LCQ13: Plugging loopholes in electronic payment services

Following is a question by the Hon Charles Peter Mok and a written reply by the Secretary for Financial Services and the Treasury, Mr James Lau, in the Legislative Council today (November 21):

Question:

It has been reported that loopholes were uncovered in the procedure for binding credit cards or bank accounts with stored value facilities (e-wallets). As the binding procedure of some credit cards did not include a two-factor authentication via mobile phone short message service (SMS) for identity verification, fraudsters could complete the binding procedure using an anonymous mobile phone card (commonly known as "prepaid SIM card"). Also, as there were loopholes in the process for e-wallet users to set up direct debit authorisation (eDDA) through the Faster Payment System, fraudsters could set up eDDA using prepaid SIM cards and stolen bank account information and then steal money through money transfers. Moreover, some members of the public have relayed to me that the frequent uncovering of security loopholes in the procedure for binding credit cards or bank accounts has undermined their confidence in electronic payment services and the development of financial technologies. After completing a review on the eDDA setup process at the end of last month, the Hong Kong Monetary Authority (HKMA) requested e-wallet operators and banks to refine such process. In this connection, will the Government inform this Council:

(1) of (i) the total number of reports on frauds involving e-wallets received by the Police and HKMA since January this year and the total amount of money involved, and (ii) the details of the follow-up actions taken on such cases, including the investigation progress and the respective numbers of persons arrested and prosecuted;

(2) of the details and effectiveness of the measures taken to refine the eDDA setup process;

(3) whether it had required e-wallet operators and card-issuing banks to conduct security risk assessments before they launched e-wallets; if so, whether the scope of such assessments included if reliable identity verification arrangements were in place for the procedure for binding credit cards with e-wallets;

(4) whether it will stipulate that the procedure for binding credit cards with e-wallets must adopt a two-factor authentication (such as via SMS verification) or other effective measures for identity verification, in order to eradicate the aforesaid frauds; and

(5) as HKMA, in collaboration with the Mainland authorities, is introducing

measures to facilitate cross-boundary electronic payment services (e.g. the trial use of Hong Kong's e-wallets on the Mainland), whether HKMA has assessed the risks posed by such measures to the personal data privacy of Hong Kong residents; if so, of the outcome and the corresponding measures; in view of the differences in the laws and regulations between the two places, how the authorities protect the consumer rights and interests as well as personal data privacy of those Hong Kong people who use cross-boundary electronic payment services?

Reply:

President,

The Faster Payment System (FPS) is a new financial infrastructure, connecting banks and stored-value facility (SVF) operators. It enables the public to transfer funds instantly anytime, anywhere, across different banks and SVF operators. While the FPS should bring convenience to the public, we need to ensure that the system is safe and reliable so that the public can use the system with ease and confidence. In response to reports of fraud cases involving the FPS, the Hong Kong Monetary Authority (HKMA) had taken immediate remedial actions by requesting SVF operators to strengthen the verification requirement so as to close the security loophole.

Our reply to the various parts of the question is as follows:

(1) and (2) Earlier there were suspected cases of individual's personal information and bank account information being stolen. Fraudsters used such stolen information to set up direct debit authorisation, including electronic direct debit authorisation (eDDA) through the FPS, in e-wallets provided by SVF operators. In light of these incidents, the HKMA immediately requested SVF operators to suspend direct debit authorisation services. The HKMA subsequently announced a set of refined procedures on October 26 for setting up direct debit authorisation in e-wallets to prevent an eDDA from being set up with information obtained by unlawful means. These refined procedures include:

(a) the user will receive an SMS notification from his/her bank to confirm the setting-up of eDDA;
(b) the user will need to make a one-time credit transfer from the relevant bank account to his/her e-wallet so as to confirm the e-wallet user is the same as the bank account owner; or
(c) two-factor authentication by the banks.

The above refined procedures could enhance consumer protection and allow SVF operators and banks to take appropriate measures to resume their services having regard to their operational conditions. SVF operators are gradually resuming their direct debit authorisation services in accordance with the refined procedures above.

Based on information obtained by the HKMA, some twenty bank accounts were compromised and the information therein was used to set up direct debit

authorisations through e-wallets. The amount of money involved was around HK$500,000. The Police are following up on these cases. In general, bank account owners who have not authorised direct debit authorisation set-up will not be held liable. The HKMA has been closely following up the reported cases with the relevant banks and SVF operators. The majority of the cases have been reviewed, and the bank account owners concerned have been reimbursed through their banks. While the eDDA in question were conducted through the FPS, the nature of the incidents was about stolen personal information, and did not involve the security of the FPS.

(3) and (4) Regarding the process of binding credit cards with e-wallets provided by SVF operators, the HKMA has earlier issued guidance to SVF operators that support credit card binding service. Specifically, SVF operators are required to implement appropriate arrangements to confirm that the cardholder has given consent when a credit card is bound to an e-wallet account. To enhance consumer protection, the HKMA has further clarified the above guidance and set out clearly that the binding of a credit card to an e-wallet account should only be allowed if the relevant card issuer can confirm the cardholder's consent through SMS one-time password or other effective means.

(5) SVF operators must comply with the HKMA's regulatory requirements on payment security, information system management, user protection, etc. for its day-to-day operation, including the launch of new services. For instance, an SVF operator should have policies and procedures in place on storage of account information and bear the loss of the value stored in a user account where there is no fault on the part of the user. An SVF operator is also required to comply with other relevant regulations, including the Personal Data (Privacy) Ordinance, and assess the relevant risks and control measures of the services in a prudent manner. An SVF operator should also consider the characteristics of individual services and balance them against the user experience when formulating specific security control measures. An SVF operator should keep those measures under review from time to time and make appropriate adjustment in light of the actual operations to ensure that the users' interests are protected. The HKMA will review the SVF operators' implementation of relevant measures during its regular supervision.