



HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/67C

30 November 2016

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Engagement of Intermediaries by Authorized Institutions (AIs)

Following our circular of 7 August 2015, I am writing to provide further guidance on AIs' engagement of intermediaries having regard to the progress and recent developments.

It is noted that AIs had already ceased the use of intermediaries for the purpose of sourcing retail consumer financial products or services, such as personal loans, tax loans and credit cards. In addition, all retail banks have provided customer hotlines to facilitate the public in verifying the identity of callers as genuinely from banks or not¹. The Hong Kong Monetary Authority (HKMA) has also set up a dedicated page on the website of the HKMA and launched a public education campaign to remind the public to stay alert of bogus phone calls purportedly from banks².

All these measures have helped enhance protection of the interests of bank customers and reduce the potential risks to the reputation of the banking industry arising from possible malpractices by fraudulent lending intermediaries. In particular, retail banks' hotlines have been widely and effectively used by the public to verify callers' identity, with around 2,400 to 3,400 of such enquiries received by banks' hotlines each month. It is however noted that around one-third of the enquiries involved suspected bogus calls³, suggesting that the risk of bank customers falling prey to fraudsters impersonating bank staff remains high. Besides, we note there are still cases reported to the Police where members of the public were induced by intermediaries, through fraudulent practices, to engage them for arranging loans with

¹ List of banks' hotlines can be found on the websites of the Hong Kong Monetary Authority, the Hong Kong Association of Banks and individual retail banks.

² It includes broadcasting of an Announcement of Public Interest on TV and radios, print advertisement and education drama. Relevant materials are accessible on the HKMA website (<http://www.hkma.gov.hk/eng/other-information/bogus-phone-calls.shtml>).

³ Approximately another one-third of the enquiries were confirmed to be genuine calls from banks. The remainder could not be verified due to insufficient information provided by the enquirers.

financial institutions.

In light of the developments, and having discussed with the banking industry, we have set out several measures to further enhance customer protection as well as address potential reputation risks to AIs in the loan application processes for retail customers and small and medium-sized enterprises (SMEs). The new measures require AIs to proceed with a loan application referred by a third party only if it is appointed by the AI concerned, and that the prospective borrowers are not charged any loan-related fees by that third party in general. AIs are also expected to join efforts in educating the public about responsible borrowing. Details of the measures can be found in **Annex 1**.

AIs should implement these measures as soon as practicable and no later than 31 March 2017⁴. A phased approach for full implementation is acceptable where it can be justified, and AIs are also reminded to enhance staff capacity and training as appropriate.

I would also like to take this opportunity to remind AIs to ensure compliance with the Personal Data (Privacy) Ordinance and relevant codes of practice or guidance issued by the Office of the Privacy Commissioner for Personal Data when handling customers' personal data, for example, when using personal data collected and disclosed by the appointed third parties. AIs are also reminded to follow the requirements as set out in the Code of Banking Practice including, for example, that AIs should endeavour to ensure that the prospective borrower understands the principal terms and conditions of any borrowing arrangement, in particular those related to the rate of interest, terms of repayment, and consequences of default.

Feedback from recent reviews by AIs on customer data protection

As was also required in our circular of 7 August 2015, all AIs have undertaken reviews regarding their systems of control on sales agents and sales/marketing staff in relation to customer data protection. I would like to share some key observations and practices that we have noted in the reviews. Our supervisory experience revealed that whilst AIs in general had put in place policies and procedures to protect customer information, some issues and good practices identified warrant further attention by AIs. Details are set out in **Annex 2**. In respect of the control weaknesses mentioned, the AIs concerned have been required to undertake remedial and follow-up actions.

AIs should review from time to time their policies and procedures, and promptly implement necessary enhancement measures and strengthen staff training where necessary, referring to the practical examples as set out in Annex 2.

If you have any questions relating to this circular, please contact Mr Dennis Lau at 2878-8288 or Ms Joey Chan at 2878-1216.

⁴ For avoidance of doubt, these measures are also applicable to AIs' subsidiaries except for those which have obtained money lenders licences under the Money Lenders Ordinance.

