LCQ9: Combating frauds involving deepfake

Following is a question by Dr the Hon Tan Yueheng and a written reply by the Secretary for Security, Mr Tang Ping-keung, in the Legislative Council today (June 26):

Question:

A study has reportedly found that the number of scams involving deepfake in Hong Kong in the first quarter of this year has scored a 10-fold increase year-on-year, which is among the highest in the Asia-Pacific region, and the rate of deepfake identity fraud involving the fintech industry in Hong Kong is the highest in the Asia-Pacific region. On the other hand, some members of the public are worried that there is no way to guard against law-breakers who have in recent years successfully committed frauds by making use of deepfake technology to create highly realistic faces and voices. In this connection, will the Government inform this Council:

(1) of the respective numbers of proactive investigations conducted and reports received by the Government in each of the past three years in respect of fraudulent activities using deepfake technology, and set out for each case the type of fraud and amount of money involved; the detection rate of such cases;

(2) whether it has assessed the effectiveness of the measures introduced by the Government to combat fraud cases involving deepfake-generated false information; and

(3) of the measures in place to enhance the regulation of the application of deepfake technology, and what new measures are in place to step up efforts to combat the dissemination of disinformation on the Internet and social media?

Reply:

President,

Deception is a serious offence. Deepfake refers to the use of deep learning (namely a technique of artificial intelligence (AI)) to synthesise images for the purpose of creating falsified images. In recent years, the Police have noticed a new online deception tactic that involves the use of deepfake technology to impersonate government officials or celebrities for promoting suspicious investment products in fraudulent messages and videos. The Police will continue to enhance public awareness and combat all types of fraud through stepped-up law enforcement measures, including those against deepfake deception, publicity and education, intelligence analysis, cross-boundary collaboration, as well as collaboration with sectors that have a higher chance of being affected by deepfake deception (such as advertisers

and website operators).

In consultation with the Innovation, Technology and Industry Bureau, the reply to the question raised by Dr the Hon Tan Yueheng is as follows:

(1) In view of the emergence of new modus operandi involving deepfake technology in recent years, the Police have maintained separate statistics on this type of fraud since 2023. Up to May 31, 2024, the Police have received three cases relating to deepfake technology, which occurred in August 2023, January 2024 and May 2024 respectively. The first case has been successfully detected and the remaining two cases are still under investigation.

The first case was detected after the Police's proactive intelligence-led investigation. In August 2023, the Police smashed a local fraud syndicate in an operation code-named Smashscam. The syndicate was suspected of stealing others' identities and using an AI face-swapping programme to apply for loans online from finance companies between September 2022 and July 2023, involving money amounting to HK$200,000. Subsequently in August 2023, the Police arrested a total of nine persons, including the mastermind of the syndicate, for the suspected offence of "conspiracy to defraud". This is the first detected case involving AI face-swapping.

In end-January 2024, the Police received one fraud case involving the use of deepfake technology to fabricate a pre-recorded video conference. The informant received a phishing email from a fraudster, who impersonated the Chief Financial Officer of the informant's head office in the United Kingdom (UK) and invited the informant into a group video conference for some alleged confidential transactions. As instructed, the informant eventually gave authorisation to transfer funds to five local bank accounts and suffered a loss of about HK$200 million. After investigation, the Police believed that the pre-recorded video conference was generated using downloaded online public video clips and voices of the impersonated officer. Since the meeting was pre-recorded, there was actually no interaction between the informant and the fraudster. After making the instruction to the informant, the fraudster ended the meeting under some pretext and then continued with the payment transfer instructions using instant messaging software. The case is still under Police investigation.

On May 20, 2024, a staff member of a multinational trade company received a WhatsApp message from a fraudster, who impersonated the Chief Financial Officer of the head office in the UK, and they took part in a video conference for nearly 30 minutes. During the meeting, the "fake boss" instructed the staff member to transfer nearly HK$4 million to a local bank account. According to Police investigation, it is believed that the suspect had used online public videos as materials for alteration using deepfake technology, and then played the altered content at the video conference to mislead the victim into making money transfers. Police investigation is ongoing.

In addition, since November 1, 2023, the Police have started to maintain statistical figures of cases identified or reports received in respect of

online deepfake video clips. As at May 31, 2024, a total of 21 online deepfake video clips involving impersonation of government officials or celebrities were identified by or reported to the Police. Two of them were identified as a result of proactive investigations and 19 cases were reported by members of the public. Of the 21 videos, 20 were identified between November 2023 and January 2024 and the remaining one in March 2024. At the request of the Police, the online or social media platforms concerned had already removed those 21 videos to prevent the public from being defrauded. So far, the Police have not received any reports involving members of the public being defrauded as a direct result of these deepfake video clips.

