DEACONS
的近律師行

Newsletter

Banking and Finance

1 September 2022

What's inside?

Supervisory Policy Manual ("SPM") Module on "The Sharing and Use of Consumer Credit Data through Credit Reference Agencies"

Simon Deane and Ruby Hui

The Hong Kong Monetary Authority ("**HKMA**") recently released a revised SPM module IC-6 "The Sharing and Use of Consumer Credit Data through Credit Reference Agencies". It sets out guidelines under section 16(10) of Banking Ordinance (Cap 155).

Pursuant to the changes in the revised SPM, the HKMA expects authorised institutions ("**AIs**") to participate to the extent possible in the sharing and use of consumer credit data through credit reference agencies ("**CRAs**") under the Multiple CRAs Model via the Credit Reference Platform ("**CRP**"). CRP is a computer network and system operated independently which serves as a data switch between credit providers and the CRAs.

The launch date of the CRP is scheduled for the end of 2022, and the effective date of the CRP will be announced by the HKMA in due course.

To access a full copy of the revised SPM, please see here.

HKMA's seventh issue of the Regtech Adoption Practice Guide

Simon Deane and Sally Lau

Further to the sixth issue of the Regtech Adoption Practice Guide published in April this year, the HKMA issued a circular ("**Circular**") in relation to the seventh issue of the Regtech Adoption Practice Guide ("**Guide**") on 18 July 2022.

The Guide focuses on the Regtech solutions used in Third-Party Monitoring and Risk Management ("**TPRM**"). There has been significant growth in the reliance by businesses on third-parties in recent years. TPRM Regtech solutions can help to ensure the risks associated with third-parties are properly managed and allow the business to keep functioning efficiently in a stable environment.

The Guide explains how Regtech solutions can be used to support TPRM and provides practical implementation guidance to banks on the adoption of Regtech solutions for TPRM. Banks are reminded that as a pre-requisite for Regtech adoption, banks should have a clear understanding of their operating model and the capabilities of their people. There needs to be a clear articulation of the TPRM mandate across different departments and functions. Lastly, the Guide offers advice on how banks can use TPRM Regtech solutions to address the risks and challenges associated with TPRM.

For more information on the Circular, please see here. To access a full copy of the Guide, please see here.

Updates to the HKMA's Guideline on Minimum Criteria for Authorisation

Simon Deane and Kelly Poon

An updated guideline on minimum criteria for authorisation under the Banking Ordinance ("**Guideline**") was issued by the HKMA on 22 July 2022 superseding the previous version issued on 10 July 2020.

The Guideline provides guidance in relation to the Banking Ordinance's minimum criteria for obtaining a banking or deposit taking license. Some of the key amendments are listed as follows:-

In relation to the requirements for boards of directors, the HKMA now specifically refers to "authorised institutions" (instead of just banks) in item 13, meaning that the requirements under item 13 will now apply not just to licensed banks, but also to restricted licence banks ("**RLBs**") and deposit-taking companies ("**DTCs**") that are designated by the HKMA as systemically important. Under item 13, the HKMA expects one-third of the board of directors or three of the members of the board of relevant AIs (whichever is higher) to be independent non-executive directors. At least two of these independent non-executive directors should possess a background in banking or accounting or some other relevant financial industry. It is also stated that independent non-executive directors should not perform any executive functions within the AIs and should be free from any relationship which may impede the exercise of their independent and objective judgment concerning the affairs of the institution.

Similarly, the original requirements of item 14 now also apply to RLBs and DTCs that are not designated by the HKMA as systemically important (rather than to all RLBs and DTCs).

Item 19 further specifies that in assessing the fitness and propriety of a proposed candidate for an AI's board of directors, chief executive or executive officer, if the candidate has any outside mandates, the HKMA will take into account whether he/she is able to devote sufficient time and attention to perform his/her role, and any potential conflicts of interest in performing his/her role. (Please see item 19(g) of the Guideline.)

Under item 25, in determining the fitness and propriety of an executive officer, the HKMA now also considers whether the person passed the relevant local regulatory framework papers specified in the SFC guidelines. (Please see item 25(b) of the Guideline.)

Under item 27, in determining whether an executive officer has sufficient authority, it is now further specified that an executive officer should not be more than one rank below the chief executive, alternative chief executive director or manager appointed under section 72B of the Ordinance.

In relation to resolution planning, item 85 specifically refers AIs to the Code of Practice chapter on "Resolution Planning – Operational Continuity in Resolution" (OCIR-1) on maintaining adequate management information systems for supporting operational continuity in resolution. The HKMA also refers AIs to the Code of Practice chapter on "Resolution Planning – Contractual Recognition of Suspension of Termination Rights" (ST-1) regarding compliance with requirements concerning systems of control and record keeping.

Under item 101, in relation to considering whether an institution is conducting its business prudently and with competence, the HKMA now also takes into account the institution's risk governance and compliance culture. (Please see item 101(e) of the Guideline.)

A new item 104 has been added, emphasising the requirement for AIs to build a strong compliance culture within the institution and not to engage in any act that has the effect of circumventing any applicable laws and regulations. AIs are expected to deal with the HKMA and other regulators in an open, cooperative and timely manner. To access a full copy of the updated Guideline, please see here.

