

CHAPTER 9

AUTHORIZATION OF DIGITAL BANKS

Introduction

- 9.1 The MA, pursuant to section 16(10) of the Ordinance, has issued a “Guideline on Authorization of Digital Banks” (the Guideline) which sets out the principles which the MA will take into account in deciding whether to authorize “digital banks” applying to conduct banking business in Hong Kong.¹ The Guideline is subject to review from time to time. This Chapter reproduces the contents of the latest version of the Guideline, but may also incorporate updated information such as changes in certain regulatory guidelines that may not yet have been included in the Guideline.
- 9.2 A “digital bank” is defined as a bank which delivers banking services exclusively or primarily through the internet or other forms of electronic channels.

General

- 9.3 The MA welcomes the establishment of digital banks in Hong Kong. The development of digital banks will promote the application of financial technology and innovation in Hong Kong and offer a new kind of customer experience. In addition, digital banks can help promote financial inclusion as they normally target the retail segment, including the small and medium-sized enterprises (SMEs).
- 9.4 In considering whether to approve or refuse an application for authorization, the MA needs to be satisfied that the minimum criteria for authorization in the Seventh Schedule to the Ordinance are met. Reference should be made to the “Guideline on Minimum Criteria for Authorization” issued by the MA under section 16(10) of the Ordinance for details about the manner in which the MA will interpret these licensing criteria.
- 9.5 For a company applying to set up a digital bank (digital bank applicant), fulfilment of the minimum criteria essentially means that it must have substance and cannot simply be a “concept”, taking advantage of the popularity of new technology. The applicant must have a concrete and credible business plan setting out how it intends to conduct

1 This Chapter does not address the use of websites outside Hong Kong by entities outside Hong Kong to solicit deposits from members of the public in Hong Kong. As mentioned in paragraph 2.6, provided that the deposits were placed outside Hong Kong, the entity concerned would not be taking deposits in Hong Kong and would not be required to be authorized under the Ordinance. However, section 92 of the Ordinance makes it an offence for any person to issue any advertisements, invitations or documents (advertising materials) to members of the public in Hong Kong to make a deposit, even if it is made outside Hong Kong, unless the disclosure requirements in the Fifth Schedule to the Ordinance are complied with. The factors that the MA will take into account in considering whether advertising material for deposits issued over the internet or other technological means is targeted at members of the public in Hong Kong are set out in the Supervisory Policy Manual (SPM) module [TM-E-2](#) “Regulation of advertising material for deposits issued over the internet”.

its business and how it proposes to comply with the authorization criteria on an ongoing basis.

- 9.6 Like conventional retail banks, digital banks should play an active role in promoting financial inclusion in delivering their banking services. Digital banks should endeavour to take care of the needs of their target customers. Digital banks should not impose any minimum account balance requirement or low-balance fees on their customers.
- 9.7 In addition to technology and related risks, a digital bank must attach equal importance to the management of credit, liquidity and interest rate risks. In addition, the MA must be satisfied that the controllers, directors and chief executives of the applicant are fit and proper persons.

Ownership

- 9.8 Since digital banks' banking businesses will include retail banking businesses covering a large segment of retail customers, they are expected to operate in the form of a locally-incorporated bank. This is in line with the established policy of requiring banks that operate significant retail businesses to be locally-incorporated entities.
- 9.9 In addition, it is generally the MA's policy that a person who holds more than 50% of the share capital of a bank incorporated in Hong Kong should be a bank or a financial institution in good standing and supervised by a recognised authority in Hong Kong or elsewhere. If a locally-incorporated digital bank applicant is not owned by such a bank or financial institution, the MA expects the applicant to be held through an intermediate holding company incorporated in Hong Kong, with supervisory conditions imposed on this intermediate holding company. The supervisory conditions to be imposed will normally cover requirements on capital adequacy, liquidity, large exposures, intra-group exposures and charges over assets, group structure, activities undertaken, risk management, fitness and propriety of directors and senior management and the submission of financial and other information to the MA. Accordingly, both financial firms (including existing banks in Hong Kong) and non-financial firms (including technology companies) may apply to own and operate a digital bank in Hong Kong.
- 9.10 The ownership of digital banks is important because they are usually new ventures which can be subject to higher risks in the initial years of operation. It is therefore essential that the parent companies of a digital bank are committed to supporting the bank and are capable of providing strong financial, technology and other support when necessary.

Ongoing supervision

- 9.11 Digital banks will be subject to the same set of supervisory requirements applicable to conventional banks. That said, some of these requirements will be adapted to suit the business models of digital banks under a risk-based and technology-neutral approach. For example, although digital banks will be required to satisfy the same corporate

governance standards as conventional banks, given their technology-driven business models, the board of directors and senior management of digital banks should have the requisite knowledge and experience to enable them to discharge their functions effectively.

