For discussion
on 14 July 2025

Legislative Council
Panel on Information Technology and Broadcasting

Latest Progress of Initiatives Taken for Combating Phone Deception and Proposed Enhancements to the Real-name Registration Programme for SIM Cards

PURPOSE

The Government has attached great importance to the effective operation of Hong Kong's communications system and is committed to combating fraudulent messages transmitted through telecommunications networks. This paper aims to brief Members on the latest progress of the Office of the Communications Authority (OFCA)'s measures to combat phone deception and proposals to enhance the effectiveness of the Real-name Registration Programme for SIM Cards (RNR Programme).

IMPLEMENTATION SITUTATION OF MEASURES TO COMBAT PHONE DECEPTION

2. OFCA has been assisting the Police in taking enforcement actions to combat phone deception from the perspective of telecommunications services. In this regard, OFCA, the Police and major telecommunications service providers (TSPs) jointly set up a working group in September 2022 to devise and implement a series of measures to combat deception at the source, with details set out as follows –

(a) Promptly blocking phone numbers and websites suspected to be fraudulent

3. Under the mechanism established by the Police and major TSPs, since September 2022, TSPs have, based on the fraud records provided by the Police, blocked the phone numbers and suspicious websites suspected to be fraudulent as soon as possible. As at end-May this year, over 50 000 websites and about 9 000 local and non-local phone

numbers have been successfully intercepted. In the first five months of this year, there has been a significant upward trend[1] in the number of fraudulent websites blocked compared to the same period last year. This increase might be attributed to heightened public awareness of reporting scams and the targeted enforcement actions taken by the Police. The number of local phone numbers with services being suspended has significantly decreased[2], indicating that fraudsters might be shifting to other means of deception, such as social media and fraudulent websites, etc.

(b) Suspending services of phone numbers with specific operational patterns

4. Investigations conducted by the Police in the past revealed that criminals often use communications networks or devices (such as modem pools, commonly known as "cat pools") to make or send a large number of calls or text messages within a short period of time for conducting phone scams. In this regard, the Communications Authority (CA) formulated the "Code of Practice on Management of Scam Calls and Scam SMS by Telecommunications Service Providers" in April 2023 and required TSPs to monitor calls and messages originating from their networks and systems. Once call patterns of suspected phone deception have been identified (e.g. making or sending a large number of calls or text messages within a short period of time), TSPs will suspend the services of the relevant phone numbers. As at end-May this year, about 1.43 million local phone numbers were thereby suspended. The number of local phone numbers with services suspended in the first five months of this year has recorded a significant decline[3] compared to the same period last year. Among the suspended numbers, only a very small number had services restored upon users' requests after further verification, showing the effectiveness of the measure.

---

1 The average number of fraudulent websites blocked per month has increased more than fivefold, from approximately 800 per month between January and May 2024 to around 5 100 per month during the same period this year.

2 The average number of suspended local phone numbers per month decreased by 48%, from approximately 270 per month between January and May 2024 to around 140 per month during the same period this year.

3 The average number of phone number suspected of being involved in fraudulent activities due to their operational patterns decreased by 81%, from approximately 62,000 per month between January and May 2024 to about 12,000 per month during the same period this year.

(c) Combating non-local deception calls

5. Noting that some overseas criminal syndicates have attempted to commit fraud against members of the public by using Hong Kong phone numbers, CA has requested TSPs to block suspicious calls starting with "+852" since February 2023, and send voice or text alerts to mobile service users for other incoming external calls prefixed with "+852" since May 2023 to alert call receivers. As at end-May this year, TSPs have blocked over 5.7 million suspicious calls and have sent over 30 million voice or text alerts. The number of voice or text message alerts sent per month and the number of suspicious overseas calls intercepted per month in the first five months of this year have both decreased compared to the same period last year[4], indicating that the above measures have been effective in containing the spread of such suspicious calls and scam messages.

