**Annex**

## Details of Major Enhancements on Protection of Payment Card Customers

### A. Empowerment

1. **Management of card-not-present (CNP) transactions** – To allow cardholders to minimise the risk of unauthorised CNP transactions (for example online purchases), banks should allow cardholders to enable or disable CNP transactions (except for recurring payments) as well as setting a limit on CNP transactions (within the overall credit limits) for their cards. Banks should provide convenient channels, for example hotline and Internet banking platforms[1], for cardholders to manage CNP transactions.

2. **Suspension and reactivation of cards** – While currently cardholders can request suspension of cards through bank hotlines or other channels, banks should also allow cardholders to instantly suspend their cards through Internet banking platforms, if they are not already doing so. Banks should also remind the cardholders to report any unauthorised transactions to the banks through hotline or Internet banking platforms when the cardholders proceed to suspend their cards. In addition, banks should enable cardholders to reactivate their cards through Internet banking platforms with proper authentication and verification by the banks.

3. **Management of credit limits** – To allow cardholders to have more control over their card borrowing, banks should:

   a. explicitly inform and agree with cardholders on the credit limits of newly approved cards. The banks should also on the same occasion clearly indicate to the cardholders the means to reduce the credit limits;

   b. where banks offer increases to the credit limits of existing cards, obtain explicit agreement of the cardholders before the increases become effective; and

   c. provide convenient channels, for example hotline and Internet banking platforms, for cardholders to reduce credit limits of newly approved and existing cards, and effect the reduction as soon as practicable.

   The above requirements also apply to spending limits of debit cards.

4. **Management of over-the-limit facilities** – Banks should obtain explicit agreement of cardholders for over-the-limit facilities of cards. (For details of the requirements, please refer to the HKMA Circular "Principles for Handling of Unauthorised Payment Card Transactions" issued on 25 April 2023.)

[1] Internet banking platforms refer to banks' platforms which deliver financial services over the Internet to customers' devices, including personal computers and mobile devices.

5. **Reporting unauthorised transactions** – While banks are already receiving reports of unauthorised transactions from cardholders through bank hotlines or other channels, banks should also allow cardholders to report unauthorised transactions through Internet banking platforms, if they are not already doing so. Banks should in general ensure sufficient resources for the operation of their hotlines to avoid undue delay in reporting by cardholders.

## B. Support, Communication and Education

*Support*

6. **Specialised handling team** – While cardholders reporting unauthorised transactions are generally received by bank hotline staff, banks should set up specialised teams to be responsible for the subsequent handling of such reports and cardholder communications. The specialised teams should get in contact with the cardholders within seven business days from the date of the reporting of the unauthorised transactions. In addition, the specialised teams should:

    a. have proper training to ensure the cardholders are handled in a proper manner, for example, adopting an uninquisitive manner when collecting information from the cardholders;

    b. be properly equipped to have ready information on the status of the cardholders and their transactions throughout the process and provide information and advice that are specific to the cardholders' circumstances;

    c. ensure appropriate information and advice are clearly and properly provided to the cardholders; for example, how the reported unauthorised transactions will be handled and the related chargeback arrangement, and action(s) that the cardholders should take;

    d. clearly inform the cardholders of, and provide reasons upon request for, any information and documents that the banks collect from the cardholders; and

    e. properly handle and timely follow up the unauthorised transactions reports and provide updates to the cardholders.

7. **Mobile Point-of-Sale (POS) Terminals** – Banks should encourage their merchants to use mobile POS terminals when conducting card transactions with cardholders so that they can swipe/tap their cards in person, instead of having the cards being taken away from them for conducting the transactions.

8. **Monitoring of not-yet-posted transactions** – While there are limited actions that banks can take immediately on reported unauthorised transactions which are not yet submitted by the merchants for settlement (i.e. "not-yet-posted transactions"), banks should properly record and monitor

such transactions upon receipt of reports from the cardholders, and endeavour to take follow up actions when the transactions are posted.

*Communication*

9. **Notification for card-present transactions** – While banks are currently required to send timely notifications to cardholders for all CNP transactions (except for recurring payments or transactions with an amount within the threshold specified by the customers), they should also adopt a risk-based approach to notifying cardholders of suspicious card-present transactions via effective means (e.g. SMS or in-App notifications). In particular, for binding of cards to contactless mobile payment services, banks should provide timely notifications for the first three contactless mobile payment transactions after the cards are newly bound.

