



MAYER | BROWN

IP & TMT Quarterly Review

First Quarter 2021

The background of the page is a complex, abstract network graphic. It features a dense web of interconnected nodes and lines. The nodes are represented by small, glowing blue and white spheres, while the lines are thin, multi-colored strands in shades of blue, green, yellow, and red. The overall effect is a sense of dynamic connectivity and data flow, typical of a digital or telecommunications network. The colors are vibrant and contrast sharply against the dark blue background.



Contents



2

Arbitration

Hong Kong

ARBITRATION UPDATE: HKIAC RELEASES 2020 STATISTICS

4

Intellectual Property

China

THE SUPREME PEOPLE'S COURT OF CHINA CLARIFIES STANDARDS FOR APPLYING THE DOCTRINE OF REVERSE CONFUSION IN TRADE MARK INFRINGEMENT CASES

7

V-COMMERCE – A NEW PLATFORM FOR COUNTERFEIT GOODS IN MAINLAND CHINA

10

Data Privacy

Southeast Asia

FINDING HARMONY – ASEAN MODEL CONTRACTUAL CLAUSES AND DATA MANAGEMENT FRAMEWORK LAUNCHED

13

Cybersecurity

Singapore and APAC

AFTERMATH OF THE SOLARWINDS CYBER ATTACK – NEW RULES ANNOUNCED IN SINGAPORE AND THE ASIA PACIFIC REGION

19


Technology

Hong Kong

ONLINE DISPUTE RESOLUTION DURING COVID-19 IN HONG KONG

22

Contact Us



HONG KONG

Arbitration

Arbitration Update: HKIAC Releases 2020 Statistics

By **Amita Haylock, Partner**
Mayer Brown, Hong Kong

Jacqueline W.Y. Tsang, Associate
Mayer Brown, Hong Kong

On 9 February 2021, the Hong Kong International Arbitration Centre (“**HKIAC**”) released its latest case statistics for 2020. The statistics illustrate a record year for the HKIAC in terms of number of cases and total amount in dispute.

In 2020, the HKIAC received 318 new arbitration cases, representing a 3.2% increase compared to the previous year. This is also the highest number of cases recorded in the past decade. Out of the 318 new arbitration cases, 203 were administered by the HKIAC under the HKIAC Administered Arbitration Rules, the UNCITRAL Arbitration Rules and the HKIAC Electronic Transaction Arbitration Rules.

The total amount in dispute also increased to HK\$68.8 billion. The types of cases administered by the HKIAC remain diverse, with the top three types of cases being international trade or sale of goods (27%), maritime (18.6%) and corporate (18.3%).

Arbitrations filed with the HKIAC continue to be international in nature. 72.3% of the total number of arbitrations have at least one party which was not from Hong Kong. 31.8% of the arbitrations submitted to HKIAC in 2020 involved no Hong Kong party at all. The geographical origins or nationalities of the parties extended across 45 different jurisdictions. The top five geographical origins or nationalities were Hong Kong, Mainland China, the British

Virgin Islands, the United States and the Cayman Islands.

The vast majority of the arbitrations (99.4%) were seated in Hong Kong. Disputes were subject to 12 different governing laws. Hong Kong law remains the most commonly selected governing law, followed by English, Chinese, California and New York laws.

117 hearings were hosted by the HKIAC, despite the COVID-19 pandemic. 80 of these hearings were fully or partially virtual hearings and 37 were in-person hearings that were held at the Hong Kong premises of the HKIAC.

In our previous article published in our [Fourth Quarter 2019 IP & TMT Quarterly Review](#), we discussed the new arrangement facilitating cross-border arbitration between Mainland China and Hong Kong – “*The Arrangement Concerning Mutual Assistance in Court-ordered Interim Measures in Aid of Arbitral Proceedings by the Courts of the Mainland and the Hong Kong Special Administrative Region*” (the “**Arrangement**”). The Arrangement came into force on 1 October 2019.

Under the Arrangement, Chinese courts can now grant interim measures in favour of Hong Kong-seated arbitrations, when administered by qualified institutions (including the HKIAC). In 2020, parties

in arbitrations involving Chinese parties utilised the distinct advantage offered by the Arrangement. 22 applications under the Arrangement were processed by the HKIAC. These applications were made to 14 different Mainland Chinese courts to preserve evidence, assets, or conduct. In these applications, the Mainland Chinese courts ordered the preservation of assets valued at RMB4.4 billion in total (approximately HK\$5.23 billion) in 2020.

Conclusion

Through the COVID-19 pandemic, the HKIAC demonstrated continued growth both in the number of arbitration cases and the total amount in dispute. The same trend of increased number of cases was recorded in the 2020 statistics released by The International Chamber of Commerce (ICC) and The China International Economic and Trade Arbitration Commission (CIETAC). This signals a growing confidence in arbitration as an effective means of dispute resolution. The flexible and confidential nature of arbitration also attracts parties to opt for arbitration over litigation. An additional factor is that these international arbitral institutions were able to quickly respond to the pandemic by implementing adaptive measures, such as virtual hearings and online filings.



CHINA

Intellectual Property

The Supreme People's Court Of China Clarifies Standards For Applying The Doctrine Of Reverse Confusion In Trade Mark Infringement Cases

By **Michelle G.W. Yee, Counsel**
Mayer Brown, Hong Kong

Introduction



Trade mark infringement actions have long been an important tool for brand owners to combat copycat brands and counterfeit products. The typical fact pattern for such cases is familiar: a smaller, lesser-known trader seeks to profit from the goodwill and reputation of an established brand owner by using an identical or similar trade mark on their goods or services to mislead consumers into believing that those goods or services originate from or are associated with the established brand owner. The harm caused to the established brand owner by this type of consumer confusion ("traditional" or "forward" confusion) includes diverted profits and damage to their goodwill and reputation, particularly if the infringer's goods and services are of inferior quality.