(d) Combating fraudulent SMS messages involving identity impersonation

6. To combat SMS messages fraud, apart from that TSPs will suspend the services of phone numbers sending a large number of SMS messages as mentioned in paragraph 4 above, OFCA launched the SMS Sender Registration Scheme in December 2023. Under the Scheme, only those companies or organisations being Registered Senders are able to send SMS messages using their Registered SMS Sender IDs with the prefix "#" to further assist members of public in identifying the identity of SMS senders and enhance public awareness of fraud prevention. As at end-May this year, over 540 public and private organisations have participated in the Scheme. OFCA has made available the SMS Sender Registry on its website for checking of registered organisations by members of the public and will continue to encourage more organisations to participate in the Scheme.

(e) Playing voice alert message for calls made from newly activated local pre-paid SIM (PPS) cards

7. Given that PPS cards are generally easier being exploited by criminals in conducting phone deception as compared to SIM Service Plan (SSP) cards, and the modus operandi of certain deception cases indicated

---

[4] The average number of voice or text message alerts sent per month decreased by 27%, from approximately 740 000 per month between January and May 2024 to around 540 000 per month during the same period this year. The average number of suspicious international calls intercepted per month dropped by 42%, from approximately 310 000 per month between January and May 2024 to around 180 000 per month during the same period this year.

that criminals would exhaust a large number of PPS cards within a short period of time and use new ones for carrying out deception, since December 2024, when local mobile and fixed services users answer calls made from newly activated local PPS cards, TSPs will first play a voice alert message stating, "This call is made from a new PPS card", before the call is connected, to raise public awareness of suspicious phone calls.

(f) Strengthening identification of suspicious calls by the public

8. In February 2023, the Police launched the mobile application "Scameter+" to assist the public in identifying suspicious online platform accounts, payment accounts, phone numbers, email addresses, and websites, as well as providing anti-fraud tips. As at end-May this year, "Scameter+" has recorded over 980 000 downloads, and the search engine has logged 8.8 million searches, issuing 1.04 million alerts to 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-May this year, "Scameter+" had issued over 850 000 warnings about suspicious calls and websites to the public through its automatic function.

9. In response to phone deception that impersonating government departments, OFCA has established a mechanism to provide designated phone numbers for government departments or public organisations in need of hotline numbers or communication with the public. Examples include the Government's one-stop service hotline 1823, the Police's Anti-Deception Coordination Centre hotline 18222, etc. to facilitate the public in identifying calls from government departments and public organisations. In addition, under OFCA's active appeal, several TSPs now offer free call filtering value-added services to all or some of their customers (e.g. customers aged 60 or above). Members of the public can make reference to OFCA's thematic website[5] to check the detailed terms and conditions of call filtering value-added services provided by individual TSPs. OFCA has also maintained regular liaison with developers of call management services and filtering applications to enhance public confidence in using call-filtering applications.

---

[5] https://www.ofca.gov.hk/tc/consumer_focus/guide/hot_topics/fraudulent_calls/index.html

RNR PROGRAMME

10. The RNR Programme was fully implemented on 24 February 2023, requiring that all SIM cards issued and used locally (including SSP and PPS cards) must complete real-name registration before service activation, to ensure the integrity of telecommunications services and the security of communications networks. OFCA, since the implementation of the RNR Programme, has been closely monitoring market developments to ensure the effective operation of the registration systems, and has launched various enhancement measures of the RNR Programme taking into account the operational experience. Since February 2023, TSPs have been required to conduct regular sampling checks on the registration information of registered PPS cards, step up checks on suspected cases and refer suspected illegal cases for the handling by the Police. 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-May this year, around 4.84 million PPS cards were rejected for registration as 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 3.46 million non-compliant PPS cards have been deregistered (including cases where users failed to verify their identities as required during TSPs' sampling checks and were suspected of using forged documents for registration, etc.).

11. To strengthen the effective implementation of the RNR Programme, since October last year, OFCA has required TSPs to adopt "iAM Smart" as the default registration method for Hong Kong identity (HKID) card holders. For PPS cards with registration made by non-HKID holders via the online registration platform, TSPs will first verify the identity document with their systems before activating relevant PPS cards, followed by manual checking to verify the authenticity of the identification documents of the registered users. If any PPS cards are found to be non-compliant with the regulatory requirements (e.g. suspected use of forged documents for registration), such registration will be cancelled.

