Telecommunications Regulatory Affairs Advisory Committee

Measures to Combat Fraudulent Calls and Messages

PURPOSE

This paper updates Members on the various measures adopted by the Office of the Communications Authority ("OFCA") to combat fraudulent calls and messages.

BACKGROUND

2. In view of rising number of reported scam cases since 2022[1], OFCA in collaboration with the Police and the telecommunication industry have worked together and implemented a number of measures to raise the public awareness, block transmission or delivery of fraudulent calls and messages, and suspension of service due to fraudulent use, in order to protect the interests of consumers of telecommunications services.

3. According to the Police, there are three main modi operandi of fraudulent calls:

(a) "Detained Son": the fraudster would falsely claim that a relative or friend of the victim has been detained and demand a ransom for release of his/her relative or friend;

(b) "Guess Who": the fraudster would falsely claim to be a relative or friend of the victim, inducing him/her to believe in the alleged identity of the fraudster for further deception; and

(c) "Pretend Officials": the fraudster would play a voice recording

[1] According to the Police, between January and June 2022, there were 500 reported cases of scam calls involving callers impersonating Government officers. The monetary loss suffered by the victims amounted to about HK$ 387 million.

purporting to be from the staff of Government departments/authorities, logistics companies or other public or private organisations alleging that the victim or the service used by him/her has been involved in criminal cases, and getting his/her trust and personal information through deceit to commit further deception.

4. In order to lower down the alertness of the victim so as to gain his/her trust, a fraudster may make use of caller identity spoofing to change or falsify the caller identity, pretending that the call is made from a local phone number (e.g. using telephone number of a hotline centre prefixed with Hong Kong area code "852") and tricking the victim into believing that the call is made from a Government department or authority.

MEASURES TO COMBAT FRAUDULENT CALLS AND MESSAGES

5. With a view to safeguarding the integrity of telecommunications services and the security of communications networks, OFCA has been adopting a multi-pronged approach in collaboration with the Police to combat fraudulent calls.

Working Group on Tackling Fraudulent Calls and Messages by the Telecommunications Industry

6. In September 2022, OFCA set up a Working Group on Tackling Fraudulent Calls and Messages by the Telecommunications Industry ("Working Group") with participation from the Police and telecommunications operators to explore, identify and implement various measures and initiatives to combat fraudulent calls and messages conveyed via telecommunications networks.

7. Through the concerted effort of all members of the Working Group, a number of new measures have been introduced since the fourth quarter 2022 by the telecommunications industry, including (a) sending voice or text alerts for incoming "+852" calls, (b) blocking transmission or delivery of calls bearing suspicious or spoofed calling line identification ("CLI"), and (c) blocking access to suspicious websites and suspension of telecommunications services of local

phone numbers suspected to be involved in scam cases based on information provided by the Police.

8. According to the information of the Security Bureau, the number of cases of telephone deception in the first quarter of 2023 decreased by 48% compared with that of the fourth quarter of 2022.

Sending Voice or Text Alerts for Incoming "+852" Calls

9. To alert the public on suspicious calls originating from outside Hong Kong, mobile network operators are sending voice or text alerts for incoming calls with caller number prefixed with "+852" to alert mobile services users that these calls are from outside Hong Kong. The alert arrangement has been fully implemented by all mobile service providers starting from 1 May 2023.

10. The alert message contains the standardised wording that "Call is from outside Hong Kong. Beware of deception".[2] The voice alert is read out in the order of Cantonese, Putonghua and English, while the text alert is provided in both English and Chinese. The alert service is provided free of charge by mobile service providers. Users are not required to pre-register, install any mobile apps or make any changes to their phone settings.

11. To raise public awareness of the introduction of the voice or text alerts for "+852" calls by mobile service providers, OFCA launched a new set of television and radio announcements[3] in the public interest to publicise the measure.

