LCQ2: Crimes of online financial fraud

Following is a question by the Hon Chan Kin-por and a reply by the Secretary for Financial Services and the Treasury, Mr Christopher Hui, in the Legislative Council today (January 6):

Question:

From time to time in recent years, there have been fraudsters creating websites, social media groups and mobile applications disguised as those of banks, securities firms, insurance companies and insurance intermediaries, who then trick customers of such financial institutions into logging in them, so as to steal the personal data and financial assets of these customers. Regarding crimes of online financial fraud, will the Government inform this Council:

(1) of the respective numbers of reports and requests for assistance regarding online financial fraud received by the Police in each of the past three years, and the total value of the assets involved in these cases; the number of the relevant law enforcement operations by the Police, and the number of persons arrested;

(2) whether the Hong Kong Monetary Authority (HKMA) will set up a task force in collaboration with the Securities and Futures Commission and the Insurance Authority to look into the causes for crimes of online financial fraud becoming increasingly rampant and explore means to combat such crimes (such as imposing heavier penalties); and

(3) of the measures put in place by the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force as well as the HKMA to step up efforts in combating crimes of online financial fraud?

Reply:

President,

As an international financial centre, the provision of safe, efficient and innovative online financial services is conducive to the inclusive development of the financial industry in Hong Kong. Over the past year, we have noticed the broader application of financial technology and development of online financial services by financial institutions due to the pandemic situation. Regulatory authorities, including the Hong Kong Monetary Authority (HKMA), the Securities and Futures Commission (SFC) and the Insurance Authority (IA), have been assessing the risks associated with financial technology and related service development, while continuously monitoring cyber security and the security of financial institutions' computer systems, with a view to protecting the interests of customers and investors. They have also promulgated supervisory guidelines or codes of practice on technology risk management and security measures for online financial services provided

by financial institutions and financial institutions are required to take adequate precautionary measures.

The Hong Kong Police Force (the Police) has maintained close co-operation with regulatory authorities to combat online fraud cases. To protect the public from fraudulent financial websites, upon receipt of reports on such websites regulatory authorities will make prompt announcements to alert the public and refer the cases and provide necessary assistance to the Police for investigation.

Having consulted the Security Bureau, our specific response to the various parts of the question is as follows:

(1) According to the figures kept by the Police, in respect of online fraud (including online business fraud, email scam, social media scam, etc.), in the past three years (as at October 31, 2020) the Police recorded 6 354, 5 157 and 8 843 cases respectively, involving losses of about $2 600 million, $2 900 million and $2 400 million respectively.

The Police does not maintain breakdown of figures relating to online financial fraud as requested in the question.

(2) The HKMA, the SFC and the IA meet regularly through different platforms to discuss issues relating to the development and regulation of the financial services industry, which include financial technology crimes and cyber security. They will also share information and exchange views on industry best practices and appropriate regulatory model in response to the latest technological development and operational risks. The regulatory authorities will review the regulatory requirements related to financial technology regularly and update the relevant guidelines in a timely manner to increase the sector's capability in safeguarding against online crimes. They also work closely with the enforcement authorities to step up efforts in combating relevant crimes.

(3) To combat online fraud effectively, the Police has adopted a multi-pronged strategy with focus on three aspects, covering intelligence exchange and enforcement actions, inter-agency co-operation, and enhanced publicity and education.

Regarding intelligence exchange and law enforcement operations, to help officers better understand the latest trends of and investigation techniques for online fraud, the Police proactively exchanges intelligence and conducts working meetings with Mainland and overseas law enforcement agencies. The Cyber Security and Technology Crime Bureau (CSTCB) of the Police has also been exchanging intelligence with Interpol and other law enforcement agencies, with a view to combatting cross-boundary online fraud through international co-operation.

As for inter-agency co-operation, the Cyber Security Centre under the CSTCB provides support to various critical infrastructure in Hong Kong (including facilities from the financial sector), and also conducts regular

meetings with the HKMA, the Hong Kong Association of Banks (HKAB), and the banking sector to examine risks arising from security incidents of online banking and cyber security of the banking sector, with a view to raising the industry's awareness in enhancing cyber security and preventing crime. Besides, the Commercial Crime Bureau (CCB) of the Police maintains close liaison with regulatory authorities, government departments and various stakeholders to discuss crime trends and typologies. The CCB also co-operates with the banking sector to intercept payments to fraudsters with a view to minimising the loss of victims.

On publicity and education, the Police regularly produces short videos and anti-crime information, and makes use of traditional media and online platforms to alert the public to the latest typologies of fraudsters and disseminate anti-crime messages.

To further strengthen the combat against deception cases and raise the public's anti-deception awareness, the CCB of the Police established the Anti-Deception Coordination Centre (ADCC) in 2017 to monitor and analyse the trends of deception cases, formulate and implement combating strategies, and co-ordinate anti-deception publicity work. The ADCC also operates a 24-hour hotline, "Anti-Scam Helpline 18222" and co-operate with the banking sector to intercept payments to fraudsters, so as to minimise the loss of victims. Meanwhile, the CCB has set up the Fraud and Money Laundering Intelligence Taskforce, which exchanges information and shares intelligence with the HKMA, the HKAB and the banking sector for preventing and deterring criminals from exploiting bank accounts for fraud and money laundering activities.

In addition to the Police, the HKMA has also imposed stringent guidelines requiring banks to take effective measures to manage the risk of fraud. The HKMA has also taken a series of measures to assist members of the public to identify fraudsters impersonating as banks, such as requiring banks to provide customer hotlines for the public to verify the identity of callers claiming to represent banks, and reminding the public through different channels including educational videos, social media and seminars on issues to watch out when using online banking services.

In light of the heightened threat of cyber security during the pandemic, the regulatory authorities (including the HKMA, the SFC and the IA) have stepped up efforts to remind the public to stay vigilant to the possible deceptive acts by fraudsters. Separately, the HKAB established in May last year the Fraud Risk Management Taskforce, which has launched public educational activities on the prevention of online financial fraud and other scams, and to remind the public of the common fraud typologies and preventive strategies.

Thank you President.