LCQ10: Combating crimes of deception

Following is a question by the Hon Starry Lee and a written reply by the Acting Secretary for Security, Mr Michael Cheuk, in the Legislative Council today (June 21):

Question:

It has been reported that there has been a significant increase in the number of deception cases in Hong Kong in recent years. According to a questionnaire survey conducted by the Democratic Alliance for the Betterment and Progress of Hong Kong, over 30 per cent of the respondents claimed that they received five or more suspected fraudulent messages every week while over 10 per cent of the respondents claimed that they had fallen prey to fraud and suffered losses. There are views that the continual substantial increase in the number of fraud cases has reflected that the current measures are inadequate to fend off the increasingly serious attacks launched by fraudsters. In this connection, will the Government inform this Council:

(1) of the respective numbers of persons arrested, prosecuted and convicted on suspicion of fraud as well as the penalties imposed on the convicted persons, in each of the past five years, with a breakdown by nature of the fraud cases;

(2) whether it knows if the Hong Kong Monetary Authority (HKMA) will hold discussions with banks about simplifying the procedure for freezing the money involved in suspicious transactions and more actively examining suspicious accounts suspected to be fraudulent; if the HKMA will, of the details; if not, the reasons for that;

(3) as it is learnt that the Police have set up different task forces to address various types of fraud cases in a targeted manner, whether the Police will invite representatives of the banking industry to join such task forces with a view to enhancing the procedure for identifying suspicious accounts, thereby raising the chance of thwarting fraudsters' attempts to commit fraud; if so, of the details; if not, the reasons for that;

(4) whether it will formulate more stringent requirements and guidelines for the Real-name Registration Programme for Subscriber Identification Module (SIM) Cards in order to plug the existing loophole whereby lawbreakers can use false identity card information to register a large number of SIM cards; if so, of the details; if not, the reasons for that;

(5) whether it will strengthen intelligence exchanges with Mainland and overseas law enforcement agencies with a view to keeping abreast of the latest situation of fraud cases and conducting joint law enforcement operations if necessary; if so, of the details; if not, the reasons for that;

(6) whether it will, in the light of the frequency, organised nature and

seriousness of fraud cases in recent years, collect sufficient information and relay it to the Judiciary, so as to facilitate the court to consider aggravating factors in sentencing and even laying down sentencing guidelines, thereby achieving a deterrent effect; if so, of the details; if not, the reasons for that; and

(7) as the Government indicated in reply to a question raised by a Member of this Council on March 15 this year that the Police planned to organise another "Anti-Deception Month", of the progress and details of the relevant work?

Reply:

President,

Deception is a serious offence. Regardless of how it is committed, stern enforcement actions will be taken as long as there are illegal activities involved. Any person who commits the offence of "fraud" under section 16A of the Theft Ordinance (Cap. 210) is liable to imprisonment for up to 14 years, while any person charged with "obtaining property by deception" under section 17 of the same Ordinance is liable to imprisonment for up to 10 years. In addition, any person charged with "dealing with property known or believed to represent proceeds of indictable offences" under section 25 of the Organized and Serious Crimes Ordinance (Cap. 455) for proceeds of deception is liable to maximum penalties of 14 years' imprisonment and a fine of $5 million. With the global trend of Internet proliferation, many countries and regions have seen a significant increase in deception cases in recent years. The Police will continue to enhance public awareness and combat all types of deception through stepped-up law enforcement measures, publicity and education, multi-agency co-operation, intelligence analysis and cross-boundary collaboration.

In consultation with the Department of Justice (DoJ), the Commerce and Economic Development Bureau, the Financial Services and the Treasury Bureau, the Judiciary and the Police, the consolidated reply to the Member's question is as follows:

(1) The numbers of persons arrested, prosecuted and convicted and the penalties imposed in relation to deception cases in the past five years are at Annex. We do not have a breakdown of figures by nature of the fraud cases.

(2) and (3) The Hong Kong Monetary Authority (HKMA) is responsible for providing guidance and supervising banks' compliance with legal and regulatory requirements such as those related to bank operation and anti-money laundering, and has worked closely with the Police and the banking industry through public-private partnerships to proactively detect and disrupt deception.

