

LCQ7: Measures to combat telephone fraud

Following is a question by the Hon Duncan Chiu and a written reply by the Acting Secretary for Commerce and Economic Development, Dr Bernard Chan, in the Legislative Council today (June 18):

Question:

In recent years, the HKSAR Government has adopted diversified measures to actively combat telephone fraud, including introducing the Real-name Registration Programme for Subscriber Identification Module (SIM) Cards (RNR Programme) and the Hong Kong Police Force's "Scameter+" and requiring local telecommunications service providers (TSPs) to play a voice alert message for calls made from newly activated pre-paid SIM (PPS) cards and block suspicious calls, as well as strengthening co-operation with Mainland and international law enforcement agencies. However, there are views pointing out that local telephone fraud cases have not shown a decreasing trend, causing inconvenience and disturbance to the public in their daily lives. In this connection, will the Government inform this Council:

- (1) of the number of telephone fraud cases received by the Police from January to May this year, as well as the amount of money involved in such cases, the number of victims and their age distribution;
- (2) of the total number of PPS cards which have been rejected as the clients failed to provide information in compliance with the registration requirements since the introduction of the RNR Programme; the total number of the registration records of non-compliant PPS cards which have been cancelled by the TSPs, together with a breakdown and percentage by reason for non-compliance;
- (3) whether it has estimated the number of registered PPS cards resold in the market under the RNR Programme; of the authorities' countermeasures currently in place against the resale practice concerned, and how they follow up cases of members of the public purchasing and using PPS cards that have long been registered by other persons;
- (4) as the 2024 Policy Address has mentioned that the Government would introduce a legislative amendment proposal into this Council to prohibit the resale of registered SIM cards with a view to further enhancing the RNR Programme, of the latest progress of such work and the legislative timetable;
- (5) of the accumulated downloads of "Scameter+" since its launch by the Police in February 2023 and the respective numbers of call alerts issued to users and local and non-local suspicious telephone numbers which the TSPs have been required to block; of the details and outcome of the Police's follow-up actions in respect of such suspicious and blocked telephone numbers; and

(6) whether it has comprehensively reviewed the effectiveness of the various measures introduced by the Government to combat telephone fraud; if so, of the results, and the measures in place to cope with the situation where the number of telephone fraud cases has not decreased, including whether it will adjust the existing overall strategy for combating telephone fraud, as well as introduce relevant enhancement measures and new measures?

Reply:

President,

The Office of the Communications Authority (OFCA) has been devising and implementing a series of preventive measures from the perspective of telecommunications services to assist the Hong Kong Police Force (Police) in combating phone deception at the source. In response to the question raised by the Hon Duncan Chiu, having consulted the Security Bureau, OFCA and the Police, our consolidated reply is as follows:

The Real-name Registration Programme for SIM Cards (RNR Programme) has been fully implemented since February 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. Under the RNR Programme, OFCA has requested telecommunications service providers (TSPs) to conduct regular sampling checks on registered SIM card information, to step up verification of suspicious cases, and to refer cases suspected of violating the law to the Police for handling. If the users subject to sample checks are unable to verify their registered information in accordance with the instructions of the respective TSPs, the relevant PPS cards will be deregistered and cannot be used thereafter. As at end-April this year, around 4.71 million PPS cards were rejected for registration as the clients failed to provide information in compliance with the registration requirements (including cases where registration was done using a copy of an identity document and the information provided was inconsistent with the identity document, etc). Besides, the registration records of about 3.4 million non-compliant PPS cards have been deregistered (including cases where users failed to verify their identities as required during the TSPs' sampling checks and were suspected of using forged documents for registration, etc). According to the information provided by the TSPs, the majority of deregistration was due to users failing to submit required identity documents for verification as required. OFCA does not maintain information on specific reasons for deregistration by breakdown.

To enhance the effective implementation of the RNR Programme, OFCA has required the TSPs to adopt "iAM Smart" as the default registration method for Hong Kong identity card (HKID) holders. For non-HKID holders, their real-name registration information will be manually verified. Currently, provision of false information and/or false documents under the RNR Programme may constitute a criminal offence. OFCA does not maintain information on the resale of registered PPS cards in the market.

In addition, the Police launched the mobile application "Scameter+" in February 2023 to help members of the public distinguish suspicious online

platform accounts, payment accounts, phone numbers, email addresses, websites, etc, and to provide the public with anti-fraud tips. As at end-April this year, "Scameter+" had recorded over 960 000 downloads, 8.4 million searches in its search engine and 1 million alerts issued to members of the public. "Scameter+" has now been upgraded and is equipped with automatic detection functions. The Call Alert function and the Website Detection function within the mobile application will automatically identify scam calls and fraudulent websites. If potential fraud or cyber security risk is detected, "Scameter+" will issue a real-time notification, reminding users not to answer the call or browse the website. As at end-April this year, "Scameter+" had issued over 800 000 warnings about suspicious calls and websites to the public through its automatic function. Under OFCA's co-ordination, the Police and major TSPs have established a mechanism where the TSPs will, based on the fraud records provided by the Police, block the telephone numbers suspected to be involved in deception cases and intercept suspicious website links as soon as possible. As at end-April this year, more than 50 000 website links and about 9 000 local and non-local phone numbers have been successfully blocked. The Police will also actively investigate cases related to these suspected scam phone numbers.

Apart from the above-mentioned measures, OFCA has also required the TSPs to intercept suspicious calls starting with "+852", send voice alerts or text messages to all mobile users for overseas calls prefixed with "+852", and play voice alerts for newly activated PPS cards, as well as has launched the SMS Sender Registration Scheme to assist members of public in distinguishing the identity of the SMS senders. OFCA has also been conducting continuous market surveillance and strengthening publicity activities, as well as has launched the District Anti-Phone Deception Ambassador Scheme in January this year, appointing over 300 District Council members and staff members of their ward offices as District Anti-Phone Deception Ambassadors. Starting from May this year, OFCA has collaborated with District Anti-Phone Deception Ambassadors through community activities to further promote anti-scam messages.

For telephone deception trends, the Police recorded a total of 1 816 telephone deception cases between January and April this year, averaging 454 cases per month and representing a significant 52.3 per cent decrease compared to the monthly average of 951 cases in the fourth quarter of 2024. The financial losses associated amounted to approximately HK\$320 million, involving a total of 1 759 victims aged between 15 and 97. For telephone deception cases involving impersonation of customer service emerged since early last year, after focused enforcement efforts by the Police, the monthly average for the first four months this year dropped to approximately 190 cases, recording a decrease of over 80 per cent from the peak of about 1 110 cases in July 2024. These trends highlight the effectiveness of measures implemented by the Government in combating phone deception.

The Government will continue to adopt a multi-pronged approach to combat phone deception and protect the interests of the public. Regarding anti-phone deception measures and the RNR Programme, with reference to the overall implementation experience and the Police's provision of scam trends on

criminal groups using PPS cards, the Government is reviewing the implementation effectiveness of relevant measures and overall operation of the RNR Programme, including reviewing the limit on the number of PPS cards, the arrangement for prohibiting the sale of registered SIM cards or using information of others to conduct real-name registration for profit making, etc. The Government aims to consult relevant Legislative Council Panel within this year.