In recent years, an increasing number of trade mark infringement actions have been brought before the Chinese courts on the

grounds of “reverse confusion”. Reverse confusion turns forward confusion on its head – here, the consumer confuses the goods or services of a smaller, lesser-known brand owner with those of a larger company due to the latter’s later use of an identical or similar trade mark. Whilst reverse confusion could conceivably benefit the smaller brand owner (such as through increased sales from the association with a more reputable company), the larger company’s greater resources and operations could also saturate the market and stifle the smaller trader’s brand.

A recent judgement of the Chinese Supreme People’s Court (“**SPC**”) involving a Chinese handbag manufacturer Shantou Chenghai Jianfa Handbag Craft Factory (汕头澄海区建发手袋工艺厂 (“**Plaintiff**”) and the American fashion brand Michael Kors (“**Defendant**”)¹ provides some guidance on assessing reverse confusion in trade mark infringement cases.

Background

In 1997, the Plaintiff filed an application to register the trade mark **mk** in Mainland China in class 18 covering handbags, sports bags, leather bags, purses and related goods, and the mark was granted registration in 1999 (“**Plaintiff’s Mark**”). The Plaintiff’s Mark has been used on handbags and purses, mainly for export to other countries, and only occasionally for sale in Mainland China. The Defendant entered the Chinese market in 2011 and began selling goods including handbags and bag accessories under the following marks: **mk**, **MK**,  and  (“**Defendant’s Marks**”).

In 2017, the Plaintiff commenced trade mark infringement proceedings against the Defendant before the Hangzhou Intermediate People’s Court on the grounds of reverse confusion, arguing that use of the Defendant’s Marks led consumers to mistakenly believe that the Plaintiff’s goods originate from the Defendant, thereby damaging the Plaintiff’s brand identity and destroying the momentum acquired by the Plaintiff’s Mark in the market. The Defendant argued, amongst other things, that confusion was unlikely given that the two brands target very different consumers. Both the Hangzhou Intermediate People’s Court (at first

instance) and the Zhejiang Province Higher People’s Court (on appeal) found in favour of the Defendant. The Plaintiff then appealed to the SPC.

Likelihood of Confusion Test for “Reverse Confusion” Cases

The SPC affirmed the decision of the Zhejiang Province Higher People’s Court and held that the Plaintiff failed to establish a valid claim of reverse confusion.

The SPC determined that for both forward and reverse confusion cases, the same “likelihood of confusion” test applies, that is, whether an average consumer would be misled as to the origin of the goods or services in question. Factors to be taken into account when applying this test include:

1. whether the registered mark and the alleged infringing mark are identical or similar, and whether the alleged infringing use relates to identical or similar goods/services;
2. circumstances relating to actual use in the market of both the registered mark and the alleged infringing mark;
3. the distinctiveness and reputation of both the registered mark and the alleged infringing mark.

The SPC also noted that the assessment of similarity between the registered mark and the alleged infringing mark (factor 1 above) cannot be undertaken independently of the other two factors. In other words, whether or not the registered mark and the alleged infringing mark are considered to be “similar marks” will depend not only on the visual, phonetic and conceptual similarities between the marks themselves, but also on how the marks are actually used in the market and their reputation amongst consumers.

The SPC’s Findings

The SPC applied the above test to the specific facts of the case and determined that they did not support a finding of reverse confusion. In particular, the SPC found as follows:

¹ Shantou Chenghai Jianfa Handbag Craft Factory v Michael Kors Trading (Shanghai) Company Limited & Michael Kors (Switzerland) International GMBH (2019) 最高法民申6283号.

Mere fact that the parties' respective marks consist of the same two-letter combination insufficient

As the Plaintiff's Mark consists of a simple combination of the two lowercase letters "m" and "k", its distinctiveness mainly stems from the stylised font used, and accordingly the mere fact that the Defendant's Marks also consist of the same two-letter combination does not mean they are identical to the Plaintiff's Mark.

Confusion unlikely due to parties' different market reputation and target consumers


The following circumstances make consumer confusion unlikely:


- the Plaintiff's Mark has mainly been used on products for export, with limited sales and reputation in Mainland China;
- since entering the Chinese market in 2011, the Defendant has extensively used and promoted its products bearing the Defendant's Marks, causing Chinese consumers to exclusively associate the Defendant's Marks with the Defendant;
- the Defendant's Marks are often used in conjunction with the Defendant's house mark "MICHAEL KORS";
- the parties' products are sold at different price points through different sales channels with different target consumers; and
- consumers tend to pay closer attention when purchasing pricier goods such as those of the Defendant.

Bad faith also relevant


In addition to considering the likelihood of consumer confusion, the SPC also took into account the intent behind the parties' actions.

The SPC determined that there was no bad faith on the part of the Defendant – it was reasonable for the Defendant to adopt "MK" as an acronym for its house mark "MICHAEL KORS", and the fact that the Defendant often used the Defendant's Marks in conjunction with "MICHAEL KORS" clearly indicated they had no intention to freeride on the Plaintiff's reputation.

The SPC also found that there was bad faith on the part of the Plaintiff. Since 2015, the Plaintiff has been attempting to register trade marks that imitate the Defendant's Marks, including  and

. The SPC criticised the Plaintiff for actively seeking to create consumer confusion through its attempts to copy the Defendant's Marks.

Caveat

Despite its finding that no infringement occurred, the SPC did not deliver a total victory to the Defendant. The SPC upheld the Zhejiang Province Higher People's Court's decision in its entirety, including the lower court's order for the Defendant to refrain from using the marks **mk** and **MK**, and to always use **MK** and  together with "MICHAEL KORS" or other distinguishing elements to avoid confusion with the Plaintiff's Mark.

Conclusion

This SPC decision confirms that the same "likelihood of confusion" test would be applied for both forward and reverse confusion cases. This is not an unreasonable approach, as similar factors could give rise to both types of confusion (for example, both forward and reverse confusion would be more likely if there is an overlap between the parties' target consumers and trade channels).

The SPC's choice to take into account the Plaintiff's bad faith should also be uncontroversial, as the Plaintiff should not be allowed to claim that its brand identity has been damaged by confusion with the Defendant's Marks on the one hand, whilst actively creating more consumer confusion by copying the Defendant's Marks on the other.

