HONG KONG MONETARY AUTHORITY
香港金融管理局

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

4 April 2022

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Sound practices for customer data protection

I am writing to share with the industry some sound practices with respect to customer data protection observed from a recent round of thematic examinations undertaken by the Hong Kong Monetary Authority (HKMA). The examinations form part of the HKMA's supervisory response to the elevated risk of data breach amid a growingly challenging cyber landscape. The objective of the examinations was to assess the adequacy and effectiveness of authorized institutions' (AIs') customer data protection controls.

As stated in the relevant Supervisory Policy Manual modules and other supervisory documents, including "TM-E-1 Risk Management of E-banking" and "Cyber Resilience Assessment Framework (C-RAF) 2.0", AIs are expected to put in place effective measures to prevent and detect the loss or leakage of customer data throughout the data lifecycle, including classification, access, storage and transmission.

The thematic examinations revealed that the AIs examined generally have put in place effective control measures to protect their customer data. For areas that required improvement, the AIs concerned have subsequently taken appropriate remedial actions to strengthen their controls. In the course of the examinations, the HKMA has observed some sound practices for customer data protection. They are grouped into four areas and summarised below for reference:

- *Data governance* – AIs are expected to put in place proper governance frameworks encompassing risk management process and data security strategy over customer data protection. To this end, some AIs have developed a customer data governance framework to i) define the roles and responsibilities of data owners and the three lines of defence; and ii) evaluate the adequacy and effectiveness of the AIs' control practices for customer data protection. The board and senior management oversee the development of the AI's data protection strategy and endorse the relevant customer data governance framework.

- *Customer data inventory management* – AIs should identify and document the locations of their customer data residing in different parts of AIs' networks, systems and premises. A comprehensive customer data inventory provides visibility of the customer data in custody and enables AIs to better manage the risk of data loss or leakage. Some AIs have developed clear policies and procedures for maintaining and updating an effective customer data inventory. The customer data inventory of these AIs is regularly reviewed to ensure completeness and accuracy.

- *Controls over transmission and storage of customer data* – AIs should adopt effective security measures to minimise the risk of data breach when handling customer data in transit, at rest and at end of life. Many AIs have developed effective data security policies to safeguard customer data against unauthorized access or transmission through various channels, including portable storage media. Data loss prevention (DLP) measures are implemented for internal and external communications. The more advanced AIs regularly test the effectiveness of customer data protection controls to ensure they address the changing business environments.

- *Physical and logical security controls of customer data* – AIs should implement proper physical and logical security controls to prevent customer data from unauthorized access or theft. Many AIs have put in place security controls and multi-factor authentication for premises and systems where massive customer data are processed or stored.

Details of the above sound practices are set out in the **Annex**. AIs are expected to regularly assess whether their existing data security controls remain adequate amid rapid developments in the cyber landscape.

Should you have any questions regarding this circular, please feel free to contact Ms Connie Tse on 2597 0617 or Mr Kevin Yau on 2878 1044.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)

Encl.