LCQ21: Regulation of third-party payment platforms

Following is a question by the Hon Ho Kai-ming and a written reply by the Secretary for Financial Services and the Treasury, Mr James Lau, in the Legislative Council today (June 20):

Question:

Electronic payment services have become popular in recent years, bringing considerable convenience in consumption to members of the public. However, as some third-party payment platforms fail to properly verify payers' identities when processing online transactions (for instance, payers are only required to input credit card/debit card numbers and security codes, as well as cardholders' names), unauthorised transactions are prone to occur. In this connection, will the Government inform this Council:

(1) of the number of complaints involving third-party payment platforms received by the authorities in the past three years, with a breakdown by type of complaints;

(2) of the measures taken by the authorities in the past three years to step up the regulation of the operation of third-party payment platforms (including collection of users' personal data and charging of handling fees or other fees);

(3) whether the authorities will consider making it a mandatory requirement for third-party payment platforms to adopt, when processing online transactions, two-factor authentication for verifying payers' identities, such as by requiring payers to input a one-time password either sent via short message service or generated by security tokens, in addition to credit card/debit card numbers and cardholders' names; and

(4) whether it has plans to promote the acceptance of payment for all government bills and payment notices through third-party payment platforms; if so, of the details and timetable?

Reply:

President,

The Payment Systems and Stored Value Facilities Ordinance (PSSVFO) (Cap 584) prescribing the licensing and regulatory regime of stored value facilities (SVFs) came into operation in 2015. The Hong Kong Monetary Authority (HKMA) considers licence applications and supervises SVF licensees to ensure their safe and sound operation and to foster the development of a secure, efficient, and diversified electronic payment industry.

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

(1) Since the granting of the first batch of SVF licences in August 2016 under the PSSVFO, the HKMA has received around 140 SVF-related complaints. Two cases were related to unauthorised transactions and the remaining were related to SVF licensees' service qualities, commercial arrangements, etc.

(2) The HKMA has issued regulatory guidelines requiring SVF licensees to implement relevant control measures in their operations. The HKMA also monitors and reviews licensees' implementation of the guidelines through ongoing supervisory work. On personal data and privacy protection, the HKMA's guidelines require SVF licensees to put in place robust information security measures and to comply with the Personal Data (Privacy) Ordinance (PDPO) (Cap 486) as well as relevant guidelines issued by the Office of the Privacy Commissioner for Personal Data (PCPD) to ensure that their users' personal data are properly handled and safeguarded. The HKMA also maintains regular liaison with the PCPD and has reminded SVF licensees to contact the PCPD on issues relating to the implementation of the PDPO and relevant guidelines. On fees and charges, SVF licensees are required to set out and explain clearly the applicable fees and charges relating to the use of their services and products, and ensure that such details are effectively communicated and made available to users.

(3) The HKMA's guidelines require SVF licensees to implement adequate payment security controls to ensure the authenticity and traceability of transactions and to institute mechanism for preventing and detecting unauthorised transactions that may arise from fraud. Where needed, SVF licensees should implement additional controls to detect unauthorised transactions, such as introducing two-factor authentication to verify users' identity and issuing transaction notifications to users. The HKMA also requires banks to implement appropriate measures to confirm the authenticity of credit card transactions and protect customers' interest.

SVF licensees are required to implement appropriate payment security measures having regard to individual circumstances. However, the adoption of two-factor authentication or other payment security technology (e.g. biometric authentication) depends on various factors, such as the risk of the relevant SVF, the security level of the authentication technology, the convenience of the payment method, transaction patterns of users, etc. As the design of relevant security measures needs to be balanced against the nature of an SVF's operation, it may not be appropriate for the HKMA to require all SVF licensees to adopt the same measures. Some SVF licensees have already adopted two-factor authentication in processing payment transactions. With regard to online credit card transactions, some banks verify the identity of their customers by using two-factor authentication such as SMS one-time password, whereas some other banks send SMS notifications to their customers after the transactions. In general, if a cardholder did not act fraudulently or with gross negligence, he or she will not be held liable for unauthorised transactions.

(4) The Government currently accepts a wide range of electronic payment

means, including Internet banking, phone banking, PPS, autopay, automated teller machine, etc., for the public's convenience. We note that the e-wallets offered by some SVF operators provide bill payment service as well. Users can scan the barcodes on their bills (such as phone bills and Towngas bills) and make payments through the e-wallets on their mobile phones. To facilitate the development of the SVF market, the Financial Services and the Treasury Bureau is exploring with relevant Government departments on a pilot scheme under which members of the public can settle government bills in the same manner.