

MCRA Model (Credit Data Smart) - Type Two Member Onboarding Criteria

- Money lenders under Money Lenders Ordinance, Cap. 163 of the Laws of Hong Kong, or persons who engage in the business (whether or not the person carries on any other business) of providing finance for the acquisition of goods by way of leasing or hire purchase can apply to be a Type Two Member upon fulfilment of requirements under Clause 4.1.3.3 of the Multiple Credit Reference Agencies Model Governance Framework (Governance Framework).
- An applicant for Type Two membership shall engage an independent assessor to perform an independent assessment. The independent assessor shall collect, as far as possible, the information set out in the checklist below and make an assessment based on the criteria and assessment standards as agreed by the Industry Associations. An independent assessment report, which shall be annexed with the available supporting information set out in the checklist, shall then be submitted to the Business Operator for processing the membership application.
- The checklist and assessment standards are set out as follows:

	Onboarding criteria (Clause 4.1.3.3 of <i>Governance Framework</i>)	Specific checklist with reference to the <i>Code of Practice on Consumer Credit Data</i> issued by The Office of the Privacy Commissioner for Personal Data (CCD Code)	Assessment standards (or areas)
Company Due Diligence	i. Positive company background	a) Organization chart, company profile and company structure in relation to its parent company, i.e. directorship and ownership b) Certificate of Incorporation, Articles of Association, Business Registration Certificate, and information of shareholders, executives and board members c) Company search report and court order and prosecution check d) List of major joint venture (with over 50% shareholding), partnership or other cooperation	1. Any major ongoing or past regulatory and enforcement actions by local authorities on the company, its directors and substantial shareholders (with effective interest of over 5%) involving any “red flag” issues (e.g. privacy, data leakage, previous bankruptcy or other business failure; fraud; embezzlement; tax evasion; bribery & corruption; links to organized crime or arms trafficking; cyber threats; and involvement in terrorist financing or terrorist activities); if there is any, additional information would be required; 2. Any major ongoing or past criminal or civil legal proceedings naming the company, its directors and substantial shareholders (with effective

Onboarding criteria (Clause 4.1.3.3 of <i>Governance Framework</i>)	Specific checklist with reference to the <i>Code of Practice on Consumer Credit Data</i> issued by The Office of the Privacy Commissioner for Personal Data (CCD Code)	Assessment standards (or areas)
	arrangement in relation to the business of providing credit e) Government and regulatory permits and licences in relation to the business of providing credit (e.g. Money Lender Licence), where appropriate	interest of over 5%) as defendant involving any “red flag” issues (e.g. privacy, data leakage, previous bankruptcy or other business failure; fraud; embezzlement; tax evasion; bribery & corruption; links to organized crime or arms trafficking; cyber threats; and involvement in terrorist financing or terrorist activities); if there is any, additional information would be required; 3. Any listing of the company or its directors and substantial shareholders on global watch lists. 4. Any adverse media reports (screening for past 5 years is recommended) on the company and its directors and shareholders in relation to “red flag” issues (e.g. privacy, data leakage, previous bankruptcy or other business failure; fraud; embezzlement; tax evasion; bribery & corruption; links to organized crime or arms trafficking; cyber threats; and involvement in terrorist financing or terrorist activities); 5. Nature of business including existing/target customer groups, distribution channels, and products not involving high risk business types (please refer to Note 1 for high-risk business types)

Onboarding criteria (Clause 4.1.3.3 of <i>Governance Framework</i>)	Specific checklist with reference to the <i>Code of Practice on Consumer Credit Data</i> issued by The Office of the Privacy Commissioner for Personal Data (CCD Code)	Assessment standards (or areas)
ii. Sustainable financial capability	a) Audited financial statements for 2 years prior to the submission of application or any other proof acceptable to the Industry Associations b) Name of auditor c) Disclosure of change of auditor within 3 years before submission of onboarding application Remark: If a company is established less than 2 years, items ii a)-c) above are to be exempted.	1. No adverse opinion and no qualified opinion on the financial statements expressed by the auditor 2. Legitimate sources of finance for business 3. Satisfactory financial sustainability assessment by independent assessors (eg the applicant's ability to continue as a going concern)
iii. Necessity for the Consumer Credit Reference Service by validating its provision of Consumer Credit Service	a) Valid Business Registration Certificate, a Money Lender Licence (required for all money lender applicants) b) Credit facility documents c) Loans approval procedures d) Loans approval policy e) Handling process and procedures regarding loans collection f) Handling process and procedures of all loan applications g) Forms for loans application	1. Validity of the Business Registration Certificate and Money Lender License 2. Compliance with Personal Data (Privacy) Ordinance (PDPO) and CCD Code (please refer to Note 2)

