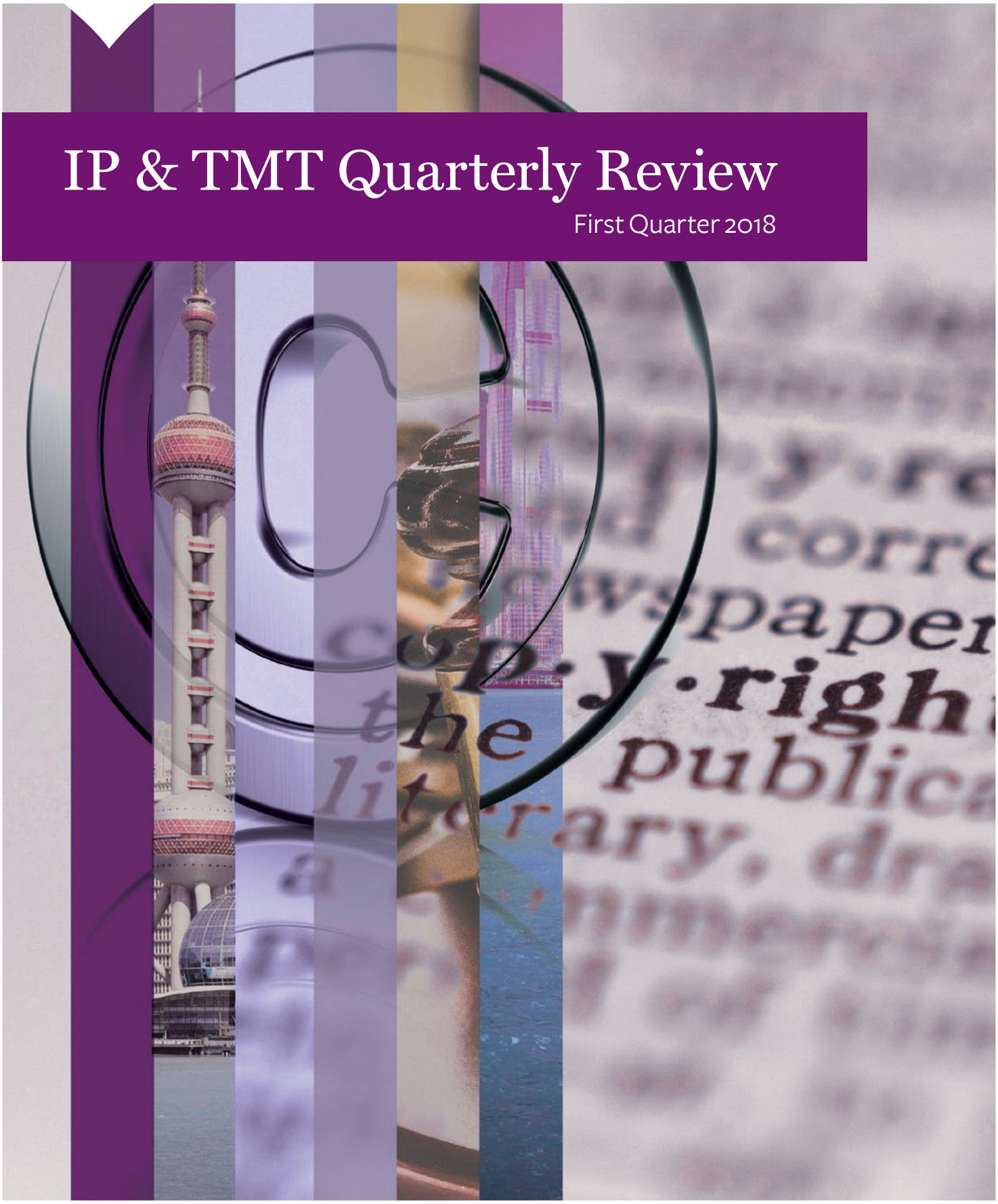
MAYER·BROWN
JSM

IP & TMT Quarterly Review

First Quarter 2018



www.mayerbrownjsm.com

Contents

Key: Click to Navigate

Intellectual Property

By Benjamin Choi, Partner, Mayer Brown JSM, Hong Kong
Hester Qiu, Head of Agency, Mayer Brown JSM, China

