HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref: B1/15C

23 June 2021

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Complaints Watch

The Hong Kong Monetary Authority (HKMA) has today published the seventeenth issue of its Complaints Watch.

Complaints Watch is a periodic newsletter prepared by the HKMA to share with the banking industry information on complaints received by the HKMA. It highlights the latest complaint trends, emerging topical issues, and shares good practices that authorized institutions (AIs) may find helpful. It forms part of the HKMA's work to promote proper standards of conduct and prudent business practices among AIs.

A copy of the seventeenth issue of the Complaints Watch is enclosed for your perusal. You may wish to forward it to members of your institution who have responsibilities for the selling of retail and investment products, risk management, compliance and complaint handling for reference.

If there are any questions on the above, please contact Mr Gabriel Ho on 2878 7504 or Ms Yolly Lee on 2878 7549.

Yours faithfully,

Carmen Chu
Executive Director (Enforcement and AML)

Encl.

55th Floor, Two International Finance Centre,
8 Finance Street, Central, Hong Kong
Website: www.hkma.gov.hk

香港中環金融街8號國際金融中心2期55樓
網址： www.hkma.gov.hk

HONG KONG MONETARY AUTHORITY
香港金融管理局

Complaints Watch

Issue No. 17
23 June 2021

Complaints Watch is published by the Complaint Processing Centre (CPC) of the Hong Kong Monetary Authority (HKMA). It highlights the latest complaint trends, emerging topical issues, and areas that Authorized Institutions (AIs) may wish to place greater focus on. It forms part of the HKMA's work to promote proper standards of conduct and prudent business practices among AIs.

Complaint statistics

Mar to May 2021	General banking services	Conduct-related issues	Total
In progress as of 28 Feb 2021	437	196	633
Received during the period	678	92	770
Completed during the period	(585)	(128)	(713)
In progress as of 31 May 2021	530	160	690

The HKMA received 770 complaints against AIs between March and May 2021. The major types of complaints received were related to provision of banking services (132), credit card transactions (95), service quality (85), remittance services (73), fund transfers (63), and fees and charges (47).

Enhancing consumer protection against phishing scams

In this digital era, many consumers have already adapted to making purchases of goods and services online with payments commonly made through credit cards or other mobile channels. The COVID-19 pandemic has provided impetus to further the growth of online shopping. Such a change in consumer behavior has also presented opportunities for criminals to set up various scams in disguise to steal consumers' credit card information and one-time-passwords (OTPs) through phishing SMS messages/emails with embedded fraudulent hyperlinks for conducting "authorised" credit card transactions. The HKMA noted the surge in phishing SMS messages/emails leading to financial losses for the customers and/or banks concerned.

Based on the observations from handling complaints of this nature, for better protection of consumers' and their own interests, banks should take steps[1] to accord appropriate consumer protection and enhance control measures including but not limited to the following:

a) review current arrangements to ensure all OTP messages will provide sufficient transaction details (e.g. merchant name, transaction type, amount and currency) for customers to be able to spot anomalies and raise with banks for assistance if in doubt. Where SMS OTP messages are sent to customers for binding their credit cards with mobile payment services (e.g. Apple Pay), the information provided therein should be clear, specific, easy to understand and preferably bilingual. Reference should also be made to the relevant supervisory guidance issued by the HKMA.

1 The steps taken/to be taken should also apply to transactions made through debit cards that are issued under different Card Associations' networks (e.g. Visa, Mastercard, etc) where applicable.

b) handle each complaint in a fair, consistent and prompt manner. A pragmatic approach should be adopted when assessing whether the cardholders in phishing scams are wholly liable for the transactions concerned, taking into account the clarity and effectiveness of individual bank's SMS OTP messages and customer communications/notifications, as well as the circumstances of individual cases.

c) ensure proper handling and addressing of customers' enquiries about (i) why the card-issuing bank is unable to stop payment to a merchant once the cardholder enters the relevant OTP to authorise a transaction; (ii) whether the OTP authenticated credit card transactions under dispute are subject to the chargeback mechanism; and (iii) the obligations of customers, merchants and card-issuing banks on the transactions under dispute. In respect of (ii), banks should endeavour to assist the cardholders concerned and handle their requests with respect to the disputed transactions in a reasonable and pragmatic manner. Banks are also reminded to check the chargeback rules carefully and consult the relevant Card Associations in case of need before communicating with customers.