In 2017, the Police, the HKMA, the Independent Commission Against Corruption and the Customs and Excise Department established a financial intelligence exchange platform, namely the Fraud and Money Laundering Intelligence Taskforce (Taskforce). Ten retail banks participated in the

Taskforce initially, which will increase to 28 by end-June 2023. Besides holding regular meetings and exchanging intelligence on deception and money laundering activities, the Taskforce provides training to the banking sector on identification of suspicious bank transactions and victims of suspected deception cases. Since the Taskforce's establishment, banks have identified over 21 000 previously unknown mule accounts through sharing information and applying data analytics, and taken prompt actions in support of law enforcement investigations. In 2022, the number of intelligence-led suspicious transaction reports increased by 319 per cent as compared to 2021, and the amount of criminal proceeds restrained or confiscated increased by 113 per cent.

In addition, in 2017, the Police established the Anti-Deception Coordination Centre (ADCC) that operates in a round-the-clock manner and set up a Stop-Payment Mechanism with the banking sector to render timely assistance to the general public in handling suspected deception cases. With the assistance of banks, the Mechanism successfully intercepted nearly $1.3 billion in 2022, minimising losses to victims.

The Police have been enhancing and deepening co-operation with the banking sector, and have been working out various new strategies with the HKMA and the banking sector to combat deception activities. These include providing immediate assistance to the Police regarding deception cases, strengthening analysis and exchange of intelligence, enhancing the capability to identify suspicious accounts and to trace and intercept crime proceeds, and taking immediate anti-deception actions in a targeted manner to promptly identify and assist victims, with a view to combatting deception activities and criminal groups more effectively through concerted efforts. The Police are planning to work jointly with the major banks to set up a new platform to render immediate assistance to the Police regarding deception cases.

(4) The Telecommunications (Registration of SIM Cards) Regulation (Cap 106AI) (the Regulation) has stipulated various requirements of the Real-name Registration Programme for SIM Cards (RNR Programme). The Communications Authority has also issued guidelines (Guidelines) to provide specific operational details and requirements of the RNR Programme for telecommunications service providers (telecommunications operators). The Guidelines has mandated that the telecommunications operators should adopt different measures to verify information of the users, including face-to-face registration, making use of optical character recognition to automatically extract information from identity documents, manual verification of information, etc, so as to effectively verify identity documents of users and to ensure that the registration systems comply with the requirements of the Regulation and the Guidelines.

In addition, the Regulation and the Guidelines have stipulated that if a telecommunications operator finds that the registration information of the relevant SIM card is incomplete or irregular, it shall take reasonable steps to request the relevant user to provide further information for verification and rectification if necessary. Otherwise, the SIM card will be deregistered. Since the full implementation of the RNR Programme on February 24 this year,

the Office of Communications Authority (OFCA) has been carrying out a series of monitoring and enforcement actions to ensure the effective implementation of the RNR Programme and that telecommunications operators have implemented the RNR Programme in compliance with the law and the Guidelines.

To prevent unlawful use of false information to complete real-name registration for the SIM cards, the OFCA has requested telecommunications operators to continue to enhance the registration platforms taking into account the operational experiences since the implementation of the RNR Programme, and to conduct regular sample checks on the registration information. If the users subject to sample checks are unable to verify the registration information pursuant to the instructions of the respective telecommunications operators, the relevant pre-paid SIM (PPS) cards will be deregistered and cannot be used afterwards. The OFCA will continue to maintain close contact with telecommunications operators. If any suspicious cases are identified, telecommunications operators will promptly refer them to the law enforcement agencies for follow-up actions. In April 2023, the Police carried out an arrest operation with various intelligence, including suspicious cases reported by telecommunications operators, and neutralised a criminal group suspected of using false identity documents to register real name PPS cards online and reselling them to deception syndicates for defrauding. The Police arrested four persons suspected of "conspiracy to use false instruments" and "obtaining property by deception" and seized over 60 000 SIM cards. Two of the persons were charged with "conspiracy to use false instruments" and the other two were released on bail pending further investigation.

Besides the offences mentioned above, anyone who registers and transfers SIM cards for illicit purpose may have committed the offence in relation to "aiders, abettors and accessories" under section 89 of the Criminal Procedure Ordinance (Cap. 221).

The Police will continue to rigorously monitor the situation, maintain close liaison with the OFCA and telecommunications operators and take follow-up and enforcement actions as appropriate.

The OFCA will also continue to conduct market surveillance and publicity activities to enhance public understanding of the requirements of the RNR Programme. Members of the public and traders are reminded to complete the real-name registration with their own identity documents and not to purchase or sell PPS cards from unknown sources in the market or that have allegedly completed registration, so as to protect their own interests and avoid any loss or criminal liability.