Yours faithfully,

Carmen Chu
Executive Director (Banking Conduct)

Encl.

c.c. Ms Doris Ma, Secretary, The Hong Kong Association of Banks
Mr Pui-Chong Lund, Association Secretary, The DTC Association

Measures to further enhance customer protection and address potential reputation risks to Authorized Institutions (AIs) in the loan application processes

1. Before processing a loan application from retail customers or small and medium-sized enterprises¹ (SMEs), AIs should obtain from prospective borrower confirmation² as to whether or not the loan application was referred to AIs by a third party, and information, if any, on the name of the third party and its identifying numbers³ as well as the amount of fees charged or to be charged by the third party on the prospective borrower for referring such loan application to AIs (“loan-related fees”).
2. AIs should not proceed with the loan application if the third party is confirmed not to be an appointed third party⁴ of the AI concerned. AIs should explain to the prospective borrower about the reasons for not proceeding with the loan application.
3. It is generally expected that the appointed third party should not charge loan-related fees on prospective borrowers, and thus it is a possible reason for not proceeding with the loan application if an AI is aware that the appointed third party does so. Where exceptional circumstances exist, AIs may proceed with the loan application on a case-by-case basis, while such exceptions should be adequately justified, properly approved and documented. The AI should be able to provide the documented records upon request by the HKMA.

¹ The definition of small and medium-sized enterprises adopted by individual AI should be the same as that being used for internal business segmentation / risk management purposes, OR the definition as agreed with the HKMA where appropriate. In addition, customers to which any granted facilities are being covered by the SME Loan Guarantee Scheme (SGS), SME Financing Guarantee Scheme (SFGS), Special Loan Guarantee Scheme (SpGS), or other similar guarantee schemes should be considered as SMEs.

² For example, in the form of declaration embedded in the loan application forms, or separate confirmation forms signed off by customers.

³ Including telephone number, business registration or licence numbers, if any, of the third party.

⁴ AIs should have effective and adequate controls in place to manage the risks associated with the appointment of and engagement with third parties and monitor the business practices of the appointed third parties, including, among others, estate agents in mortgage referral arrangements with AIs. Relevant guidance includes but is not limited to Module SA-2 of the HKMA Supervisory Policy Manual on Outsourcing and HKMA circular dated 20 August 2014 on “Engagement of External Business Referral Service Providers”.

4. If an AI intends to proceed with a loan application after checking relevant information provided by the prospective borrower, the AI should also obtain a confirmation⁵ from the appointed third party as to whether or not loan-related fees have been or will be charged, and information, if any, on the amount of loan-related fees charged or to be charged on the prospective borrower. This step is for cross-checking with information obtained separately from the prospective borrower. Any inconsistency should be clarified.
5. AIs should also set up and publicise a convenient channel, such as a dedicated hotline, for the public to enquire whether a person is an appointed third party of the AI concerned for sourcing retail customer and SME loans.
6. All advertisements in relation to AIs' lending business to retail customers and SMEs, whether in textual, audio or visual form, must contain the following educational message of responsible borrowing⁶ in a clear and prominent manner, so that it is easily legible and clearly audible:

“借定唔借？還得到先好借！”

“To borrow or not to borrow? Borrow only if you can repay!”

⁵ For example, in written form or audio recording.

⁶ Same as that in the HKMA's public education materials on responsible borrowing.
(<https://www.hkma.gov.hk/eng/smart-consumers/personal-credit/#responsible-borrowing>)

Feedback from recent reviews by AIs on customer data protection

1. Scope of customer information provided for telemarketing activities

1.1. Some AIs provided some or all of the following customer information to their telemarketing staff / agents for conducting telemarketing calls: customer name, identity document number, address, date of birth, information related to customers' loan and / or deposit accounts, and employment information. The AIs concerned explained that the information might be used for verifying customers' identity and answering customers' enquiries during the telemarketing. However, the AIs have not given due consideration to the circumstances of each promotional and marketing campaign when deciding on the scope of customer information provided.

Good Practices

There were cases that only customer name and telephone number were provided to telemarketing agents to conduct telemarketing calls and such customer information could only be accessible via the AI's systems. Upon a customer indicating interests in an offer, the telemarketing agent would then request the customer to provide partial identification number and partial date of birth with which to unlock the system and access the customer's other information, such as address and credit card account number. This arrangement pursues the principle of "need-to-have" basis, limits the customer information accessed by telemarketing agents at the outset of the marketing process and enables audit trail for detection of unusual activities.

