Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Asia Pacific news

Gabriela Kennedy *

Mayer Brown JSM, Hong Kong

Keywords:
Asia Pacific
IT/Information technology
Communications
Internet
Media
Law

ABSTRACT

This column provides a country-by-country analysis of the latest legal developments, cases and issues relevant to the IT, media and telecommunications industries in key jurisdictions across the Asia Pacific region. The articles appearing in this column are intended to serve as 'alerts' and are not submitted as detailed analyses of cases or legal developments.

1. Hong Kong

Gabriela Kennedy *(Partner), Mayer Brown JSM* (gabriela.kennedy@mayerbrownjsm.com);

Karen Lee *(Senior Associate), Mayer Brown JSM* (karen.hf.lee@mayerbrownjsm.com).

1.1. *Virtual banks – new reality welcomed by the Hong Kong Monetary Authority*

1.1.1. *Introduction*

A virtual bank is defined as "a company which delivers banking services primarily, if not entirely, through the internet or other electronic delivery channels".[1] The Proposed 2018 Guideline is intended to supersede the previous Guideline on Authorization of Virtual Banks as issued by the HKMA in 2000 ("**2000 Guideline**"). With virtual banking still in its infancy, the HKMA adopted a more cautious approach in the 2000 Guideline by simply stating that it would "not object to the establishment of virtual banks in Hong Kong provided they satisfy the same prudential criteria that apply to conventional banks".[2] In contrast, the HKMA is now actively encouraging the establishment of virtual banks in the Proposed 2018 Guideline.

Almost two decades have passed since the 2000 Guideline was issued, and the appetite for technology on the part of consumers has evolved with consumers now demanding more efficient banking solutions. Fintech is the latest buzzword amongst the industry, and if Hong Kong does not want to be left behind, it must step up and make virtual banks more accessible, particularly to small and medium sized enterprises ("**SMEs**"). However, a balance needs to be struck between enabling more players to enter the virtual banking market, and offering the right consumer protection.

1.1.2. *2018 Guideline – what is different?*

The Proposed 2018 Guideline sets out the principles that the HKMA will take into account in deciding whether to authorise a virtual bank in Hong Kong. Many of the existing principles stipulated in the 2000 Guideline remain applicable, such as the requirement for a virtual bank to have a concrete and credible business plan and the importance of risk management. However, some key changes introduced in the Proposed 2018

* Mayer Brown JSM, 16th–19th Floors, Prince's Building, 10 Chater Road Central, Hong Kong.
E-mail address: gabriela.kennedy@mayerbrownjsm.com.
For further information see: www.mayerbrown.com.

[1] http://www.hkma.gov.hk/eng/key-information/press-releases/2000/20000505-3.shtml.

[2] Ibid 1.

https://doi.org/10.1016/j.clsr.2018.02.005
0267-3649/

Guideline will open the door to new virtual bank operators. In brief, some of these changes include the following.

1.1.2.1. *Ownership*. Under the 2000 Guideline, a virtual bank could only be established by converting or upgrading a locally incorporated authorised institution into a virtual bank (i.e. a bank, a restricted licence bank or a deposit-taking company). The virtual bank also had to be at least 50% owned by a well established bank or other authorised institution which had good standing and the requisite experience.

In contrast, the Proposed 2018 Guideline does not require a bank or financial institution to own 50% or more of the shares in a virtual bank applicant, so long as the owner is a holding company incorporated in Hong Kong. Such holding company will be subject to supervisory conditions, including requirements on minimum capital and the submission of certain information to the HKMA. In short, technology companies and any other businesses established in Hong Kong will be able to own and operate a virtual bank.

1.1.2.2. *Capital requirement*. Under the 2000 Guideline, virtual banks had to maintain a minimum share capital of HK$300 million. Under the Proposed 2018 Guideline, virtual banks will simply be required to maintain adequate capital that is commensurate with their operations and banking risks. This provides greater flexibility to virtual bank applicants, and allows the HKMA to determine on a case-by-case basis the capital adequacy of each applicant.