The more controversial aspect of the decision is the SPC's conclusion that the Zhejiang Province Higher People's Court did not err in ordering the Defendant to refrain from using the Defendant's Marks alone and only to use them in conjunction with "MICHAEL KORS" or other distinguishing elements. The imposition of an obligation on the Defendant to take proactive steps to avoid confusion seems to be inconsistent with the SPC's finding that there was no reverse confusion taking into account various factors such as the parties' different target consumers and trade channels. Given the absence of a precedent system in Mainland China, it is not clear whether such orders will be made in similar reverse confusion cases going forward.

*The author would like to thank **Stephanie Yung**, Trainee Solicitor at Mayer Brown, for her assistance with this article.*

CHINA

Intellectual Property

V-Commerce – A New Platform for Counterfeit Goods in Mainland China

By **Amita Haylock, Partner**
Mayer Brown, Hong Kong

On 5 February 2021, Mainland Chinese short video app company Kuaishou began trading as a publicly listed company in Hong Kong, raising more than HKD 41 billion (USD 5.3 billion) in Hong Kong's largest initial public offering.²

A key revenue driver for Kuaishou is its live-streaming business, in which users buy virtual gifts on the company's platform to gift to streamers. Live-streaming brought in RMB 25.3 billion (USD 3.9 billion) in revenue in the first nine months of 2020, or 62% of the company's total sales.³

Companies such as Kuaishou are at the forefront of Mainland China's booming e-commerce market, which already accounts for around 30% of total retail sales. These companies also operate in the "livestreaming e-commerce" space, otherwise known as "video commerce", or "V-commerce". Typically, goods are promoted and sold through livestreams on the social media channels of 'key opinion leaders' ("KOLs"), on Mainland China's various online shopping malls. Top KOLs have their own shows and appear on livestreams each night, from roughly 8 pm to midnight, selling products such as cosmetics, fashion goods, and food, often at steep discounts.

2 <https://www.bloombergquint.com/business/tiktok-owner-s-no-1-rival-kuaishou-s-mega-ipo-by-the-numbers>

3 <https://www.cnn.com/2021/02/05/kuaishou-ipo-everything-you-need-to-know-about-the-tiktok-rival.html>

V-commerce is not only good business for Mainland China's online sales platforms, but for top KOLs too. For example, one popular KOL known as "Lipstick King", who was a former makeup salesman, is now reportedly worth USD 5 million, largely due to the hefty commissions manufacturers pay him for products sold. In Mainland China, KOL commissions can reach up to 50% of sales. This is different from the typical remuneration of influencers in the US, where brands generally pay a flat fee per social media post.⁴

Given their potential commission fees, Mainland China's KOLs have every incentive to make the largest amount of sales in the shortest amount of time without much regard for the authenticity of the goods being sold.

Some KOLs sell counterfeits on their livestreams using various methods including:

1. Mentioning brand names indirectly, implying that the goods are designed in a similar style of well-known brands;
2. Concealing trade marks by partially hiding logos (for example, pixelating logos on products); and
3. Claiming to be an authorised distributor of the brand owner.

Responding to the proliferation of counterfeit goods in the V-commerce sphere, the Mainland Chinese authorities have taken initial steps to tighten regulation in this area. On 5 November 2020, the State Administration for Market Regulation ("SAMR") issued the "Guiding Opinions of the State Administration for Market Regulation on Strengthening Supervision over Live Streaming Marketing Activities" ("Guiding Opinions"). The Guiding Opinions contain specific provisions on the protection of intellectual property rights, namely for SAMR to "investigate and punish" acts such as:

1. Passing off counterfeit products as genuine ones, passing off inferior products as superior ones, passing off substandard products as standard products, forging the place of origin of a product, and forging or falsely using a factory

name or factory address. (**Article 10**);⁵ and

2. Infringing on the right to exclusively use a registered trade mark and counterfeit patents (**Article 11**).⁶

There has been some evidence of SAMR enforcement against counterfeit goods in the V-commerce space. Pinduoduo, one of Mainland China's largest V-commerce platforms, was investigated by SAMR after several news reports were published in Mainland China about counterfeit goods being sold on the platform.⁷ In October 2020, the SAMR announced that 14 member agencies led by SAMR have launched an extensive campaign to regulate V-commerce, including cracking down on online sales of counterfeit goods.⁸

However, KOLs and streamers have been mostly successful in avoiding detection of their counterfeit goods. They do this by taking one or a combination of several strategies, including:

1. **Asking viewers to pay directly offline** – this is typically done via third party online payment platforms to bypass payment on the e-commerce platform. For example, one livestream showed viewers providing their name and size of the counterfeit product to be purchased which the host recorded in writing. By not redirecting viewers to online stores, the host minimised the risk of detection by the platforms.
2. **Creating product pages that do not mention the brand** – for example, one KOL advertised the sale of luxury handbags, but the link redirected the viewer to a page showing a completely different product. The page has since been taken down.
3. **Taking down product pages rapidly** – this prevents the authorities from tracing the counterfeit goods back to the livestream host. For example, a product page promoting counterfeit branded sports shoes was taken down within a week.

Until the authorities take a more proactive approach to combat counterfeit goods in V-commerce, counterfeiters are enjoying a free rein selling counterfeit goods on these platforms, which

4 <https://www.forbes.com/sites/michellegreenwald/2020/12/10/live-streaming-e-commerce-is-the-rage-in-Mainland-China-is-the-us-next/?sh=13a73b566535>

5 Article 10, Guiding Opinions on the State Administration for Market Regulation on Strengthening the Supervision of Livestreaming Marketing Activities (available at: http://gkml.samr.gov.cn/nsjg/ggjgs/202011/t20201106_323092.html)

6 Article 11, Guiding Opinions on the State Administration for Market Regulation on Strengthening the Supervision of Livestreaming Marketing Activities (available at: http://gkml.samr.gov.cn/nsjg/ggjgs/202011/t20201106_323092.html)

7 <http://www.ipraction.gov.cn/article/xwfb/mtgd/202004/156795.html>; <http://english.ipraction.cn/article/ns/202004/223280.html>

8 http://www.samr.gov.cn/xw/zj/202010/t20201024_322597.html

is ultimately hurting intellectual property rights owners and to some degree, end consumers. With over 600 million Mainland Chinese shopping online in 2020 generating sales upwards of USD 1 trillion,⁹ there is a pressing need for more robust enforcement actions against online counterfeiting activities.