China Unveils Plan to Restructure State Intellectual Property Office

On 17 March 2018, the 13th People's National Congress ("**NPC**") approved the State Council's proposal to restructure China's State Intellectual Property Office ("**SIPO**") as part of a more general overhaul of government ministries. The proposal contemplates the following major changes:

A new SIPO will be set up and will be responsible for:

1. Patent examination, registration and administration as originally regulated by SIPO;
2. Trademark examination, registration and administration as currently managed and administered by the State Administration of Industry and Commerce ("**SAIC**");
3. Registration and administration of geographic indicators as currently managed and administered by the General Administration of Quality Supervision, Inspection and Quarantine ("**GAQSIQ**");
4. Providing general guidance to patents and trademarks enforcement agencies; and
5. Facilitating the establishment of a comprehensive system to reinforce protection of intellectual property rights ("**IPR**").

A new State Administration for Market Supervision ("**SAMS**") will be established, taking over the responsibilities of, among others, SAIC and GAQSIQ. SAIC (including its subordinates, namely the China Trademark Office ("**CTMO**") and the Trademark Review and Adjudication Board ("**TRAB**")) and GAQSIQ will no longer exist after the restructuring.

The Market Supervision & Comprehensive Law Enforcement Teams as subordinates to the SAMS will become the trademark and patent enforcement agency.

The new SIPO and the patents and trademarks enforcement agency will be supervised by SAMS.

The proposal intends to consolidate the administration of trademarks and patents and to streamline the enforcement of IPR. The aim of the restructuring is to achieve a more systematic system for the management and protection of IPR. A simpler and more transparent IPR regime may also lead to a decrease in operating costs for technology companies in China.

Currently, there are 2 major routes to pursue IPR infringement claims in China, namely through court proceedings or administrative enforcement. IPR owners normally only consider court proceedings for more serious and egregious cases which justify the time and costs involved, or in cases where administrative enforcement is not feasible because the case presents less clear cut legal issues. Following the proposed restructuring, the SAMS will carry out patent and trademark enforcement actions thus rendering administrative enforcement more efficient. The shared view amongst the legal community is that administrative enforcement will now become a more popular route to pursue infringement claims in China.

To someone more familiar with the PRC hierarchy, the new SIPO is considered to have been elevated one level up to a General Administration within the State Council structure, which is somewhat closer to a Ministry level agency – this reflects the strong dedication of the PRC Government to protect and enforce IPR.

Such scale of change will naturally bring along uncertainties. For instance, copyright administration and enforcement, which is currently regulated by the National Copyright Administration, as well as trade secret protection (under SAIC), plant variety protection, already divided between two agencies (Agriculture, Forestries) within the SIPO are noticeably not addressed or specified as falling within the remit of the new SIPO. No time frame has been set yet for the commencement or completion of this proposed restructuring, but there is every expectation that the restructuring will be officially announced by the Government in the coming months. Stay tuned for further news! ◆

Intellectual Property

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong
Amita Haylock, Counsel, Mayer Brown JSM, Hong Kong

A Case of Shared Goodwill?

Introduction

A recent judgment of the Hong Kong High Court where summary judgment for trade mark infringement and passing off was granted to an American medical charity against its former licensee, brought into the spotlight the issue of goodwill in a trade mark in the context of a licensing arrangement[1].

Background

The case involved Operation Smile (the "**Plaintiff**"), an American charity, and its former licensee, a Hong Kong regional foundation, who was incorporated and operated as "Operation Smile – China Medical Mission Ltd" (the "**Defendant**"). The Plaintiff's essential charitable purpose is to provide medical treatment to children born with cleft palate or other lip defects in countries with limited medical resources.

