HONG KONG MONETARY AUTHORITY 香港金融管理局		
Supervisory Policy Manual		
IC-7	**The Sharing and Use of Commercial Credit Data through a Commercial Credit Reference Agency**	V.~~4 – 24.11.17~~5 – Consultation

This module should be read in conjunction with the Introduction and with the Glossary, which contains an explanation of abbreviations and other terms used in this Manual. If reading on-line, click on blue underlined headings to activate hyperlinks to the relevant module.

Purpose

To specify the minimum standards that AIs should observe in relation to the sharing and use of commercial credit data through a commercial credit reference agency.

Classification

A statutory guideline issued by the MA under the Banking Ordinance, §16(10).

Previous guidelines superseded

IC-7 "The Sharing and Use of Commercial Credit Data through a Commercial Credit Reference Agency" (V.3 dated 25.01.08).

Application

To AIs which are involved in the provision of credit to commercial enterprises which fall within the definitions of SME Limited Companies and Unlimited Companies.

Structure

1. Introduction
2. Definition

3. Comprehensive participation
   3.1 Participation by AIs
   3.2 Participation by subsidiaries of AIs
4. Customer consent
   4.1 General
   4.2 Consent to disclosure from SME Limited Companies
   4.3 Consent to disclosure from Unlimited Companies
5. Safeguards by AIs to protect information security
   5.1 General
   5.2 Policies and procedures
   5.3 Scope of data to be provided to CCRA
   5.4 Revocation of consent by SME Limited Companies
   5.5 Access to CCRA database
   5.6 Access control
   5.7 Confidentiality and retention of CCRA credit data
   5.8 Data accuracy
   5.9 Requests for data access or correction
   5.10 Audit trail
   5.11 Compliance audit
   5.12 Staff training
   5.13 Providing credit data of Unlimited Companies to debt collection agencies
6. Safeguards by CCRA to protect information security
   6.1 General
   6.2 Handling of commercial credit data

6.3 Limitation on the use of commercial credit data

6.4 Retention of commercial credit data

6.5 Maintaining commercial credit data accuracy and integrity

6.6 Requests for data access or correction by SME Limited Companies

6.7 Independent audit

7. Complaints in relation to the sharing and use of commercial credit data

8. Hong Kong Approach to Corporate Difficulties

---

1. Introduction

1.1 A commercial credit reference agency (CCRA) is an organisation which gathers and collates information about the indebtedness and credit history of commercial enterprises and makes such information available to lending institutions.

1.2 The HKMA believes that the establishment of a fully-fledged CCRA will bring about significant benefits to Hong Kong. On the one hand, a CCRA will provide AIs with a fuller picture of the credit worthiness of their corporate customers, and thus help to strengthen their credit risk management. This will be conducive to the HKMA's efforts in maintaining the safety and soundness of the banking system. On the other hand, a CCRA will improve the credit transparency of the corporate sector, thereby making it easier and quicker for borrowers to seek bank finance.

1.3 In view of the above benefits of a CCRA, the Hong Kong Association of Banks (HKAB) and the DTC Association (DTCA) jointly established a CCRA scheme in Hong Kong in 2004.

1.4 When Phase I of the CCRA was launched in 2004, only those small and medium-sized enterprise (SME) customers which were non-

listed limited companies were covered. Building on experience and market development, Phase II of the CCRA has expanded the coverage to include sole proprietorships and partnerships (generally referred to as Unlimited Companies) in 2008. Since the credit data relating to these Unlimited Companies are regarded as personal data, the sharing of such data is governed by the Personal Data (Privacy) Ordinance (the "PDPO") and the Code of Practice on Consumer Credit Data (the "Code") issued thereunder. In case of any conflict between this module and the Code in the governance of the credit data of these Unlimited Companies, the Code should prevail. In the light of the latest market development and to further enhance the comprehensiveness of commercial credit data sharing, Phase III of the CCRA seeks to expand coverage through revising the definition of SME Limited Company under the CCRA scheme.

