LCQ17: Combating crimes involving fraudulent messages

Following is a question by the Hon Gary Zhang and a written reply by the Acting Secretary for Commerce and Economic Development, Dr Bernard Chan, in the Legislative Council today (July 12):

Question:

On combating crimes involving fraudulent messages, will the Government inform this Council:

(1) of the respective numbers of cases involving fraudulent messages (including mobile phone SMS messages and messages received from instant messaging applications such as WhatsApp) which were detected and investigated by the Government on its own initiative and reported to it in the past five years, with a breakdown by the place from which such messages were sent and the type of fraud involved (including pretending to be banks, courier companies, head hunting agencies, and companies providing pornographic services or information);

(2) as some members of the public consider that since the implementation of the Real-name Registration Programme for Subscriber Identification Module Cards (Real-name Registration Programme), the number of fraudulent messages mentioned in (1) has been on the rise, whether the Government has analysed the causes of such phenomenon and taken corresponding follow-up actions;

(3) of the measures put in place by the Government after the implementation of the Real-name Registration Programme to combat crimes of using local telephone numbers to send fraudulent messages; whether it has established a notification mechanism with operators of instant messaging applications such as WhatsApp to facilitate law enforcement actions; and

(4) of the measures put in place by the Government currently to combat fraudulent messages sent locally and from overseas, and whether it has assessed the effectiveness of the relevant measures; the policies to be put in place by the Government in future to improve communication and network systems, so as to plug the loopholes concerned?

Reply:

President,

The Government is very concerned about crimes involving fraudulent messages and attaches great importance in combating them seriously. Any form of deception is a serious criminal offence and enforcement action will be undertaken by the Police. 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 enhanced law enforcement measures, publicity and education, multi-agency co-operation, intelligence analysis and cross-boundary collaboration. The Office of the Communications Authority (OFCA) has also been committed to, from the perspective of telecommunications services, providing assistance to the Police in their law enforcement operations so as to combat fraudulent messages transmitted via telecommunications networks.

In consultation with the Security Bureau, Hong Kong Police Force and OFCA, the reply in response to the question raised by the Member is as follows:

(1) According to the Police's statistics, "phishing scams" are one of the common types of fraud in recent years, which involves scammers impersonating banks, telecommunications companies and other institutions to send fraudulent messages through SMS and other instant messaging applications to lure victims to fake websites to provide their personal information or credit card information. The culprits will then use such information to make redemption by using the victims' gift points or make online purchases by using their credit cards. According to the information maintained by the Police since 2023, a total of 2 369 "phishing scams" were reported in the first five months of 2023. The Police does not keep breakdown on the number of scams involving different communication software or by the origin of the messages of "phishing scams".

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

The RNR Programme aims to plug the loophole arising from the anonymous nature of PPS cards used in conducting illegal activities in the past, and is one of the ways to assist law enforcement agencies in the detection of crimes involving the use of PPS cards (including phone deception). It helps safeguard the integrity of telecommunications services and the security of the communications networks, thereby maintaining social order and preventing crimes. OFCA has been collaborating with mobile telecommunications service providers (telecommunications service providers) to ensure the effective implementation of the RNR Programme through conducting sample checks and verification of suspicious PPS cards so as to assist the Police in combating phone deception. Recently, based on a telecommunications service provider's report, the Police successfully arrested suspects of using fake identity card information to register a large number of PPS cards.

The culprits would turn to different defrauding tricks and adjust their deception channels and tactics constantly in response to the measures implemented by the Government. OFCA will maintain close contact with telecommunications service providers to monitor the situation, and will continue to adopt proactive measures to follow up with the implementation of the RNR Programme in order to assist the Police in combating phone deception.

(3) and (4) New measures introduced by the Police to prevent cyber fraud have included the one-stop scam and pitfall search engine "Scameter" and its application "Scameter+" launched in September last year and February this year respectively. These measures provide the assessment of the risk of fraud and cybersecurity by analysing information such as suspicious platform account names, bank account numbers, phone numbers, email addresses, etc. input by the users. They help the public in distinguishing, strengthening prevention, detecting and curbing fraud behaviours, as well as reducing financial losses. These applications have recorded about 1 million searches and have gained the support of the Hong Kong Monetary Authority, the Hong Kong Association of Banks, and the banking and stored value facility sectors. Besides, the Police's Anti-Deception Coordination Centre has set up a 24-hour "Anti-Scam Helpline 18222" to provide immediate consultation services to members of the public so as to handle suspicious deception cases more effectively.

On combating cross-boundary technology crimes, the Police have been working closely with Mainland and overseas law enforcement agencies, other government departments and key industry stakeholders to actively exchange intelligence, share the latest investigation techniques, and establish research and experience-sharing partnerships with various overseas public and private organisations.

OFCA, the Police and the telecommunications service providers have also strengthened co-operation and established a working group in September last year to devise and implement feasible technical measures to co-operate with the Police in combating deception cases from the telecommunications perspectives. Under the co-ordination of OFCA, major telecommunications service providers are actively following up with implementation details of various measures and strengthening their network management.

We have noticed that in many cases, SMS messages with embedded phishing links were used to lure victims to access suspected fraudulent websites. To combat fraud through SMS messages, the telecommunications service providers and the Police have established a liaison protocol, based on the deception record and identified deception websites provided by the Police, to block or suspend services of the phone numbers suspected to be involved in deception cases and to prevent users from accessing the suspicious fraudulent websites. The measure has effectively forestalled users' access to fraudulent websites upon the receipt of phishing SMS messages.

In addition, to assist the public in ascertaining the authenticity of SMS sender addresses, OFCA, joined by the telecommunications service providers, the Police, the banking sector and its regulatory authority, have worked together to formulate technical proposals and details for launching the registration scheme for SMS senders. It is our target to commence a pilot run of the scheme for the banking industry by end of this year. We will review the effectiveness of the above scheme and consider extending the measure to other industries and sectors.

With regard to more scams being committed through instant messaging applications (such as WhatsApp), since these applications operate on the Internet, they are not among the telecommunications services regulated by the Telecommunications Ordinance. Moreover, given most of these applications are provided by non-locally registered companies with encrypted content, local laws are not able to regulate the operation of these applications. Hence, such messages cannot be blocked by the local telecommunications service providers. We would call upon members of the public who receive suspected fraudulent messages via such applications to block or report the cases through the function provided by the applications. They may also report the suspicious links to the Police so as to facilitate the telecommunications service providers to, on the basis of the Police's investigation results, prevent users from logging onto the related websites.

All in all, the most effective anti-deception means is to remind oneself, our families and friends to stay highly vigilant at all times. If members of the public receive calls or messages from strangers, regardless of the displayed number or SMS sender address, they should stay highly vigilant, and not disclose personal information, transfer money to unknown callers or senders, or click the hyperlinks embedded in SMS messages, to avoid suffering from losses. If in doubt, they should report the cases to the Police immediately.

OFCA, the Police and the telecommunications service providers will continue to strengthen co-operation in stepping up public education and publicity through different channels, such as issuing press releases and consumer alerts, launching announcements on TV channels, arranging roving exhibitions, seminars for the community and consumer education programmes, with a view to widely disseminating anti-deception messages to all members of the public and reminding them to stay alert to all calls and messages received.