Prior to 2014, the Plaintiff and the Defendant cooperated under an informal licence and consent arrangement. In 2014, the Plaintiff announced its intention to launch a formal trade mark licensing program covering all of its regional foundations worldwide. The Defendant refused to enter into a formal agreement, and as a result the Plaintiff terminated the Defendant's right to use the trade mark "OPERATION SMILE" and its variants. Post-termination, the Defendant then changed its name to Beam International Foundation Ltd, but continued to use "operationsmile" and "opsmile" as domain names which resolved to its website.

The Defendant further continued to use the mark "OPERATION SMILE CHINA" in English and Chinese.

The Plaintiff successfully registered variations of its trade marks in Hong Kong including "OPERATION SMILE" and "OPERATION SMILE and Device". However, the Plaintiff did not apply to register

1 *Operation Smile, Inc. v Beam International Foundation Ltd [2018, 1 HKLRD 120]*

"OPERATION SMILE" in Chinese characters even though the Plaintiff used this mark in Hong Kong and Mainland China. Post-termination, the Defendant attempted to register the marks "OPERATION SMILE CHINA MEDICAL MISSION and Device" in English and Chinese respectively.

Even though the Defendant admitted to using the Plaintiff's trade marks post-termination, it argued that it shared goodwill in the trade marks with the Plaintiff.

Judgement

The court held that before moving from the charge of the Plaintiff, the Defendant had been no more than the Plaintiff's *alter ego*, enjoying its goodwill, name and trade marks with its consent. After the termination of the relationship between the Plaintiff and Defendant, the Defendant was in fact trying to establish an ego of its own, a separate identity unconnected to the Plaintiff.

Despite the change of its company name, the Defendant continued to use the Plaintiff's name as part of its domain name and as part of its online identity and the court held that this amounted to a misuse constituting an act of deceit on potential donors and sponsors. Applying the guidance set out in *Reckitt & Colman Ltd v Borden Inc [1990] 1 All ER 873*, the Judge had no hesitation in finding that the Defendant's acts amounted to passing off.

The Judge also held that the similarity to the Plaintiff's trade marks, and in some respects, the identical reproduction of the Plaintiff's registered trade marks in Hong Kong would likely confuse the public into thinking that the Defendant was related to the Plaintiff.

The Plaintiff was granted *inter alia* an injunction to restrain the Defendant from infringing the Plaintiff's registered trade marks and using the domain names and an order for the Defendant to withdraw its trade mark applications as well as damages for wrongful acts of passing off and trade mark infringement.

Conclusion

This case serves as a reminder that it is always best to have written licence arrangements in place which set out the rights and intention of the parties (for example whether the goodwill from the use of the mark by the Defendant accrued to the Plaintiff), in a clear and precise manner. This would have saved both parties substantial legal costs. ◆

Intellectual Property

By Rosita Li, Partner, Mayer Brown JSM, Hong Kong
Iris Mok, Senior Associate, Mayer Brown JSM, Hong Kong

House of Rules: Cannot be Too Slow or Too Quick!

On 7 March 2018, Deputy High Court Judge Joseph Kwan handed down a decision dismissing the application of Duracell U.S. Operations, Inc. ("**Duracell**") for default judgment against Matsushima Electric (H.K) Co. Limited ("**First Defendant**") and other defendants (collectively "**Defendants**") in a claim for trademark and copyright infringement and passing off. What appeared to be a straight-forward case in fact involved interesting procedural aspects which were described as a "procedural tripwire for the unwary" by DHCJ Marlene Ng in a previous case, and thus deserves closer scrutiny by litigants and practitioners alike.

The Plaintiff, Duracell, sells batteries in Hong Kong and uses its DURACELL mark on both batteries and their packaging. Duracell claimed that the First Defendant supplied "DURACELL" batteries under counterfeit packaging. It therefore obtained an Anton Piller Order and an interim injunction against some of the Defendants.