1.5 The minimum authorization criterion under paragraph 10 of the Seventh Schedule to the Banking Ordinance provides that the MA must be satisfied that an AI has, among others, adequate systems of control. The MA considers that this would include adequate systems of control to enable the AI to manage its credit risk effectively, and to properly protect and use commercial credit data. In this regard, the MA will take into account the extent to which AIs make full use of all relevant information (including that obtained from a CCRA) in managing their credit exposure and whether AIs have adequate controls to ensure that their commercial credit data are properly safeguarded.

1.6 Failure to adhere to the standards and requirements set out in this module may call into question whether the AI continues to satisfy the relevant authorization criterion under the Banking Ordinance.

2. Definition

2.1 The terms used in this module have the following meaning:

- "Commercial credit" means any credit facilities provided by an AI to and for the use of a commercial enterprise, except those types of

facilities excluded from the coverage of the CCRA as specified in the Relevant Guidelines.

- "Commercial credit data" means any data concerning a commercial enterprise collected by an AI in the course of or in connection with the provision of commercial credit, or any such data collected by or generated in the database of a CCRA in the course of or in connection with the provision of a commercial credit reference service.
- "Commercial credit reference agency" (CCRA) means any person who carries on a business of providing a commercial credit reference service, whether or not that business is the sole or principal activity of that person.
- "Commercial credit reference service" means the service of collecting and compiling commercial credit data and providing such data to others for the purpose of assessing commercial credit.
- "Commercial Data Interchange" (CDI) is a data infrastructure that allows AIs to access machine-readable commercial data securely to facilitate automation of the credit assessment process. Such data include commercial credit data from a CCRA.
- "Commercial enterprise" includes, for the purpose of this module, a non-profit making or charitable organisation which obtains credits from AIs.
- "Database", in relation to a CCRA, means the collection of commercial credit data maintained by the CCRA for the purpose of providing a commercial credit reference service. It does not include the data contained in the internal archives of the CCRA to which no persons other than the CCRA itself may have access.
- "Debt Relief Plan" means an agreement to be concluded between an individual and all creditors, having an exposure to the individual, for partial relief and/or rescheduling of debts owed to those creditors pursuant to the terms of the Agreement for Debt Relief Plans endorsed by the Hong Kong Association of Banks, the DTC

Association and the Hong Kong S.A.R. Licensed Money Lenders Association.

- "Default" has the same meaning as in the Glossary.
- "Designated terminal" means a terminal restricted only to designated persons through which access to the CCRA database can be made.
- "Industry Associations" means HKAB and the DTCA.
- "Material default" means a default in payment for a period of more than 60 days.
- "Participating subsidiary" means a subsidiary of an AI which shares and uses commercial credit data through a CCRA.
- "Public record data", in relation to a commercial enterprise, means any information contained in official records that are publicly available, including but not limited to:

  (i) information relating to any action for recovery of a debt owed by the enterprise or any proceedings relating to the winding up or bankruptcy of the enterprise;

  (ii) information relating to the enterprise which is kept by the Companies Registry.

- "Relevant Guidelines" means guidelines and circulars issued by the Industry Associations concerning the design, operation or other matters in relation to the CCRA in Hong Kong. It is important to note that these guidelines may be updated and revised from time to time.
- "Relevant Requirements" means the requirements laid down in this module, the Relevant Guidelines, IC-6 "The Sharing and Use of Consumer Credit Data through ~~a~~ Credit Reference ~~Agency~~Agencies", the Personal Data (Privacy) Ordinance ("PDPO") and the Code of Practice on Consumer Credit Data (the "Code") issued thereunder.
- "Scheme of arrangement" means any restructuring, rescheduling or other modification of terms of whatsoever nature in relation to debts

owed by an individual, whether as borrower or as guarantor, towards a single creditor or more than one creditor.

- "SME Limited Company" and "Unlimited Company" have the same meaning as in the Relevant Guidelines. They are collectively referred to as "Qualifying Companies" in the Relevant Guidelines and in this module.