(2) In response to various challenges posed to cyber policing by AI such as deepfake technology, the Police have been exchanging intelligence with the International Criminal Police Organization (Interpol), law enforcement agencies of different jurisdictions and the AI industry. The Police have also been keeping track of the latest modus operandi and criminal trends worldwide, which included the application of deepfake technology.

To combat different technology crimes, the Police set up the Cybercrime Policing Advisory Panel (CPAP) in December 2022. Led by the Director of Crime and Security and comprising 12 experts and leaders from the technology sector, the CPAP seeks to look into risks of crime and fraud involving AI (including deepfake technology) and to enhance public awareness on the potential risks of AI. The Police will continue to step up co-operation with stakeholders of relevant sectors, and will jointly explore and formulate effective measures to combat relevant crimes.

Regarding strengthening of professional competence, the Police have been organising internal training from time to time to enrich colleagues' knowledge on deepfake technology and its related cybercrimes. Related equipment will also be upgraded on a timely basis to achieve greater capability in combatting different types of cybercrimes.

On publicity and education, the Police have been working on various fronts to educate members of the public about the general concepts of AI as well as the fraudsters' latest modus operandi, so as to prevent the public from falling into traps. The Police also hold press conferences from time to time to explain common tricks of fraudsters, and demonstrate how fraudsters use deepfake technology to conduct video conferencing. Through its Facebook page and the CyberDefender website, the Police have been disseminating information about the latest crime situation and anti-deception advice related to deepfake technology.

In fact, the AI powered deepfake technology utilised by fraudsters is not infallible. On various occasions, the Police have called on the public to stay alert to fraud at all times and reminded them to verify the authenticity of videos with different methods so as to avoid falling into deepfake traps. These methods include:

1) requesting the person to make certain movements in front of the camera, such as turning their head up, down, left or right, and then observe whether

there is any abnormality of the person's image on the screen;

(2) using the content of the conversation to test the authenticity of the other party;

(3) staying alert and verifying with a phone call when a relative or a friend makes a request for remittance via a video or an audio recording; and

(4) avoiding answering unknown video calls and, in case of doubt, utilising the Scameter and Scameter+ or calling the Anti Scam Helpline 18222 for enquiry.

The Police have also been conducting online patrols and enforcement actions from time to time to proactively combat various cybercrimes. To minimise the chances of the public's access to suspicious fraudulent online advertisements, video clips or posts (including those involving the use of deepfake technology), the Police will swiftly request relevant advertisers and website operators to remove them in cases where they are identified. In fact, all the 21 deepfake video clips mentioned above have been removed promptly to prevent members of the public from falling victims to deception. So far, the Police have not received any reports involving members of the public being defrauded as a direct result of these deepfake video clips.

We will not let down our guard. The Police will continue to monitor closely the various new modus operandi of deception and continue to combat fraud cases, including those involving the use of deepfake technology, through the various channels mentioned above.

(3) We note that the pace of AI development and its popularity vary in different regions, and the impact of AI technology on various industries and sectors are not entirely the same. Different regions and organisations have started to look into various measures in light of the latest development in order to cope with the implications and challenges brought by AI, while striking a balance between promoting technology innovation and ensuring compliance of relevant requirements.

As regards combatting the dissemination of false information on the Internet and social media, the Internet is not an unreal world that is beyond the law. Under the existing legislation in Hong Kong, most of the laws enacted to prevent crimes in the real world are applicable to the online world. There are various provisions in place under the existing legal framework to deal with the dissemination of untrue or inappropriate information. For instance, the Crimes (Amendment) Ordinance 2021 introduced the offences of publication or threatened publication of intimate images without consent. The offence is also applicable to intimate images that have been altered (including that altered by AI technology).

In addition, a sub-committee was set up under the Law Reform Commission (LRC) in 2019 to commence a study on cybercrime. At the first stage, a public consultation exercise on cyber-dependent crimes (e.g., illegal access to programme or data) was completed in October 2022. For the next stage, the

sub-committee will study cyber-enabled crimes, i.e., traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of information and communications technology (e.g., offences such as setting up a phishing website). The Government will closely monitor the progress of the LRC's study as well as its final recommendations, and review the legislation in due course.