

LCQ9: Prevention of telephone fraud

Following is a question by the Hon Sunny Tan and a written reply by the Secretary for Commerce and Economic Development, Mr Algernon Yau, in the Legislative Council today (April 10):

Question:

It has been reported that in the first nine months of last year, the Hong Kong Police Force received a total of over 23 000 cases involving telephone and online fraud, and the situation was getting more rampant. Regarding the prevention of telephone fraud, will the Government inform this Council:

(1) whether it will explore the feasibility of introducing a "whitelisting" registration mechanism for caller identity so that members of the public can identify calls from whitelisted agencies or organisations, such as telecommunications service providers, banks, government departments and commercial organisations, in order to reduce their fraud risks;

(2) how it will take the initiative to combat fraud by enhancing cross-bureau, cross-government department and cross-sector coordination and cooperation, such as working together with government departments or quasi-government organisations related to innovation and technology to review, study and develop platforms (such as mobile applications) for implementation of call whitelisting; and

(3) as it is learnt that many fraudsters would make frequent and random phishing calls to different telephone numbers by cold calling in search of victims, whether the Government will consider proactively following up unusual behaviour of suspicious users who make frequent phone calls by strengthening cooperation with the telecommunications industry and drawing reference from the "Know Your Customer" authentication process adopted by the banking industry, so as to prevent crimes relating to fraudsters making frequent phone calls in search of victims?

Reply:

President,

In view of the trend of phone deception, the Government has been taking a multi-pronged approach to combat phone deception vigorously. In response to the Member's question, in consultation with the Office of the Communications Authority (OFCA), the Security Bureau, the Hong Kong Police Force (HKPF), the Office of the Government Chief Information Officer, our reply is as follows:

(1) and (2) The Government understands that members of the public are very concerned about unsolicited calls and recognises the need to protect them from scams and nuisances. Various government departments have also launched

different measures to help members of the public distinguish legitimate calls, including:

(i) OFCA has established a mechanism to provide designated telephone numbers to government departments or public organisations in need for their communications with the public. Examples of such include the Hong Kong Special Administrative Region's one-stop service hotline 1823 or the HKPF's Anti-Deception Coordination Centre hotline 18222. OFCA will continue to encourage government departments and public organisations to apply for telephone numbers with designated prefixes when making calls to the public to assist members of the public to recognise calls from government departments and public organisations;

(ii) OFCA will further expand the SMS Sender Registration Scheme (the Scheme) to government departments, public organisations, and statutory bodies that need to communicate with the public via text messages. Under the Scheme, all participating companies or organisations will use Registered SMS Sender IDs with the prefix "#" when they send SMS messages to local subscribers of mobile services, so as to further help members of the public verify the identities of SMS senders and raise their anti-deception awareness, guarding against telephone and SMS fraud. As of end February this year, major telecommunications service providers, banks, and 11 government departments or statutory bodies (such as the Immigration Department, the Department of Health, the HKPF, the Hong Kong Customs and Excise Department, the Transport Department, the Consumer Council, the Mandatory Provident Fund Schemes Authority, etc.) with needs to communicate with the public via SMS messages have participated in the Scheme. OFCA will continue to actively invite more government departments, public organisations, and statutory bodies as well as the Legislative Council which use text messaging to communicate with the public to participate in the Scheme;

(iii) In response to OFCA's active appeal, major telecommunications service providers have been providing their users with call-filtering services. Among which, such services provided by individual service providers are free, including providing complimentary call management services for elderly customers to encourage their use of these services and mitigate the problems caused by suspicious and nuisance calls. Additionally, there are currently many call-filtering apps available for use by members of the public and these apps have been widely used by the public. OFCA has coordinated the information of various call-filtering apps available in the market currently and uploaded to its thematic website to encourage members of the public to download. These call-filtering apps can help screen scam calls and telemarketing calls, as well as identify calls from government departments, public organisations and statutory bodies in general. OFCA has also been visiting various districts and working with Legislative Council Members as well as District Councillors since the end of last year to appeal to members of the public to beware of phone scams and assist them to download relevant call-filtering apps;

(iv) The HKPF has added an automated function in February this year to identify fraudulent calls in the mobile application of "Scameter+" which will

automatically compare the calls received by users and visited websites with the latest fraudulent database. When potential fraud or network safety risk is detected, a warning alert will be issued to users for early detection and prevention of fraud. Users can also report suspicious phone calls or websites through the public reporting platform of the application to ensure the relevant database remains updated and accurate. The Government will continue to strengthen public promotion of "Scameter+" to encourage members of the public for downloading, such as through access and promotion for downloading "Scameter+" through various websites and mobile applications of various government departments. As of end February this year, the search engine has recorded over 2.5 million searches and issued over 430 000 alerts on fraud and cyber security risks. The number of downloads of "Scameter+" has also increased from 228 000 at end January this year to 315 000 as at March 21; and

