



HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref: B1/15C

26 March 2021

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Complaints Watch

The Hong Kong Monetary Authority (HKMA) has today published the sixteenth 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 sixteenth 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.



Complaints Watch

Issue No. 16
26 March 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

Jun 2020 to Feb 2021	General banking services	Conduct-related issues	Total
In progress as of 31 May 2020	417	121	538
Received during the period	1,724	258	1,982
Completed during the period	(1,704)	(183)	(1,887)
In progress as of 28 Feb 2021	437	196	633

The HKMA received 1,982 complaints against AIs between June 2020 and February 2021. The major types of complaints received were related to provision of banking services (359), service quality (241), remittance services (212), credit card transactions (163), fees and charges (137), and fund transfers (126).

Access to consumer credit data

With the increasing popularity and convenience of digital devices and e-banking services, and given the need for social distancing under COVID-19 situation, more customer enquiries and complaints have been received by the HKMA in this connection. In this issue of Complaints Watch, we will share key observations from handling relevant cases, particularly with regard to customer protection measures.

In one complaint case, the potential customer was interested in a loan facility offered by an AI on its online platform and proceeded to fill in the electronic application form with personal particulars, but changed mind subsequently and did not complete the application process. He later found out an enquiry record at the credit reference agency and was concerned about any adverse impact on his credit scores.

We noted that the complainant had checked a box in the electronic application form, which was regarded by the AI as giving consent for it to make an enquiry with credit reference agency regardless of the completion or result of a loan application. With our follow-up, the AI concerned has arranged to enhance its online credit application workflow to state clearly the purpose for accessing consumer credit database and obtain customer consent for its access in respect of completed loan applications.

Drawing reference to the above, and in line with the guiding principles as set out in the Code of Banking Practice and the Treat Customers Fairly Charter, AIs should review their digital processes to ensure clear and prominent disclosure of the purpose for making enquiries with the credit reference database and to obtain consent for access from customers for completed credit applications.

Identity theft in making online credit card applications

Recently, the HKMA received complaints related to suspected identity theft or impersonation of customers to make online credit card applications. In these cases, complainants received requests from the AIs concerned to repay overdue credit card balances and it was then found out that the complainants' Hong Kong Identity Card copies had been used by fraudsters to apply for credit cards through AIs' online platforms. Other supporting information (including contact information and salary proof) submitted by the fraudsters was falsified. When these AIs approached the victims through their genuine contact details maintained at the credit reference database, such identity theft incidents were uncovered. And since the victims in these cases had not acted with gross negligence, they were not held liable for the credit card transactions.

The AIs concerned have enhanced their fraud prevention and financial crime risk mitigating measures, including corroboration of personal information provided online by customers with other independent sources such as the consumer credit database. Efforts were also made to explore the greater use of technology in identity authentication and matching when offering e-banking services.

AIs are reminded to stay alert and make reference to the experience as shared above, and consider appropriate control system enhancement. It is also important for AIs to sustain efforts in consumer education and to provide, from time to time, security tips (e.g. verify using other channels like telephone before providing sensitive personal or financial information to trusted websites/parties) as well as alerts reminding customers to safeguard personal data.

Replacement of life insurance policies

The HKMA noted from a number of complaints that some AIs did not adequately monitor life insurance policy replacement activities, and thus having negative impacts on customer interests.

In one complaint case, the AI concerned did not check an existing customer's transaction records to identify any life insurance policy held, surrendered or lapsed within the past 12 months but only relied on recollection and self-declaration by the customer of any outstanding life insurance policies. As a result, policy replacement was not identified and relevant implications have not been explained to the customers concerned.

It is noted that, on one occasion, while the customer surrendered an existing policy and purchased a new one on the same day, the frontline staff only handled the purchase transaction and asked another staff to process the policy surrender. This created a false impression of no policy replacement, hence no records were made and the potential implications were not explained to the customer. On another occasion, the frontline staff was found to have misrepresented the expiry of the existing policy while it would actually be due in a few years' time.

As revealed in these complaints, post-sale monitoring of transactions to track policy replacement was either lacking or ineffective, especially on cross-insurer policy replacement involving policies sold by the same AI.

AIs should constantly review and enhance system effectiveness to protect customers' interest. The HKMA's circular of "Life Insurance Policy Replacement" of October 2020 elaborates that AIs should take appropriate steps to check at the point of sale their internal records for the statuses of a customer's existing policy(ies) and explain to the customer any adverse consequences arising from policy replacement. AIs should also monitor life insurance transactions after point of sale to identify potential policy replacement and take appropriate follow-up actions.

In their staff training, AIs should seek to incorporate observations and examples as shared above, and also highlight the importance of conducting insurance business with honesty and integrity.

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