LCQ17: Combat fraudulent calls and SMS messages

Following is a question by the Hon Kingsley Wong and a written reply by the Secretary for Security, Mr Tang Ping-keung, in the Legislative Council today (June 11):

Question:

Many members of the public have relayed to me about the increasing number of fraudulent calls, as well as fraudulent SMS messages sent via instant messaging applications (e.g. WhatsApp) and phones in recent years. In this connection, will the Government inform this Council:

(1) as it is learnt that many members of the public have been repeatedly added to suspected fraudulent groups on instant messaging applications by unknown accounts, many of which are registered with overseas phone numbers, and that these groups use "like-and-earn-rewards" and "stock investments", etc as bait, of the number of reports received by the Police from members of the public in the past year, the total amount of money defrauded, and the number of arrests made; what targeted measures are in place by the authorities to combat fraud by such groups;

(2) as it is learnt that many fraudsters have hacked into the instant messaging application accounts of members of the public to request money and virtual point card top-ups from their contacts, of the number of reports received by the Police from members of the public in the past year, the total amount of money defrauded, and the number of arrests made; whether the authorities have analysed which insecure practices when using such applications increase the risk of account hacking, and what targeted measures are in place to combat such account hacking by fraudsters;

(3) as it is learnt that fraudsters falsely pretending to be the official platforms of government departments and organisations, banks, telecommunications service providers or neighbours via mobile phone SMS messages to commit fraud has become increasingly prevalent, of the number of reports received by the Police from members of the public in the past year, the total amount of money defrauded, and the number of arrests made; what respective follow-up actions the authorities have taken regarding fraudulent SMS messages sent from local and overseas sources; the average time required for the authorities to block the phone numbers concerned after such phone numbers are confirmed to be involved in fraud; and

(4) as many members of the public have relayed that they have frequently received repeated promotional calls containing fraudulent content, causing them nuisance and indicating a worsening trend, whether the authorities will review if the existing legislation governing such calls is inadequate; if so, of the details; if not, the reasons for that?

Reply:

President,

Deception is a serious crime. Any person who commits the offence of "fraud" under section 16A of the Theft Ordinance (Cap. 210) is liable to imprisonment for up to 14 years, while any person charged with "obtaining property by deception" under section 17 of the same Ordinance is liable to imprisonment for up to 10 years. In addition, any person charged with "dealing with property known or believed to represent proceeds of indictable offence" under section 25 of the Organized and Serious Crimes Ordinance (Cap. 455) for proceeds of deception is liable to maximum penalties of 14 years' imprisonment and a fine of $5 million. Regardless of whether it is committed through telephone, messaging applications or other methods, the Government of the Special Administrative Region will take stern enforcement actions as long as there are illegal activities involved. With the global trend of Internet proliferation, many countries and regions have seen a significant increase in fraud cases in recent years. The Police will continue to combat all types of frauds and to enhance public awareness in full force through enhanced law enforcement measures, publicity and education, multi-agency co-operation, intelligence analysis as well as cross-boundary collaboration.

In consultation with the Commerce and Economic Development Bureau and the Police, the reply to the Member's question is as follows:

(1) "Stock investment" scams mentioned in the question involve fraudsters using online social media platforms, discussion forums, or instant messaging apps to lure victims into participating in fake investment schemes by promising "low risk, high returns". The Police classify such scams as "online investment fraud". In 2024, there were a total of 3 930 cases, involving approximately $2.26 billion in losses; in the first four months of 2025, there were 1 534 cases, involving approximately $1.02 billion.

As for "like-and-earn-rewards" scams mentioned in the question, they involve fraudsters using online social media platforms to recruit victims to register as "like clickers". The scammers claim that victims can earn rewards by paying a "deposit" and then clicking "like" on a designated social media platform; the more deposit paid, the higher the reward per "like". However, this is in fact a scheme to defraud victims of their deposits. The Police classify such scams as "online employment fraud". In 2024, there were 3 853 reported cases, with total losses amounting to approximately $800 million; in the first four months of 2025, there were 1 515 cases, involving approximately $340 million.

The Police do not maintain any breakdown of arrested person by types of deception.

In combatting such fraudulent activities, the Police have taken measures in law enforcement, cross-border collaboration, and public education. Since most fraud cases in Hong Kong currently use stooge accounts to receive

payments, cracking down on stooge accounts is an effective method to combat the fraud industry chain. In 2024, the Police arrested a total of 10 496 individuals involved in various types of fraud and money laundering offences; in the first four months of 2025, a total of 2 532 individuals were arrested, approximately 70 per cent of which were holders of stooge accounts. Since the end of 2023, the Police have also applied to the court to invoke Section 27 of the Organized and Serious Crimes Ordinance to impose heavier penalties in cases involving stooge accounts, thereby enhancing deterrence.

In terms of cross-border collaboration, the Hong Kong Police Force recently joined hands with the Police forces of the Macao Special Administrative Region, Malaysia, Maldives, Singapore, Korea, and Thailand, conducted the first joint operation of the Cross-border Anti-Scam Collaboration Platform "FRONTIER+", working together to combat cross-border fraud crimes. They successfully identified and dismantled multiple cross-border fraud networks, arresting a total of 1 858 individuals involved in 9 268 fraud cases, including investment fraud.