The author would like to thank **Douglas Yang**, Trainee Solicitor at Mayer Brown, for his assistance with this article.

9 https://www.jpmorgan.com/merchant-services/insights/reports/Mainland_China-2020

SOUTHEAST ASIA

Data Privacy

Finding Harmony – ASEAN Model Contractual Clauses and Data Management Framework Launched

By **Gabriela Kennedy, Mayer Brown**
Mayer Brown, Hong Kong

Karen H. F. Lee, Counsel
Mayer Brown, Hong Kong/Singapore

On 22 January 2021, it was announced that the Association of Southeast Asian Nations (“**ASEAN**”) had approved the new Data Management Framework (“**DMF**”) and Model Contractual Clauses for Cross Border Data Flows (“**MCCs**”).

Introduction

ASEAN was established in 1967 with the key aim of improving economic growth and social progress, and collaboration and mutual assistance in South East Asia, amongst other things. There are currently ten member states of ASEAN (“**AMS**”), namely Singapore, Brunei, Cambodia, Indonesia, Lao, Malaysia, Myanmar, Philippines, Thailand and Vietnam.

The DMF and MCCs were developed to help harmonise the standards on cross-border data flows and data governance practices across the region. Adoption of the DMF and MCCs is not mandatory. However, AMS are encouraged to promote compliance with the DMF and MCCs by businesses in their respective jurisdictions. To this effect, the Singapore’s Personal Data Protection Commission immediately issued additional guidance for organisations in

Singapore on the use of the MCCs on 22 January 2021. Other AMS are expected to follow suit.

Data Management Framework

The DMF is designed to provide practical guidance for all private sector businesses operating in any AMS, including small and medium sized enterprises, and help them implement a data management system based on good management practices and fundamental principles, using a risk-based methodology. The role of DMF is to provide transparency and confidence to both individuals and foreign companies, in the hope of furthering business opportunities, particularly in the digital space.

There are six foundational components of the DMF that cover the entire data life cycle and require companies to take measures as set out below:

| | |
|--|--|
| Governance and oversight | Set out roles and responsibilities in the organization for implementing and executing the DMF and ensuring adoption, operation and compliance |
| Policies and procedural documents | Put in place data management policies and procedures to support the implementation of the DMF and ensure a clear mandate within the organization |
| Data inventory | Identify and understand the data that the organisation is in possession of, so as to better manage datasets and establish a data inventory |
| Impact / risk assessment | Self-tailor own parameters in order to categorise data based on an assessment of the impact to the organisation if the confidentiality, integrity or availability of the data is compromised |
| Controls | Develop and implement risk-based controls in accordance with the assigned data categories to prevent, detect and correct errors during data processing |
| Monitoring and continuous improvement | Improve and keep the DMF up-to-date by performing continuous monitoring, measurement, analysis and evaluation activities |

Model Contractual Clauses for Cross Border Data Flows

The MCCs are standard contractual terms and conditions that are recommended in agreements relating to the cross-border transfer of personal data between businesses in the region, and which are meant to encapsulate key data protection obligations and reduce negotiation and compliance costs. The MCCs detail the parties' responsibilities, required personal data protection measures and related obligations. Similar to the standard contractual clauses in the EU, there are two models provided by the MCCs – one that concerns transfers between data controllers, and the other that addresses transfers between a data controller and data processor (which also applies to any onward transfers to sub-processors).

The adoption of the MCCs does not ensure compliance with all data privacy laws across the region, and amendments may need to be made to take into account national requirements. Some of the terms in the MCCs may actually impose higher obligations than what is required under national law, particularly with the AMS that do not currently have a comprehensive data protection law in place. The MCCs confer rights on data subjects to enforce data protection warranties and undertakings against both parties to the MCC. This may not be in line with commercial realities, as many parties will seek to minimise their liabilities to data subjects.

A single model data transfer agreement is the holy grail for multinational companies as it is supposed to ensure predictability and consistency in data management, and is much preferable to a piecemeal approach to data processing arrangements. The MCCs offer this to an extent, but additional wording may need to be added (in appendices) to deal with specific requirements unique to a jurisdiction (e.g. timeline for data breach notifications). The MCCs also do not come with a guarantee that the recipients of the data can actually meet the requirements imposed upon them.

Conclusion

The DMF and MCCs provide a great starting point for companies in the region to help manage and protect their data, and to negotiate cross-border transfer terms. The adoption of the DMF and use of the MCCs will not automatically render a company compliant with all data privacy laws of the AMS.

Close attention still needs to be paid to requirements under national data privacy laws and due diligence on the recipients of data will still need to be undertaken.

*The authors would like to thank **Sophie Huang**, Intellectual Property Officer at Mayer Brown, for her assistance with this article.*



SINGAPORE AND APAC

Cyber- security

Aftermath of the SolarWinds Cyber Attack – New Rules Announced in Singapore and the Asia Pacific Region

By **Gabriela Kennedy, Partner**
Mayer Brown, Hong Kong

Karen H. F. Lee, Counsel
Mayer Brown, Hong Kong/Singapore

Cheng Hau Yeo, Associate
Mayer Brown, Singapore

In December 2020, SolarWinds, a US-based provider of IT management software to a host of high profile entities, was revealed to be the subject of a cyber attack that had begun as early as March 2020. Cybersecurity firm FireEye was the first to report the incident after it discovered that it had suffered a supply chain attack through the use of SolarWinds software. The exact number of entities affected by the incident and the extent of the damage caused is unclear and still being investigated.