3. Comprehensive participation

3.1 Participation by AIs

3.1.1 As noted above, the HKMA believes that a fully-fledged commercial credit database, including both positive and negative data, will be beneficial to AIs and commercial enterprises. However, to realise such benefits, the database must be adequately comprehensive and AIs need to make full use of the database in their credit decisions.

3.1.2 In order to enable an adequately comprehensive database to be built up, which would help AIs better manage their commercial credit exposure, the HKMA expects all AIs that are involved in the provision of commercial credit to participate as fully as possible in the sharing and use of commercial credit data through a CCRA within the framework laid down in the Relevant Requirements.

3.1.3 The HKMA also considers that using commercial credit data from a CCRA for assessing credit applications and conducting credit reviews is an essential part of an AI's credit management system unless there are satisfactory alternative arrangements for the comprehensive sharing of commercial credit data.

3.1.4 AIs can usually access commercial credit data from a CCRA through (i) designated terminal(s); or (ii) the CDI. Generally speaking, accessing commercial credit data through the CDI and its designated Application Programming Interface (API)

for CCRA may allow an AI to automate part of its credit approval process, reduce manual handling and the corresponding risk of human errors, and enhance overall operational efficiency. Taking into account these factors, AIs should adopt the means of data access that is commensurate with the scale of their commercial banking operation. AIs with frequent access to commercial credit data are expected to access commercial credit data through the CDI for more effective risk management.

3.1.43.1.5 The HKMA will take into account the extent to which an AI participates in the contribution of commercial credit data to and makes full use of the same from a CCRA, as well as the means of data access (including CDI), in assessing the effectiveness of the AI's credit management system.

3.1.53.1.6 Where an AI does not, in the opinion of the HKMA, make appropriate use of the relevant facilities of a CCRA, one option would be for the HKMA to require the AI concerned to mitigate the risk by restricting the amount of commercial credit business that it undertakes.

3.1.63.1.7 The senior management of AIs should ensure that sufficient priority and resources, commensurate with the scope of their commercial credit business, are devoted to making sure that their institution can contribute information to and access the database of the CCRA in a timely and effective manner.

3.2 Participation by subsidiaries of AIs

3.2.1 Subsidiaries of AIs which are involved in the provision of credit to Qualifying Companies are allowed to share and use commercial credit data through the CCRA on a voluntary basis. This will not only benefit these subsidiaries, but also enhance the comprehensiveness of the CCRA database.

3.2.2 A participating subsidiary should comply with the

requirements in sections 2, 4 – 8 of this module as if it were an AI. If a participating subsidiary breaches any of these requirements, the HKMA may, through the AI with which the participating subsidiary is associated, order the participating subsidiary to notify the CCRA of the breach and cease to share and use commercial credit data through the CCRA.

3.2.3 Where a subsidiary of an AI participates in the sharing of commercial credit data, the AI concerned should ensure that the participating subsidiary complies with sections 2, 4 – 8 of this module. If the AI fails to do so, this will call into question whether the AI itself fulfils the requirements of this module.

4. Customer consent

4.1 General

4.1.1 In keeping with their contractual and legal duty to maintain customer data confidentiality, AIs should seek the consent of their customers before disclosing their credit data to the CCRA for the purpose of conducting credit checks or assisting other AIs to conduct credit checks.

4.2 Consent to disclosure from SME Limited Companies

4.2.1 As the usefulness of a CCRA lies in the comprehensiveness of its database which, in turn, hinges on the willingness of SME Limited Companies to allow their credit data to be reported to the CCRA, AIs' efforts in seeking customer consent are very important. In this connection, AIs should observe the following ground rules in seeking customer consent from SME Limited Companies:

(i) AIs should seek the consent of an SME customer upon application for new credit facilities (including application for an increase in the credit limit of existing facilities). Such consent should be a condition of the granting of the facility;

