LCQ5: Cases of fraud through mobile phone SMS messages

Following is a question by the Hon Leung Man-kwong and a reply by the Acting Secretary for Commerce and Economic Development, Dr Bernard Chan, in the Legislative Council today (June 21):

Question:

It has been reported that despite the Government's implementation of the Real-name Registration Programme for Subscriber Identification Module Cards, there are still quite a number of overseas fraudsters who steal the credit card or online banking information of members of the public by sending them mobile phone SMS messages impersonating various retail shops and telecommunication companies the authenticity of which is hard to identify, causing members of the public to suffer losses. In this connection, will the Government inform this Council:

(1) as some phishing mobile phone SMS messages originate from overseas, whether the Government will consider, by making reference to the practice of issuing alerts for incoming overseas calls, adding alerts to mobile phone SMS messages originating from overseas, so as to raise the alertness of members of the public and prevent fraud cases; if so, of the details; if not, the reasons for that;

(2) whether it will expeditiously launch a SMS sender registration system or other mobile phone SMS message authentication systems to provide special authentication for SMS messages sent by reputable organisations, so as to increase the identifiability of such SMS messages; if so, of the details; if not, the reasons for that; and

(3) as most of the cases of fraud through mobile phone SMS messages involve fraudulent use of credit card information, whether the Government has plans to step up publicity on the security issues of online banking and mobile payment services and introduce new safeguards, so as to prevent cyber frauds; if so, of the details; if not, the reasons for that?

Reply:

President,

Any form of deception is a serious criminal offence and enforcement action will be undertaken by the Police. The Police has been implementing new measures to prevent cyber fraud. For fraudulent calls and messages transmitted via telecommunications networks, the Office of the Communications Authority (OFCA) is also committed to, from the perspective of telecommunications services, providing assistance to the Police in their law enforcement operations. At the same time, the Police has been working with

the Hong Kong Monetary Authority (HKMA) and the banking industry to explore various new approaches to combat deception activities.

In consultation with the Security Bureau, Financial Services and the Treasury Bureau and the Police, the consolidated reply in response to the question raised by the Member is as follows:

OFCA established a working group with the Police and major mobile network operators (MNOs) in early September last year to devise and implement feasible technical measures to cooperate with the Police in combating deception cases from the telecommunications perspectives. Under the coordination of OFCA, major MNOs 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. In this connection, MNOs 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 MNOs, the Police, the banking sector and its regulatory authority, have established another dedicated working group to formulate technical proposals and details in relation to the implementation of 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.

New measures introduced by the Police to prevent cyber fraud include the one-stop scam and pitfall search engine "Scameter" and its application "Scameter+" launched in September last year and February this year respectively, which would assess the risk of fraud and cybersecurity by inputting suspicious platform account names, bank account numbers, phone numbers, email addresses, etc. They help the public in distinguishing, strengthening prevention, detection and curb on fraud behaviors, as well as reducing financial losses. These applications have recorded about 900 000 searches and have gained the support of the HKMA, the Hong Kong Association of Banks, the banking and stored value facility sectors.

The Police are exploring with the HKMA and the banking industry a number of new measures to combat fraudulent activities, including enhancing co-operation with the banking industry, providing immediate assistance to the Police in fraud cases, strengthening intelligence analysis and exchange, enhancing the ability to identify suspicious accounts, detecting the whereabouts of fraudulent funds and intercepting fraudulent funds, and conducting targeted and immediate anti-fraud operations to identify and

assist victims at an early stage so as to combat fraudulent activities and related criminal syndicates more effectively together. In particular, the Police are planning to set up a new joint platform with major banks to provide immediate assistance to the Police in fraud cases.

As for the HKMA, card issuing banks have all along been required to implement effective measures to ensure the security of credit card transactions in order to protect the interests of customers. In view of the recent rise in unauthorised transactions involving the binding of the victim's credit card to a new mobile payment application, the HKMA has provided new guidance to the industry, requiring banks to perform additional authentication apart from issuing an SMS one-time-password for binding of credit cards to a new mobile payment application, in order to confirm that the customer has actually given such binding instructions. Moreover, with the development of payment card services and related scams, the HKMA and the Hong Kong Association of Banks have established a taskforce earlier this year to proactively explore the enhancement of protection measures for payment cards. Details will be announced after finalisation.

Concurrently, in order to safeguard the integrity of telecommunications services and the security of the communications networks, the Government has implemented the Real-name Registration Programme for SIM Cards (the RNR Programme) on 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 can 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 including phone deception involving the use of PPS cards. OFCA will work with MNOs to ensure that the RNR Programme is effectively implemented through conducting sample checks and verification of suspicious PPS cards with a view to assisting the Police in combating phone deception.

All in all, the most effective anti-deception means is to remind ourselves, our families and friends to stay highly vigilant at all times. Once again, we would like to remind members of the public that upon receiving calls or messages from strangers, regardless of the displayed number, they stay highly vigilant and do not disclose personal information or 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 case to the Police immediately. On this, 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.

OFCA, the Police and MNOs will continue to strengthen co-operation to step up public education and publicity through different channels, such as issue of press releases and consumer alerts, launching announcements on TV channels, arranging roving exhibitions, community seminars 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

received calls and messages.