HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/29C

10 October 2024

The Chief Executive
All Authorized Institutions issuing payment cards

Dear Sir/Madam,

Enhancement measures for online payment card transactions

I am writing to provide further guidance for authorized institutions (AIs) to implement enhanced anti-fraud/scam measures to strengthen the security of online payment card transactions, following the announcement of this initiative in August alongside the launch of Suspicious Account Alerts for internet banking and physical branch transactions[1]. Feedback and suggestions from the subsequent industry engagements have also been incorporated.

Retail banks introduced an anti-malware measure in February 2024 in view of intelligence shared by law enforcement agencies, the Hong Kong Monetary Authority (HKMA) and overseas regulators. This measure entails restricting customers' access to their mobile banking applications (Apps) if suspicious apps are detected on their devices. Since the implementation of this measure, no new cases have been reported by AIs regarding malware manipulating mobile banking Apps, as compared to more than 30 reported cases in 2023.

/…page 2

[1] HKMA press release: Expansion of Suspicious Account Alert for internet banking and physical branches transactions (https://www.hkma.gov.hk/eng/news-and-media/press-releases/2024/08/20240801-5/)

Recently, the HKMA observed new tactics of malware scam cases, where fraudsters tricked customers into installing a malicious mobile App and disclosing their credit card details and SMS One-Time Passwords (OTPs). In some cases, the SMS OTPs were intercepted by the malicious App. The fraudsters then conducted unauthorized transactions using the phished credentials. These incidents highlight the need for enhanced security measures to protect customers from evolving fraud schemes.

In this connection, the HKMA has collaborated with the Hong Kong Association of Banks and the Police in developing enhanced measures to reduce the risk of SMS OTPs being phished or intercepted by malware. Card-issuing AIs should, working with card scheme operators, ask customers with mobile banking Apps to authenticate online payment card transactions via a bound device by default, instead of using SMS OTPs, provided that the arrangement is compatible with the relevant authentication protocol (e.g. 3D Secure is adopted by merchants). Any change to such default authentication method should be regarded as a high-risk transaction and SMS OTP should not be used to authenticate the change[2].

If customers with mobile banking Apps encounter difficulties in authenticating payment card transactions using a bound device, AIs should consider the circumstances of each case and take appropriate follow-up actions. This may include providing suitable arrangements for vulnerable customers who may lack sufficient knowledge about mobile banking Apps, or for dormant users of mobile banking Apps.

While customers without mobile banking Apps may continue to use SMS OTPs for authentication of online payment card transactions, considerations should be given to incentivise customers to install and use mobile banking Apps as appropriate and with proper education and awareness initiatives. In addition, AIs should tighten their fraud monitoring for online payment card transactions authenticated via SMS OTPs.

/ … page 3

[2] In such cases, AIs should use other means than SMS OTP for authentication, for example, biometric authentication measures, or identity verification at a physical branch.

AIs should regularly review and assess the effectiveness of their authentication processes and related controls, making reference to applicable Supervisory Policy Manual modules, circulars and guidelines issued by the HKMA from time to time, including this circular. The above enhanced measures should be implemented as soon as practicable, and no later than 31 December 2024. To date, a few AIs have already rolled out the enhanced measures. Meanwhile, individual AI with genuine difficulties in meeting the requirements and/or timeline is welcome to discuss its alternative proposals and mitigation measures with us.

The HKMA will continue to work closely together with the industry and relevant stakeholders in staying alert to the latest modus operandi of fraud/scam, keeping the control measures up-to-date and relevant, as well as promoting public awareness and customer empowerment against fraud/scam. Should you have any questions regarding this circular, please feel free to contact us at ebanking@hkma.iclnet.hk.

Yours faithfully,

Carmen Chu
Executive Director (Banking Supervision)