(ii) Where there are existing credit facilities granted to an SME customer, AIs should also seek the consent of the SME customer upon renewal, restructuring and rescheduling of the existing credit facilities of the customer in case the SME customer has not already given such consent. They should endeavour to secure such consent as a condition of renewing, restructuring or rescheduling of the credit facilities. Where an SME customer refuses to give consent, AIs should inform it that this may provide grounds for AIs to decline to renew its facilities. However, in recognition of the fact that these are existing facilities which were previously granted with no such requirement in place, the HKMA accepts that it would be difficult for AIs to insist on incorporating such a consent clause if the SME customer refused to do so. Although some flexibility is provided for such customers, the HKMA still expects AIs to explain the aim and benefits of CCRA to their customers and make their best efforts to seek to obtain consent from such customers; and

(iii) AIs should, where practicable, also stand ready to revise their existing loan documentation upon request by any SME customers who voluntarily approach them to seek to be included in the CCRA database before their current facilities come up for renewal.

4.2.2 To ensure a level playing field and the comprehensiveness of the CCRA database, the HKMA will where necessary monitor through a regular survey that AIs are not selective in seeking the consent of customers.

4.2.3 A customer consent referred to in para. 4.2.1 above may provide that, where an SME customer has revoked the consent, the AI may notify all persons to whom the AI is permitted to disclose information pursuant to the consent of

the fact that a notice of revocation has been given by the SME customer.

4.3 Consent to disclosure from Unlimited Companies

4.3.1 For Unlimited Companies, AIs should include in their relevant loan documentation the necessary provision to enable them to report the Unlimited Companies' data to the CCRA. AIs should also follow the requirements of the PDPO and the Code in the sharing and use of the Unlimited Companies' credit data through the CCRA. In particular, they should comply with the notification requirements provided therein.

5. Safeguards by AIs to protect information security

5.1 General

5.1.1 For any credit information sharing arrangement to be effective and credible, the data must be properly safeguarded. Otherwise, AIs would be subject to substantial legal and reputation risks. AIs should therefore adopt all reasonable procedures to ensure that commercial credit data disclosed to or obtained from a CCRA are properly safeguarded, with regard to the confidentiality, accuracy, relevance and proper utilisation of the information.

5.2 Policies and procedures

5.2.1 AIs should have clear and comprehensive policies and procedures for the sharing and use of commercial credit data through a CCRA to ensure compliance with the Relevant Requirements. The policies and procedures should be designed to:

(i) ensure the security, confidentiality and integrity of commercial credit data; and

(ii) guard against unauthorized access to or use of such information that could result in a breach of the Relevant Requirements.

5.2.2 These policies and procedures should be approved by the Board or a designated authority and be properly documented. They should be reviewed and updated regularly to ensure that they remain appropriate in the light of any changes to the Relevant Requirements. Any material amendments to the policies and procedures should be submitted to the Board or a designated authority for formal ratification and adoption.

5.2.3 The policies and procedures should specify how commercial credit data should be handled in cases where the credit application is submitted by an intermediary, who is commissioned by the credit applicant to handle its application, rather than by the credit applicant itself. In processing such a credit application, the AI concerned should ensure that the intermediary has obtained the authorization of the credit applicant to apply for credit on its behalf and to authorize the AI concerned to access the applicant's credit data held by a CCRA. Where the intermediary does not have such authorization, the AI should contact the credit applicant directly to confirm its intention to apply for credit from the AI and advise the credit applicant that it may access its credit data held by a CCRA for the purpose of assessing its application. In these latter cases, the AI should also address all future correspondence, including any statements or notifications to Unlimited Companies as required under the Code, to the credit applicant rather than the intermediary.

5.2.4 AIs should ensure adequate management oversight, at an appropriate senior level, on the development, implementation, and maintenance of these policies and procedures. There should also be an effective mechanism in place to monitor compliance with them. Any non-compliance should be

followed up, investigated, rectified and reported to management.

5.3 Scope of data to be provided to CCRA

5.3.1 AIs should follow the scope as specified in the Relevant Guidelines in providing data to a CCRA.

5.4 Revocation of consent by SME Limited Companies

5.4.1 This section only applies to AIs' dealings with SME Limited Companies. For Unlimited Companies, AIs should follow the opt-out requirements of the Code.

