Comprehensive Measures to Protect Personal Data in the Financial Sector

The following is a summary of the press releases made by the Financial Services Commission on 10 March 2014. These are action items and policies that the FSC and relevant ministries are seeking to implement. The following measures have developed from a series of measures previously announced since the data leakage from the three credit card companies were revealed last January[1].

1. Strengthen Personal Data Protection At Each Stage That Financial Institutions Collect, Retain & Use and Discard Customers' Data

- **Financial institutions will be given greater responsibility in handling their customers' personal data at each stage that they collect, retain, use and discard such information.**

Collect Stage

- Financial institutions will only be allowed to collect only minimal necessary information from their customers. Currently 30 to 50 items of information are collected which will be reduced to up to 6 items. This will mean the current forms that financial institutions have created with respect to personal information will need to be amended.
- Customers' national resident registration numbers will be collected in a safer manner (e.g. key-in) only once in their initial transactions with financial institutions and will need to be stored in an encrypted form.

Retain & Use Stage

- Affiliates of financial holding companies will be restricted from sharing their customer information without customers' consent.

1. Press release <Measures to Protect Personal Data from Illegal Circulation and Use> (Jan.24, 2014), <Measures to Prevent a Recurrence of Personal Data Breach> (Jan.22m 2014) available at the FSC website.

- Financial institutions' marketing activities through non-face-to-face channels such as SMS, telephone and e-mail will be restricted (e.g. sending text messages (SMS) for marketing purpose on a random basis will be banned).
- A 'do-not-call' system will be established by the Association of Financial Institutions.

Discard Stage

- All collected information will be destroyed when a contract with customers terminates, except for certain prescribed information that is required to be kept for an extra period.
- Even for the information that is required to be retained longer will also need to be destroyed within five years, unless there is a statutory requirement for a longer period of storage.

2. Ensure Financial Consumers' Right To Personal Information

- **Financial consumers' right to their personal information will be ensured so that they can decide for what, when and how their own personal data are used by financial institutions**

- Financial institutions will establish a system to enable customers to check how their information are being used any time they want.
- Consumers will be able to withdraw their consent even if they previously agreed to provide their personal information.
- Financial institutions should establish a so-called "do-not-call" system that allows customers to reject any marketing call from certain financial institutions.
- Financial consumers will also be able to request financial institutions to suspend checking their credit information for a certain period to prevent their personal information from being illegitimately used by scammers.

3. Greater Responsibility Of Financial Institutions In Customers' Data Protection

- **Financial institutions must be responsible for data protection and security at an executive officer level and must ensure greater independence and responsibility of Chief Information Security Officer (CISO).**

- Financial institutions will be required to submit an annual report on how customers' credit information is being protected to their CEO and board of directors as well as the supervisory authority.
- If consumers' information collected by financial institutions are leaked and illegally circulated by marketing agents, financial institutions that hired such agents will also be subject to criminal sanctions.

- **Punitive damage liability will be imposed on financial institutions in the event of a data security breach**
  - Financial institutions will be fined up to 3% of their sales revenues originated through illegally-circulated information.
  - Financial institutions that have their customers' data leaked will have to pay up to KRW 5 billion as penalty.

- **Punishments for data leaks will be raised to the highest levels, for example, 10-years imprisonment, under the Credit Information Act and the Electronic Financial Transaction Act.**

- **Credit bureaus that are liable for a leak of personal information will could face suspension of its business for up to 6 months or fines. Its business license will be revoked if such incident is repeated within three years.**

4. Strengthen Financial Industry's Cyber Security

- **The government will implement additional measures to strengthen cyber security on top of the 'Comprehensive Measures to Reinforce Financial Institution's Data Security' announced in July 2013.**
  - Financial institutions' intranet and internet networks will be separated and personal identification information such as national resident registration numbers will be encrypted.
  - The government will allow private evaluation agencies such as Korea Internet and Security Agency to evaluate a financial institution's cyber security system.

- **The government will prevent 'man-made disasters' such as the recent credit card data leaks by strengthening inspection and management of data security.**
  - Financial institutions will be required to conduct monthly security inspection under the responsibility of Chief Information Security Officer (CISO) and report the results to CEOs and the FSS.
  - The relevant governmental authorities will conduct irregular spot inspections to check whether financial institutions are faithfully complying with the security standards.

5. Establish Response System To Future Data Leak Accidents

- **Financial institutions will establish a contingency plan under the responsibility of CEOs to ensure swift responses to future data leak accidents.**
- **In case of an emergency, the financial institutions will be required to immediately action its emergency response system and respond in cooperation with the financial authorities, related government bodies and agencies.**

6. Future plan

- **The government will immediately implement the measures which do not require any amendment of the relevant laws.**
- **The FSC is exerting its best efforts to pass bills which amend the Use and Protection of Credit Information Act and Electronic Financial Transaction Act within H1 2014.**

Should you have any questions regarding any of the foregoing, please feel free to contact us at any time.

- Young-Hee Jo TEL : +82 2 316 4236 E-Mail: yhjo@shinkim.com
- Michael Chang TEL : +82 2 316 4653 E-Mail: mchang@shinkim.com

Chambers Asia-Pacific Awards 2014
South Korea Law Firm of the Year : Shin & Kim