Following the news of the SolarWinds cyber attack, on 18 January 2021, the Monetary Authority of Singapore (“**MAS**”) published a set of revisions to its Technology Risk Management Guidelines (“**Guidelines**”). Incorporating expert opinion and feedback gathered from a public consultation exercise held in 2019, the revised Guidelines set out more stringent rules on technology risk mitigation to be imposed on financial institutions in Singapore, with a focus on the enhanced oversight of technology outsourcing arrangements.

Amended MAS Guidelines

The Guidelines were first issued by the MAS in 2013 to provide financial institutions in Singapore with guidance on how they should manage the procurement and use of technology. The Guidelines apply not only to licensed banks and finance companies, but also to payment services, insurance and brokerage firms, and licensed credit card or charge card issuers. Against the backdrop of heightened cybersecurity risks, highlighted by the SolarWinds incident, and the growing reliance by financial institutions on third party technology service providers, the MAS amended the Guidelines to help financial institutions strengthen their technology risk governance and mitigation strategies, and maintain their cyber resilience.

The MAS introduced revisions to the Guidelines in three key areas: (1) the introduction of a more stringent vetting process for third party technology vendors; (2) the establishment of a detailed process for monitoring and sharing cyber threat intelligence, as well as for stress testing cyber defences; and (3) the broadening of responsibilities of the institution's board of directors and senior management in order to cultivate a stronger culture of accountability.

STRINGENT VETTING OF THIRD PARTY TECHNOLOGY SERVICE PROVIDERS

The previous version of the Guidelines simply provided generic rules requiring financial institutions to carry out due diligence on third party vendors. The amendments now introduce more prescriptive guidance – thereby emphasising the need to ensure proper oversight of third party technology providers.

The revised Guidelines require financial institutions to establish standards and procedures for assessing potential third party technology vendors. When carrying out assessments, financial institutions should consider the robustness of the vendor's software development, quality assurance practices, and security controls to protect any sensitive data to which the vendor has access. Prior to deploying commercial off-the-shelf solutions, financial institutions should ensure that such solutions meet requisite security requirements, and should implement adequate mitigation controls in the event that they fall short of those requirements. Financial institutions have an ongoing duty to ensure that

third party service providers employ a high standard of care and diligence in protecting data confidentiality and integrity, as well as safeguarding system resilience.

The Guidelines also address the use of a financial institution's open API. Under the revised Guidelines, financial institutions are now required to undertake a vetting process that includes assessing a third party's nature of business, cyber security posture, industry reputation and track record before granting such third party access to its API. Any sensitive data transmitted through the API should be encrypted to prevent hackers from installing malicious codes, and there should be real-time monitoring of the API to facilitate the prompt detection of suspicious activities. Financial institutions should also maintain a log of the identity, and the dates and times of all access to its API, by such third party.

REQUIREMENTS FOR MONITORING AND SHARING CYBER THREAT INFORMATION, AND TESTING OF CYBER DEFENCES

The previous version of the Guidelines only provided general guidance on the establishment of security plans for addressing disruptions to the delivery of IT services. The revised Guidelines now contain a requirement for financial institutions to establish a detailed cyber incident response and management plan that incorporates procedures for identifying and investigating security defects, and procedures for handling any potential cyber threats. Financial institutions must also establish a security operations centre to monitor and analyse any vulnerabilities, unauthorised access and intrusions, etc., together with system logs, to facilitate its operations.

The revised Guidelines also requires the procurement of a cyber intelligence monitoring system, under which financial institutions can collect, process and share cyber information, including cyber threats and vulnerability alerts, with trusted parties within the financial sector in order to ensure timely action is carried out to defuse any potential cybersecurity threats. This is keeping in line with the trend amongst other jurisdictions, such as Hong Kong, which have seen the value of sharing cyber threat information across the financial sector.

Under the previous Guidelines, financial institutions were already required to carry out regular

vulnerability and penetration assessments of their IT systems. However, the revised Guidelines has expanded the scope of such tests and specifies the manner in which such tests should be carried out. Financial institutions are now required to carry out regular scenario-based cyber exercises with relevant stakeholders and service providers to test the effectiveness of its cyber defences and response plans by simulating the tactics, techniques and procedures used by real-world attackers.

BROADENED ROLES AND RESPONSIBILITIES OF THE BOARD OF DIRECTORS AND SENIOR MANAGEMENT

Prior to the latest revisions, the Guidelines only required the Board of Directors ("**Board**") and senior management staff of financial institutions to maintain a general oversight of the technology-related risks. However, the revised Guidelines has introduced new requirements in relation to the appointment of technology specialists, as well as more stringent responsibilities for those in control of the financial institution.

Given that the Board and senior management staff are typically best placed to cultivate a culture of technology risk awareness within the institution, the revised Guidelines require at least one of its members to be equipped with the requisite knowledge for understanding and managing technology risks. The Board and senior management staff are also required to appoint a Chief Information Officer and Chief Information Security Officer possessing adequate expertise and experience. The former will be responsible for establishing and implementing IT strategies, overseeing day-to-day operations and managing IT risks, whereas the latter will be responsible for formulating information security policies and procedures, implementing security controls and managing information security.

The Board and senior management staff will be responsible for, among other things, undertaking regular reviews of the technology risk management strategy, clearly defining the responsibilities of staff members in managing technology risks, and apprising relevant stakeholders in a timely manner of any salient and adverse technology risk-related developments that are likely to have a large impact on the financial institution.

The MAS Rules in an APAC Context

In the past few years, various countries in the Asia Pacific ("**APAC**") region have also introduced or updated legislation or guidelines to manage the technology risks faced by financial institutions, in order to keep pace with the rapid changes occurring within the technology field.

Key parallels can be drawn between the revised Guidelines and those in other APAC jurisdictions, as summarised below.