5.4.2 An SME Limited Company may revoke its consent by giving the AI 90 days' prior notice in writing. In such situation, the AI should report the revocation to the CCRA as soon as practicable and stop reporting the commercial credit data of that enterprise to the CCRA after the 90-day period.

5.5 Access to CCRA database

5.5.1 An AI may at any time, for the purpose of providing or updating the commercial credit data of a Qualifying Company, access from a CCRA such commercial credit data of the enterprise as were previously provided by it to the CCRA.

5.5.2 In addition, an AI may, through a credit report provided by a CCRA, access commercial credit data held by the CCRA relating to a Qualifying Company:

(i) in the course of considering any grant, review or renewal of credit to the enterprise as borrower or to another person for whom the enterprise proposes to act or acts as guarantor; or

(ii) for the purpose of the reasonable monitoring of the indebtedness of the enterprise while there is currently a default by the enterprise as borrower or as guarantor.

5.5.3 In the cases of Unlimited Companies, for the purpose of para. 5.5.2 above, the word "review" means consideration by the AI of any of the following matters (and those matters only) in relation to the existing credit facilities, namely:

- an increase in the credit amount;
- the curtailing of credit (including the cancellation of credit or a decrease in the credit amount); or
- the putting in place or the implementation of a scheme of arrangement with the enterprise.

5.5.4 An AI should not access the commercial credit data relating to a Qualifying Company held by a CCRA for purposes other than those mentioned in paras. 5.5.1 to 5.5.3 above. In particular, it must not access the database of a CCRA for the purpose of offering or advertising the availability of goods, facilities or services to a Qualifying Company. Where Unlimited Companies are involved, any contravention by the AI of this prohibition will give rise to a presumption of contravention of Data Protection Principle 1(2) and/or Data Protection Principle 3 under section 13(2) of the PDPO.

5.6 Access control

5.6.1 AIs should have written policies specifying who may authorize access to the CCRA database (through whatever channel) and the criteria that may need to be met for making such access. The policies should define clearly the circumstances under which an AI may make such access.

5.6.2 Only designated persons authorized by management should be able to access the CCRA database. There should be clearly defined procedures for the authorization of such designated persons. Such authorization, and any subsequent changes, must be documented.

5.6.3 AIs should maintain stringent control over the use of and changes made to the passwords for access to the CCRA

database. The passwords should only be made available to the designated persons who are authorized to access the CCRA database. AIs should avoid using shared passwords (i.e. two or more persons sharing the same password). Under no circumstances should passwords be disclosed to unauthorized persons, e.g. IT maintenance, service contractors or unauthorized staff of AIs.

5.6.4 ~~Where access~~Access to the CCRA database ~~is made (~~through ~~designated terminals, access to the CCRA database through such terminals~~whatever channel) should be restricted only to designated persons with proper access control, such as by way of password protection.

5.6.5 AIs should change the passwords regularly for accessing the CCRA database, preferably at least quarterly.

5.6.6 AIs should maintain an access log on ***all*** instances of access to the CCRA database. The access log should contain sufficient details as evidence of compliance with the Relevant Requirements. It should, as a minimum, contain information about the purpose of the access, the date on which the access was made and the staff who made the access.

5.6.7 The AI's internal access log and billing records from the CCRA should be regularly reviewed, at least on a monthly basis, for unusual access activities, such as an unusually high volume of access activities that is inconsistent with the AI's business. Such unusual access activities might suggest that the designated persons have abused the system. Alternatively, any unexplained shortfall in the number of instances of access in the AI's internal access records when compared with the CCRA's billing records might suggest unauthorized access or breaches of the AI's access control.

5.6.8 AIs should undertake prompt investigation of any unusual access activities and take prompt remedial actions to follow

up any irregularities. Such irregularities, and the reasons for them, should be brought to management's attention.

5.7 Confidentiality and retention of CCRA credit data

5.7.1 AIs should establish a policy on the safeguarding and retention of customer data obtained from the CCRA. Specifically, the policy should provide that access to the CCRA credit report should be on a need to know basis. There should also be restrictions on how such reports may be duplicated, copied or circulated.