1.1.2.3. *Supervision*. In light of the removal of restrictions on the ownership and capital requirements for virtual banks, there is a new principle requiring virtual bank applicants to be subject to the same supervisory requirements that apply to banks. Some adjustments will need to be made to take into account the different nature of virtual banks compared with a conventional one.

1.1.2.4. *Physical presence*. Whilst the Proposed 2018 Guideline expressly states that no physical branches are expected to be established by virtual banks, it must maintain a physical office in Hong Kong as its principal place of business.

1.1.2.5. *No minimum account balance*. In order to reflect the aim of making virtual banks more inclusive and accessible to SMEs and individuals, the Proposed 2018 Guidelines prevents virtual banks from stipulating a minimum account balance or imposing low-balance fees on their customers.

1.1.2.6. *Exit plan*. Virtual banks must have in place an exit plan that causes the least amount of disruption to its customers. This is seen as a key requirement under the Proposed 2018 Guideline in light of the potential risks in virtual banking.

1.1.3. *Cybersecurity and outsourcing*

Cybersecurity has dominated the HKMA agenda in recent years, and is likely to continue to be a top priority in relation to virtual banks. Maintaining a high level of cybersecurity will not only provide increased protection to customers, but also increase the public's trust and confidence in virtual banking. The Proposed 2018 Guideline requires virtual bank applicants to obtain an independent and expert assessment report of their IT systems, which must be provided to the HKMA. A regular review of its systems and security must also be carried out by the applicant, taking into account any changes in technology.

In addition, if the virtual bank applicant wants to use third party service providers to assist with their operations, then it must discuss its outsourcing plan with the HKMA beforehand. The virtual bank applicant must ensure that its outsourced service provider is subject to adequate security controls, that customer information will remain secure and confidential and in compliance with the Personal Data (Privacy) Ordinance (Cap. 486). The HKMA will also have the right to scrutinise the outsourced service provider's security measures.

1.1.4. *Takeaway*

The Proposed 2018 Guideline opens the gateway for technology companies to tap into the financial market in Hong Kong. However, caution still needs to be exercised to ensure that sufficient cybersecurity measures are in place, and outsourcing arrangements do not leave virtual banks vulnerable to security breaches or liability. Strong outsourcing contracts need to be entered into to ensure that minimum security measures are maintained and appropriate indemnities are included to shift some of the risk and liability to the service provider. However, virtual banks will still be ultimately responsible to the HKMA and its customers in the event of any wrongdoing or security breaches concerning the virtual bank's service provider.

The Proposed 2018 Guideline is open for public consultation until 15 March 2018, following which the HKMA will issue a revised version.

2. China

Gabriela Kennedy *(Partner), Mayer Brown JSM (*gabriela.kennedy@mayerbrownjsm.com*);*

Qi Chen *(Associate), Mayer Brown LLP (*qchen@mayerbrown.com*).*

2.1. *China issues new standards on Personal Information Security*

China's National Information Security Standardization Technical Committee (NISSTC) released the final draft of its "Information Security Technology – Personal Information Security Specification" ("PI Specification") on 29 December 2017. The PI Specification will come into effect on 1 May 2018.[3] For an analysis of the December 2016 draft version of the PI Specification, please see https://m.mayerbrown.com/files/Publication/3972eec0-4dc2-4638-9a6a-e758b38eb273/Presentation/PublicationAttachment/1a80f585-ea34-49b9-83cd-ec27c24535e0/161228-PRC-Cybersecurity-DataPrivacy-TMT.pdf.

The PI Specification provides guidance on the collection, storage, use, transfer and disclosure of personal information.

[3] A Chinese version of the PI Specification can be accessed at http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=4FFAA51D63BA21B9EE40C51DD3CC40BE.