



HONG KONG MONETARY AUTHORITY
香港金融管理局

Circulars

22 Dec 2004

Safeguarding customer assets and information

Our Ref: B1/15C

22 December 2004

The Chief Executive
All authorized institutions

Dear Sir / Madam,

Safeguarding customer assets and information

In the light of the recent incident relating to the mistaken destruction of rented safe deposit boxes and observations arising from our routine review of the operations of authorized institutions ("AIs"), the HKMA has identified certain control issues which, if not managed properly, may give rise to considerable operational, reputation and security risks. This circular suggests measures that AIs should take in order to minimise their exposure to these risks¹.

Controls over operations that involve the handling of customer assets

A major lesson that can be learnt from the recent safe deposit box incident is that AIs should never under-estimate the need to have adequate supervisory oversight and control over operations that involve the handling of customer assets. These operations, even though they may seem straight-forward and simple, can pose significant operational and reputation risks to AIs if they are not handled properly. AIs must adhere to sound internal control principles when undertaking these operations, which should include ensuring sufficient planning for the operations, adequate supervisory oversight and control throughout the whole process, detailed records of customers assets (or items containing customers assets) being handled, and independent verification of the accuracy of these records.

In the light of the safe deposit box incident, the Hong Kong Association of Banks issued a circular in November 2004 enclosing a set of best practice recommendations on the relocation of safe deposit boxes. The HKMA supports the Association's recommendations and expects AIs that provide safe deposit box service to follow the recommendations.

Customer information security

It is common for AIs' marketing staff to meet customers at open-plan design customer service desks or cubicles within an AI's premises. When front-line marketing staff receive customers at such locations, confidential customer information (either in physical or

electronic form) may be collected and retained for further processing. Computer equipment (e.g. desk-tops, notebooks, and PDAs) may be used for internal or marketing purposes. To safeguard the confidentiality of customer information, Als should ensure that their data security procedures comply with the standards set out in the Supervisory Policy Manual module on Technology Risk Management issued in June 2003. In particular, Als should have security controls (including computer log-on password and application-specific access control password) in place for the protection (e.g. against theft and unauthorized access) of computer equipment. Als should also ensure that staff log-off from the bank computer system after use, that unattended computers are protected by "screen-saver passwords", and that all customer records are kept safely in locked cabinets. Appropriate security measures, such as surveillance cameras and security guards, should be deployed to monitor any unauthorized access to unattended service desks and meeting rooms.

Where customer information is downloaded and stored onto mobile computer devices by Als' staff for business purpose, controls are required to manage the risks of working in an unattended environment or outside AI premises. Computer devices should be properly switched off and not be left unattended after use. Data encryption technology should be used where available to protect sensitive customer information and business transactions stored in the mobile computer devices.

The internal audit function or an independent unit of each AI should conduct reviews or surprise checks on the enforcement of and compliance with the guidelines on data security on a regular basis.

If you have any questions on this circular, please feel free to get in touch with your usual contact at the HKMA.

Yours faithfully,

Nelson Man
Acting Executive Director
(Banking Supervision)

¹ Please refer also to the circular "Review of Terms and Conditions for Safe Deposit Box Service" issued by the HKMA on [17 December 2004](#).

c.c. HKAB (Attn. Ms Katie Yip)