10. **Frontline communications** – Bank hotline staff who receive unauthorised transaction reports from cardholders should have clear and appropriate communication with the cardholders throughout the handling process. They should ensure that the cardholders have clear understanding of the situations and the actions to be taken. Among all, the following information and advice specific to the reported unauthorised transactions should be provided to the cardholders:

    a. information and explanation about the banks' dispute handling and follow-up/investigation processes, and the expected timeframe within which the specialised handling teams noted under Item 6 will get in contact with the cardholders;

    b. the cardholders' right to withhold repayment of the transactions concerned and the circumstances under which repayment, and interest and charges if any, may be required;

    c. advice on making reports on the unauthorised transactions to the Police as soon as possible, and whether the banks may require written statements made to the Police at any stage; and

    The banks should provide acknowledgements of the unauthorised transaction reports to the cardholders (in paper or electronic forms) within seven business days from the date of the reports.

11. **Clarity of transaction notifications** – In order to facilitate cardholders to effectively identify suspicious card transactions and promptly take necessary actions, in the pre- or post-transaction instantaneous communications provided to cardholders in relation to card transactions (for example, one-time-password (OTP), alert messages, post-transaction notifications, etc.), banks should include the transaction details (i.e. transaction type, partial information of the account, merchant name, transaction amount and transaction currency), as well as the following message:

    Chinese: "如懷疑電 <the bank's designated telephone number>" and

    English: "Any doubt call <the bank's designated telephone number>".

*Education*

Recognising cardholders' role to stay vigilant and take precautions against unauthorised transactions, it is important to enhance cardholders' awareness of the need and their ability to protect themselves against unauthorised transactions.

12. **Security advice to cardholders** – Banks should from time-to-time remind cardholders to safeguard their cards, card information and authentication factors and the potential liabilities for not duly doing so, and of the measures that they should take to guard against card frauds and scams.

13. ***Modus operandi* of frauds and scams** – Banks should provide cardholders with information on the latest large-scale *modus operandi* of card frauds and scams, and advice on precautionary measures and actions to take when fallen victims of unauthorised transactions.

14. **Industry education collaboration** – The industry should organise collaborative educational programmes on card security and prevention of unauthorised transactions to increase the public awareness.

(For details of the relevant requirements, please refer to the HKMA Circular "Principles for Handling of Unauthorised Payment Card Transactions" issued on 25 April 2023.)

## C. Unauthorised Transaction Handling and Security

*Unauthorised Transaction Handling*

15. **Treatment of customers** – When cardholders report unauthorised transactions, banks should adopt a pragmatic and sensitive approach throughout the handling and investigation process.

16. **Circumstances of unauthorised transactions** – Banks should consider all relevant circumstances of the reported unauthorised transactions and information available to the banks, with due regard that the circumstances of individual cases may differ.

17. **Liability for losses** – Banks should, in addition to the relevant provisions set out in the Code of Banking Practice, give due consideration to the role of the banks and the role of the cardholders in the reported unauthorised transactions.

18. **Industry common practices** – To facilitate effective handling of unauthorised transactions, some common practices have been developed for sharing among banks, and will be reviewed and kept up-to-date from time to time.

19. **Transparency of investigation and result** – Banks should ensure transparency of the handling/investigation process and provide customers with the results as soon as practicable. Where banks cannot provide the results within reasonable time in exceptional circumstances, banks should provide progress update to the cardholders. Where any losses arising from the reported unauthorised transactions are to be borne by the cardholders, banks should ensure the transparency of the process and clearly explain the underlying rationale and, where appropriate, relevant evidence to the cardholders.

20. **Appeal mechanism** – Banks should put in place a mechanism, with sufficient checks and balances, for cardholders to appeal against the amount of losses to be borne by the cardholders.

(For details of the relevant requirements above, please refer to the HKMA Circular "Principles for Handling of Unauthorised Payment Card Transactions" issued on 25 April 2023.)

*Security*

21. **Authentication factors** – Currently, if 3D Secure (3DS) is adopted by merchants for their online transactions, banks commonly require cardholders to authenticate the transactions via SMS OTP. While SMS OTP is considered a valid authentication factor, banks should offer an alternative authentication factor (e.g. soft token, biometric authentication) that is more robust against phishing or malware. Cardholders can choose the alternative factor if they prefer not to be authenticated via SMS OTP. For the avoidance of doubt, cardholders without mobile banking app should be allowed to continue to use SMS OTP.

22. **Utilisation of rich data from 3DS 2.0 for fraud monitoring** – If 3DS 2.0 is adopted by merchants, banks should utilise the rich data available via 3DS 2.0 (e.g. IP address, cardholders' phone number) to enhance their ability to monitor fraud trends and identify suspicious transactions.

