the cardholder’s better understanding for every transaction.

The promotion of cashless payment also energizes business. However, without ensuring the security of the consumers, other problems may occur. Therefore, the cross-industrial “Credit Transaction Security Council” was inaugurated, aiming at reinforcing security to promote cashless payment. Measures are taken under close cooperation between the government and the private sector.

Losses due to fraudulent use in 2014 amounted to approximately 113.9 billion yen, increasing 1.7-fold from two years earlier. About 60% occurred in Card-Not-Present (CNP) merchants, such as e-commerce.

Promote the introduction of IC credit cards, which are difficult to counterfeit, and reinforce the identification stage by making customers enter a PIN code at the store.

Countercraft fraudulent use of credit card account number with new ways to identify cardholders.

Ensure the safety and security of credit card transactions

Do not allow the use of counterfeit cards at stores!

Promote the introduction of IC credit cards, which are difficult to counterfeit, and reinforce the identification stage by making customers enter a PIN code at the store.

Do not allow the use of stolen credit card data on the Internet!

Counteract fraudulent use of credit card account number with new ways to identify cardholders.

The total number of credit cards issued in Japan as of 2015 is approximately 258.9 million. In addition to in-store payment, they are also used for e-commerce. In 2014, the usage increased by 10.7% from the previous year to approximately 46 trillion yen. However, cases of identity card data breach and fraudulent credit card transactions are also increasing rapidly. While other countries are taking strict security countermeasures, if Japan lags behind and becomes a "security hole," society here may even become a nest for card criminal fraud. There is an urgent need to implement countermeasures.

Envisaging the Tokyo 2020 Olympic and Paralympic Games, it is necessary to ensure the safety and security of credit card transactions, which have become a staple modern payment method, and realize a cashless society. In order to do so, multi-layered actions at each and every occasion of handling credit cards, such as the prevention of card data breach and the prohibition of fraudulent credit card transactions are necessary. If data such as card numbers and expiration dates are stolen, it will lead to fraudulent credit card transactions. Therefore, countermeasures taken by relevant business operators to prevent information leaks are essential. Recommended measures include stopping storage of card data at member merchants, which tend to have lax security, and compliance with PCI DSS, which is the international security standard.

IC cards are effective in preventing fraudulent credit card transactions at stores. It is difficult to counterfeit an IC credit card, and identification can be done by entering a PIN code at a store. On the other hand, the payment terminal at the store must be chip migration, and the introduction of POS terminals is lagging. To prevent fraudulent use of credit card account number on e-commerce, there are measures such as the use of a pre-registered password or identification process which asks the user to enter the security code shown on the back of the card which require the cardholder’s better understanding for every transaction.

The promotion of cashless payment also energizes business. However, without ensuring the security of the consumers, other problems may occur. Therefore, the cross-industrial “Credit Transaction Security Council” was inaugurated, aiming at reinforcing security to promote cashless payment. Measures are taken under close cooperation between the government and the private sector.

Losses due to fraudulent use in 2014 amounted to approximately 113.9 billion yen, increasing 1.7-fold from two years earlier. About 60% occurred in Card-Not-Present (CNP) merchants, such as e-commerce.
A principle is “do not store card holder data.” Comprehensive information security measures are necessary for any card holder data retention.

The major target of recent attacks and leakage of credit card data is merchants; many of them with insufficient security measures. The number of cases targeting relatively small merchants has been increasing sharply since 2015. “It’s not uncommon to see cases where the password for the merchant operation screen of an e-commerce website is left as the default password and the screen is attacked, with the data on the server being stolen. On the Internet, anyone can attack the default password and the screen is attacked, with the merchant operation screen of an e-commerce website is left unsecured. In the U.S., lawsuits of the damages are taking place. Even if you introduce a “link-type” service where the card holder data transmitting, processing and storage is not done on the server of your own, it is necessary to constantly reinforce the security countermeasures of the in-house system,” says Mr. Okochi, and he encourages people to take comprehensive measures.

12 PCI DSS requirements

1. Install and maintain a firewall configuration to protect cardholder data.
2. Use strong password management policies and procedures.
3. Regularly test security systems and processes.
4. Maintain a secure maintenance process.
5. Regularly test system controls and security applications.
6. Restrict access to cardholder data to a minimum business need.
7. Identify and authenticate access to system components.
8. Maintain physical access control for cardholder data.
9. Limit access to cardholder data to only personnel who need it.
10. Ensure that there is no access to cardholder data from the network.
11. Regularly test firewall and intrusion detection systems and processes.
12. Maintain a policy that will require information security for all users.

Mr. Takayuki Okochi
Forensic Senior Consultant, Payment Card Forensics, Inc.

Do not allow card holder data to be stolen!

Do not allow the use of counterfeit cards at stores!

Increased introduction of IC credit cards, which are difficult to forge, and making payment terminals compatible with ISAIC cards is the key to the prevention of the illegal use of credit cards at retail stores. Tobu Department Store Co., Ltd. made its payment terminals compatible with ISAIC in 2004, being among the first in the industry.

