HONG KONG MONETARY AUTHORITY
香港金融管理局

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

23 September 2022

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Payment card security

I am writing to share with authorized institutions (AIs) the HKMA's supervisory expectations with respect to payment card security.

There has been a growing number of data breaches involving payment cards over the past years around the world. In the light of this development, the Retail Payment Oversight Division of the HKMA has provided additional guidance (the Guidance) to the system operators and settlement institutions of retail payment systems (Card Scheme Operators) designated under the Payment Systems and Stored Value Facilities Ordinance (PSSVFO). The Guidance requires the relevant Card Scheme Operators to put in place a robust data security framework covering their participants and third-party service agents used by these participants, with a view to minimising the risk of data breaches, and when such breaches do occur, reducing the resulting damages.

Card Scheme Operators are expected to incorporate the requirements of the guidance into their rules and procedures. The updated rules and procedures should require the scheme participants (including AIs operating as card issuers or merchant acquirers) to:

(i) apply specified baseline technical and operational standards designed to protect payment data and payment card credentials within their operations;

(ii) subject the third-party service agents used by them to specified data security standards as promulgated by the Card Scheme Operators, and periodically monitor and validate compliance with the specified standards by these service agents; and

(iii) timely report actual or suspected data breaches and cyberattacks, including those occurring to their service agents, to the Card Scheme Operators, the HKMA, and other relevant regulators, where appropriate.

AIs play important roles in the payment card networks as card issuers and merchant acquirers. The HKMA expects AIs which are participants in payment card networks to take active steps to comply with the updated rules and standards of the Card Scheme Operators. The key areas deserving management attention are:

(a) **Conducting proper due diligence on service agents before engagement**: Prior to engaging a third-party service agent, AIs should conduct proper due diligence to ensure that the service agent has implemented necessary controls to protect payment card data, in a manner consistent with the security standards specified by the Card Scheme Operators. These controls may include, for example, strong encryption, restriction of logical and physical access, system and network security, and security monitoring and testing. The service agents to be covered should include, among others, payment gateways and point-of-sale service providers in relation to merchant acquiring; and 3-D Secure service providers in relation to card issuing. The requirements to be observed by the service agents should be duly reflected in the contracts between the AIs and the service agents.

(b) **Undertaking ongoing monitoring and reporting incidents promptly**: AIs should take steps to validate the ongoing compliance with the relevant data security standards by their service agents. This may be achieved through conducting regular assessments and reviewing validation reports on third-party service agents required under the updated rules of the Card Scheme Operators. Instances of major non-compliance by the service agents should be brought to the attention of the Card Scheme Operators so that suitable follow-up actions can be taken. Additionally, AIs which issue payment cards should have procedures in place to detect potential data breaches affecting their cardholders, for example through transaction monitoring and regular surveillance of the dark web. In cases where a data breach (or a suspected data breach) is identified, AIs should promptly report to the Card Scheme Operator, the HKMA, and other relevant regulators as appropriate, following the rules of the Card Scheme Operator. They should also take proactive steps to protect the interests of the affected cardholders, for example by issuing replacement cards to them, and keep them informed of the incident where appropriate.

(c) **Supporting Card Scheme Operators to perform their roles**: There may be cases where a service provider which handles a significant volume of payment card data does not maintain any direct relationship with AIs (e.g. a data service provider engaged by a large number of merchants). Given the important roles played by AIs in the payment card networks, they are expected to report data breaches or other anomalies involving these service providers detected by them in their ordinary course of surveillance to the Card Scheme Operators, and the HKMA where appropriate. This would be in the AIs' own interests and would be important to protect the overall security of the payment card networks.

The HKMA will consider undertaking a round of thematic examinations to ensure compliance with the above supervisory expectations by AIs. Going forward, the HKMA will continue to work with the banking sector and Card Scheme Operators to explore ways, including those involving the use of new technologies, to further strengthen payment card security. An example being considered is the tokenisation of payment card data. AIs will be consulted and their support will be sought as and when appropriate.

Should you have any questions regarding this circular, please feel free to contact Ms Connie Tse on 2597 0617 or Mr Terence Chan on 2878 1439.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)