	Onboarding criteria (Clause 4.1.3.3 of <i>Governance Framework</i>)	Specific checklist with reference to the <i>Code of Practice on Consumer Credit Data</i> issued by The Office of the Privacy Commissioner for Personal Data (CCD Code)	Assessment standards (or areas)
System / Technology	iv. Sufficient security measures and protection on Consumer Credit Data	a) Information security measures and requirements with reference to the requirements specified in CCD Code and industry best practices b) Information security policy (including access control policies) c) Incident management procedures d) Handling process and procedures of data breach incidents e) Information security and privacy management of staff (including training record) f) Information Security Controls – refer to the HKCERT Seven Habits of Cyber Security for SMEs (https://www.hkcert.org/security-guideline/seven-habits-of-cyber-security-for-smes) g) The proof of fulfilment of the Platform Operator’s minimum security standards (please refer to Note 3)	1. Compliance with PDPO and CCD Code (please refer to Note 2) 2. Compliance with PDPO and CCD Code with respect to Third Party Usage and the data usage disclosure 3. Completion of Information Security/Cybersecurity Risk Assessment by independent third party by taking reference to ISO 27001 / 27002 [<i>Satisfactory for risks with a definite fixation date; further consideration for open risks without a fixation date.</i>] 4. Fulfil the Platform Operator’s minimum security standards 5. Confirmation on no history of data breach; and if there was, additional information would be required on how the applicant has remedied the relevant issue through revamping information security controls and policies.
	v. Compliance with the CCD Code	a) Handling process and procedures of Data Access Requests, including Data Access Requests Form b) Documentation for customers on their right to personal data privacy and purposes for which personal data will be used following collection (e.g. Personal Information Collection Statement (please refer to Note 4))	1. Compliance with PDPO and CCD Code (please refer to Note 2) 2. Confirmation on compliance and no history of breach of the PDPO or the CCD code; and if there was any breach involved, additional

	Onboarding criteria (Clause 4.1.3.3 of <i>Governance Framework</i>)	Specific checklist with reference to the <i>Code of Practice on Consumer Credit Data</i> issued by The Office of the Privacy Commissioner for Personal Data (CCD Code)	Assessment standards (or areas)
		c) Other documentation relating to the handling of consumer credit data, such as policies and guidelines for the sharing and use of consumer credit data, Positive Mortgage Data Sharing consent form, request for deletion of data from CRA, decline letter for loan applications, confirmation / rejection letter for deletion of data from CRA, measures against misuse of consumer credit data etc.	information would be required on how the applicant has remedied the relevant issue.
	vi. Data integrity and data quality	a) Data integrity check against the standardized data format (<i>subject to future development</i>) b) The proof of fulfilment of the Platform Operator's minimum security standards	1. Fulfil the requirement of contributing valid and accurate data in accordance with the standardized data format to be provided by the Platform Operator, to prevent any error during the process of converting raw data to the data submission file. 2. Satisfactory result from the simulation test which aims at allowing Platform users to rehearse their business operations in a production-like environment. 3. Fulfill the Platform Operator's minimum security standards
Others	vii. Subscribing to the services of one or more of the Selected CRAs	a) Letter(s) from one or more Selected CRA(s) confirming the applicant will subscribe to its service	Availability of the confirmation letter

Note 1: Some of the business types deemed to be high risk include: shell companies (i.e. companies with no material business activity), companies without legitimate banking or moneylender licenses, illegal gambling operations, exposure to potential criminal activities (e.g. human trafficking, terrorist financing).

Note 2: The independent assessment report shall comprise, amongst other areas of assessment, assessment of compliance with PDPO and CCD Code for the past one year and such other requirements as prescribed by the Industry Associations and set out in the table above.

Note 3: Subscribed Members and Selected CRAs (Platform users) shall use their reasonable endeavours to follow the industrial security practices to safeguard the connection with Credit Reference Platform. The following guidelines shall be followed as a pre-requisite before connecting to ICLNet2:

- i. Platform users should ensure their infrastructure facility have proper network segregation and sufficient security measures to prevent unauthorized access to ICLNet2 (e.g. Internet traffic is prohibited to flow into ICLNet2).
- ii. Proper network traffic filter and inspection via network-related security devices including firewalls and Intrusion Prevention System (IPS) are in place to ensure legitimate traffic in ICLNet2.

An applicant can confirm its compliance with the Platform Operator's minimum security standards after subscribing to ICLNet2 and passing the connectivity test.

For Common Module users, they shall also meet the following requirements:

- A dedicated personal computer device shall be used for connecting to ICLNet2 and assessing the Common Module Web Portal.
- For such dedicated personal computer device, the latest security patches/updates and antivirus software as recommended by respective product vendors should be installed and compliant with users' own internal policies and controls.

The Indirect Membership application is no longer open for application.

Note 4: The Personal Information Collection Statement (PICS) of an applicant should be able to address the collection and disclosure of consumer credit data under Credit Data Smart including the applicant's provision of consumer credit data (including mortgage data if the applicant has mortgage business) to credit reference agency(ies), and its acquisition of credit report(s) on a customer from credit reference agency(ies). A template PICS of the Industry Associations may be provided to the applicant for reference upon request.