AUSTRALIA

In July 2019, Australia's financial services regulatory body, the Australian Prudential Regulation Authority ("**APRA**"), issued the Information Technology Standards (CPS 234) ("**Standards**") for the purpose of ensuring that all APRA-regulated entities including banks and insurance companies take measures to remain resilient against information security incidents. The Standards contains similar provisions to the MAS's Guidelines in relation to the vetting of third party service providers, and obliging relevant financial entities to assess the service provider's information security capacity including the design of its information security controls. The Standards also require financial entities to test their own information security controls. In particular, instead of simply conducting simulation-based tests, entities should engage independent specialists to carry out actual systematic tests. It is worth noting that most banks in New Zealand also refer to the Standards from Australia when managing technology risks.

In the wake of the SolarWinds incident, on 7 January 2021, the Australian Cyber Security Centre ("**ACSC**") published a set of revisions to its guidance notes on "Cyber Supply Chain Management" and "Identifying Cyber Supply Chain Risks". Whilst not specifically targeted at financial institutions, the two guidance notes provide best practices for all businesses to follow in order to mitigate any supply chain risks when engaging suppliers, distributors and other service providers. The guidance on Cyber Supply Chain Management encourages businesses to identify and understand the supply chain, set out clear cybersecurity expectations in contracts with third parties, and to continuously monitor its supply chain cyber security practices.

The guidance on Identifying Cyber Supply Chain Risks sets out factors for businesses to consider when identifying technology procurement risks, such as determining the nationality of the contractor and assessing the likelihood of the business being subject to foreign interference, and reviewing the contractor's cyber security practices and its willingness to carry out vulnerability and penetration tests.

MAINLAND CHINA

For the past several years, Mainland China has enacted a series of piecemeal regulations in relation to cybersecurity, particularly the Cybersecurity Law ("**CSL**"), which came into effect in June 2017. Under the CSL, any critical network equipment and specialised cybersecurity products (including routers, switch servers, programmable logic controllers, intrusion prevention systems, and antispam products¹⁰) must be certified by qualified institutions before they can be sold or distributed to businesses in Mainland China. Additional requirements are imposed on operators of critical information infrastructures ("**CII**"), which include banks and other financial institutions, when engaging third party technology service providers. Under the Draft Regulations on Protection of Critical Information Infrastructure (2017), a legislation that complements the CSL, CII operators are required to conduct security testing of any network systems, software or products that are developed by third party service providers before they can be integrated in the CII operator's IT systems. The CSL also requires network products or services¹¹ procured by CII operators that may affect national security to be subject to a cybersecurity review. The rules for implementing such cybersecurity reviews can be found in the Measures for Cybersecurity Review (2020), which require CII operators to undertake an initial assessment to determine whether the network products or services may pose a national security risk. If the CII operator determines the presence of such risk, it must apply to the Cyberspace Administration of China ("**CAC**") for a cybersecurity review prior to procuring the relevant products or services. This requirement for cybersecurity review is unique to

Mainland China, and a failure to comply constitutes an offence that is punishable by fines of up to RMB 100,000.

Other provisions similar to the new MAS's Guidelines can also be found under the CSL. For example, CII operators may from time to time be required by the CAC to carry out cybersecurity drills for testing its capacity in responding to cybersecurity incidents, and are encouraged to share cybersecurity information with relevant departments, other CII operators, and research and cybersecurity service institutions. For the purpose of fostering a culture of accountability, CII operators are required to appoint a designated person, whose background has to be vetted, to be in charge of different aspects of cybersecurity management.

HONG KONG

The Hong Kong Monetary Authority ("**HKMA**") issued a Supervisory Policy Manual on General Principles for Technology Risk Management in 2003 ("**Supervisory Policy Manual**"), which contains a set of rules on technology risk management for financial institutions. Despite being one of the earliest of its kind in the APAC region, the Supervisory Policy Manual still manages to contain the crux of most of the rules for engaging and managing third party technology service providers found in the MAS's Guidelines. In particular, under the Supervisory Policy Manual, prior to engaging third party technology service providers, financial institutions should assess whether the potential service provider has sufficient resources and expertise to comply with the institution's IT controls. If the service provided is a critical technology service, such as data centre operations, the institution would have to undertake a detailed assessment of the service provider's IT control environment. Institutions are also advised to avoid relying on a single third party service provider in relation to critical services.

In September 2015, the HKMA also released a Circular on Cyber Security Risk Management ("**Circular**") which contains provisions that are largely comparable to those in the MAS's

10 For full list of products that must be certified, see Catalogue of Critical Network Equipment and Security Products (First Batch) (2017).

11 Network products and services in this context include, among others, high performance computers and servers, large capacity storage equipment, large database and application software, network security equipment, cloud computing services.

Guidelines. In particular, the Circular notes that the Board of Directors and senior management staff should play a proactive role in ensuring effective security risk management by establishing management accountability, carrying out regular evaluations and monitoring of the institution's cyber security controls having regard to new cyber threats, and exploring opportunities to share cyber threat intelligence with other institutions. Similar to the Standards in Australia, the Circular also recommends that institutions undergo regular independent assessments and penetration tests.

In addition, the HKMA launched a cybersecurity fortification initiative ("**CFI**") in December 2017, which was subsequently updated in November 2020. The CFI broadly sets out a cyber resilience assessment framework, a professional development programme, and a cyber intelligence sharing platform. The cyber resilience assessment framework consists of an inherent risk and maturity assessment of all HKMA-regulated institutions via the simulation of real life cyber attacks. The tests were set to be carried out in phases and are targeted to be completed by 2023.

Lastly, the Securities and Futures Commission ("**SFC**") has issued circulars relating to the use of third party technology service providers by financial institutions. A notable example is the Circular to Licensed Corporations on Use of External Electronic Data released in October 2019 ("**SFC Circular**"). The SFC Circular targets the use of cloud services and other services by financial institutions for data storage, and requires due diligence to be conducted in relation to the service provider's network infrastructure security, IT systems, cyber security management, and identity and access management prior to engagement of its services.