Under the Rules of the High Court, the Defendants must file an Acknowledge of Service ("**AS**") within the stipulated time after service of the Writ. However, the Defendants failed to do so and Duracell obtained an Unless Order against the Defendants to file the AS by 25 October 2017, failing which the Defendants would be debarred from filing the AS. Instead of filing the AS by the deadline imposed by the Unless Order, the Defendants applied to Court for leave to file a defence. The application was dismissed as being misconceived as the Defendants had been debarred from filing the AS, and therefore were not entitled to file a defence. The Defendants then took out another application on 8 November 2017 for leave to file the AS ("**November Summons**").

It was against this background that Duracell applied on 9 November 2017 for default judgment against the Defendants.

When the Defendants failed to file the AS by the deadline stipulated in the Unless Order, the only and immediate consequence was that they would be sanctioned by the Unless Order and debarred from filing the AS. Any subsequent application to the Court for a time extension to file the AS would not succeed as the Defendants no longer had any right to file the AS. To reinstate such right, the Defendants would have needed to apply for relief from sanction pursuant to Order 2, rule 4 of the Rules of the High Court. This procedure has often been misunderstood by practitioners in the past.

The wording used in the November Summons was simply to seek leave to file the AS, which led to the argument on whether the November Summons was an application for time extension, or for relief from sanction. Although the November Summons could have been drafted in a more unequivocal manner, DHCJ Kwan concluded that the Defendants made an appropriate application for relief in view of the express reference to Order 2, rule 4 and the Unless Order in the Summons.

The next issue that the Court had to consider was whether relief should be granted to the Defendants by lifting the bar to file the AS. The Court considered all circumstances of the case, particularly the following:

(1) *Whether the grant of relief is in the interests of the administration of justice*

As one of the factors to be taken into account, the Judge considered at length whether the Defendants had an arguable defence.

Duracell sold its batteries under two channels: to wholesale/retailer customers, and at a lower price to OEM customers strictly for use in their manufactured products. The OEM customers were naturally prohibited from selling the batteries in retail or wholesale. Duracell pleaded that the Defendants acquired batteries from OEM customers, repackaged and then sold them to retail/wholesale customers. Duracell claimed trademark infringement, passing off and copyright infringement against the Defendants.

For the trademark infringement claim, Duracell relied on a European case law and argued that the repackaging of the batteries which bore its trademarks amounted to an infringement of its rights. The Defendants relied on section 20 of the Trade Marks Ordinance ("**TMO**"), which provides a defence to infringement if the goods have been put on the market anywhere in the world under that trademark by the owner, unless the condition of the goods has been changed. The Defendants contended that as the batteries had been put on the market elsewhere in the world by Duracell, and there was no indication that the condition of the batteries had been changed, they were entitled to rely on the defence. Senior Counsel for the Defendants also pointed out that the European case relied on by Duracell was based on Article 7 of an European directive which was fundamentally different from section 20 of the TMO.

As for the claim for passing off, Duracell alleged that the Defendants passed off the batteries as genuine products and made misrepresentations that they were the authorised dealers of Duracell. The Defendants responded that there was no misrepresentation as the products were indeed genuine and that the alleged misrepresentation as authorised dealers was unsupported by evidence.

Duracell also claimed infringement of the copyright in its batteries' packaging. The Defendants' defence was that Duracell had failed to establish copyright subsistence (which was acknowledged by Duracell in its Anton Piller order application), and that Duracell had knowledge of and allowed the Defendants to continue their business for almost 20 years and was therefore now estopped from claiming against them.

Having considered the above without going into the merits, and as the application of the European authority relied on by Duracell had not yet been tested in Hong Kong (in light of the different wordings between Article 7 of the European directive and section 20 of the TMO), the Judge concluded that the Defendants had an arguable defence.

Intellectual Property Cont'd

(2) Whether the failure to comply was intentional

The Defendants contended that the failure to comply with the Unless Order was due to the wrong advice given by their solicitors, who were under the misapprehension that they could still defend the action by seeking time extension to file the defence. The Defendants also gave explanations supported by contemporaneous correspondence indicating that they were sincerely considering whether to contest the action at the time they were required to file the AS. After having considered all of the circumstances, the Judge concluded that the Defendants' failure to comply, was neither intentional nor an attempt at tactical gain.

