HONG KONG MONETARY AUTHORITY
香港金融管理局

Circulars

10 Jul 2008

Customer Data Protection

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

10 July 2008

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Customer Data Protection

In the light of recent incidents involving loss of personal data by different parties, I am writing to remind authorized institutions (AIs) of the importance in protecting confidentiality of customer data, particularly personal data as defined under the Personal Data (Privacy) Ordinance (PDPO).

The recent incidents highlighted the need to ensure a high degree of general alertness among staff of AIs in protecting personal data, especially those stored in portable electronic devices (e.g. tapes, CD-ROMs and USB memory keys). In some reported cases, the leakage of personal data is believed to be related to the use of less secure home personal computers (PCs), which have been installed with high-risk freeware (e.g. peer-to-peer file-sharing software[1]), for office work. The use of such freeware significantly increases the risk of unauthorised access to data stored in the computers.

I would like to reiterate the importance of implementing data security measures set out in relevant circulars and guidelines[2] issued by the HKMA. Given the increasing usage of portable IT equipment/devices and the need to access customer data by a wide range of staff, AIs should ensure that adequate control measures are in place to protect customer data, especially those stored in portable electronic devices.

To contain and minimise the possible impact in the event of loss or leakage of customer data, AIs should have in place effective incident handling and reporting procedures. Specifically, each AI should designate an officer of sufficiently senior ranking for overseeing the process of handling and reporting of incidents in relation to loss or leakage of customer data. 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 where appropriate; ascertaining the nature of data lost and

identity of customers affected; taking prompt actions to protect affected customers' interests and notifying affected customers.

As incidents involving loss or leakage of customer data are likely to have high impact on the reputation of the institution and the number of customers affected is normally large, institutions are expected to report the incident to the HKMA as quickly as possible and notify the affected customers as soon as practicable. 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 AIs' remedial actions.

More importantly, AIs should ensure that their staff members are at all times alert to the importance of protecting customer data confidentiality. The data security policies should be effectively communicated to staff and promoted within the institution on an on-going basis.

To ensure that the risk of leakage of customer data is fully and properly addressed, I would like to request your institution to review the adequacy and effectiveness of existing control measures over customer data protection and the incident handling procedures having regard to the recently reported data leakage incidents and emerging data security threats. A list of the key control measures for customer data protection, which are largely extracted from the relevant circulars and guidelines issued by the HKMA previously and suitably enhanced where appropriate, are set out in the Annex. The review should be completed as soon as possible. In case the outcome of the review highlights any areas for improvements, your institution should implement such improvements promptly. The HKMA will continue to assess the adequacy and effectiveness of AIs' control measures over customer data protection through its on-going supervisory efforts. Your institution is also required to notify the usual contact of the HKMA of the name and position of the designated officer mentioned above by 31 July 2008.

Should you have any questions on the content of this letter, please feel free to contact Mr Shu-Pui Li at 2878 1826 or Mr James Tam at 2878 8043.

Yours faithfully,

Arthur Yuen
Executive Director
(Banking Supervision)

Annex

Control measures for customer data protection

Designated officer and incident handling process

- AIs should assign a designated officer for overseeing the process of handling and reporting incidents of loss or leakage of customer data. Such an officer should hold a sufficiently senior position. The key roles of the officer are, among others, to assess the seriousness of the incidents, determine the possible immediate remedial actions to mitigate the risk of AIs and affected customers, and consider the need for further escalation of the incidents.

- AIs should also have adequate and effective procedures in place for handling incidents of loss or leakage of customer data. In case of any incidents of loss or leakage of customer data, the designated officer of the AI should coordinate the escalation process and ensure that the HKMA is informed as soon as possible through the most convenient and effective means. The AI concerned should also promptly submit a written preliminary incident report to the HKMA, containing details and impact of the incident and immediate remedial actions to protect customer interests (such as enhanced transaction monitoring of the affected customers' accounts) and, where possible, prevent the problem from happening again. A detailed investigation report should then be submitted to the HKMA covering, inter alia, the root cause analysis, the action plan and schedule for implementing other related remedial actions, as appropriate, to prevent similar incidents from happening again once the investigation of the incident is complete.

Data security policies and awareness

- AIs should develop a set of comprehensive policies and procedures on data security. The policies and procedures should set out controls to safeguard customer data stored in relatively less controlled peripheral equipment/devices and in paper form, covering areas on, inter alia, use of portable storage devices, end-user and mobile computing, physical security controls and outside service providers.
- AIs should also formulate an awareness programme to communicate the data security policies to staff as well as to promote within the institution the importance of protecting customer data on an on-going basis. The programme may cover regular internal data security reminders/circulars, promotion posters, periodic training sessions, and policy orientations for new recruits.

