LCQ20: Combating online and phone fraud

Following is a question by the Hon Chan Kin-por and a written reply by the Secretary for Security, Mr Tang Ping-keung, in the Legislative Council today (January 24):

Question:

It is learnt that in order to combat the increasingly rampant online and phone fraud, the United Kingdom and Singapore have enacted new legislation and introduced many new measures in recent years. In this connection, will the Government inform this Council:

(1) whether it will, by drawing reference from the practice of the United Kingdom, consider enacting legislation to require large online companies to take measures to prevent members of the public from being exposed to fraudulent advertisements (including advertisements for investment schemes with fake celebrity endorsements);

(2) whether it will consider making reference to Singapore's practice of taking the initiative to combat fraud by enacting legislation empowering the Government to order the cessation of the dissemination of the relevant online content where it suspects or has reason to believe that the online activity in question is preparatory to the commission of a scam;

(3) whether it will draw on Singapore's experience and consider rolling out a mobile application which utilises artificial intelligence to automatically filter scam SMSs and phone calls for users who have installed the application by running the suspected fraudulent SMSs and phone calls against a scam database of the Police; and

(4) apart from the aforesaid measures, whether the Government is considering or will introduce other practicable measures to combat online and phone fraud; if so, of the details; if not, the reasons for that?

Reply:

President,

Fraud cases have become increasingly serious in recent years. The Government is very concerned about the situation. Relevant departments have been adopting a multi-pronged approach to combat various types of frauds and enhance public awareness through enhanced law enforcement, publicity and education, multi-agency co-operation, intelligence analysis and cross-boundary co-operation on an ongoing basis.

In consultation with the Commerce and Economic Development Bureau, the Financial Services and the Treasury Bureau and the Hong Kong Police Force,

the reply to the Member's question is as follows:

(1) and (2) The Police and the Communications Authority (CA) have been working closely with stakeholders to combat fraud, including stopping the circulation of fraudulent content on the Internet.

On co-operation with the telecommunications industry, with reference to the practice in other jurisdictions and considering the implementation feasibility in Hong Kong, the CA, in accordance with the Telecommunications Ordinance (Cap. 106) (TO), introduced in 2022 a condition in the licence of telecommunications service providers to stipulate clearly that telecommunications service providers must, upon the request of law enforcement agency, take prompt and necessary actions to block or suspend telephone services and websites which are suspected to be involved in fraudulent activities, so as to assist the Police in combating fraudulent cases. As the licence holders, the telecommunications service providers must comply with the relevant licensing conditions. In case of breach, the CA may, depending on the circumstances, impose penalties according to the TO. Telecommunications service providers have, based on the information provided by the Police, successfully intercepted more than 6 800 website links involved in fraud cases and blocked or suspended more than 2 400 telephone numbers suspected to be involved in fraud cases.

In the course of carrying out their duties, the Police will, for the prevention and detection of crime, request information or seek co-operation from relevant persons or organisations (including information and communications technology companies). Among others, the Police may request Internet platforms to remove posts or other information (such as videos, texts and images). Examples include removal of content suspected to involve fraud, fraudulent accounts opened under pretences to defraud others, etc. The Police and the relevant stakeholders have been co-operating smoothly in this regard and the Police's requests have been actively followed up.

We call upon members of the public who receive suspected fraudulent messages via online platforms to block or report the messages through the function provided by the platforms. They may also report the suspicious links to the Police so as to facilitate the telecommunications service providers to, according to the investigation results by the Police, prevent users from accessing the related websites.

The above measures of multi-agency co-operation and interception of fraudulent cases at source are in line with the practices in different jurisdictions around the world (including the United Kingdom and Singapore). We will continue to proactively enhance our anti-fraud measures, and at the same time keep in view and make reference to the means and measures adopted by overseas jurisdictions in tackling fraudulent cases.

(3) In September 2022, the Police launched a one-stop scam and pitfall search engine, Scameter, and a mobile application version, Scameter+, in February the following year to help members of the public distinguish suspicious online platform accounts, payment accounts, telephone numbers, email addresses and websites, etc, and to provide anti-fraud tips. As at December

31, 2023, the Scameter has recorded over 2.13 million searches, with about 360 000 fraud and cyber security risk alerts issued. We note that similar applications are also available in other countries (e.g. Singapore) to help protect the public from being defrauded.