INDONESIA

Indonesia's Financial Authority, Otoritas Jasa Keuangan, issued a Regulation on the Implementation of Risk Management in the Use of Information Technology by Commercial Banks in 2016, which was recently revised in 2020 ("**Regulation**"). While the Regulation does not set out specific vetting procedures to be followed prior to engaging third party technology service providers, any bank that wishes to utilise third party technology service providers have to ensure that service providers are selected based on a cost-benefit analysis. When engaging a third party service

provider, the bank must ensure that the service provider implements a risk management framework, and the bank has a continuous duty to monitor and evaluate the effectiveness of that framework, as well as the overall performance of the service provider.

The Regulation also sets out an extensive list of responsibilities of the service provider, which includes guaranteeing information security, implementing IT controls that are verified by independent parties, and periodically submitting audit results to Bank Indonesia – in comparison, the relevant rules of other APAC jurisdictions do not generally contain the same level of specificity. The Regulation further provides that Bank Indonesia's approval may be required before procuring certain technology service providers, such as an overseas provider of IT-based transaction processing services.

MALAYSIA

In January 2020, Malaysia's Central Bank, Bank Negara Malaysia ("**BNM**"), issued a Policy Document on Risk Management in Technology ("**RMiT Policy**"), which is largely analogous to the revised Guidelines issued by the MAS in Singapore. The RMiT Policy sets out rules on ensuring rigorous vetting of third party technology service providers prior to their engagement. This includes the testing of source codes and conducting proper due diligence that takes into account risks relating to data leak, service disruption, processing errors, cyber threats, and mishandling of personal information.

In terms of system monitoring and testing, the RMiT Policy requires financial institutions to perform vulnerability assessment and penetration tests on its infrastructure on a quarterly basis having regard to emerging cyber threat scenarios. Institutions are also strongly encouraged to exchange cyber threat intelligence with relevant stakeholders and authorities.

Similar to the MAS's Guidelines, the board of directors of the financial institution has to have at least one member possessing technology expertise or experience, and has to designate a Chief Information Security Officer for overseeing the technology risk management controls of the financial institution.

PHILIPPINES

In 2017, the Philippines' Central Bank, Banko Sentral ng Pilipinas ("**BSP**"), issued a Circular no. 982 on Enhanced Guidelines on Information Security Management ("**Circular 982**"). Under Circular 982, when engaging third party technology vendors, financial institutions have to carry out proper due diligence and consider the strength of the third party's information security. Financial institutions have to set out in detail information security requirements in contracts with third party vendors, and have to ensure that proper mechanisms are put in place to monitor the security controls of third parties.

Circular 982 also recommends that vulnerability and penetration tests are regularly carried out in the form of simulation-based exercises. Like many other neighbouring jurisdictions, Circular 982 encourages financial institutions to collaborate and share any threat intelligence. In fact, it goes one step further to suggest that financial institutions should formulate policies for intelligence sharing activities, and should obtain approval from their board of directors and senior management staff before engaging in such sharing activities. Circular 982 also requires the institution's board of directors to appoint a Chief Information Security Officer to oversee the institution's risk management framework.

THAILAND


In 2018, the Bank of Thailand published the Regulations on Information Technology Risk of Financial Institutions ("**RTRFI Regulations**"). Similarly, the RTRFI Regulations sets out procedures for financial institutions to comply with when vetting and managing third party technology service providers. In particular, when selecting

service providers, financial institutions have to consider the potential service provider's credibility, system security, and maintenance support offered. Vulnerability and penetration tests should be carried out at least once a year or when there is any significant change. The tests are not required to be simulation-based, but should be carried out by independent internal or external experts. In relation to the roles and responsibilities of the board of directors and senior management staff, at least one director has to possess relevant IT knowledge or experience, and a member of senior management with IT competence must be appointed to oversee the financial institution's IT security.

Conclusion

With the continued uptake of digital transformation by many companies comes the ever present threat of cyber attacks. The nature of these cyber attacks is not static, and hackers are developing new and innovative ways to circumvent the firewalls erected by companies. The SolarWinds incident, which went undetected for months, is just one example of hackers employing sophisticated and advanced tactics to bypass robust security controls. Regulators across the world are catching on to the fact that companies need to keep pace with these threats and ensure that no holes or backdoor threats are introduced by third party vendors. The recent revisions to the Guidelines made by the MAS may turn out to be the first of similar regulation throughout the APAC region.

*The authors would like to thank **Stephanie Yung**, Trainee Solicitor at Mayer Brown, for her assistance with this article.*



HONG KONG

Technology

Online Dispute Resolution during COVID-19 in Hong Kong

By **Amita Haylock, Partner**
Mayer Brown, Hong Kong

The COVID-19 pandemic has brought about many challenges to individuals and businesses alike, but also represents an opportunity for innovation in sectors and industries which can no longer rely on traditional modes of operation. One such innovation is Hong Kong's "COVID-19 Online Dispute Resolution (**ODR**) Scheme".

The ODR Scheme was established by the Government under the Anti-epidemic Fund.¹² With social distancing regulations still in place in Hong Kong, in-person meetings in often tight and confined conference rooms are impractical. As such, the ODR Scheme seeks to provide a method for parties to resolve their legal disputes without having to meet physically. All disputes under the ODR Scheme are conducted electronically by way of the eBRAM International Online Dispute Resolution Centre and in accordance with the Centre's rules ("**eBRAM rules**").

What Sort of Disputes are Eligible?

The ODR Scheme only covers COVID-19-related disputes in which the amount claimed is HK\$500,000 or less. The definition of "COVID-19-related dispute" is very wide- it covers "any commercial, contractual, tortious, property, family or tenancy disputes arising out of or in connection with

¹² <https://www.info.gov.hk/gia/general/202006/29/P2020062900651.htm>

directly or indirectly the outbreak of the Covid-19 pandemic in any part of the world.”¹³ The policy reasoning for the financial cap is that the ODR Scheme is intended to benefit Hong Kong’s micro, small and medium-sized enterprises that may be adversely affected by the COVID-19 pandemic.¹⁴

Are There Any Requirements?