23. **Intelligence sharing** – The industry should utilise existing platform(s) or develop a common platform for sharing card frauds and scams related intelligence and good fraud detection practices.

24. **Fraud detection tools** – Banks are encouraged to leverage on the fraud detection tools of card scheme operators or other relevant tools to enhance their fraud monitoring.

25. **Additional confirmation for suspicious transactions** – Banks should obtain additional confirmation from cardholders (e.g. via 2-way SMS and in-App confirmation) if suspicious card transactions are detected, even though cardholders may have entered an SMS OTP to proceed with the card transactions.

26. **Additional authentication of binding cards to contactless mobile payment** – Banks are required to conduct additional authentication (on top of the input of correct card data and the one-time password) to confirm that cardholders have indeed given the instructions to bind their cards with new contactless mobile payment services. (For details of the relevant requirements above, please refer to the HKMA Circular "Binding payment cards for contactless mobile payments" issued on 25 April 2023.)

27. **Promotion of tokenisation of card data** – Tokenisation replaces sensitive card data with a unique token, which can minimise the impact of data breaches. A dedicated joint taskforce, comprising representatives from HKMA, Hong Kong Police Force, banks, and card scheme operators, has been formed under the Hong Kong Association of Banks to discuss how to encourage the relevant stakeholders in the payment ecosystem to adopt tokenisation. In support of the taskforce, banks should strive to explore ways to promote the adoption of tokenisation of card data.

28. **Retrieval of card information via Internet banking platforms** – The HKMA encourages banks to consider not showing card data on physical cards, if applicable, and allow cardholders to retrieve card information via Internet platforms instead.

## D. Responsible Borrowing

29. **Implication of card repayment –** While banks are already required to provide proper disclosure of the interest rates, fees and charges, etc. to the applicants for credit cards and cardholders, in order to allow the customers to more fully appreciate the financial implications of different card repayment practices, banks should:

    a. include an illustrative table[2] in the Key Facts Statements of credit cards to provide customised information about the period of time and total cost for different repayment practices.

    b. ensure the illustrative table is provided in the card statements, and a card repayment calculator is provided in the Internet banking platforms where applicable.

30. **Reminder on utilisation of credit limit** – Where cardholders have opted for over-the-limit facilities for their cards, banks should on a best effort basis provide notifications to cardholders when their card spending approaches the credit limits (for example, at 80 to 95%) so as to remind the cardholders to consider taking any actions with respect to the potential of going over limit and the related fees and charges.

31. **Assistance to cardholders with potential persistent card borrowing** – To assist cardholders to prevent their card borrowings from developing into

[2] Banks should adopt the table depicted in Annex III of the Code of Banking Practice.

persistent debts, banks should issue reminders to cardholders whose repayment patterns (for example, making minimum payment for consecutive months) indicate that their card borrowings may potentially develop into longer term debts.

a. The reminders should (i) encourage the cardholders to increase the level of repayment to reduce the cost of borrowing and the time needed to repay the balances; and (ii) inform the cardholder that they may contact the banks to discuss their financial circumstances and the banks could assist them to see whether and how they could better manage their repayment without an adverse effect on their financial situations and credit record.

b. For cardholders whose repayment patterns show little improvement subsequently, banks should issue similar reminders to them and set out the possible options that can help the cardholders to reduce the cost of borrowing and potential financial burden.

c. Where cardholders with potential persistent card borrowing approach the banks for assistance, the banks should take reasonable steps to assist the cardholders to more manageably repay their card borrowings and in ways that would not adversely affect the cardholders' financial situation.

d. Banks should exercise caution in offering credit limit increase and cross-selling other lending products to cardholders with potential persistent card borrowing.

32. **Disclosure of cash advance transactions** – Commonly, interest imposed on cash advance transactions is calculated on a daily basis. The interest charge shown in the card statement of which a cash advance transaction is billed only covers the interest accrued up to the statement cut-off date, while the interest accrued after the statement cut-off date will be indicated in the next statement. In order to facilitate cardholders to take actions to minimise the interest charges, banks should provide in the fee schedules and card statements a generic remark to remind the cardholders that the interest charge may be accrued after the statement cut-off date, and the customer may contact the banks on how to fully settle the interest charge before the next statement date.

## E. Other

33. **Engagement of stakeholders** – The HKMA and the industry will continue to engage other relevant stakeholders (e.g. telecommunication companies) to explore the use of technology in enhancing protection of cardholders.