



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

1 June 2011

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Strengthening Security Controls for Automatic Teller Machine (ATM) Services

As you may be aware, the Task Force on ATM Fraud Prevention (“Task Force”) was established by the Hong Kong Association of Banks (HKAB) in May 2010¹ to strengthen ATM security in Hong Kong. The Task Force has reached a consensus that authorized institutions (AIs) offering ATM services should adopt chip-based ATM technology² in order to enhance their security against ATM frauds. We welcome the Task Force’s decision and recommend AIs to implement the chip-based ATM technology as soon as practicable.

Given the technical complexity and substantial number of ATM terminals and cards to be covered by this project, it is recognised that AIs may need some time to implement the chip-based ATM technology. As such, the Hong Kong Monetary Authority (HKMA) expects AIs offering ATM services to complete upgrading their ATM terminals by end of February 2013 to support chip-based ATM cards (“chip cards”) issued by the AI concerned. The AIs concerned are also expected to complete the card replacement process³ not later than end of March 2014 for debit cards and credit cards which are linked to customers’ bank accounts, and not later than end of 2015 for credit cards not linked to customers’ bank accounts. Chip-based authentication on chip cards issued by AIs should be mandated by 1 March 2013 for local ATM transactions⁴ in Hong Kong.

¹ Prior to the establishment of the Task Force on ATM Fraud Prevention, ATM security related issues were covered in the e-Banking Security Sub-Committee (formerly known as e-Banking Working Group) established by HKAB.

² A chip card generally offers enhanced security and protection. For the purpose of this circular, a chip card refers to a card with security related contents stored within the chip on the card which are protected by additional security controls and are non-duplicable.

³ Including the issuance of new cards and replacement of existing cards to support chip-based technology.

⁴ Except cross-network transactions.

We understand that magnetic stripe will be retained on chip cards to allow customers to use ATM services in locations outside Hong Kong that have not adopted chip-based ATM technology. To enhance the security of using overseas ATM services after the launch of chip-based ATM technology in Hong Kong, the overseas ATM cash withdrawal capability for the chip cards should be pre-set as “deactivated” and customers are required to activate such capability and specify an expiry date for the activation period through appropriate channel(s) (e.g. at local ATMs) before overseas ATM cash withdrawal could be conducted. In addition, customers should also be given an option to set a lower withdrawal limit for overseas ATM cash withdrawal transactions. AIs should provide such activation mechanism for chip cards with effect from 1 March 2013.

As regards cross-network ATM services, in general customers are currently able to use their ATM cards at ATM terminals of different ATM networks in Hong Kong (i.e. cross-network ATM transactions). Such transactions are currently treated as overseas transactions and rely on authentication based on magnetic stripe. Under the implementation of chip-based ATM technology, while the activation mechanism for overseas ATM cash withdrawal transactions mentioned above will not be applied to the cross-network ATM transactions in Hong Kong, chip-based (instead of magnetic-stripe based) authentication needs to be adopted for such transactions. As there is additional work required for implementing the security measure for cross-network ATM transactions, the HKMA expects that such cross-network service should adopt chip-based authentication by 1 April 2014.

To ensure that customers have adequate time to understand the new ATM security measures and related procedures, AIs should launch relevant education campaigns to promote public awareness of the new measures with sufficient lead time ahead of the effective date (i.e. 1 March 2013) of the activation mechanism mentioned above.

As the project involves implementation of the above-mentioned enhanced security features at different timelines within the schedule, AIs should continue to review and, if necessary, enhance their ATM precautionary measures having regard to the HKMA circular issued on 14 October 2003 before the full implementation of the project because during that time some of the ATM functionalities still rely on authentication based on magnetic stripe. In particular, AIs should ensure frequent patrols of ATMs at all times to detect any suspicious devices, regularly monitor transactions to identify any suspicious or fraudulent events, and strengthen customer education against ATM frauds.

If you have any questions on this letter, please feel free to contact Mr George Chou at 2878 1599 or Mr James Tam at 2878 8043.

Yours faithfully,

Nelson Man
Executive Director (Banking Supervision)