LCQ11: Prevention of telephone fraud

Following is a question by Dr the Hon Dennis Lam and a written reply by the Secretary for Commerce and Economic Development, Mr Algernon Yau, in the Legislative Council today (February 26):

Question:

The Office of the Communications Authority announced at the end of last year that starting from December 31 last year, local mobile service providers would play a voice alert message to local users for calls made from newly activated local prepaid Subscriber Identification Module (SIM) cards, stating, "This call is made from a new prepaid SIM card", so as to further assist members of the public in staying vigilant against suspicious calls. On the other hand, it has been reported that the number of telephone fraud cases has remained high since the Government introduced the Real-name Registration Programme for SIM Cards. In this connection, will the Government inform this Council:

(1) whether it has estimated the effectiveness of the aforesaid voice alert measure;

(2) of the number of telephone fraud cases received by the Police last year and the total amount of money involved;

(3) of the respective numbers of cases received by the Police last year concerning the purchase and registration of local SIM cards using false identity documents, and the sale of SIM cards registered in the names of others;

(4) of the respective numbers of cases in which telecommunications service providers rejected SIM card registration requests and deregistered suspicious SIM cards last year;

(5) of the number of cases received by the Police last year concerning the use of artificial intelligence image synthesis technology to create falsified images and commit fraud through video calls; and

(6) the number of downloads of "Scameter+" since its launch, and the number of suspicious calls it has successfully blocked?

Reply:

President,

The Real-name Registration Programme for SIM Cards (RNR Programme) has been fully implemented since February 24, 2023, requiring that all SIM cards issued and used locally (including SIM service plans and pre-paid SIM cards (PPS cards)) must complete real-name registration before service activation.

The RNR Programme helps plug the loophole arising from the anonymous nature of PPS cards used in conducting illegal activities in the past, and assists law enforcement agencies in the detection of crimes involving the use of PPS cards (including phone deception). To combat phone deception, the Office of the Communications Authority (OFCA) has been collaborating with the Hong Kong Police Force (Police) and telecommunications operators to devise and implement a series of measures from the telecommunications services perspective to combat such illegal activities by tackling the problem at source. Regarding the question raised by Dr the Hon Dennis Lam, having consulted the Security Bureau, the Police and OFCA, our reply is as follows:

(1) and (4) To assist the public in guarding against suspicious calls, local mobile service providers have been required since December 31 last year to send voice alerts to local mobile and fixed service users for calls made from newly activated local PPS cards to raise users' awareness of suspicious calls. The voice alerts are applicable to newly activated local PPS cards while the SIM service plans are not affected. The measure has been implemented for about two months and has been operating smoothly overall. OFCA will continue to review the implementation of the measure, and make appropriate adjustments as necessary to ensure its effective implementation.

In addition, to ensure the effective implementation of the RNR Programme, OFCA has been requiring telecommunications operators to continuously enhance their registration platforms taking into account the implementation experiences, including the request for telecommunications service providers to adopt "iAM Smart" as the default registration method for Hong Kong identity (HKID) card holders under the RNR Programme since October last year or otherwise, telecommunications operators must manually verify the registration information submitted upon receipt of a registration request for completing the necessary procedures before activating the PPS cards. At the same time, telecommunications operators have to conduct full manual verification of the registration information submitted on the online registration platforms by all non-HKID holders (e.g. holders of valid travel documents or passports) for PPS cards. Moreover, telecommunications operators are required to conduct regular sampling checks on the registration information of registered PPS card users and manual checks on suspected cases. If users subject to sample checks are unable to verify the registration information following the instructions of the respective telecommunications service providers, the relevant PPS cards may be deregistered and cannot be used further.

Since the implementation of the RNR Programme, as of the end of January this year, around 4.1 million PPS cards were rejected as the clients failed to provide information in compliance with the registration requirements. In addition, telecommunications operators have cancelled the registration records of about 3.2 million non-compliant PPS cards. OFCA will continue to maintain close liaison with telecommunication operators and will refer any suspicious cases to the Police for follow-up action as soon as possible.

To further enhance the RNR Programme, the Government is reviewing the overall implementation of the RNR Programme, including the limit on the

number of PPS cards, as well as prohibiting the resale of registered SIM cards. The Government plans to introduce the relevant legislative amendments to the Legislative Council within this year.

(2) and (3) The Police received a total of 9 204 telephone deception cases in 2024, involving a total amount of $2.91 billion. The Police does not keep statistics on the number of cases concerning the purchase and registration of local SIM cards using false identity documents or the sale of SIM cards registered in the names of others.

(5) and (6) The Police received a total of three fraud cases related to deepfake technology in 2024, involving fraudsters impersonating senior executives of companies to lure victims to make money transfers, and cases of deepfake technology being used to lure victims in Hong Kong, the Mainland and various places in Southeast Asia to invest in cryptocurrencies.

In addition, the Police launched a one-stop scam and pitfall search engine, Scameter, in September 2022, 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, websites, etc, and to provide anti-fraud tips. As of the end of last year, "Scameter+" had been downloaded for over 874 000 times, and had alerted users to over 90 000 suspicious calls and over 600 000 suspicious websites. In addition, since September 2022 and up to the end of last year, the Police have asked telecommunications operators to block more than 8 300 local and non-local suspicious telephone numbers and nearly 30 000 suspicious website links.