For a claim to fall under the ODR Scheme, either one of the parties (claimant or respondent) must be a Hong Kong resident or a Hong Kong-incorporated company. There is a small registration fee of just HK\$200 by each party. Finally, all parties to the dispute under the ODR Scheme will have to reach and sign an ODR Agreement and upload it on to the eBRAM Platform to commence proceedings.¹⁵

How Does the ODR Scheme Work?

The ODR Scheme is described as “a multi-tiered dispute resolution mechanism comprising negotiation, mediation and arbitration.”¹⁶

Initially, each tier of the ODR Scheme was specified to be conducted “within a limited time”.¹⁷ Since the initial Government press release, new details have been released regarding the timing of each tier. At the negotiation stage, which is not mandatory,¹⁸ the parties only have three calendar days from the commencement of the negotiation stage to conduct negotiations, after which the mediation stage must commence. At the mediation stage, parties have three calendar days from the date of being notified of the appointment of a mediator to settle the dispute via mediation. If that fails, the proceedings will move into the final stage- arbitration. At the arbitration stage, parties have one month from the date of the appointment of an arbitrator to make all submissions. The arbitrator is required to

grant an award within seven calendar days from the filing of the last submissions.¹⁹

How is the Mediator or Arbitrator Appointed?

At each stage, eBRAM will generate a list of five names from which the parties may agree to appoint as a mediator or arbitrator to the proceedings. If the parties fail to reach an agreement within three calendar days, eBRAM will appoint a mediator or arbitrator, depending on the stage of the proceedings.²⁰

What are Some COVID-19-Related Trends in Dispute Resolution?

Two types of disputes that have increased during the COVID-19 pandemic are claims arising from long-term supply contracts and force majeure claims.

LONG-TERM SUPPLY CONTRACTS

Many supply agreements in Asia take the form of long-term supply contracts, in which there is usually a mechanism requiring the parties to review certain contractual terms, including provisions such as price and timing of supply obligations. Given the significant disruptions to different industries as a result of certain government-mandated, pandemic measures, parties may find it difficult to come to an agreement on review negotiations. Consequently, questions such as whether a party has a right to refer a failure to agree on new contractual terms to arbitration are likely to present before the ODR Scheme.

FORCE MAJEURE CLAIMS

Commercial contracts often contain force majeure clauses, which are clauses exempting parties from the performance of a contractual obligation due to the occurrence of an event or circumstance beyond

13 Article 2.1, eBRAM Rules for the Covid-19 ODR Scheme, 1

14 *Supra* (n 12)

15 Article 4, eBRAM Rules for the Covid-19 ODR Scheme, 4

16 *Supra* (n 12)

17 *Supra* (n 12)

18 Article 6.3(c), eBRAM Rules for the Covid-19 ODR Scheme, 6

19 Article 8.8, eBRAM Rules for the Covid-19 ODR Scheme, 7

20 Articles 7 and 8 eBRAM Rules for the Covid-19 ODR Scheme, 6-7

their control. While force majeure clauses are often drafted broadly so that COVID-19 falls under descriptions of “pandemic” or “epidemic”, difficulties may arise where contractual performance is simply made more difficult or costly due to lockdowns or supply chain disruptions, but not excessively onerous or impossible. As such, disputes of this nature may be suitable for settlement via the ODR Scheme.

Despite the launch of the ODR Scheme, parties’ concerns over the process of appointment of mediators and arbitrators may arise due to the rigid

timeframes stipulated in the eBRAM rules. However, given the often expensive and time-consuming process of litigation in Hong Kong, the launch of the ODR Scheme, which already has a panel of more than 150 mediators and arbitrators available for appointment,²¹ is a step in the right direction to facilitate a more efficient dispute resolution framework.

*The author would like to thank **Douglas Yang**, Trainee Solicitor at Mayer Brown, for his assistance with this article.*

²¹ “eBRAM launches an innovative and cost-effective online platform to resolve COVID-19 related disputes”, eBRAM, 30 June 2020, available at: https://www.ebram.org/press_release.html.

Contact Us



Gabriela Kennedy

Partner

+852 2843 2380

gabriela.kennedy@mayerbrown.com



Amita Haylock

Partner

+852 2843 2579

amita.haylock@mayerbrown.com



Karen H. F. Lee

Counsel

+65 6327 0638

karen.hf.lee@mayerbrown.com



Michelle G. W. Yee

Counsel

+852 2843 2246

michelle.yee@mayerbrown.com



Jacqueline W. Y. Tsang

Associate

+852 2843 4554

jacqueline.tsang@mayerbrown.com



Cheng Hau Yeo

Associate

+65 6327 0254

chenghau.yeo@mayerbrown.com

Mayer Brown is a distinctively global law firm, uniquely positioned to advise the world's leading companies and financial institutions on their most complex deals and disputes. With extensive reach across four continents, we are the only integrated law firm in the world with approximately 200 lawyers in each of the world's three largest financial centers—New York, London and Hong Kong—the backbone of the global economy. We have deep experience in high-stakes litigation and complex transactions across industry sectors, including our signature strength, the global financial services industry. Our diverse teams of lawyers are recognized by our clients as strategic partners with deep commercial instincts and a commitment to creatively anticipating their needs and delivering excellence in everything we do. Our “one-firm” culture—seamless and integrated across all practices and regions—ensures that our clients receive the best of our knowledge and experience.

Please visit [mayerbrown.com](https://www.mayerbrown.com) for comprehensive contact information for all Mayer Brown offices.

This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively the “Mayer Brown Practices”) and non-legal service providers, which provide consultancy services (the “Mayer Brown Consultancies”). The Mayer Brown Practices and Mayer Brown Consultancies are established in various jurisdictions and may be a legal person or a partnership. Details of the individual Mayer Brown Practices and Mayer Brown Consultancies can be found in the Legal Notices section of our website. “Mayer Brown” and the Mayer Brown logo are the trademarks of Mayer Brown.

© 2021 Mayer Brown. All rights reserved.

Attorney Advertising. Prior results do not guarantee a similar outcome.