Considering that Duracell would be able to get default judgment against the Defendants if the Defendants were barred from defending the Action, and that Duracell would still be at liberty to go to trial or apply for summary judgment at a later stage, the Judge found that the Plaintiff would not be significantly prejudiced if the Judge granted relief to the Defendants. Accordingly, he ordered the Defendants to be relieved from the sanction imposed by the Unless Order.

The Judge also considered whether Duracell was entitled to apply for default judgment. Having computed the deadlines imposed under the Rules of the High Court, the Judge came to the conclusion that Duracell took out the application for default judgment prematurely before the expiry of the deadline to file the defence, and therefore did not satisfy the requirement of Order 19 rule 7. As a result, the default judgment application was dismissed.

The implication of the failure for the parties to conduct their cases in accordance with the procedural rules was significant. The failure to comply with the rules resulted in a waste of substantial time and costs on arguing procedural issues in a 2-day hearing. Further, the Defendants were liable for Duracell's costs for the November Summons for relief from sanction, and Duracell was liable for the Defendants' costs for its dismissed default judgment application.

Takeaway

The case serves as a lesson to legal advisors and litigants that non-adherence to procedural rules can cost parties dearly. Neither party was the winner; the parties incurred substantial time and costs in an early stage of the proceedings to argue procedural issues, which was clearly undesirable. The situation could have been avoided by strict compliance with court deadlines and the relevant court procedures. Further, the Defendants would have lost their opportunity to defend the case if no relief was granted to the Defendants to file a defence. Parties to a litigation must therefore comply with procedural rules at all times to avoid such dire consequences. ◆

Data Privacy and Cybersecurity

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong
Qi Chen, Associate, Mayer Brown LLP, Chicago

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, 2018.2 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. It also sets out guidance on expected data breach incident responses and enterprise standards for safeguarding and processing of data. While the PI Specification is voluntary and not legally binding, it is likely that Chinese regulators will take into account breaches of the PI Specification when enforcing cybersecurity obligations imposed by various laws, including the Cybersecurity Law that has been in effect since 31 May 2017.

Definition of Personal Information and the Data Protection Principles

The PI Specification defines "personal information" as any information, recorded in electronic or other form, and either alone or together with other information can identify a natural person or a natural person's activities. According to the Examples of Personal Information given in Appendix A of the PI Specification, personal information can either be information that 1) can be used to "identify" a person due to its special

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

Data Privacy and Cybersecurity Cont'd

characteristics or 2) information that is "associated" with an identified person, produced as a result of that person's activities (e.g., geo-location, call logs, browser history). Furthermore, information created from the processing of personal information is also personal information (so long as the created information still fits under the definition provided by the PI Specification) and is treated in the same way as the personal information collected. The definition of personal information is reminiscent of the definition in the December 2016 draft in that it includes information that is not recognised as personal information in other jurisdictions.

The PI Specification also provides a definition for "sensitive personal information", defined as personal information, relating to a person's reputation or physical and mental health, which can harm a person, property, or easily lead to damage or discriminatory treatment. Sensitive personal information is subject to additional protection under the PI Specification as discussed in more detail below.

The PI Specifications are reminiscent of the Organisation for Economic (OECD) privacy principles, such as the use limitation principle and the accountability principle, and such principles are reflected in the guidance set out for the collection, use and sharing of personal information by personal data controllers. Curiously, while the draft PI Specification included the data quality principle - that personal data should be relevant to the purpose for which they are to be used, and to the extent necessary for those purposes, should be accurate, complete and kept up-to-date – the published PI Specification no longer includes this principle.