Blocking Transmission or Delivery of Calls Bearing Suspicious or Spoofed CLI

12. OFCA amended the *Code of Practice in relation to Calling Line Identification and Other Calling Line Identification Related Services* ("CoP for CLI") in February 2023 to require that telecommunications operators shall, to the extent technically feasible and practicable, take all reasonable and necessary

---

[2] The alert message in Chinese is 來電源自香港境外，慎防詐騙。

[3] https://www.ofca.gov.hk/en/consumer_focus/galley/video/index_id_98.html.

steps to identify and block transmission or delivery of calls bearing suspicious or spoofed CLI and ensure that only calls with valid CLI shall be transmitted across networks and delivered to the end users.

13. The amended CoP for CLI sets out requirements and call scenarios for telecommunications operators to block transmission or delivery of calls bearing suspicious or spoofed CLI to prevent fraudulent calls, including blocking incoming external calls containing CLI of "+852" as prefix and numbers/codes not conforming to the numbering plan of Hong Kong or 8-digit fixed numbers.

14. By end March 2023, all telecommunications operators have implemented the relevant blocking arrangement in accordance with the CoP for CLI.

Blocking Access to Suspicious Websites and Suspension of Telecommunications Services of Local Phone Numbers Suspected to be Involved in Scam Cases

15. Under OFCA's coordination, the Police and telecommunications operators have established a liaison protocol for implementation of blocking access to suspicious websites and suspension of telecommunications services of local phone numbers suspected to be involved in scam cases based on deception records and information provided by the Police.

Code of Practice on Management of Scam Calls by Mobile Service Providers

16. From network management perspectives, calls generated in high volume from telephone numbers / codes within a short period of time have a high risk of engaging in scam activities and will affect normal operation of telecommunications networks and systems. The CA has, after consulting the telecommunications industry in the first quarter of 2023, issued the *Code of Practice on Management of Scam Calls by Mobile Service Providers* ("Scam CoP") on 21 April 2023 for compliance by all mobile service providers[4].

[4] The Scam Cop (public version) is available at – https://www.coms-auth.hk/filemanager/statement/en/upload/620/cop202304.pdf.

17. The Scam CoP aims at providing practical guidance to mobile service providers in managing suspected scam calls made from local mobile networks and systems as well as ensuring the efficient and reliable operation of mobile networks and systems. The Scam CoP sets out (a) the responsibilities of mobile service providers for identifying scam calls, suspending telecommunications service / function of local telephone numbers / codes generating such scam calls, resuming suspended telecommunications service/function, as well as record keeping and reporting; and (b) the characteristics of call patterns on mobile networks and systems deemed to have generated scam calls. The Scam CoP has taken effect since 30 June 2023.

Registration Scheme for SMS Senders

18. OFCA, together with the Police, mobile service providers as well as the banking sector and its regulator, set up a Technical Working Group to Combat Spoofing SMS ("TWG") in November 2022 to formulate a registration scheme for SMS sender addresses to help the public ascertain the authenticity of the SMS sender's address.

19. With inputs from members of the TWG, OFCA prepared a draft *Code of Practice on Transmission and Delivery of Short and Multimedia Messages from Registered Sender* ("SMS CoP") and consulted the relevant stakeholders in June 2023. OFCA plans to finalise and promulgate the SMS CoP by end July 2023.

20. At present, OFCA is working with the Hong Kong Association of Banks to implement the Registry of Registered Senders and promulgate the list of Registered Sender IDs for the banking sector. Moreover, OFCA will also work with the mobile service providers to implement the registration process for the Registered SMS Service Providers and the necessary network system upgrade. The target is to launch a pilot run of the registration scheme for the banking sector by end of this year.

PUBLIC EDUCATION AND PUBLICITY

21. OFCA will continue to strengthen cooperation with the Police and the telecommunications industry 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.

WAY FORWARD

22. OFCA will continue to work with the Police and the telecommunications industry on the adoption of additional measures from telecommunications perspective to combat fraudulent calls and messages.

VIEWS SOUGHT

23. Members are invited to take note of the content of this paper. Any views and comments from Members are welcome.

Office of the Communications Authority
July 2023