5.7.2 AIs may need to retain credit reports from a CCRA as documentary support for the relevant credit decisions for which the credit reports were obtained, and as file records in the event of subsequent queries or disputes raised by customers. With the CCRA database being updated regularly, AIs should ensure that they do not use out of date credit reports for making credit decisions. Where Unlimited Companies are involved, AIs should ensure compliance with the Data Protection Principles of the PDPO which require, inter alia, that personal data shall not be kept longer than is necessary for the fulfilment of the purpose for which the data are or are to be used, and that there would be a breach of the Principles if "out-of-date" information were to be retained and used for making subsequent credit decisions.

5.7.3 Where a CCRA credit report is obtained for the purpose of assessing a credit application and the AI subsequently refused the application, or when a customer ceases to have any borrowing relationship with the AI, the AI should destroy the relevant credit reports within a reasonable period unless such reports are to be used for other permitted purposes.

5.8 Data accuracy

5.8.1 AIs should take reasonably practicable steps to check the accuracy of their customers' credit data before passing them

to the CCRA. Clear procedures should be laid down on how changes to customers' credit data are to be implemented, verified and transmitted to the CCRA. As for data updating, AIs should, subject to para 5.8.2 below, follow the pertinent requirements in the Relevant Requirements.

5.8.2 If an AI discovers any inaccuracy in the data which have been provided to a CCRA, the AI should update such data held in the database of the CCRA as soon as practicable.

5.9 Requests for data access or correction

5.9.1 Where a Qualifying Company informs an AI that it wishes to access its data held by a CCRA, the AI should advise the company how to contact the CCRA, including the name, address and telephone number of the CCRA.

5.9.2 Where any commercial credit data provided by an AI to a CCRA are disputed by the Qualifying Company to which such data relate, the AI should, as soon as practicable, notify the CCRA of the existence of the dispute. If it is necessary to correct the relevant data, the AI should as soon as practicable update the data held by the CCRA accordingly.

5.9.3 If a Qualifying Company has requested a CCRA to correct its data and the correction is subsequently complied with by the CCRA, the AI concerned should at the request of the Qualifying Company reconsider its credit decision on the basis of a new credit report obtained from the CCRA.

5.10 Audit trail

5.10.1 The access log records, any investigation reports and follow up actions on irregularities or exceptions should be properly documented and kept for not less than 2 years. They should be maintained in such a manner that would facilitate compliance reviews and audits.

5.11 Compliance audit

5.11.1 An AI should conduct a compliance audit at least annually to verify whether its data management practices are adequate to ensure compliance with the requirements of the Relevant Requirements and its own policies and procedures regarding the sharing and use of commercial credit data.

5.11.2 The audit report should be submitted to the AI's Board or a designated authority for review. This report should assess the overall effectiveness of the data management practices in ensuring compliance with the Relevant Requirements. The reports should cover issues such as security breaches or violations, management's responses and recommendations for improvement.

5.12 Staff training

5.12.1 An AI should provide appropriate guidance and training to staff who are involved in the sharing and use of commercial credit data through a CCRA. In particular, staff involved in the handling of commercial credit data should familiarise themselves with the Relevant Requirements and the AI's own policies and procedures.

5.13 Providing credit data of Unlimited Companies to debt collection agencies

5.13.1 An AI should follow the requirements specified in the Code before they provide any credit data of an Unlimited Company to a debt collection agency for debt collection purpose.

6. Safeguards by CCRAs to protect information security

6.1 General

6.1.1 Apart from the safeguards mentioned in the previous section, an AI should also require the CCRA whose service it has engaged to adopt all reasonable procedures to protect the commercial credit data it holds, with regard to the confidentiality, accuracy, relevance and proper utilisation of the information.

6.1.2 In deciding on the engagement of a CCRA for the provision of commercial credit reference service, and in considering, from time to time, the continued engagement of the CCRA, an AI should treat as an important criterion the demonstration by the CCRA of its compliance with the data protection requirements specified in subsections 6.2 – 6.7 below which a CCRA is expected to follow.

