



HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref: B1/15C

28 June 2022

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Complaints Watch

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

Should you have any questions regarding this Complaints Watch, please contact us at bankcomplaints@hkma.gov.hk.

Yours faithfully,

Carmen Chu
Executive Director (Enforcement and AML)

Encl.



Complaints Watch

Issue No. 20
28 June 2022

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

Jan to May 2022	General banking services	Conduct-related issues	Total
In progress as of 31 Dec 2021	486	134	620
Received during the period	1,178	121	1,299
Completed during the period	(984)	(100)	(1,084)
In progress as of 31 May 2022	680	155	835

The HKMA received 1,299 complaints against AIs and/or their staff between January and May 2022. The major types of complaints received were related to credit card issues (259), provision of banking services (243), service quality (215), fund transfer disputes (128), system failings (83) and mis-selling (76).

Business partnership with online personal financial service platforms

With the greater use of technology, customers are now increasingly relying on personal financial service platforms, which help identify and compare products offered by different financial institutions for meeting individual financial needs with attractive offers/gifts. Some AIs have established business relationships with these platforms for promotion of their banking products, such as credit cards and loans. On top of welcome offers provided by the AIs concerned, their agent platforms may also provide exclusive gifts (Exclusive Gifts) as incentives to attract customers to apply for such banking products through the platforms, subject to relevant terms and conditions. While it is highlighted on their websites that these agent platforms, and not the AIs concerned, will be responsible for gift offerings, unsatisfactory performance of the platforms in gift fulfilments may have an impact on the reputation of the AIs concerned given their close business relationship.

Recently, the HKMA noted a rise in complaints against AIs in relation to delays in the provision of Exclusive Gifts to eligible customers by their agent platforms, and there were also disputes about customers' eligibility for the relevant gifts. Such delays were triggered by various issues encountered by the platforms, including the lack of adequate human resources for administrative arrangements as well as delays in the delivery by suppliers during the COVID-19 pandemic. While following up each case with the AIs concerned, the HKMA observed some sound practices which are shared below:

- a) **Complaint handling**: The AIs concerned sought to provide appropriate assistance to the complainants where potential issues about their agent platforms were revealed. For example, while advising the customers to contact the respective

platform directly for efficient handling of their complaints, the AIs concerned also proactively followed up with their agent platforms to monitor that the latter had provided timely and appropriate responses to the complainants and that customer concerns were properly addressed.

- b) Partnership management: Close communications were maintained with their agent platforms such that the AIs concerned would be promptly informed of any potential delays in gift fulfilments and actions taken to resolve the issues, including prompt notifications to impacted customers, more expeditious gift fulfilments e.g. through the use of digital channels, and offering alternative gifts. In addition, for ongoing monitoring of the gift fulfilment process, the AIs concerned have established protocols to obtain regular updates from their agent platforms.
- c) Improving customer experience: Some AIs are exploring the use of technology to, for example, enable secured and controlled transmission of data, including the application reference numbers, and therefore facilitate their agent platforms to validate customers' eligibility for the relevant gifts. Such arrangement would help enhance the accuracy of validation by the agent platforms and avoid disputes.

AIs are reminded to review their partnership arrangements from time to time, taking into account insights from complaint handling and sound industry practices. AIs should take due care of customers' interest in managing their relationships with business partners and handling complaints with a view to strengthening customer confidence in the digital banking era.

Fraud prevention in loan application processes

Whilst the availability of digital channels for personal loan and other banking service applications is bringing convenience to customers, it is also noted that scammers are finding new ways to exploit the remote processes to perpetrate frauds. The HKMA has observed in recent complaint cases that victims of scams were offered attractive pay for full/part-time jobs or quick money-making opportunities, and lured to provide their personal data which later were found to be used by scammers for securing bank loans.

In one case, the complainant provided his personal data (including HKID copy, credit report, existing bank account information and address proof) to a scammer for job application whilst in fact such personal information was exploited by the scammer to apply for a personal loan from a bank via online channel. When the bank concerned was validating personal information sourced from the credit reference agency (CRA), it identified discrepancies in the applicant's contact phone numbers and therefore requested the customer to appear in person at a bank branch for follow-up, including identity verification. Unaware of the conspiracy, the complainant followed the scammer's advice and went to the bank branch for completing the HKID verification.

The bank branch staff verified customer's identity and informed the complainant that the verification process for the bank's loan department had been completed. The complainant further followed the instruction given by his "employer" to transfer the fund deposited into the account, which in fact were loan proceeds applied by the scammer in the complainant's name, from his own bank account to a third-party account, or a mule account as was found out later.

In accordance with various HKMA guidance, AIs are required to put in place prudent loan approval procedures, including effective measures to identify and verify loan applicants and to take additional steps in corroborating information and documents in dubious cases. AIs should also stay alert of evolving modus operandi of scams as shared in the public-private partnerships with law enforcement agencies (LEAs) and the HKMA. Some examples of good practices in managing fraud and money laundering risks are shared below:

- a) identifying and verifying the applicant's identity, and corroborating documents, data or information provided by other independent sources, such as CRAs. Where applications are made through mobile channels, AIs should ensure the relevant eKYC solutions can effectively authenticate the identity of the applicants;
- b) where AIs identify red flags, for example, contact details such as telephone number provided in a loan application differ from records available through other sources, AIs should reach out to the applicant to establish the reason for the discrepancy and issue notifications to the applicant through different channels (e.g. SMS, letter) to confirm receipt of the loan application. AIs should also consider enhancing their call-back scripts to draw the applicants' attention to possible frauds;
- c) if verification of identity in person is required, AIs should obtain the applicant's clear acknowledgement of the purpose of the verification, confirm details of the submitted loan application, and verify the authenticity of supporting documents;
- d) the approved loan proceeds should only be deposited into the applicant's designated account under the same name;

- e) implementing additional fraud rules to detect excessive applications from single mobile number/IP address, income anomalies, etc.;
- f) immediately report any suspected fraud and criminal activities to LEAs for appropriate follow-up actions, and to cooperate and extend full assistance to LEA investigations; and
- g) working together with the HKMA and LEAs to collectively promote consumer education through different channels (e.g. posters, TV and social media) for enhancing public awareness of fraud prevention and the importance of protecting personal information as well as integrity of bank accounts¹. Remind customers to immediately contact the AIs concerned for clarification or report to LEAs when having doubt of any unknown fund deposited into their bank accounts or noting any suspicious transactions.

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

¹ For example, see HKMA Publicity Materials at <https://www.hkma.gov.hk/eng/smart-consumers/dont-lend-sell-your-account/>