HONG KONG MONETARY AUTHORITY
香港金融管理局

Circulars

13 Jul 2009

# Strengthening Security Controls for Internet Banking Services (superseded by TM-E-1 of Supervisory Policy Manual)

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

13 July 2009

The Chief Executive
All Authorized Institutions offering Internet banking services

Dear Sir/Madam,

## Strengthening Security Controls for Internet Banking Services

In the light of recent Internet banking fraud cases reported locally and overseas, I am writing to require authorized institutions (AIs) to step up the security controls over their Internet banking services provided to both retail and corporate customers.

The recent fraudulent technique adopted by fraudsters is believed to involve infecting the customer's personal computer (PC) with Trojan horse programs[1] (Trojan) to hijack the Internet banking login credentials of customers during the Internet banking login process. It is believed that when customers attempt to login to the genuine bank's website, the Trojan intercepts the process at the customers' PCs and displays a fake or modified login screen requesting for their login ID and password as well as the one-time password (OTP)[2] for two-factor authentication. The captured login credentials by the Trojan were transmitted to and then used by the fraudsters almost simultaneously at a remote location to login the victims' Internet banking account for conducting high-risk Internet banking transactions, including registering a third-party payee account or making fund transfer to an unregistered third-party account. Fortunately, most of the unauthorised attempts have been detected and/or stopped by the customers or the AIs concerned.

Although the use of OTP for two factor authentication is still recognised as an effective security measure for Internet banking services, adequate protection of the OTP is essential for ensuring continuing effectiveness of two factor authentication. In this connection, AIs are required to implement, where applicable, the security measures set out in the Annex if these measures have not yet been put in place. In addition, the HKMA expects AIs to complete the implementation of these security measures before the end of September 2009. Should AIs find it difficult to complete the implementation within the aforesaid period, they should discuss their timetable with the HKMA individually through their usual contact of the HKMA.

Meanwhile, AIs should step up their online fraud monitoring and reporting mechanism before the above security measures are fully implemented. Where necessary, AIs should verify with their customers on any suspicious and unusual transactions, particularly fund transfers to overseas bank accounts. The HKMA will continue to work with the Hong Kong Police Force and the banking industry to monitor the latest technological developments and trends of Internet banking frauds and to consider other possible preventive and detective measures if required.

If you have any questions on this letter, please feel free to contact Mr Nelson Chow at 2878-1470.

Yours faithfully,

Nelson Man
Executive Director
(Banking Supervision)

Annex

## Recommended measures to strengthen Internet banking security

### *Protection of OTPs and customer alerts*

- AIs should ensure that the OTPs used for logging into Internet banking and/or authenticating online high-risk transaction should expire within a short period of time. In general, the period of validity of such OTPs should not exceed 100 seconds and each online high-risk transaction should require a different OTP.
- With respect to the SMS message containing the OTP, AIs should ensure that the details of the transaction are prominently displayed before the OTP, including among others, the transaction type, partial payee account number and transaction amount if relevant. Customer should be reminded to review the accuracy of the transaction details prior to entering the OTP to initiate online high-risk transactions.
- AIs should notify customers immediately via an effective alternative channel (e.g. SMS message) after completing an online high-risk transaction such as registering a third-party payee account and transferring fund to an unregistered third-party account. The notification message should contain the transaction details, including among others, the transaction type, partial payee account number, and transaction amount if relevant.
- Customers, who choose not to adopt the above notification scheme, should be restricted from using online high-risk transaction facilities. Such customers will need to register third-party accounts and/or increase the transaction limits at bank branches or by post before they can conduct any online fund transfers or bill payments to these accounts.

### *Digital certificate security*

- If digital certificate is adopted for two factor authentication, AIs should ensure that the digital certificate and its associated private key is non-duplicable and stored in a secure media (e.g. a smart card). Customers should be reminded to remove the media storing the digital certificate from their PCs after use.

*Controls over fund transfers*

- The default transaction limit for online fund transfers to unregistered third-party accounts (including both local and overseas payees) should be set to zero when a new Internet banking account is first activated. Customers should only be allowed to increase the transaction limit through secure channels (e.g. at branches or by post) with adequate identity checks conducted by AIs.
- The service for online fund transfers to unregistered third-party accounts should be disabled or the relevant transaction limit should be reset to zero if such a facility has not been used for a prolonged period, say one year.

*Monitoring of unusual activities*

- AIs should have a robust and an effective automated fraud monitoring mechanism in place to detect, in a timely manner, suspicious online transactions and unusual activities based on predefined rules and criteria (e.g. transactions initiated from an Internet Protocol (IP) address[3] different from the one usually used by the customer, fund transfers which have not been done before or fund transfers of amount up to the maximum allowable transaction limit of the customer account).
- Formal incident reporting and management procedures should be put in place to handle detected suspicious and unusual online transactions. For instance, AIs should, as soon as practicable, check with the customers of such transactions or activities before effecting the transactions. AIs should also keep the HKMA apprised immediately of any suspected or confirmed fraud cases relating to Internet banking.

*Customer education*

- AIs should regularly review the security advice to ensure that it remains adequate and appropriate taking into account the latest developments of Internet banking security and fraudulent techniques.
- AIs should pay special attention to the provision of easy-to-understand and prominent advice to customers on Internet banking precautions, in particular, advising the customers to ensure that their PCs are securely configured and that they are adequately protected from computer viruses and malicious programs.
- Customers should be reminded to provide a valid mobile phone and contact numbers for notification purpose and notify the AI timely if any of these numbers are changed.

[1] A Trojan horse is a computer program in which a harmful code is contained inside an apparently harmless program. Trojan horses can infect a PC in circumstances such as when the attacker exploits the vulnerabilities of certain operating systems, and the victim opens contaminated e-mail attachments or visits malicious websites. Trojan horses can be used to capture screen displays and keystrokes, to steal information stored in, or to take over the control of, victims' PCs.

[2] A one-time password for two-factor authentication is typically generated by a security device (e.g. a security token) given by the bank or contained in a short message service (SMS) message sent by the bank.

[3] An "IP address" is a numerical identification and logical address that is assigned to each computer on the Internet. A computer's IP address may be permanently assigned or supplied each time that it connects to the Internet by an Internet service provider.

Last revision date : 01 August 2011