Portable storage devices (e.g. USB memory keys and CD-ROMs)

- In general, AIs should prohibit staff members from downloading customer data from their computer workstations into portable storage devices. Appropriate security controls such as disabling floppy drives and USB ports on computer workstations should be implemented to prevent downloading of customer data. If there is a business or operational need for downloading customer data into such devices, prior formal approval from the information owner or responsible senior management staff of the AIs should be obtained. The customer data stored in such devices must be protected by data encryption and password, and be erased from the devices immediately after use. Proper records on the usage of such devices for storage of customer data should be maintained and any loss of the devices should be immediately reported to and followed up by the designated officer of the AIs.

End-user computing

- While end-user computing[3] may offer advantages (e.g. higher productivity), it may also increase the risk of data leakage as customer data are normally required to be downloaded from an AI's centralised computing facility onto end-userscomputer workstations. As a result, customer data can be easily further transferred to portable storage devices or to external parties through users' Internet email account (if their workstations have Internet connection). AIs should therefore have adequate policies and procedures in place to control end-user computing activities. Appropriate security

controls should be implemented to safeguard the computer workstations used for end-user computing, including disabling the Internet access of, and the facilities for "copying" or "downloading" of customer data onto, these workstations.

Mobile computing

- Occasions may arise where AIs' staff members need to work outside the AIs' premises (e.g. work from home, when travelling or visiting clients' premises). Staff members should only use the computing equipment provided by the AIs for storing or accessing AIs' customer data. Use of their own equipment should be disallowed for such purposes. All mobile computing equipment of AIs should be protected with adequate security measures (e.g. anti-virus software, password protection and data encryption).
- If remote access to the AIs' internal network environment is required, adequate controls (such as network encryption, strong access authentication and firewall protection) should be in place to safeguard against data leakage and unauthorised access through remote access points.

Physical security controls over customer data

- To ensure data confidentiality, customer data stored either in electronic or paper form should be safeguarded by adequate physical security controls. Adequate policies and procedures should be in place for protecting documents containing customer data and controlling the transportation and storage of such documents (e.g. customer documents collected at promotion booths outside AIs' premises). These documents should also be properly disposed of when they are no longer required by the AIs (e.g. shredded before transported to wastes destruction centre).
- AIs should have adequate controls to safeguard tapes containing sensitive data, particularly customer data (e.g. computer backup tapes, digital tapes), that are required to be transported outside of an AI's premises (e.g. between an AI's premises or to a third party's premises). All sensitive information stored in the tapes must be encrypted. AIs should also consider adopting more advanced technology (e.g. data mirroring technology) to avoid the need for transporting tapes outside of their premises where appropriate.
- Adequate physical security (including physical access controls, security guards and surveillance cameras) should be deployed to areas where appropriate to safeguard customer data against theft or unauthorised access. When AIs renovate premises or move offices, it is also important to have adequate physical security control procedures in place for protecting AIs' assets and customer data.

Outside service providers

- Since outsourcing arrangements normally involve storage of and/or access to AIs' customer data by outside service providers, AIs should implement effective controls with adequate management oversight of outsourcing arrangements taking into account the relevant guidelines[4] issued by the HKMA. In particular, the contractual agreements between the AIs and their outside service providers should fully set out the data protection liabilities and obligations of their service providers. AIs should also conduct regular reviews to ensure compliance with the agreed terms in the contract by the outside service providers.

- If AIs have outsourced the storage and/or transportation of tapes and/or documents containing sensitive data to a service provider, AIs should assess and satisfy themselves that the service provider has put in place adequate and effective controls relating to the outsourced service.

[1] Peer-to-peer file-sharing software allows Internet users to connect with others via a shared network for sharing data or document files.

[2] Including circulars on "Personal Data (Privacy) Ordinance" (1996), "Safeguarding Customer Assets and Information" (2004), "Examinations on Controls over Customer Data Protection" (2006), as well as the Supervisory Policy Manuals modules on "Outsourcing" (2001), "General Principles of Technology Risk Management" (2003) and "Supervision of E-banking" (2004).

[3] End-user computing is the transfer of information processing and system development capabilities from centralised data centres onto the end users' desktop/workstation computer.

[4] Including Supervisory Policy Manuals on "Outsourcing" (2001) and "General Principles of Technology Risk Management" (2003), and circular on "Examinations on Controls over Customer Data Protection" (2006).

Last revision date : 01 August 2011