Supervisory Policy Manual

IC-7	The Sharing and Use of Commercial Credit Data through a Commercial Credit Reference Agency	v.1 – 03.06.2004

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Previous guidelines superseded

This is a new guideline.

Application

To AIs which are involved in the provision of credit to small and medium-sized enterprises (SMEs).

Structure

---

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) are jointly establishing such a scheme in Hong Kong. At the initial stage, the CCRA will only cover SME customers of AIs and their participating subsidiaries. It is expected that the CCRA will be up and running in the second half of 2004.

1.4 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.

1.5 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 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.
- “Default” has the same meaning as in the Glossary.
- “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 proposed CCRA in Hong Kong. It is important to note that these guidelines may be updated and revised from time to time.
- "Small and medium-sized enterprises (SMEs)" has the same meaning as in the Relevant Guidelines.

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 SMEs. 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 SMEs to participate as fully as possible in the sharing and use of commercial credit data through a CCRA within the framework laid down in this module and the Relevant Guidelines.

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 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 in assessing the effectiveness of the AI's credit management system.

3.1.5 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 SME credit business that it undertakes.

3.1.6 The senior management of AIs should ensure that sufficient priority and resources, commensurate with the scope of their SME business, are devoted to make 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 As agreed with the Industry Associations, subsidiaries of AIs which are involved in the provision of commercial credit to SMEs would be allowed to share and use commercial credit data through the CCRA on a voluntary basis. This would 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 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 As the usefulness of a CCRA lies in the comprehensiveness of its database which, in turn, hinges on the willingness of SMEs 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:

(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. 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 make their best efforts to persuade their SME customers to give consent and not to opt out of the reporting arrangement; 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.

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

4.4 A customer consent referred to in para. 4.1 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.

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 requirements of this module and the Relevant Guidelines. 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 requirements of this module.

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 this module or the Relevant Guidelines. 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 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 The Relevant Guidelines have specified the scope of data which AIs should report to a CCRA. AIs should follow the relevant requirements in providing data to a CCRA.

5.4 Revocation of consent by SMEs

5.4.1 An SME 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 an SME, 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 an SME:

(i) in the course of considering any grant, review or renewal of commercial 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 An AI should not access the commercial credit data relating to an SME held by a CCRA for purposes other than those mentioned in paras. 5.5.1 and 5.5.2 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 an SME.

5.6 Access control

5.6.1 AIs should have written policies specifying who may authorize access to the CCRA database 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 to the CCRA database is made through designated terminals, access to the CCRA database through such terminals should be restricted only to designated persons, 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 this module. 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.

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 Guidelines.

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 by SMEs

5.9.1 Where an SME informs an AI that it wishes to access its data held by a CCRA, the AI should advise the enterprise 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 SME 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 an SME 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 SME 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 this module, the Relevant Guidelines 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 this module and the Relevant Guidelines. 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 this module, the Relevant Guidelines and the AI's own policies and procedures.

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 – 6.6 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 – 6.6 below. The agreement should empower the AI to terminate the service of the CCRA if the CCRA fails to comply with these requirements.

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 – 6.6 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 6.6 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 Limitation on the use of commercial credit data

6.2.1 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 SMEs 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.

6.3 Retention of commercial credit data

6.3.1 Subject to paras 6.3.2 and 6.3.3, a CCRA should follow the requirements pertaining to the retention of commercial credit data specified in the Relevant Guidelines.

6.3.2 Where a CCRA has collected from an AI any data relating to an SME 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.

6.3.3 Where a CCRA is notified by an AI that an SME 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; and

(ii) such information which is necessary for the purpose of notifying other relevant persons of the revocation as mentioned in para. 4.4 above.

6.4 Maintaining commercial credit data accuracy and integrity

6.4.1 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:

6.4.1.1 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;

6.4.1.2 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.

6.4.2 Without prejudice to the generality of paragraph 6.4.1 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.

6.5 Requests for data access or correction by SMEs

6.5.1 A CCRA should allow an SME 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.

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

6.5.3 A CCRA should promptly consult the relevant AI upon receiving a request made by an SME 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.

6.5.4 A CCRA should, upon receiving a request made by an SME 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 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 to provide proof of such inaccuracy.

6.6 Independent Audit

6.6.1 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 an SME 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" to deal with such borrowers.

8.2 AIs should consider such cases sympathetically and discuss with the SME to work out a solution that is mutually beneficial for both the enterprise and the AIs concerned. They should not hastily withdraw facilities or put the enterprise into receivership, or issue writs demanding repayment.

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

Contents	Glossary	Home	Introduction