In terms of publicity, given the increase in the two aforementioned types of fraud at the beginning of 2025, the Police have held press conferences on multiple occasions over the past few months and utilised various channels, namely the CyberDefender website and Facebook, to enhance publicity efforts and remind the public to remain vigilant (including explaining the latest deception tactics employed by fraudsters and outlining how the public can protect themselves), such as making use of WhatsApp's privacy settings to allow only contacts from one's address book to add the user to groups, thereby preventing being added to fraudulent groups by strangers.

(2) Scammers often use various methods to steal social media accounts, including fake customer service and fake websites. A common tactic is to send phishing messages claiming that the account has encountered security risks, luring users to click on links, enter account login information on fake websites or scan QR codes, thereby hijacking the account and sending messages to the user's friends and family to request loans or the purchase of game point cards.

Such scams are categorised as "online account hijacking" cases, with 2 989 cases reported in 2024, involving approximately $91 million. The Police do not maintain any breakdown of arrested person by types of deception.

The Police have strengthened efforts to combat such scams from multiple angles, including requesting telecommunication service providers (TSPs) to block websites containing false WhatsApp advertisements by the end of 2023, and submitting requests to relevant search engines and overseas authorities to remove the fake websites. They also continue to promote anti-deception information through various channels to enhance public awareness of fraud prevention, and promoting the use of the Scameter and Scameter+. Among these measures, the Police urge the public to enable two-factor authentication; regularly review the devices linked to their accounts and log out of any unknown connected devices; not to blindly trust search engine results, and

instead bookmark frequently used websites; and avoid connecting to public Wi-Fi or logging into online accounts on public computers.

Following the Police's series of educational campaigns, the number of "online account hijacking" cases last year decreased by 13 per cent compared to 2023, and in the first four months of 2025, the figure further dropped by 63 per cent compared to the same period last year. The Police will continue to closely monitor deception trends, regularly review measures and strategies to combat fraud and strengthen protection for the public.

(3) Depending on the method used, fraud cases involving identity theft can be classified as phishing scams, online investment frauds, or even online romance scams. The Police do not maintain breakdown of fraud cases involving identity theft.

In response to scammers sending text messages by impersonating as government departments, official institutions, and banks, the Office of the Communications Authority (OFCA) launched the SMS Sender Registration Scheme (the Scheme) on December 28, 2023, and fully opened it to all industries to join in February 2024. As at end May 2025, over 540 public and private organisations (including the Immigration Department, the Department of Health, the Police, the Consumer Council, major banks and TSPs) have participated in the Scheme. Under the Scheme, only those companies or organisations qualified as Registered Senders are able to send SMS messages using their Registered SMS Sender IDs with the prefix "#". TSPs will block fraudulent SMS messages sent by non-Registered Senders via the Internet.

In February 2023, the Police launched the mobile application "Scameter+" 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. "Scameter+" has now been upgraded and is equipped with automatic detection functions. The Call Alert function and the Website Detection function 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.

Moreover, under the co-ordination of the OFCA, the Police and major TSPs have established a mechanism where 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. The OFCA does not maintain any record of the average time required for relevant actions by TSPs.

(4) The Government understands that members of the public are concerned about marketing calls. However, the nature of marketing calls is fundamentally different from scam calls. Marketing calls do not necessarily involve fraud or illegal activities, and hence, the two should not be conflated. Some businesses, particularly small and medium-sized enterprises, still rely on voice marketing calls for promotional activities and service follow-ups. Therefore, it is essential to strike a balance between regulating

marketing calls and maintaining normal business activities. In fact, other regions around the world also face similar challenges in managing marketing calls. Practical difficulties remain in operation and enforcement (for example, distinction between marketing calls from nuisance calls or scam calls, evidence collection, cross-border enforcement, etc). As such, the Government believes that regulation by legislation may not be the most effective approach for managing marketing calls.

To mitigate the possible nuisance caused by marketing calls to the public, the OFCA has enhanced the Industry Regulatory Scheme for Marketing Calls in 2024 to introduce industry-specific regulation to limit the number of calls made by telemarketers to the same telephone number within a specific time frame, as well as requiring telemarketers to provide their names and contact numbers upon recipients' requests, and to honour any unsubscribe requests from the called party. At present, 12 trade associations from seven industries (including finance, insurance, telecommunications, call centres, beauty, estate agencies and money lenders) have joined the scheme.

In addition, the OFCA has requested TSPs to provide their users with call-filtering services, and actively encourage the use of call-filtering apps by the public, while also promoting relevant information on their websites. The number of enquiries and complaints related to marketing calls received by the Government has drastically reduced from 2 060 cases in 2011 to 93 cases in the first five months of 2025, reflecting the effectiveness of the above measures.

On combating fraudulent calls, the OFCA will continue to collaborate with the telecommunications industry and the Police to mitigate the risk of phone deception on various fronts, including requiring TSPs to block/suspend suspected fraudulent phone numbers and websites, 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 prepaid SIM cards, so as to assist the public in guarding against suspicious calls and messages.