Frequently Asked Questions in relation to Anti-Money Laundering and Counter-Financing of Terrorism

Simon Deane and Crystal Choi

Frequently Asked Questions ("**FAQs**") in relation to Anti-Money Laundering and Counter-Financing of Terrorism ("**AML/CFT**") have been developed by the Hong Kong Association of Banks ("**HKAB**") with input from the Hong Kong Monetary Authority ("**HKMA**"). The FAQs do not form part of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorised Institutions) ("**AML/CFT Guideline**") and are designed to be read in conjunction with the AML/CFT Guideline.

The FAQs aim to assist Authorised Institutions ("**AIs**") in their understanding of relevant AML/CFT requirements. AIs are expected to be fully conversant with the FAQs, and to have regard to them in meeting their AML/CFT legal and regulatory obligations. The FAQs are, however, by their nature, framed as general statements and do not take into account the particular circumstances of an AI. AIs should therefore consider the money laundering and terrorist financing risks to which they are exposed and their own circumstances (among others) before taking action on matters to which the FAQs may be relevant. The FAQs are last updated on 30 June 2022. To access the latest version of the FAQs, please see here.

HKMA issues sound practices for payment operations

Simon Deane and Natalie Chan

In response to an increasing number of payment-related operational incidents reported to the HKMA, the HKMA issued a circular on 28 July 2022 to remind AIs of the importance of maintaining stability in their payment systems and advised that it would step up its surveillance of AIs' payment operations, including undergoing the relevant examinations. The circular also identified a range of sound practices in respect payment operations by AIs:

(i) **Prevention of payment-related operational incidents** – AIs should test any new or enhanced payment system with the same level of rigorousness before any system update or enhancement goes live and closely liaise with group counterparts in advance and during the testing process before any system changes are effected

(ii) **Monitoring of payment operations** - AIs should appoint a dedicated team responsible for ongoing monitoring of payment operations so as to identify any payment irregularities at an early stage and make contingency arrangements

(iii) **Robust business continuity planning** – AIs should have robust and well-defined business continuity planning which should cover a variety of scenarios (including system failures) and the corresponding contingency options to mitigate any residual risk

(iv) **Timely deployment of contingency options** – AIs should have processes to escalate any payment-related operational incidents to management and obtain prompt responses at an early stage

(v) **Periodic testing** – AIs should conduct regular testing of the effectiveness of their business continuity planning so as to identify critical action points and develop practical solutions to expedite recovery

(vi) **Incident reporting and communication to stakeholders** – AIs should identify internal and external key stakeholders in the payment process upfront and include the communication plan in the business continuity planning, so as to facilitate timely communications with their customers and other relevant parties (such as the HKMA) in case of any payment-related irregularities.

To access a full copy of the circular, please see here.

Office of the Privacy Commissioner for Personal Data released guidance note on data security measures for information and communications technology

Simon Deane and Ruby Hui

In the light of the more extensive use of information and communications technology with the growth of hybrid working and hybrid learning, the Office of the Privacy Commissioner for Personal Data ("**PCPD**") released the "Guidance Note on Data Security Measures for Information and Communications Technology" ("**Guidance**") on 30 August 2022. The Guidance sets out recommendations relating to data security measures for data users' information and communications technology ("**ICT**") systems, so that data users can fully comply with the requirements of the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**").

The Guidance briefly discusses the requirements under the PDPO and lists recommended data security measures for ICT in the following areas through the use of case studies and illustration diagrams:

1. data governance and organisation measures: formulation of internal policies on (i) data security risk assessments and (ii) handling data security incidents;
2. risk assessments: (i) risk assessments of data security to test the new systems and applications and (ii) ongoing risk assessments after the launch of such systems and applications;
3. technical and operational security measures: (i) adoption of physical access controls to limit access to locations of ICT assets and (ii) periodic reviews to make sure system settings meet the current requirements;
4. data processor management: (i) assessments to assure engagement of qualified data processors only and (ii) requesting data processors to report all data security incidents promptly;
5. remedial actions in the event of data security incidents: (i) termination of affected information and communication systems promptly where practicable and (ii) informing the PCPD and other law enforcement agencies or regulators, where applicable, in a timely manner;
6. monitoring, evaluation and improvement: data users may engage external experts to monitor compliance with the data security policy and evaluation of the effectiveness of the data security measures regularly; and
7. recommendations about data security measures for Cloud Services, "Bring Your Own Device" and Portable Storage Devices.

To access a full copy of the Guidance, please see here.

Want to know more?

Teresa Lau
Partner
teresa.lau@deacons.com
+852 2825 9701

Erica Wong
Partner
erica.wong@deacons.com
+852 2825 9418

Simon Deane
Consultant
simon.deane@deacons.com
+852 2825 9209

The information contained herein is for general guidance only and should not be relied upon as, or treated as a substitute for, specific advice. Deacons accepts no responsibility for any loss which may arise from reliance on any of the information contained in these materials. No representation or warranty, express or implied, is given as to the accuracy, validity, timeliness or completeness of any such information. All proprietary rights in relation to the contents herein are hereby fully reserved.
0922© Deacons 2022