Collection, Use and Storage of Personal Information

The requirements for the collection, use, and storage of personal information are very similar to those adopted in other jurisdictions around the world. For example, the PI Specification requires the personal data controller to notify personal data subjects of the type of personal information being collected and the rules of collection (purpose, collection method and frequency, etc.), and to obtain the personal data subject's consent prior to collecting the personal information. The collection of sensitive personal information can only be made with explicit consent.

When storing personal information, personal data controllers are required to perform de-identification of all personal information immediately after collection and to store the de-identified information separately from information that can be used to re-identify the information. Storing sensitive personal information requires additional security measures such as encryption. Different measures are required for the storage of biometric information, such as storing only a summary of the information.

Unless necessary to achieve the purpose for which the personal information was collected, personal data controllers should avoid using information containing the clear identity of the personal data subjects. For example, where secondary user profile information is sufficient for the purposes, the primary information used to create the user profile should be avoided.

Data controllers are required to provide data subjects access to their personal information and provide a way for the personal data subjects to correct or complete their personal information. Upon the data subject's request, the data controller is also required to provide a copy of basic personal information and personal information relating to personal status, health, education and work history to the data subject or a designated third party.

Privacy Policy

All data controllers are required to devise and publish a privacy policy that includes information such as: 1) contact details and basic information on the data controller; 2) the purposes and particulars of collection personal information; and 3) the data controller's cyber security capabilities relating to the personal data being collected. The PI Specification includes a model privacy policy with drafting notes. For example, in the

collection of personal information section, the drafting notes explain that if collecting ID card or passport information, a specific section should be devoted to the type and purpose of collecting information relating to such government approved identification documents.

Transfer of Personal Information

While the PI Specification does not include a definition of data processors, it does have some limited provisions regarding the transfer of personal information that would cover a data controller/data processor relationship.

Before outsourcing the processing of personal information (always with the personal data subject's consent), the data controller must evaluate the party being entrusted with the processing of personal information ("Processor"), in particular the security of the personal information being transmitted, and the cybersecurity capabilities and standards adopted by the Processor to protect the personal information entrusted to it. Personal data controllers are now required to supervise Processors through contractual provisions and audits.

In turn, Processors are required to follow the personal data controller's directions and may not further delegate the processing of the personal information without the personal data controller's express authorisation. They have an obligation to report security incidents promptly to data controllers as well as instances where they fail to follow the data controller's directions.

Other than the outsourcing of the processing of personal information, data controllers are generally not allowed to share, transfer (except in cases involving the sale, merger, or reorganisation of the personal data controller) or publicly disclose personal information. The PI Specification lists certain exceptions to the general rule, such as where required by law. In cases where sharing, transferring or publicly disclosing the personal information become necessary, the personal data controller must evaluate the risk to data security, notify the relevant personal data subjects and bear responsibility for any harm caused by such actions.

Cybersecurity Requirements

Data controllers are required to formulate a cybersecurity incident response plan and perform emergency response training and drills at least annually.

The draft PI Specification contained a requirement to report any cyber incident to the National Computer Network Emergency Response Centre within 24 hours if the data breach involved the personal information of more than ten thousand individuals or sensitive personal information of more than one thousand individuals. This is no longer a requirement in the published PI Specification. In the event of a cybersecurity incident, the data controller is required to: i) record the relevant information regarding the incident; ii) evaluate the possible harm and take the necessary steps to stabilise the situation and eliminate any danger; and iii) report the incident in accordance with the "National Cybersecurity Incident Response Plan"[3] (Response Plan). While the Response Plan does require the affected organisations to report the cybersecurity incident in a timely manner, there are no specifics in the Response Plan relating to the entity to whom the report should be made or the manner in which such reporting is to be done (see clause 4.1 of the Response Plan).

In addition, the data controller is required to notify the affected data subjects of the cybersecurity incident. Such notice should include: the nature of the incident and its impact; the steps taken or that are to be taken to address the incident; advice on how to reduce the risk to the data subjects; assistance to be provided to the data subjects; how to contact the responsible persons and departments within the organisation.