(v) To further manage person-to-person telemarketing calls, OFCA has proactively invited relevant industries to collaborate and implement industry self-regulation. There are currently four industries, namely finance, insurance, telecommunications, and call centres, participating in establishing the Benchmark Code of Practice on Person-to-Person Marketing Calls (the Code of Practice) to regulate the manner in which industry professionals make person-to-person telemarketing calls. OFCA is actively contacting and coordinating with the relevant industries to strengthen and update their Code of Practice. OFCA has also reached out and invited other industries to participate in the aforementioned self-regulation arrangements. We aim to collaborate with different industries to establish the Code of Practice as soon as possible, with a view to enhancing the self-regulation arrangements.

As regards the suggestion of implementing the "whitelist of incoming calls" to identify legitimate incoming calls, considering that this may involve hundreds of thousands of telephone numbers used by government department and public organisations as well as the number of users being affected, and that the nature and requirements of their telephone communications services with the public may vary, if a "whitelist of incoming calls" is to be implemented, the time needed for preparation and transition by individual departments and organisations may differ. This includes making large-scale changes to their current telephone systems, hotline/office telephone numbers, and it will take time to inform each user about the updated telephone numbers, etc. We anticipate that the related processes and the transitional period will take time to complete, which may cause confusion and inconvenience to the public in between. Moreover, current communication technologies may not entirely prevent the possibility of calls on the "whitelist" being spoofed. Having considered the above factors, we need to carefully and thoroughly study whether the related proposal is effective and worth implementing.

(3) Regarding the proposals mentioned in the question about "customer authentication" and "proactively following up on suspicious users", the Government has fully implemented the Real-name Registration Programme for SIM Cards (RNR Programme) in February 2023, requiring that all SIM cards issued

and used locally (including SIM service plans (SSP) and pre-paid SIM (PPS) cards) must complete real-name registration before service activation.

OFCA has been collaborating with telecommunications service providers to ensure the effective implementation of the RNR Programme, including to request telecommunications service providers to conduct regular sample checks and follow up on suspicious PPS cards, and to refer cases suspected of using false identity documents to the HKPF for follow-up actions, assisting the HKPF in combating phone deception. As of end February this year, telecommunications service providers have cancelled registration records of around 1.23 million non-compliant PPS cards in accordance with the registration requirements of the RNR Programme. Around 1.59 million PPS cards were rejected since the clients failed to provide information in compliance with the registration requirements.

In addition, OFCA has formulated the Code of Practice, requiring telecommunications service providers to monitor calls originated from their networks since last year. Once call patterns of suspected phone deception are identified (e.g. making a large number of fraudulent calls within a short period of time), the services of the relevant phone numbers will be suspended immediately. As of end February this year, about 520 000 local telephone numbers were thereby suspended. Furthermore, OFCA will also periodically revise the code to ensure that it can effectively block scam calls.

As regards other facilitative measures to combat telephone and SMS fraud, OFCA, the HKPF and the major telecommunications service providers have established a working group since September 2022 to implement a range of measures from telecommunications perspectives to combat telephone and SMS fraud. According to the advice of the working group, telecommunications service providers, based on the fraud records and information provided by the HKPF, proactively block or suspend services of the telephone numbers suspected to be involved in fraud cases, and block users from accessing suspicious fraud websites. As of end February this year, upon the HKPF's request, telecommunications service providers have successfully intercepted more than 8 100 website links involved in fraud cases and blocked or suspended more than 2 700 telephone numbers suspected to be involved in fraud cases.

In addition, the HKPF launched various anti-deception measures in collaboration with the Hong Kong Monetary Authority and the banking sector. Among others, the Faster Payment System (FPS) Suspicious Proxy ID Alert was rolled out in November 2023. Under the mechanism, FPS is linked to "Scameter" of the HKPF. During online fund transfer via FPS, the matching function of the database can identify payees whose information is related to scam reports. In such cases, an alert message will appear on the confirmation page of the transaction. As of end February this year, alerts covering high-risk transfers of over \$600 million were issued from the system.

According to the HKPF's information, since the introduction of the above-mentioned measures, the average number of telephone fraud cases in the fourth quarter of 2023 has dropped by 38.1 per cent when compared to the same

period in 2022, reflecting the positive effect of these measures in combating telephone fraud. OFCA will continue to step up collaboration with the HKPF and telecommunications service providers to conduct public education and publicity with a view to disseminating anti-deception messages to all members of the public in a comprehensive manner.

All in all, the most effective anti-deception means for members of the public is to remind themselves, their families and their friends to stay highly vigilant at all times. If members of the public receive calls from strangers, regardless of the displayed number, they should stay highly vigilant and should not disclose personal information or transfer money to unknown callers to avoid suffering from losses.