Expansion of Suspicious Account Alert for internet banking and physical branches transactions

The following is issued on behalf of the Hong Kong Monetary Authority:

The Hong Kong Monetary Authority (HKMA), in collaboration with the Hong Kong Police Force (the Police) and the Hong Kong Association of Banks (HKAB), announces today (August 1) that 32 banks and 10 stored value facility (SVF) operators (see Annex for the list of participating institutions) will, starting from August 4, 2024, extend the coverage of the Suspicious Account Alert for internet banking and physical branches transactions, for providing enhanced protection to customers against rising fraud risks.

The HKMA has been working closely with the Police and the banking industry to introduce various anti-fraud initiatives. Among them, the Suspicious Account Alert, launched in November 2023, warns customers of "High Risk" of fraud based on information of the Police's Scameter, a scam and pitfall search engine, initially covering fund transfers using Faster Payment System (FPS) proxy IDs (including mobile phone number, email address, FPS Identifier (FPS ID)). As of end-June, 2024, over 655 000 alerts were issued, with an average of 3 000 alerts per day.

To further enhance the protection against fraud risks, the alert mechanism will extend to cover retail customers' fund transfers at bank counters, and online fund transfers within the same bank or inter-bank/SVFs, using account numbers of the payees. Customers will receive an alert message indicating high fraud risk if the payee's account number, mobile phone number, email address or FPS Identifier are labelled as "High Risk" in Scameter, regardless of whether the transfer is conducted at branch or through online channels. Participating SVFs will implement similar alert mechanism and provide relevant details to their respective customers.

Two other new initiatives are also introduced to further enhance protection for bank customers. First, "Scameter+" mobile application will now provide more timely alerts of fraudulent bank websites or phone numbers. In addition, to provide a more secure authentication method for customers using mobile banking apps in the light of evolving malware threats, the authentication of online credit card transactions has to be conducted via banks' mobile banking applications instead of SMS one-time passwords.

The HKMA reminds the public to carefully verify the payment details and the payee's identity before proceeding with a transaction. If in doubt, the public should refrain from making payments to avoid potential loss. In view of the rising threat of digital frauds such as malware scams, the public is advised to:

1. fact-check by referring to the HKMA's registers of authorised institutions and SVF licensees, the Police's anti-fraud resources including "Scameter+" mobile application and Anti-Scam Helpline 18222;
2. download or upgrade mobile applications only from official app stores or websites;
3. beware of fraudulent links; and
4. always protect personal information.

The HKMA will continue to work closely with the Police and the industry to raise public awareness and combat digital frauds.