Press Release

Jaunary 22, 2014

MEASURES TO PREVENT A RECURRENCE OF PERSONAL DATA BREACH

The FSC and relevant ministries[1]announced a set of preventive measures to protect financial consumers from personal data breach. The measures are focused on alleviating people's concerns and inconvenience caused by the recent data leaks; punishing those responsible for the incident; and preventing a recurrence of data theft.

BACKGROUND

Prosecutors announced (Jan.8/Jan.19/Jan.21) that about 100 million credit card account details were leaked from Kookmin Card, Nonghyup Card and Lotte Card[2] by a contractor with the personal credit rating company Korea Credit Bureau (KCB) over the course of a year beginning in December 2012. **The contractor and the alleged buyers of the information were arrested; and the original files and USB of the stolen data were confiscated with no sign of further circulation.**

The FSS received the data from prosecutors (Jan.10) and found that about 85 million accounts were compromised in total, excluding the number of cards held by the deceased, companies or merchants, although overlaps in multiple cardholders were included.

The stolen data includes basic personal data such as names, resident registration numbers, addresses, mobile phone numbers and company names, as well as financial information such as credit card numbers, account numbers, expiry dates and annual income. However, no passwords or CVC codes[3] had been stolen.

MEASURES TO EASE CONCERNS AND INCONVENIENCE FROM THE INCIDENT

The three credit companies said that there had been no financial damage reported so far related to the breach. The FSS found that sensitive information such as credit card passwords or CVC codes was not included in the stolen data. Credit card companies will cover any financial damage incurred by fraudulent transactions.

---

[1] Ministry of Finance & Strategy, Ministry of Science, ICT & Future Planning, Ministry of Justice, Ministry of Security & Public Administration, Financial Supervisory Service

[2] 53 million accounts from KB, 25 million from NH, 26 million from Lotte

[3] Card Validation Codes helps validate that a genuine card is being used during a transaction

They will provide a service for free that sends text message notifications for each card transaction to mobile phones. KCB will provide a privacy protection service for one year to anyone who asks for it.

Regulators will consider additional identity validation process for some merchants that only require credit card numbers and expiry dates. Stringent measures to prevent any attempt for fraudulent transactions amid widespread concerns will be implemented.

In order to minimize customer inconvenience such as long lines in bank branches, the three credit companies will extend opening hours, increase call center staff and reduce time taken to issue new cards.

The card data breach was a man-made disaster that could have been prevented by complying with basic security procedures. Accordingly, it is unavoidable to ask for accountability and take a stern action to prevent a recurrence of the breach.

Severe administrative sanctions as well as criminal punishment will be pursued as soon as possible. Three card companies will be subject to suspension of business for three months in February, the most severe sanction as provided for by the current laws and regulations. Former and current executives and employees including chief executives related to the data breach will be subject to severe sanctions such as recommendation of dismissal from office or suspension of duties.

The FSC and the FSS will operate a daily monitoring taskforce for 24 hours, jointly with credit card companies, to check the number of inquiries on the websites, applications for card cancellation and reissuance, and consumer complaints or damage reports. The FSS will send six examiners to each credit card company for 24 hour support and examine the situation at credit card companies in relation to customer counseling, credit card reissuance or cancellation. The FSS will also operate an emergency support team to monitor the trends of credit card cancellation and reissuance and major consumer complaints.

MEASURES TO PREVENT A RECURRENCE

Financial companies will be required to collect and retain only the minimum amount of information required so that financial damage can be reduced in case of a possible information leak. Sharing personal information within the financial group will be restricted and the use of personal information by the third party for marketing purposes will be limited in principle.

If a loan agent uses the stolen personal data, he or she will be disqualified and the financial company that hired the loan agent will also be subject to punishment. Large financial companies should hire Chief Information Security Officer as an executive officer to take responsibility for the collection, storage and processing of personal information. The FSS will thoroughly examine the compliance with internal security rules at financial companies.

Sanctions related to the data breach will be strengthened and punitive fines will be introduced. Fines imposed on financial companies that leak personal information will be significantly raised and punishment for leaking information provided for by Use and Protection of Credit Information Act and Electronic Financial Transaction Act will also be significantly strengthened.