PROPOSED ENHANCEMENT MEASURES

12. The RNR Programme has been implemented for almost two and a half years. Taking into account factors including the implementation of the RNR Programme in the past, development of the local telecommunications market, experiences of other economies and modus operandi of deception syndicates involving the use of PPS cards as well as deception trends provided by the Police, the Government plans to further enhance the RNR Programme to strengthen efforts in combating phone deception. The specific proposed measures include —

(a) Lowering the registration limit of PPS cards for individual users

13. Under the Telecommunications (Registration of SIM Cards) Regulation (Cap. 106AI) (the Regulation), each individual user (regardless of HKID holder or non-HKID holder) may register no more than 10 PPS cards with each TSP whereas each corporate user may register up to 25 PPS cards with each TSP. There is no limit on the registration quota for SSP cards[6]. As mentioned in paragraph 10 above, TSPs, in accordance with the requirements of OFCA, have been actively conducting regular checks on users whose numbers of registered PPS cards are approaching the statutory limit. Based on the past verification experiences of TSPs, only fewer than 5% of these users would complete the required verification requests of the TSPs. PPS cards would be deregistered if the users fail to comply with the verification requirements. The above information indicates that many users holding multiple PPS cards possibly register with identity documents that do not comply with existing regulatory requirements, or they may have improperly purchased PPS cards registered by others. To increase the effectiveness of preventing criminals from using PPS cards for carrying out fraudulent activities, we believe that there is room to lower the maximum registration limit of PPS cards for individual users.

14. According to the analysis on statistics collected from TSPs in March this year, PPS cards registered under the same HKID or non-HKID document (e.g. passports and other travel documents) with one to three PPS

---

[6] In the case of SSP cards, apart from completing the real name registration requirement, users are generally required by TSPs to provide other personal information (such as proof of residential address) for daily bill management and customer service purposes.

cards accounted for 90% of all registered PPS cards[7]. To reduce the misuse of PPS cards by criminals in carrying out illegal activities, particularly phone deception, we preliminarily propose to significantly lower the maximum registration limit for individual users from the existing limit of 10 PPS cards per TSP per person to a maximum limit of 3 PPS cards per TSP per person. This measure will help minimise the risks of PPS cards being abused while causing minimal impact on the majority of users. Considering the current situation of the telecommunications market in Hong Kong[8] and there is no registration limit for SSP cards, we believe that this proposal can reasonably meet the needs of individual users.

15. Apart from the aforementioned proposal to lower the registration limit of PPS cards, OFCA will continue to require TSPs to verify the registration information of users holding multiple PPS cards and to deregister PPS cards without timely provision of identity information. Furthermore, members of the public can still opt for SSP services which do not have a registration limit. As such, the proposed measure can strike a better balance between combating crimes and addressing the practical needs of users.

(b) Establishing new offences to combat improper use of registered SIM cards

16. According to the ongoing market surveillance conducted by OFCA, it has been found that some individuals are selling registered PPS cards or offering to provide their personal information for real-name registration in the market or through online social platforms. Such practices are inconsistent with the objectives of the RNR Programme and could possibly involve fraudulent activities. Currently, providing false information and/or false documents under the RNR Programme may constitute criminal offences. To strengthen efforts against fraudulent activities involving the use of PPS cards registered with others' information, we propose **establishing new offences to criminalise the improper use of SIM cards (regardless of SSP or PPS cards) registered**

---

[7] The number of one to three PPS cards registered with the same HKID was about 87%, while the number of one to three PPS cards registered with the same non-HKID document was about 86%.

[8] As at May this year, there are 29 licensed TSPs that can sell PPS cards in Hong Kong.

with others' information without lawful authority or reasonable excuse/justification. Specifically, we suggest making the following three types of activities illegal:

(i) Providing or soliciting the provision of personal information for the purpose of registering another person's SIM card;

(ii) Selling/buying, leasing/renting, lending/borrowing or supplying/acquiring registered SIM cards; and

(iii) Possessing SIM cards registered with others' information unless with reasonable cause / excuse, otherwise the possession of 10 or more SIM cards registered with others' information will be presumed to have the intent to use such SIM cards to commit a crime or facilitate the commission of a crime.

