HONG KONG MONETARY AUTHORITY
香港金融管理局

Banking Supervision Department *銀行監理部*

Our Ref.: B1/15C
B9/29C

14 October 2014

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Customer Data Protection

In July 2008, the HKMA issued a circular "Customer Data Protection" reminding authorized institutions (AIs) of the importance of protecting the confidentiality of customer data and some key control measures for customer data protection. In the light of the developments of the industry and technologies over the past several years, I am writing to update certain relevant guidance set out in that circular.

Controls for preventing and detecting loss or leakage of customer data

To protect the confidentiality of customer data, AIs should ensure a high degree of alertness among staff members in protecting customer data. Moreover, AIs should implement "layers" of security controls (covering both IT and non-IT controls) to prevent and detect any loss or leakage of customer data. Although various Supervisory Policy Manual (SPM) modules[1] and circulars have already covered risk management principles and control measures that are useful for protecting customer data, we have elaborated and updated certain control measures as set out in the **Annex** of this circular. We have taken into account the latest developments, particularly:

(i) There has been an increasing use of system controls (i.e. controls imposed by automatic tools) in the banking industry for preventing or detecting the leakage of customer data. Accordingly, the relevant AIs are better prepared to prevent and detect incidents involving leakage of customer data and take prompt actions to contain the impact so as to reduce their reputation and legal risks. For example, these AIs could more promptly identify cases caused by individual staff members (e.g. who transmit customer data to personal email accounts without permission) so as to take timely actions to avoid further leakage of customer data;

[1] Including, among others, the SPM modules "TM-G-1 General Principles for Technology Risk Management", "OR-1 Operational Risk Management" and "SA-2 Outsourcing".

(ii) The Hong Kong Association of Banks (HKAB) has recently developed a standard of stringent minimum controls that member banks have to comply with if they allow the use of Bring-Your-Own-Device [2] (BYOD) for work. According to HKAB, the standard is commensurate with the risk of loss or leakage of customer data via BYOD and the protection offered by the standard is close to that available to computing devices owned by member banks, particularly in respect of accessing consumer or personal data. The HKMA supports the standard and permits AIs to adopt BYOD as long as they fully comply with it. Where the HKMA is aware of non-compliance with the standard, appropriate supervisory measures will be taken regarding the relevant AIs (e.g. where significant deficiencies are identified, the HKMA may require the AI to suspend its BYOD usage until the deficiencies are rectified). In addition, we expect AIs to be prepared to implement additional stringent controls related to BYOD in accordance with their data classification and risk assessment results whenever there is a need to protect their systems and networks.

For the avoidance of doubt, AIs should at all times comply with the Personal Data (Privacy) Ordinance (PDPO) and any relevant codes of practice, rules or guidance [3] issued or approved by the Office of the Privacy Commissioner for Personal Data for protecting personal data of their customers as well as staff members [4].

Controls for handling incidents involving loss or leakage of customer data

To contain and minimise the possible impact of incidents involving stealing, loss or leakage of customer data (privacy incidents), AIs should have in place effective incident handling and reporting procedures. Specifically, each AI should designate an officer of sufficiently senior ranking or a designated management committee, which is chaired by senior management, for overseeing the process of handling and reporting privacy incidents. Comprehensive procedures should be in place to assist responsible staff in handling such incidents including, among other things, reporting of the incidents to the designated officer and relevant regulatory authorities including the HKMA and the Privacy Commissioner for Personal Data (Privacy Commissioner) where appropriate; ascertaining the nature of the incidents, the causes of the incidents and identity of customers affected; notifying affected customers as appropriate (in case the AI concerned decided not to notify affected customers, it should provide justification on why it did not do so); taking prompt remedial actions to protect affected customers' interests and prevent similar incidents from happening again.

---

2 BYOD refers to the use of computing devices (e.g. personal computers, tablets or smartphones) personally-owned by staff members for work.

3 Including, among others, "Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry" issued by the Office of the Privacy Commissioner for Personal Data in October 2014.

4 Apart from the requirements of PDPO, AIs should be cautious that they are not supposed to disclose customer data to the related parties of the customers concerned without the consent from the customers.

Where the nature of a privacy incident is serious, for example, the incident will likely have a high impact on the reputation of the institution, the number of customers affected is large, the customer data stolen, lost or leaked is sensitive, institutions are expected to report the incident to the HKMA and notify the affected customers as soon as practicable after the AI concerned is aware of or notified of the incident. If a large number of customers are affected, the AI concerned should consider making a public announcement as this is an effective way to notify the affected customers quickly and to regain customers' confidence by assuring them of the AI's remedial actions. In addition, while there is no statutory requirement on AIs to report privacy incidents to the Privacy Commissioner, the AI concerned should seriously consider doing so, having regard to the severity of the incidents and taking into account the Guidance Note on Data Breach Handling and the Giving of Breach Notifications issued by the Privacy Commissioner. In case the AI concerned decided not to report the incident to the Privacy Commissioner, it should provide justification on why it did not do so.

AIs' re-assessment of their existing controls

Given the importance of protecting customer data, we expect AIs to complete a critical review of the adequacy of their existing controls by Q1 2015, having regard to the guidance set out in this circular as well as other relevant SPM modules and circulars. In case the outcome of the review reveals any discrepancies or areas for improvements, AIs should implement appropriate measures promptly to strengthen the controls.

If there are any questions on the above, please contact Mr Tsz-Wai Chiu at 2878 1389 or Ms Teresa Chu at 2878 1563 (on controls for preventing and detecting loss or leakage of customer data) and Ms Christie Yee at 2878 1370 or Miss May Cheung at 2878 1501 (on controls for handling incidents involving loss or leakage of customer data).

Yours faithfully,

Henry Cheng
Executive Director (Banking Supervision)

Encl.