The Police are actively enhancing the functions of the Scameter+, and are planning to add an automated element in February this year to issue alerts immediately when users browse suspicious websites and receive suspicious calls, so as to remind members of the public to be more vigilant. At the same time, a public reporting mechanism will also be introduced, so that members of the public who come across suspicious calls or websites can report such calls through the app, thereby enriching the content of the database. The functions are similar to those of Singapore's anti-fraud mobile filtering application. We will continue to study the feasibility of different options on how to combat fraud with the use of advanced technology (including artificial intelligence).

(4) Apart from the new measures mentioned above, the Government has also continued to strengthen existing measures to enhance the anti-fraud capability of various sectors of the community.

On co-operation with the financial sector, the Police have set up an Anti-Deception Alliance with major banks at the end of November 2023. Ten banks have stationed their staff at the Police Headquarters to communicate and co-operate with the Police in a more direct and immediate manner on the interception of fraudulent funds, identification of potential fraud victims, and exchange of intelligence. In Singapore, there are also similar arrangements for bank staff to work in police premises to enhance co-operation with the financial sector.

In addition, following the linkage of the Scameter with the Faster Payment System platform in November last year to alert members of the public when they transfer funds to suspicious accounts, the Police will explore with relevant stakeholders the extension of the alert mechanism to other platforms, such as general online banking services and automatic teller machines, in order to widen the scope of the alert mechanism. In addition, the Hong Kong Monetary Authority has required banks to implement a series of measures to enhance the security of electronic banking by March this year, such as setting up a dynamic fraud monitoring mechanism for assessing more thoroughly customers' transaction patterns and data, hence promptly identifying suspicious account activities for taking appropriate actions (including requesting customers to provide additional confirmation before executing transaction instructions).

To target fraudsters using virtual assets to commit fraud, the Securities and Futures Commission (SFC) and the Police established an inter-organisational working group in September 2023 to strengthen the risk assessment mechanism for suspicious virtual asset trading platforms and enforcement collaboration. In case of serious fraud, the SFC and the Police will make full use of the investigation and statutory powers of both parties, including issuing a cease and desist letter to the relevant website operator to terminate the suspected illegal activities, or requesting the Police to

block the suspicious website, thereby combatting the crime with the strongest efforts.

On telecommunication front, the Task Force set up by the Office of the Communications Authority (OFCA), the Police and major telecommunication service providers in September 2022 has introduced various measures to combat online and telephone frauds. They include requiring fixed and mobile telecommunication service providers to monitor and identify the calling modes suspected to be involved in deception and suspend the services of such calls; reminding users to be aware of offshore calls starting with the caller number prefixed with "+852" by sending voice or text alerts to target at fraudulent calls originating from outside Hong Kong; and continuing to enhance the Real-name Registration Programme for Subscriber Identification Module (SIM) Cards, including requesting telecommunications service providers to conduct sample checks regularly and follow up on the verification of suspicious pre-paid SIM cards, strengthening validation of user information etc.

In addition, with a view to helping members of the public verify the identities of SMS senders and guard against telephone and text scam, the OFCA has introduced in late December 2023 the SMS Sender Registration Scheme (the Scheme). The Scheme has first been implemented in the telecommunications sector. All participating companies or organisations will use Registered SMS Sender IDs with the prefix "#" to send SMS messages to local subscribers of mobile services. The OFCA will monitor the implementation of the Scheme and will take the initiative to invite other sectors and government departments that often use SMS to communicate with users to participate in the Scheme, with a view to further expand the Scheme.

The Police will continue to step up law enforcement, enhance prosecution effectiveness and vigorously combat the use of stooge accounts by fraud syndicates for money laundering by applying to the court for heavier penalties. At the same time, the Police will minimise victims' losses by intercepting fraudulent payments and early warning of fraudulent cases, and continue to enhance the public's awareness of fraud prevention through online and offline publicity work. The Police will also actively seek to maintain close co-operation with stakeholders from various sectors, relevant government departments and other law enforcement agencies, including those in the Mainland and overseas, in combating fraudulent cases.