6.1.3 An AI should enter into a formal service agreement with the CCRA whose service it intends to engage. The agreement should specify that the CCRA should comply with the data protection requirements specified in subsections 6.2 – 6.7 below. An AI should put in place appropriate arrangements to monitor regularly the performance of the CCRA, particularly in respect of its ability to comply with the Relevant Requirements. The agreement should empower the AI to terminate the service of the CCRA if the CCRA fails to comply with these requirements. The contract with the CCRA should also specify that account data provided by the AI shall remain the property of the AI and that the AI has the right to remove its data on the termination of its contract with the CCRA.

6.1.4 Where an AI becomes aware that the CCRA whose service it has engaged fails to comply with any of the data protection requirements specified in subsections 6.2 – 6.7 below, it should forthwith notify its Industry Association and consider whether to terminate the service of the CCRA.

6.1.5 Subsections 6.2 to 6.7 below set out the data protection requirements which a CCRA is expected to follow. References to AIs in these subsections include participating subsidiaries.

6.2 Handling of commercial credit data

6.2.1 A CCRA should ensure compliance with all the requirements under the PDPO and the Code in respect of data of Unlimited Companies. As for the data of SME Limited Companies, a CCRA is expected to follow the requirements specified in subsections 6.3 to 6.7 below.

6.3 Limitation on the use of commercial credit data

6.3.1 A CCRA should not use the commercial credit data provided by AIs for purposes other than the following:

(i) providing a credit report or other information to assist AIs in the making of credit decisions relating to SME Limited Companies or in the recovery of debts from such enterprises; and

(ii) using the data for reasonable internal management and research analysis, such as the defence of claims for damages by data subjects or AIs; the monitoring of the quality and efficiency of its service; and the performance of statistical analysis in relation to credit scoring activities.

6.4 Retention of commercial credit data

6.4.1 Subject to paras 6.4.2 and 6.4.3, a CCRA should follow the requirements pertaining to the retention of commercial credit data specified in the Relevant Guidelines.

6.4.2 Where a CCRA has collected from an AI any data relating to an SME Limited Company that reveal a material default, the CCRA should only retain such data in its database until the

expiry of five years from the date of final settlement of the amount in default.

6.4.3 Where a CCRA is notified by an AI that an SME Limited Company has revoked the consent which the enterprise has previously given to the AI, the CCRA should delete from its database the commercial credit data relating to the enterprise provided by the AI on the 90th day after the day on which the notice of revocation was received by the AI, except

(i) any public record data relating to the SME Limited Company; and

(ii) such information which is necessary for the purpose of notifying other relevant persons of the revocation as mentioned in para. 4.2.3 above.

6.5 Maintaining commercial credit data accuracy and integrity

6.5.1 A CCRA should take appropriate measures, including the following, to safeguard against any improper access to or mishandling of commercial credit data held by it:

6.5.1.1 On or before providing commercial credit reference service to AIs

(i) to enter into formal service agreements with the AIs which specify in detail the controls and procedures to be applied when the AIs seek access to the CCRA database;

(ii) to establish controls to ensure that only data to which an AI is entitled are released;

(iii) to train staff in relation to the requirements in this module and, in particular, good security practice;

(iv) to develop written guidelines, and disciplinary or contractual procedures in relation to the proper

use of access authorities by staff, external contractors or subscribers;

(v) to ensure that adequate protection exists to minimise, as far as possible, the risk of unauthorized entry into the database or interception of communications made to and from the database;

6.5.1.2 In its daily operations

(i) to review on a regular and frequent basis its password controls which help to ensure that only authorized staff are allowed access to its database;

(ii) to monitor and review on a regular and frequent basis usage of the database, with a view to detecting and investigating any unusual or irregular patterns of access or use;

(iii) to ensure that practices in relation to the deletion and disposal of data are secure, especially where records or discs are to be disposed of off-site or by external contractors; and

(iv) to maintain a log of all incidents involving a proven or suspected breach of security, which includes an indication of the records affected, an explanation of the circumstances and action taken.