Expected standards

Access to customer data should be granted on a need-to-have basis. Where staff / agents have access to a large quantity of sensitive customer data, AIs should satisfy themselves that adequate and appropriate controls are in place to safeguard customer data against theft or unauthorized access. AIs should also critically review the scope of customer data accessed by staff / agents having regard to the operational need and potential risk of customer data theft.

2. Transmission of customer data

- 2.1. A few AIs did not have adequate controls in place to prevent transmission of call lists which contain customer information to external networks. For example, staff who had access to call list were not restricted from having access to external web-based e-mail and / or internet services.

Good Practices

Some AIs have implemented system controls to detect outbound transmission of customer data via AI's corporate e-mail to external networks, such as web-based e-mail. Another more secure method was that the call lists are only readable from the AIs' systems and are not allowed to be printed, downloaded, or duplicated.

Expected standards

AIs should implement effective controls to prohibit unauthorized transmission of customer data from their internal systems to outside network / systems via Internet services that could store data (e.g. web-based e-mail, social media sites or websites providing file storage function). AIs should review their existing controls from time to time, having regard to the control measures set out in relevant circulars issued by the HKMA¹.

3. Safeguard of hardcopy documents containing customer information

- 3.1. Sales staff of an AI had not strictly followed the AI's requirement of returning completed credit card application documents to the AI's premises at day-end. The staff had kept the completed applications collected during weekend overnight. This might increase the risk of potential data leakage if the documents are not kept in safe custody.

Expected standards

AIs should have adequate and effective controls in place to reduce the risk of customer data theft or unauthorized access, such as putting in place procedures for controlling the transportation and storage of sensitive hardcopy documents, and

¹ They include but are not limited to the circulars on Customer Data Protection issued in October 2014 and July 2008.

performing reconciliation and inventory check as soon as practicable after transportation of hardcopy documents.

4. Control over the performance of sales staff / agents

4.1. Some AIs, on some occasions, delegated their sales staff / agents to conduct on-street marketing activities outside the AIs' premises and at no designated place (referred to as "floating sales staff") for marketing AIs' credit cards and personal loan products, during which customer information may be collected. Unlike the staff promoting products on AIs' designated premises under management supervision and sufficient security controls, the floating sales staff may carry out their duties alone and in location with insufficient security controls. This arrangement in general may increase the risks of loss or leakage of customer data.

Good Practices

Some AIs called back customers who were solicited by telemarketing staff / agents or floating sales staff as part of the AIs' monitoring mechanism on staff / agents performance. The AIs devised a number of questions to obtain customer feedbacks directly. Through the exercise, the AIs could seek to confirm with customers any information related to the selling processes, such as the source and the time of initial contacts, compliance with the AI's established procedures or the types of customer information provided to sales staff / agents. The call-back was conducted by staff independent from the selling process.

Expected standards

While AIs may use different channels and operational arrangements to achieve their business objectives, they should ensure that each arrangement is well structured and properly managed and the interests of customers will not be compromised.

AIs should have controls in place to ensure that the requirements of customer data confidentiality are observed and that proper safeguards are established to protect the integrity and confidentiality of customer information. AIs should also ensure that they have effective procedures for monitoring the performance of the sales staff / agents, and managing the risks associated with the activities outside the AI's premises. There should be proper procedures for handling customer complaints against the sales

staff / agents and incident management procedures for loss or unauthorized access of customer data. In addition, AIs should provide adequate training for all relevant staff / agents to promote their awareness of and to ensure compliance with the required data security requirement.

AIs are reminded that they remain accountable to customers for any misconduct on the part of the sales agents that they engage.

5. Screening of sales agents

5.1. Telemarketing agents employed by a few AIs' service providers were not subject to regular on-going screening to evaluate if they remained fit and proper for the position, for example, whether they remained having no adverse record. These AIs' service providers had conducted pre-employment screenings and reference checks before the on-boarding of a new telemarketing agent, but periodic post-employment screening was not performed as such requirement was not specified in the service agreements with the AIs' service providers.

Expected standards

In addition to performing due diligence checks on sales agents in the pre-employment stage, consideration should be given to recommending AIs' service providers to conduct on-going due diligence review on their employees in order to confirm that they remain fit and proper for their role.