(5) Deception cases and technology crimes are usually of cross-territorial nature, for example, involving overseas criminal syndicates or with payment transferred overseas. Through a close police co-operation mechanism, the Police Force has been sharing with overseas law enforcement agencies the latest modi operandi and information about crimes, so as to enable them to take prompt corresponding and law enforcement actions. To strengthen intelligence exchange with the International Criminal Police Organisation

(INTERPOL) and law enforcement agencies of other countries in combating various cross-border crimes, including deception cases and technology crimes, the Police has seconded a Superintendent to the INTERPOL General Secretariat in Lyon, France, as well as one Superintendent and one Chief Inspector to the INTERPOL Global Complex for Innovation in Singapore.

Moreover, the ADCC has built up collaborations with the Mainland and overseas law enforcement agencies in intercepting crime proceeds. To further enhance the capability, the ADCC established the International Stop-Payment Mechanism with the "Financial Crimes Unit" of the INTERPOL in October 2019 to enable most member states to make mutual stop-payment requests, thereby facilitating the police forces across the world to combat cross-border deception cases more effectively.

The Police will continue to strengthen liaison and intelligence exchange with law enforcement agencies across the world so as to combat various types of fraud cases more effectively.

(6) Regarding the sentencing of deception cases, the prosecution will consider the circumstances of the case, including the nature, gravity and prevalence of the offence involved, and decide whether to furnish information to the Court of First Instance or the District Court under section 27 of the Organized and Serious Crimes Ordinance (Cap. 455) to prove the prevalence of the offence, the nature and extent of any benefit accrued or intended to accrue, directly or indirectly, by the defendant from the act, the nature and extent of any harm caused to the community and the victim, as well as other relevant aggravating factors. Having considered such information, the Court of First Instance or the District Court will decide whether to impose a heavier sentence. However, such sentence shall not exceed the maximum statutory penalty for the offence.

Sentencing is an essential part in the process of administration of criminal justice. It is an exercise of the courts' independent judicial power. The main objectives of sentencing are retribution, deterrence, prevention and rehabilitation. All four objectives serve the public interest. When setting sentencing levels, the courts take into account all relevant factors. These include the prevalence of certain types of offences. For certain types of crime, the Court of Appeal would also lay down guidelines for sentencing for reference of the court at sentencing.

In addition, after the court has imposed a sentence in respect of a criminal case, the prosecutors of the DoJ will carefully consider the court's sentence and relevant information. If it is found that the sentence is not authorised by law, is wrong in principle, or is manifestly excessive or manifestly inadequate, the DoJ may take the case further under appropriate circumstances. For example, the Secretary for Justice may, under section 81A of the Criminal Procedure Ordinance (Cap. 221), apply to the Court of Appeal for review of the sentence.

In a recent deception case involving online solicitation of investment, the Court of Appeal accepted the DoJ’s application for review of sentence and

imposed a higher sentence on the defendant (Secretary for Justice v Kong Chi Kiu [2023] 1 HKLRD 72, [2022] HKCA 1745). The Court of Appeal pointed out in the case that the online nature of the fraud is one of the aggravating factors owing to its extensive impact. Online fraud is relatively easy to perpetrate but difficult to detect and recover losses. Therefore, the sentencing should carry a deterrent effect.

(7) The Police are committed to combating all types of fraud and will actively enhance collaboration with stakeholders through a multi-agency approach. A multi-channel, extensive publicity strategy is adopted to heighten public awareness of different types of fraud as well as the risks associated with computers, cyber security, use of the Internet and social media.

The Police will continue to mobilise various resources to organise anti-deception publicity campaigns, including the "All-round CyberDefence" campaign, the "Anti-money Laundering Month" campaign and the special television series "All-round CyberDefence" jointly produced with the television station on the themes of cyber security and technology crimes, etc, to promote digital literacy and awareness of anti-deception among the general public. In February, the Police launched a mobile application "Scameter+" as a one-stop scam and pitfall search engine, held a large-scale seminar "How to Strengthen Students' Resilience Against Cyber Pitfalls" in collaboration with the Education Bureau for more than 290 principals and teachers across the territory, and launched an account called "Smart Hong Kong Drifters" on Xiaohongshu to further expand the coverage of anti-deception publicity work.

The Police are planning to organise the "Anti Deception Month" again this year, and are producing a simulation game on online deception. At the end of this year, an anti-deception fun run cum carnival will be held to further raise the public's anti deception awareness.