d) step up educational efforts and alerts to remind customers of the importance of protecting their credit card information as well as OTP, and to carefully read the transaction notifications issued by banks. In particular, banks should draw customers' attention to stay vigilant to unknown hyperlinks and check the contents (e.g. merchant name, transaction type, amount and currency) displayed in SMS messages are actually referring to the intended transactions before inputting the OTP as authorisation, and immediately contact the bank for

assistance on any enquiries.

Relatedly, the HKMA is in discussion with the industry on introducing additional safeguards against phishing scams, including for example customer call-back to confirm binding of new devices, deferred execution and the lowering of limits on third-party transfers after change of devices. Moreover, complementary to the industry efforts, from time to time the HKMA also delivers educational messages through social media channels such as Facebook and Instagram to enhance public awareness to phishing scams and provide smart tips to protect personal digital keys or passwords.

With more common use of online banking and mobile payment services, the HKMA will continue to work closely with the industry Associations to explore good practices to further strengthen consumer protection and promote collective efforts in preventing abuse of card and other banking services by fraudsters.

Protecting safety of customer transactions

Banks are entrusted by customers to safeguard their financial assets, especially for deposits, and to ensure proper handling of customer's payment instructions. Appropriate arrangement and effective execution of internal controls in bank premises are crucial to protect the interests of customers as well as banks in the event of disputes or complaints arising from the risk of fraud. This is particularly important when banks are dealing with deposit withdrawals and movement of funds in large amount, and where teller counters and the seating areas for (elderly) customers are far apart or located on different floors of the branch premises.

In a few recent complaint cases and reports received by the HKMA, it is found that the bank staff concerned had abused the trusts in them by customers and co-workers and their misconduct acts were perpetrated through excuses and plots to deceive unguarded co-workers and officers with relevant approval authority in order to circumvent the internal control processes of banks concerned.

In one complaint case, the bank staff concerned was found to have kept the customers' savings passbooks and pre-signed transaction forms. A number of unauthorised transactions were conducted through using these documents or forging customers' signatures. The bank staff had further misled the unguarded tellers that the customers were physically weak to queue for counter service on a different floor of the branch premises and therefore circumvented the internal control processes of the bank concerned. In another complaint case, a branch staff was found to have left his authorisation card unattended while his password was also disclosed to other colleagues

so that a deceitful staff in the same office had processed some disputed transactions without being noticed.

Further to the HKMA's follow-up enquiries, the banks concerned gave prompt assurance to the impacted customers that financial losses arising from the disputed transactions would be followed up as soon as practicable. Full investigation into the incidents had also been conducted to ensure all misconduct acts of the bank staff concerned were identified and that any suspected criminal activities (e.g. fraud, theft) were reported to law enforcement agencies for appropriate actions.

Banks should remain vigilant at all times to protect customers and themselves from falling victim to fraud or theft. Reference may be made to the following examples of good practices and internal monitoring measures:

a) reinforce clear segregation of duties and the maker-checker arrangements through regular training and briefings to staff, conducting surprise checks and on-site visits to branches to ensure effective implementation of internal control measures, strengthening whistleblowing mechanisms and early escalation, and enhancing staff rotation.

b) carefully verify a customer's presence, identity and authorisation by, for example, contacting the customer directly to confirm large-value transactions, change of contact details or alteration of account operation instructions.

c) introduce annual customer portfolio confirmation processes for elderly and vulnerable customers, and monitor significant reduction in account balances.

Banks are expected to conduct regular reviews of operation workflows to identify areas for improvement on internal control measures which commensurate with individual business scope and risks, drawing reference to good industry practices where appropriate, in order to accord adequate protection to customer assets.

Comments and feedback on *Complaints Watch* are welcome. Please email them to *bankcomplaints@hkma.gov.hk*.