17. For the proposed new offences mentioned above, the Government preliminarily suggests adopting the current maximum penalty[9] under the Telecommunications Ordinance (Cap. 106) (TO), which is a Level 4 fine (HK$25,000) or imprisonment for 12 months, to provide sufficient deterrence. Regarding the enforcement of the new offences, the Police will be the primary enforcement agency. Under the proposed new arrangement, OFCA will continue to work closely with the Police to effectively combat illegal activities conducted through telecommunications networks.

18. The legislative intent of the Government is to combat crimes. Hence, the proposed legislative amendments in the future will specifically target the improper use of registered SIM cards. Members of the public, businesses or organisations that use or possess multiple SIM cards registered with others' information with reasonable justification or excuse[10] will not be affected by the proposed new offences.

---

[9] Pursuant to section 37(2) of the TO, regulations made under the section may specify certain contraventions as offences and provide for related penalties. However, any such penalties provided for shall not exceed the maximum penalty of a fine at level 4 and imprisonment for 12 months.

[10] For example, with proper authorisation and in compliance with the regulatory procedures, a minor or an elderly person may register a SIM card through his/her family members; an enterprise or an organisation may have multiple registered SIM cards for use by its staff to contact customers for business promotion purposes, etc.

19. The Government believes that criminalising the improper use of registered SIM cards, coupled with the reduced registration limit of PPS cards for individual users, can effectively combat fraudulent activities involving PPS cards, and thereby better protecting telecommunications service users from potential harm. Lowering the registration limit of PPS cards for individual users and introducing new offences to combat the improper use of registered SIM cards would involve amendments to the existing Regulation under the TO. We will prepare the legislative amendments for the proposals, with an aim to introducing the amendments into the Legislative Council (LegCo) for scrutiny in 2026.

ENHANCEMENT IN PUBLIC EDUCATION

20. To further promote anti-phone deception messages, OFCA has continuously encouraged the public to use call management services and filtering applications through various publicity and educational activities, as well as has helped members of the public in need to download and use relevant call filtering applications during various publicity activities. Over the past two years, OFCA has organised a total of 182 public education and promotional events, including 37 roving exhibitions, 75 community talks and 70 school touring performances, to disseminate related information to residents and students in various districts. In addition, to promote anti-phone deception messages in the community, OFCA launched the District Anti-Phone Deception Ambassador Scheme in January this year. The Scheme has garnered support from over 150 District Council members' ward offices across all 18 districts in Hong Kong, with more than 300 District Council members and their staff appointed as District Anti-Phone Deception Ambassadors. Since May this year, OFCA has collaborated with these Ambassadors to carry out a series of roadshow events in all 18 districts and will continue to organise various types of activities to strengthen public education and promotion.

CONCLUSION AND ADVICE SOUGHT

21. The Police, between January and April this year, received a total of 1 816 phone scam cases, representing an increase of 379 cases

(26.4%) compared to the same period last year but a significant slowdown compared to last year's overall growth in cases (186.5%). In addition, the total monetary amount involved in scam cases decreased by HK$950 million as compared to the same period last year, representing a decline of 29.8%. Meanwhile, the Police successfully intercepted HK$430 million in 360 scam cases, making a 10% increase as compared to the same period last year (i.e. HK$390 million). All these have demonstrated the effectiveness of the Government's efforts in combating deception. To further strengthen preventive measures, apart from the proposed enhancements to the RNR Programme, OFCA will continue to monitor the implementation of anti-phone deception measures and introduce further enhanced measures when necessary.

22. The Government will continue to adopt a multi-pronged approach in combating phone deception to protect the interests of the public. Members are invited to note the content of the panel paper and provide comments. With reference to Members' views, the Government will proactively prepare amendments to the Regulation, with an aim to introducing the legislative amendment proposals into LegCo for scrutiny in 2026.

Commerce and Economic Development Bureau
Security Bureau
Office of the Communications Authority
Hong Kong Police Force
July 2025