Mr. Naoki Inoue of the Information System Department of Tobu Department Store Co., Ltd. explains the background: “At that time, skimming (theft and copying of information) of magnetic cards was recognized as a public problem, and customers were starting to switch to IC cards. Coping with IC was, so to speak, a requirement of the times. We considered that if IC-compatible mobile POS terminals could be introduced and payment could be made right in front of the customer on the sales floor, it would also lead to improvements in the quality of customer service. The company established a rule that a PIN code must also be entered when IC cards are used, and applied the rule to all sales floors. At first, questions were raised such as whether it was necessary to enter the PIN code even when buying food, but the company stuck to the idea that IC cards that realize higher safety should be handled differently from conventional cards.” The company maintained their PIN number policy, provided polite explanations during each transaction and asked for the customers’ understanding in enforcing the policy.

In February 2013, thanks to the input from the sales floors, the company replaced its terminals with new POS terminals with enhanced safety and improved functionality. “We customized the product in cooperation with the terminal manufacturer, by improving the operability, applying a lid that hides the hand when entering the PIN number, and making the sound of the alarm softer to avoid disturbing people on the sales floor.” (Mr. Inoue)

Using Europe as an example, currently almost all credit cards in circulation have been switched to IC cards, and there are new cards that require a PIN code to be entered. Compatibility with IC is now an international security standard. The use of IC cards has also spread throughout Japan, and electric appliance retailers that handle expensive products with high cash values are following the trend. While there are difficulties particular to department stores, such as payment being made separately on each floor, the secret of the success of the Tobu Department Store was probably the cooperation between the sales floors and the Information System Department in integrating the systems. “IC cards terminals are used by millions of customers. Therefore, we aimed to develop a device which can be used for ten years or more. We will continue putting efforts into creating an environment in which customers can enjoy safe, comfortable and worry-free shopping, by also listening to opinions from sales floors,” Mr. Inoue stresses.

Mr. Naoki Inoue
General Manager, Information System Department, Tobu Department Store

Introduce POS terminals compatible with IC cards, and reinforce security through secure operation.
Prevent fraudulent use of credit card account number with the introduction of measures such as 3-D Secure and other countermeasures to ensure safer online shopping

Credit card fraud losses in 2014 amounted to approximately 11.4 billion yen. About 60% of this value consists of damages caused in CNP transactions such as e-commerce and mail/fax order.

“In particular, many e-commerce merchants are suffering from CNP fraud. There are increased cases where the server of merchant is hacked, card numbers, expiration dates, and ID/passwords are stolen and fraudulently used in transactions with other CNP merchants,” explains Mr. Hajime Sato of Toyota Finance Corporation.

Various methods to prevent CNP fraud have emerged, including verification of card security codes printed on the back of credit cards, fraud detection through checking the purchase history of the user, risk-based scoring based on attributes such as the login environment, and recording and monitoring addresses of delivery, which the fraudulently purchased products are sent. Probably the most widely recognized method among them is 3-D Secure, which authenticates cardholder with a pre-registered password.

“Our company also has started providing 3-D Secure authentication service to the cardholders since 2006. You need to register a password to our website prior to using your card on e-commerce merchant in order to make a transaction. Currently about 53% of the transactions at 3-D Secure implemented merchants are authenticated by 3-D Secure,” says Mr. Sato. In order to improve credit card security, it is effective to introduce the abovementioned countermeasures at multiple levels. However, to increase the ratio of 3-D Secure transactions and to prevent cardholders from reusing passwords for multiple merchants, which can easily allow to leak passwords followed by fraudulent use, the understanding and cooperation of cardholders are also necessary. Mr. Sato explains the efforts to be made from this point on.

“The industry continues to make efforts to inform the public of following factors; improvements in awareness of the countermeasures against card fraud in e-commerce, the risk of reusing passwords for multiple merchants, and publication method of policies and measures for card security.”

For the realization of a cashless society

Credit cards are convenient for users everywhere. Currently, approximately 260 million have been issued in Japan, meaning more than two cards per capita. Places where credit cards can be used are increasing, but the development of an environment where cards can be used safely and without worry is indispensable and must be a prerequisite.

For example, does your credit card have an IC chip? Do you enter a 4-digit PIN code when making purchases at stores? Do you enter an identification password when shopping online? People are unfamiliar with the large variety of technologies and countermeasures being introduced in relation to credit card security, but consumers should be aware of how to protect their own assets (card information). The number of tourists from abroad is increasing rapidly these days. With Japan hosting the Rugby World Cup in 2019 and Olympic and Paralympic Games in Tokyo in 2020, it is expected that the number of visitors from abroad will increase further. Creating the secure environment necessary to allow tourists to enjoy shopping in Japan on par with the highest international standards should also be a part of Omotenashi (Japanese-style hospitality). Credit cards now serve as an important transaction infrastructure for the nation. By improving the security level, we aim to realize a safe and secure cashless society.