Financial Services Commission

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

Press Release

March 10, 2014

COMPREHENSIVE MEASURES TO PROTECT PERSONAL DATA IN THE FINANCIAL SECTOR

OVERVIEW

The FSC and relevant ministries[1] jointly announced a package of measures to prevent a recurrence of personal data leaks in the financial sector, as part of the government's follow-up measures to ensure market discipline under its three-year plan for Korea's economic innovation.

The measures announced today were drawn up based on the following basic principles, further developing a series of measures[2] previously announced since the data leakage from the three credit card companies were revealed last January.

1. Financial firms will be asked a greater responsibility in handling their customers' personal data at each stage that they collect, retain, use and discard customers' information.

2. 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 being used by financial firms.

3. Financial firms will be held more accountable for personal data protection and strictly sanctioned in the event of personal data security breach.

4. Cyber security measures will be strengthened across the financial sector in response to cyber crimes such as hacking.

5. The government will make sure financial consumers' personal data previously provided or illegally-circulated not to be misused by financial scammers.

---

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

[2] 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 www.fsc.go.kr/eng

1. Strengthen Personal Data Protection at Each Stage that Financial Firms Collect, Retain & Use and Discard Customers' Data

Financial firms will be asked a greater responsibility in handling their customers' personal data at each stage that they collect, retain, use and discard such information.

'Collect' Stage

Financial firms will be allowed to collect necessary information at a minimum level from their customers. Currently, financial firms are collecting 30 to 50 items of information from their customers. The list of collected information will be shorted up to 6 items necessarily required for financial transactions.[3]

Additional information should be collected only with customers' consent on condition that customers are informed of such information is not necessarily required to sign a contract; and that financial firms explain customers for what purpose they want to collect additional information and with whom they would share such information.

Customers' resident registration numbers will be collected in a safer manner (e.g. key-in) only once in their initial transactions with financial firms and should be stored encrypted. Leaks and illegal circulation of resident registration numbers will be punished further strictly than that of other personal information.

'Retain & Use' Stage

Affiliates of financial holding companies will be banned from sharing their customer information each other without customers' consent. Financial firms will be required to gain customers' consent separately for a third-party necessary to signing a contract and for the optional one when they provide a third party with customers' personal information.

Consent forms will be revised to make financial firms collect minimum information from their customers and to help customers clearly understand which information they agree to provide. Necessary items and optional ones will be on separate pages of a consent form. Customers will be able to sign a contract with consent to necessary items. Consent forms will be made easier to read with a bigger font size and a wider space.

Financial firms' marketing activities through non-face-to-face channels such as SMS, telephone and e-mail will be restricted. Financial firms will be banned from sending random text messages (SMS) for marketing purpose. Marketing activities through telephone or email will be limited to a certain extent.

[3] Necessary information commonly required (name, resident-registration number, address, phone number, occupation, nationality), necessary information required to sign up a certain product (e.g. annual income to buy a savings product)

'DISCARD' STAGE

In principle, all collected information will be destroyed when a contract with customers terminates, except for information needed to be kept for an extra period.[4] Such information also needs to be destroyed within 5 years unless there is a statutory requirement for a longer period of storage.[5]

For information that financial firms provide a third party,

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 firms.

Financial firms 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 companies should establish so-called "do-not-call" systems that customers can reject any marketing call from financial companies.

Financial consumers will be able to request financial companies to protect their personal information even after their transactions with the companies end. Upon request, financial companies must either discard customers' information or take safety measures to protect such information. Consumers must be immediately informed of whether financial firms take actions as requested.

Financial consumers will be also able to request financial firms to suspend checking their credit information for a certain period to prevent their personal information from being falsely used by scammers.

3. GREATER RESPONSIBILITY OF FINANCIAL COMPANIES IN CUSTOMERS' DATA PROTECTION

Financial companies 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. The report will be publicly disclosed.

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

---

[4] Identification information, transaction data

[5] The Capital Markets Act, for example, requires financial firms to keep investor contract information for ten years.

Financial firms will be required to take a greater responsibility for financial consumers' information collected by marketing agents. If consumers' information were leaked and illegally circulated by marketing agents, financial firms that hired such agents will be also punished.

Punitive fines will be imposed on financial firms in the event of data security breach. Financial firms will be fined 3% of their sales raised through illegally-circulated information. Financial firms that leaked customers' data 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-year imprisonment, under the Credit Information Act and the Electronic Financial Transaction Act

Credit bureaus that leaked personal information will face either business sanctions up to for 6 months or fines. Business license will be revoked if such a incident reoccur within three years.

Fines will be raised from the current KRW 6 million to KRW 50 million against financial firms' negligence of data protection.

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. The government will strongly respond to cyber attacks in coordination with the related authorities.

Financial institutions' intranet and internet networks will be separated and personal identification information such as resident registration number will be encrypted.

The government will allow private evaluation agencies such as Korea Internet and Security Agency to conduct evaluation on financial firms' cyber security conditions and disclose the results.

The government will prevent 'man-made disasters' such as the recent credit card data leak accident by strengthening inspection on and management of data security. Financial firms 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[6].

The supervisory authorities will conduct irregular spot inspections to check whether financial firms are faithfully complying with the security standards. Moreover, a special agency for financial data security will be established.

Personal credit data protection will be significantly strengthened. The government will encourage credit card merchants to switch Point of Sale(POS) terminal devices, which are prone to personal information breach, to IC(Integrated Circuit) card payment devices until the

[6] The FSS will provide financial companies with 'financial information security checklist'.

end of 2014 while replacing the current magnetic credit cards with IC credit cards as soon as possible. Credit card companies will raise fund to provide financial support for small merchants to equip IC card devices. All credit card merchants will be required to use IC card payment devices from 2016.

Value Added Network(VAN) providers will be mandated to register for operation to the FSC. Moreover, VAN providers will be responsible for IT security, credit information protection, and control of their agencies. The government will impose sanctions such as penalty and deregistration upon violation of duty.

5. Establish Response System to Future Data Leak Accidents

The government will ensure that financial groups delete all unnecessary personal data provided to their affiliates and third party, and require them to conduct a thorough inspection on the conditions of shared personal information. Moreover, financial firms will be banned from doing business with a third party that failed to safeguard customer data. Strong sanctions will be imposed to those using or storing illegally circulated personal information.

Financial institutions will establish a contingency plan under the responsibility of CEOs to ensure swift response to future data leak accidents. The contingency plan will contain detailed action plans according to each phase of the accident in a bid to minimize customer's inconvenience and financial loss. In case of emergency, the respective financial companies will immediately operate emergency response system and respond in cooperation with the financial authorities, related government bodies and agencies if necessary.

Future Plan

Starting from the end of March, the government will immediately implement the measures which do not require amendment of the related act. For revision bills on the 'Use and Protection of Credit Information Act' and 'Electronic Financial Transactions Act' pending in the National Assembly, the FSC will make best efforts for passage of such bills within the first half of 2014. Lastly, the government will completely root out markets for illegally circulated personal information by carrying out thorough crack down in cooperation with the relevant authorities.

# # #

For any inquiry, please contact Foreign Press & Relations Team at fsc_media@korea.kr