Physical presence

- 9.12 A digital bank applicant, if authorized, must maintain a physical presence in Hong Kong, which will be its principal place of business here. This is necessary to provide an office in Hong Kong for interfacing with the MA, as well as with customers to deal with their enquiries or complaints.
- 9.13 Subject to paragraph 9.2, digital banks may establish local branches under section 44 of the Ordinance. They may also maintain local offices provided that the notification requirement under section 45A of the Ordinance is complied with. To facilitate examination and inspection by the MA pursuant to section 55 of the Ordinance, digital banks must keep a full set of their books, accounts and records of transactions which are accessible to the MA.

Technology risk

- 9.14 Technology related risk, especially information security, system resilience and business continuity management, is of vital importance to a digital bank. Security breaches and unauthorized tampering with the systems of the bank could result in financial loss as well as loss of reputation. The general principle is that the security and technology related controls in place should be “fit for purpose”, i.e. appropriate to the type of transactions which the digital bank intends to carry out.
- 9.15 In this connection, a digital bank applicant will be required to engage a qualified and independent expert to perform an independent assessment of the adequacy of its planned IT governance and systems. A copy of this assessment report should be provided to the MA as part of the documents submitted on application. A more detailed independent assessment of the actual design, implementation and effectiveness of its computer hardware, systems, security, procedures and controls should be undertaken and the report of the assessment should be provided to the MA before the digital bank commences operation. The bank should also establish procedures for regular review of its security and technology related arrangements to ensure that such arrangements remain appropriate having regard to the continuing developments in technology.

Risk management

- 9.16 Like conventional banks, a digital bank applicant must understand the types of risk to which it is exposed and put in place appropriate systems to identify, measure, monitor and control these risks. It should be aware that certain types of risk such as liquidity, operational (including protection of customer data) and reputation risk may be accentuated in the case of digital banks because of their nature of operation.

- 9.17 At a minimum, the applicant must go through the eight basic types of risk identified in the risk-based supervisory framework of the MA (i.e. credit, interest rate, market, liquidity, operational, reputation, legal and strategic risk), analyse to what extent it will be subject to these risks as a digital bank and establish appropriate controls to manage these risks.

Business plan

- 9.18 A digital bank must be able to present a credible and viable business plan which strikes an appropriate balance between the desire to build market share and the need to earn a reasonable return on assets and equity.
- 9.19 While the MA will not interfere with the commercial decisions of individual institutions, it would be a concern if a digital bank planned to aggressively build market share at the expense of recording substantial losses in the initial years of operation without any credible plan for profitability in the medium term. Predatory tactics could be detrimental to the stability of the banking sector and could undermine the confidence of the general public in the bank itself. In any case, a digital bank should not allow rapid business expansion to put undue strains on its systems and risk management capability.

Exit plan

- 9.20 As digital banking is a new business model in Hong Kong, the MA will require a digital bank applicant to provide an exit plan in case its business model turns out to be unsuccessful. The purpose of the exit plan is to ensure that a digital bank, should it become necessary, can unwind its business operations, in an orderly manner without causing disruption to the customers and the financial system. In general, an exit plan should cover matters including the circumstances under which the plan will be triggered, the authority to trigger the plan, the channels to be used to repay depositors and the source of funding for making the payments.

Customer protection

- 9.21 A digital bank should treat its customers fairly and adhere to the Treat Customers Fairly Charter. It should observe the standards contained in the Code of Banking Practice issued by the Hong Kong Association of Banks and the DTC Association. It must set out clearly in its terms and conditions what are the respective rights and obligations between the bank and its customers. Such terms and conditions should be fair and balanced to both the bank and its customers. Customers must be made aware of their responsibilities to maintain security in the use of digital banking services and their potential liability if they do not. In particular, the terms and conditions should highlight how any losses from security breaches, systems failure or human error will be apportioned between the bank and its customers.

- 9.22 In this regard, the MA's view is that unless a customer acts fraudulently or with gross negligence such as failing to properly safeguard his device(s) or secret code(s) for accessing the e-banking service, he should not be responsible for any direct loss suffered by him as a result of unauthorized transactions conducted through his account.

Outsourcing

- 9.23 The MA does not object in principle to outsourcing of computer or business operations of a digital bank to a third party service provider, which may or may not be part of the group owning the digital bank. Digital banks should discuss their plans for material outsourcing with the MA in advance. They should demonstrate that the principles in the SPM module on "Outsourcing" ([SA-2](#)) will be complied with. In particular, the MA must be satisfied that the operations outsourced remain subject to adequate security controls, that confidentiality and integrity of customer information will not be compromised and that the requirements under the Personal Data (Privacy) Ordinance and common law relating to customer confidentiality are complied with. The MA should have the right to carry out inspections of the security arrangements and other controls in place in the service provider or to obtain reports from a relevant supervisory authority, external auditors or other experts. The MA must also be satisfied that his powers and duties under the Ordinance (in particular, section 52 relating to the power of control over an institution) will not be hindered by the outsourcing arrangements.

Capital requirement

- 9.24 Digital banks must maintain adequate capital commensurate with the nature of their operations and the banking risks they are undertaking.