HONG KONG MONETARY AUTHORITY
香港金融管理局

Circulars

23 Jun 2004

Strengthening Security Controls for Internet Banking Services (superseded by TM-E-1 of Supervisory Policy Manual)

Our Ref: B1/15C
B9/29C

23 June 2004

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Strengthening Security Controls for Internet Banking Services

The purpose of this letter is to set out the HKMA's recommendations for strengthening Authorized Institutions' (AIs) security controls for internet banking services.

As you may be aware, there have been an increasing number of internet banking fraud cases, particularly involving fake bank websites and e-mails. Although no financial losses have been reported in relation to fake bank websites in Hong Kong so far, there are reported cases overseas, where consumers are known to have fallen victim to such fraudulent schemes. In view of the increasing acceptance of internet banking services and in anticipation of more sophisticated internet banking frauds targeting the public in Hong Kong, AIs would need to be careful in implementing appropriate security controls for their internet banking services. Any mishaps would undermine the public's confidence in internet banking and would not only be detrimental to the AI concerned, but also to the development of the industry as a whole.

In February 2004, the HKMA issued a guidance note on Supervision of Electronic Banking which suggested, inter alia, that AIs should employ stronger customer authentication for transactions with higher risk. In this regard, the e-Banking Working Group of the Hong Kong Association of Banks has reached a general consensus that, as a minimum standard, AIs should offer two-factor authentication for high-risk transactions to their retail internet banking customers as an option. It is also important for AIs to make their customers fully aware of the risk involved if they choose not to adopt a stronger authentication method when using internet banking services. We endorse the group's consensus and would hereby recommend AIs to adopt the minimum standard. AIs are, of course, free to adopt a higher standard, e.g. to mandate two-factor authentication[1] for all high-risk transactions.

AIs are recommended to conduct a detailed risk assessment to identify high-risk internet banking transactions that need to be subject to two-factor authentication. In general, high-risk internet banking transactions should at least include unregistered third-party fund transfers and payments, and change requests concerning customers' sensitive information (e.g. correspondence address). If AIs determine that it is not necessary to implement two-factor authentication for their internet banking services, their risk assessment should be adequately documented. This will be reviewed as part of the HKMA's on-site examinations and off-site reviews.

Passwords are commonly used as the basic factor of authentication. The choice of a second factor is considerably wider. Examples of the technologies used or being considered by a number of banks as a second factor authentication in addition to login passwords include:

- digital certificates;
- one-time passwords generated by a security device (e.g. a security token); and
- Short Message Service-based one-time passwords.

In line with the HKMA's supervisory approach, we believe that maintaining technological neutrality is crucial for allowing AIs to have the flexibility to choose and implement technologies that are appropriate to their internet banking services. The HKMA therefore will not specify a particular technology to be used. AIs should evaluate the possible technologies carefully and implement the two-factor authentication solution that is commensurate with the risks associated with the types of transactions involved.

In general, the HKMA expects AIs to complete the implementation of two-factor authentication for high-risk retail internet banking transactions they have identified within one year from the date of this letter. Should AIs find it difficult to complete the implementation within the aforesaid period, they should discuss their timetable with the HKMA individually. Meanwhile, AIs should continue to review and enhance their security measures as appropriate (e.g. enhancing fraud monitoring and reporting mechanism, or requesting customers to input an additional authentication code for high-risk transactions) before the two-factor authentication mechanism is in place. The HKMA will continue to monitor the technological developments and the trends of internet banking frauds, and work with the banking industry to consider other possible preventive and detective measures if required.

If you have any questions on this letter, please feel free to contact Mr Shu-Pui Li at 2878-1826 or Mr Raymond Suen at 2878-1817.

Yours faithfully,

Raymond Li
Executive Director (Banking Development)

[1] As set out in the guidance note on Supervision of Electronic Banking issued by the HKMA, two-factor authentication refers to the combination of the following two factors:

- something a customer knows (e.g. user IDs and passwords); and

- something a customer has (e.g. one-time passwords generated by a security token or AIs' security systems, a hardware electronic key, or the customer's private key stored in a smart card or other devices in the customer's possession).

Last revision date : 01 August 2011