Annex 2

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 HKMA[1].

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.