



## Press Release

---

January 17, 2014

### T/F FORMED TO RESPOND TO PERSONAL INFORMATION LEAKS

The FSC formed a task force (T/F) to respond to the recent leakage of personal information on credit card holders and held its first meeting on January 17 to discuss how to prevent consequences of the incident from spreading and seek for fundamental measures to prevent a repeat of such an incident.

#### **BACKGROUND**

Prosecutors announced on January 8 that personal information of credit card holders were leaked by an employee of an outsourcing company of three credit card companies.<sup>1</sup>

The stolen data does not include credit cards' pass word or CVC code; therefore, it is very unlikely that the leaked information might be misused for financial fraud. Prosecutors also judged that there was no further leakage of the stolen data as they arrested those who had stolen the information and first distributed. There has been no case yet reported as direct damage of the incident.

#### **MAJOR CONTENTS OF DISCUSSION**

##### **1. Measures to prevent further leaks and remedies for those affected**

The card companies will identify details as soon as possible about how and when personal information was leaked and will inform affected customers via SMS, phone, e-mail, and respective financial company's website<sup>2</sup>.

To prevent further damages, the three credit card companies will issue new credit cards to the victims upon request, provide free credit card payment notification SMS service(temporary service), and ban other financial companies subordinated to their mother group from using customers' private information when promoting their products.

Moreover, the responsible credit card firms will operate 24-hour call center<sup>3</sup>, damage control team, and hot line with the FSS to immediately respond to further damages. Respective credit card companies will provide financial reimbursements to the victims of further damage.

---

<sup>1</sup> Data leaks for each card issuers : 53 million cases from KB Card; 26 million cases from Lotte Card; and 25 million from NH Card \* It is estimated that the number of affected cards would be reduced with the number of cards held by the deceased or multiple card holders.

<sup>2</sup> Details about the stolen information for each individual is available on each respective credit card company's website from January 17.

<sup>3</sup> KB Card: 1899-2900

Lotte Card: 1588-8100

NH Card: 1644-4000(Jan.17~), 1644-4199(Jan.20~)

The FSS is verifying the details of the accident based on information received from the prosecutors. Damages from the data leak will be responded and normalized in a swift manner. The FSS will respond to the issues related to false credit card usage by someone else other than the actual credit card holder as a top priority. Moreover, “Center for Data Leakage Supervision<sup>4</sup>” is established on January 17 to supervise flow of the leaked data and block further distribution. Suspicious information will be reported to the investigative authorities.

## 2. Establishment and operation of the T/F

The task force is headed by the FSC vice chairman and composed of the FSC, Ministry of Security and Public Administration, Korea Communications Commission, FSS, Korea Institute of Finance, Korea Federation of Banks, Korea Financial Telecommunications and Clearings Institute, Korea Internet and Security Agency, and IT security experts.

The three working-level teams are System Reform Team(Head: General Director of the Consumer Finance and Protection Bureau, FSC), Internal Control & IT Team(Head; General Director of the Banking and Insurance Bureau, FSC), and Financial Institution Inspection and Analysis Team(Head: Acting Vice Governor of the FSS).

## 3. Major tasks of the T/F

Team	Responsibility
<b>System Reform Team</b>	<ul style="list-style-type: none"> <li>* Overhaul current private information protection system</li> <li>* Devise plan to strengthen financial institution’s responsibility on data protection</li> <li>* Reinforce punitive actions regarding customer information protection</li> <li>* Regulate use of leaked data on promoting financial products</li> </ul>
<b>Internal Control and IT Team</b>	<ul style="list-style-type: none"> <li>* Establish internal IT control system</li> <li>* Strengthen management of outsourced service company</li> <li>* Strengthen IT system security</li> </ul>
<b>Financial Institution Inspection and Analysis Team</b>	<ul style="list-style-type: none"> <li>* Announce financial customer data protection plan to each financial company</li> <li>* Inspect all financial institutions and distribute self-inspection check list</li> <li>* Set best practice on data protection</li> </ul>

## FUTURE PLAN

Damage reports to the victims and remedy procedure will begin on January 17. Each financial institution will submit customer data protection plan to the T/F at the end of January. The T/F will come up with a plan to better protect personal information on customers held by financial firms in February this year. The FSC plans to revise the Protection of Credit Information Act, Electronic Financial Transaction Act, and other related acts on the financial industry starting in March, 2014.

<sup>4</sup> Tel: 1332 (09:00~18:00, Weekdays)  
Fax: 02-3145-7852  
E-mail: [privacy@fss.or.kr](mailto:privacy@fss.or.kr)