6.5.2 Without prejudice to the generality of paragraph 6.5.1 above, a CCRA should:

(i) in the case of there being any suspected abnormal access by an AI, report such suspected abnormal access as soon as reasonably practicable to the management of the AI;

(ii) maintain a log of all instances of access to its database by AIs, which log shall include:

- the identity of the AI and the relevant department seeking access;
- the date and time of access;
- the identity of the enterprise whose data were so accessed;
- the purpose of the access; and
- instances of reporting by the CCRA of suspected abnormal access to the management of an AI,

and shall keep such a log for not less than 2 years for examination by its compliance auditor.

6.6 Requests for data access or correction by SME Limited Companies

6.6.1 A CCRA should allow an SME Limited Company to:

(a) ascertain whether the CCRA holds its commercial credit data;

(b) request access to its commercial credit data held by the CCRA –

(i) within a reasonable time;

(ii) at a fee, if any, that is not excessive;

(iii) in a reasonable manner; and

(iv) in a form that is intelligible; and

(c) request the correction of its commercial credit data held by the CCRA or be given reasons if such a request is refused by the CCRA.

6.6.2 A CCRA should respond promptly to an access request in respect of the commercial credit data held by it brought by an

SME Limited Company. Where such an access request is made at the office of the CCRA, a copy of the data held at the time of the request should, if practicable, be provided forthwith to the enterprise, or else be despatched by mail to the enterprise as soon as reasonably practicable.

6.6.3 A CCRA should promptly consult the relevant AI upon receiving a request made by an SME Limited Company for correction of commercial credit data provided by the AI. If the CCRA does not receive from the AI any confirmation or correction of the disputed data within a reasonable period from the date of the correction request, the relevant data should be deleted or otherwise amended as requested.

6.6.4 A CCRA should, upon receiving a request made by an SME Limited Company for correction of public record data, verify the accuracy of such data by checking the relevant public records. If no such verification is obtained within a reasonable period from the date of the correction request, the public record data should be deleted or otherwise amended as requested, except where the SME Limited Company alleges any inaccuracy in the data which is not apparent on the face of the public records, it should in that case be incumbent on the SME Limited Company to provide proof of such inaccuracy.

6.7 Independent audit

6.7.1 A CCRA should make available to the Industry Associations an annual compliance report prepared by a reputable independent auditor appointed by the CCRA on whether or not the CCRA has in place systems of control which are adequate to enable the CCRA to comply with the data protection requirements specified in this section.

7. Complaints in relation to the sharing and use of commercial credit data

7.1 To ensure that the data protection requirements specified in this module are adhered to by AIs and CCRAs, the HKMA will play an active role in ensuring that complaints in relation to the sharing and use of commercial credit data are properly handled.

8. Hong Kong Approach to Corporate Difficulties

8.1 When the information obtained from the CCRA reveals that a Qualifying Company has incurred a level of indebtedness that may be unmanageable and the enterprise might have genuine difficulty in repaying the loans, AIs should follow the guidelines set out in the "Hong Kong Approach to Corporate Difficulties" or the "Hong Kong Approach to Consumer Debt Difficulties" where appropriate, to deal with such borrowers. Particular care should be taken to ensure that account management policies based upon account review checks are consistent with the guidelines.

8.2 AIs should consider such cases sympathetically and discuss with the Qualifying Company to work out a solution that is mutually beneficial for both the company and the AIs concerned. They should not hastily withdraw facilities or put the company into receivership, or issue writs demanding repayment. For Unlimited Companies, AIs should also follow the framework and procedures which are laid down in the Agreement on Debt Relief Plans (including making their customers aware of the possibility of solving the problem by a Debt Relief Plan), and the framework and procedures for Individual Voluntary Arrangements, and work out a mutually acceptable solution with the customer as far as possible.

8.3 Where the AI does not have a prior credit relationship with the Qualifying Company which has applied for credit, the AI should suggest that the company discuss the problem with the financial institution with which it has the major credit relationship as soon as possible.