Financial Services Commission

*A New Era of Hope*
Creative Finance
Financial Inclusion
Solid Financial System

# GUIDELINE FOR PERSONAL DATA PROTECTION

## 10 CHECKLISTS FOR PERSONAL DATA PROTECTION

1. Be aware that **your credit cards are safe to use**. All files and USB drives containing personal information from the three credit card companies were confiscated by the prosecutors and there is **no possibility that your credit cards could be used fraudulently**.
2. Sign up for "**credit card payment notification SMS service**" provided by credit card companies free of charge to receive SMS notice on every payment settled using your credit card.
3. **Visit the website of respective credit card companies** or make a phone call to **call centers** to check whether your credit card has been misused.
4. No need for extra charge when cancelling or re-issuing credit cards.
5. Report to the respective credit card company for any loss via website, call centers, or by visiting nearby office. **Credit card companies will cover all financial loss** in case any fraudulent transaction incurs.
6. Be reminded that credit card companies, in any case, **do not send SMS related to personal data breach**.
7. **Do not click** any links attached to **emails** or **SMS from anonymous sources** and erase them immediately.
8. **Do not answer any questions** but **hang up immediately** if you receive phone calls asking for credential information such as credit card PIN number or CVC code from someone claiming to be as someone from public institutions, financial authorities, or financial companies.
9. Report immediately to the **police(☎112)**, **Financial Supervisory Service(☎1332)**, or respective **financial companies** if you suspect any financial fraud.
10. **Damage Report Center is open 24 hours** to provide any assistance related to personal data breach.

| | KB Kookmin Card | NH Nonghyup Card | Lotte Card |
|---|---|---|---|
| **Website** | www.kbcard.com | www.card.nonghyup.com | www.lottecard.co.kr |
| **Call Center** | 1899-2900 | 1644-4000, 1644-4000 | 1588-8100 |
| **Damage Report Center** | 1588-1688 | 1644-4199 | 1588-8100, 2-2211-5500, 051-606-2700 |

Listen Well
Inform Accurately

## MOST FREQUENTLY ASKED QUESTIONS ABOUT PERSONAL DATA PROTECTION

**Q1: How can I check whether my personal details have been leaked?**

A1: Please visit the websites of respective credit card companies to check the details about your personal information.

| | |
|---|---|
| **KB Kookmin Card** | www.kbcard.com |
| **NH Nonghyup Card** | www.card.nonghyup.com |
| **Lotte Card** | www.lottecard.co.kr |

Credit card companies will send emails and letters to inform you on the related details. However, please be noted that credit card companies never send any SMS related to the data leak accident.

**Q2: What should I do if my personal information has been breached?**

A2: The prosecutors confirmed that all leaked information has been confiscated before being circulated. Therefore, your credit cards are safe to use. Those who are still worried can change PIN number, re-issue, or cancel credit cards free of charge by visiting respective company's website and nearby office or simply by making a phone call to the call centers.

**Q3: Do I have to bare all the costs for credit card re-issuance?**

A3: All costs will be covered by the credit card companies when re-issuing the same type of credit card.

**Q4: Is there any service provided by credit card companies to prevent fraudulent use of leaked information?**

A4: Credit card companies provide free credit card payment notification SMS service upon application. Moreover, the Korea Credit Bureau(KCB) is providing Personal Information Protection Service[1] free for one year.

**Q5: What else do financial customers have to be aware of?**

[1] KCB sends SMS notice whenever financial firms inquire into the client's personal information for loan approval, credit card issuance, and etc.

A5: Although it is highly unlikely that the leaked data could be used fraudulently, there is a possibility for increased financial frauds such as voice phishing and smishing taking advantage of public anxiety. Please do not receive phone calls or open SMS and emails from unidentified sources claiming to be as the financial authorities or financial institutions.

**Q6: What if the leaked data has been circulated within the market, can my information be used by someone else for credit card transactions?**

A6: It is extremely unlikely that your information would be used fraudulently since credential information such as PIN number and CVC code has not been leaked. However, there are very small minority of merchants requiring only credit card number and expiry date to settle payment. Please report to the authorities immediately if you suspect any misuse of your private information.

**Q7: Can the leaked information be used fraudulently outside of Korea?**

A7: Most of overseas merchants require CVC code for credit card transaction. So, fraudulent use of personal data is very unlikely. But there are few cases when payments can be made simply by surrendering credit card number and expiry date in some overseas online stores. Please report to the authorities immediately if any misuse of the leaked information is found.

Meanwhile, fraudulent use of personal information outside of Korea can be prevented by singing up for a service that automatically denies approval of any credit card transaction made outside of Korea by allowing credit card companies to access to your immigration information controlled by the Ministry of Justice Immigration Control System. The service is applicable on credit card companies' website.

**Q8: Is there any possibility of someone else counterfeiting a credit card bearing my credit card information?**

A8: There is no such possibility since PIN number and CVC code have not been leaked.

**Q9: Is there any possibility that my money could be transferred to someone else from**

**the bank account used for credit card payment?**

A9: Transferring money from a bank account requires bank account number, authentication certificate, security card, PIN number, and additional personal identification procedures. The leaked data does not include credential information such as PIN number. Therefore, someone else transferring your money from your bank account is impossible.

**Q10: Can someone else change my bank account PIN number only with my resident registration number and name to withdraw money or misuse it?**

A10: Changing bank account PIN number is only possible by visiting respective bank and credit card offices, or going through online identification procedures and SMS authentication. Therefore, changing your bank account PIN number with the leaked information is impossible.

**Q11: What should I do if I suspect any loss incurred by the data leak?**

A11: If you suspect that your personal information has been circulated, immediately report to the authorities and credit card companies. Websites and Damage Report Centers are open all day.

| | Call Center | Email |
|---|---|---|
| **Financial Supervisory Service** | 1322 | privacy@fss.or.kr |
| **KB Kookmin Card** | 1899-2900 | - |
| **NH Nonghyup Card** | 1644-4199 | - |
| **Lotte Card** | 1588-8100 | - |

**Q12: What should I do if I received a SMS notice on credit card transaction that I didn't make?**

A12: Financial losses caused by fraudulent use of leaked personal information will be fully covered by the credit card companies. Please report to the respective company and follow instructions.

**Q13: What is the plan to reimburse financial losses from the information leak?**

A13: Credit card companies will cover all financial losses incurred from the misuse of credit card due to the data leak accident.