3 Published on 27 June 2017, a Chinese version of the document can be accessed here http://www.cac.gov.cn/2017-06/27/c_1121220113.htm

Data Privacy and Cybersecurity Cont'd

New Enterprise Requirements for Data Controllers

The PI Specification also includes certain enterprise requirements on data controllers. Data controllers must ensure that only the minimum numbers of personnel who are strictly necessary for the purposes of processing personal information are granted the rights to access such personal information. Security management, data processing and auditing should be segregated and assigned to different personnel within the organisation.

The data controller must appoint a person in charge of personal data security that has overall leadership responsibility within the organisation. Such person will oversee the overall persona data security planning, training, and the development of the enterprise privacy policy and security impact assessment. For enterprises that 1) process personal data and have over 200 employees, or 2) handle personal data of more than 500,000 people, a dedicated person should be in charge of personal data security.

Conclusion

The PI Specification provides the first detailed standards relating to the protection of personal information since the enactment of China's Cybersecurity law. Enterprises that collect or process personal information would be well advised to review these standards against their current business practices to help them comply with the Cybersecurity law and other related laws and regulations. ◆

HONG KONG

Virtual Banks

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong
Karen H.F. Lee, Senior Associate, Mayer Brown JSM, Hong Kong

Virtual Banks – New Reality Welcomed by the Hong Kong Monetary Authority

On 6 February 2018, the Hong Kong Monetary Authority ("**HKMA**") issued a revised Guideline on Authorization of Virtual Banks for public consultation ("**Proposed 2018 Guideline**")[4]. This is part of the seven initiatives unveiled by the HKMA in September 2017 to lead the way in "smart" banking[5].

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[6]". 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[7]". 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 buzz word 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

4 http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/g_Authorization_of_Virtual_Banks.pdf
5 http://www.hkma.gov.hk/eng/key-information/press-releases/2017/20170929-3.shtml
6 Ibid 4
7 http://www.hkma.gov.hk/eng/key-information/press-releases/2000/20000505-3.shtml

Virtual Banks Cont'd

between enabling more players to enter the virtual banking market, and offering the right consumer Ibid 1. protection .

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

(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 owned at least 50% 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.

(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.

(3) *Supervision*

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

(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.

(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.

(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.

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 its 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 the Personal Data (Privacy) Ordinance (Cap. 486) will be complied with. The HKMA will also have the right to scrutinise the outsourced service providers security measures.

Takeaway

The Proposed 2018 Guideline opens the gateway for technology companies to tap into the financial market in Hong Kong. But 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 was open for public consultation until 15 March 2018. The HKMA will soon issue a revised version. ◆

Contact Us

GABRIELA KENNEDY
Partner
+852 2843 2380
gabriela.kennedy@mayerbrownjsm.com

ROSITA LI
Partner
+852 2843 4287
rosita.li@mayerbrownjsm.com

BENJAMIN CHOI
Partner
+852 2843 2555
benjamin.choi@mayerbrownjsm.com

AMITA HAYLOCK
Counsel
+852 2843 2579
amita.haylock@mayerbrownjsm.com

KAREN H. F. LEE
Senior Associate
+852 2843 4452
karen.hf.lee@mayerbrownjsm.com

IRIS MOK
Senior Associate
+852 2843 4263
iris.mok@mayerbrownjsm.com

QI CHEN
Associate
+1 312 701 8735
qchen@mayerbrown.com

HESTER QIU
Head of Agency
+86 10 6599 9308
hester.qiu@mayerbrownjsm.com

About Mayer Brown JSM

Mayer Brown JSM is part of Mayer Brown, a global legal services organisation, advising clients across the Americas, Asia, Europe and the Middle East. Our geographic strength means we can offer local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, CAC 40, DAX, Hang Seng and Nikkei index companies and more than half of the world's largest banks. We provide legal services in areas such as banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; employment and benefits; environmental; financial services regulatory and enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and private clients, trusts and estates.

Please visit www.mayerbrownjsm.com for comprehensive contact information for all our offices.