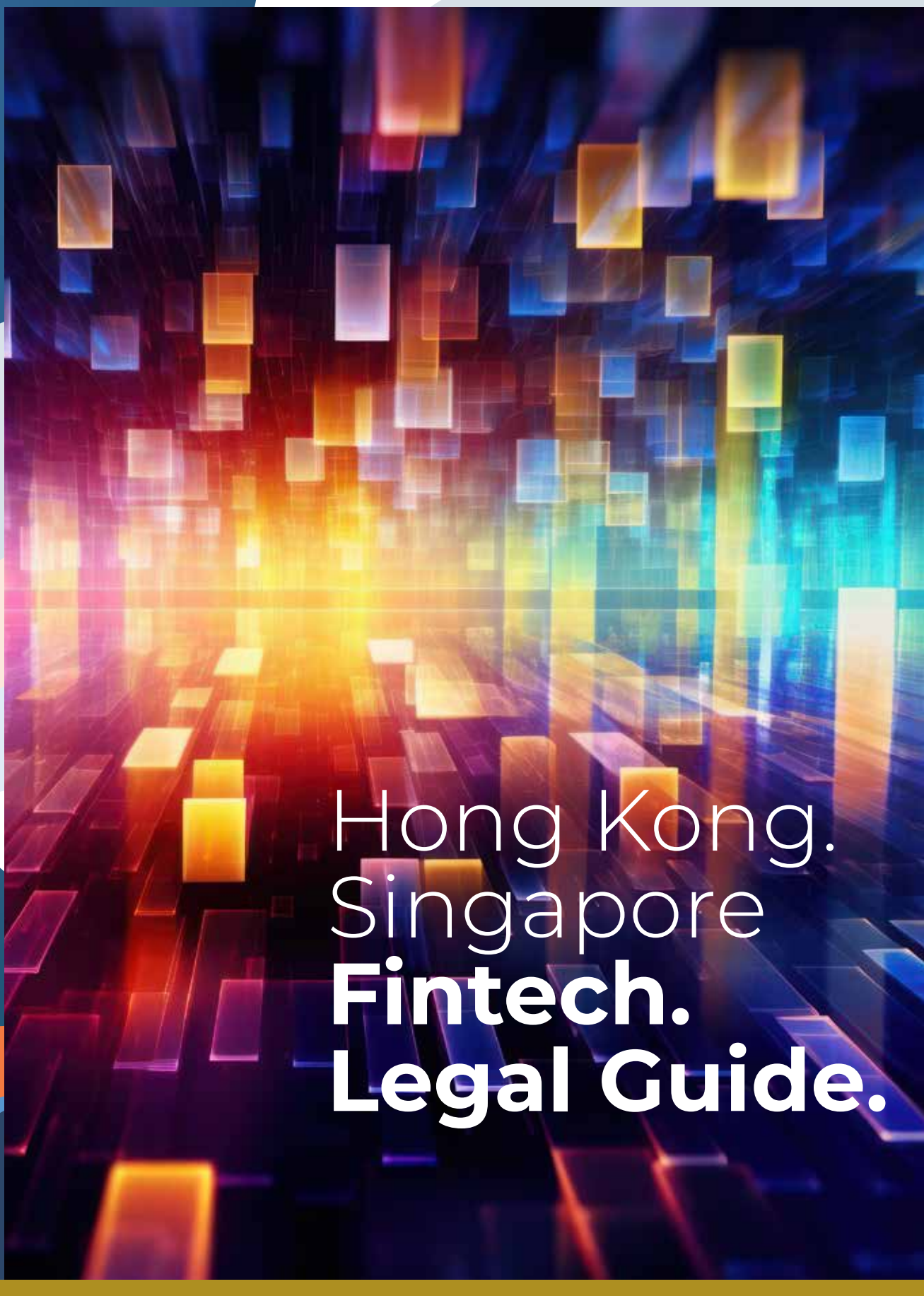
DEACONS 的近律師行 | RAJAH & TANN ASIA

2024 Edition



Hong Kong. Singapore **Fintech. Legal Guide.**

Content

Objectives of the Guide

Both Hong Kong and Singapore are dynamic international financial centres that are renowned for fostering business growth and innovations whilst ensuring that their financial markets are regulated to ensure protection of investors and to promote international confidence in market stability. With this in mind, both jurisdictions have adopted policies to be attractive places for Financial technology ("fintech") businesses to set up and thrive.

As fintech is fast evolving, the legal and regulatory regime supporting fintech needs to be flexible to ensure that the balance between innovation and market confidence is maintained. Both Hong Kong and Singapore have mature common law based legal systems with a sophisticated regulatory framework and robust, experienced institutions.

Fintech is transforming the financial services industry and creating growth opportunities in the global market. As the fintech industry continues to develop rapidly, businesses looking to expand internationally may wish first to understand the legal and regulatory framework of their next destination before taking the leap.

Deacons (Hong Kong) and Rajah & Tann (Singapore) are delighted to collaborate to present our first edition of a side-by-side comparative overview of the laws and regulations which are most relevant to fintech businesses wishing to operate in either or both jurisdictions, covering areas from the regulatory landscape, marketing and selling digital products, data protection and privacy, intellectual property, anti-money laundering regime, setting up companies and utilising human talent.

We sincerely hope that you find this guide helpful – we would be pleased to receive any feedback which will help us improve future editions of this guide and would further welcome the opportunity to help guide clients through the legal and regulatory regime.

Deacons (Hong Kong) and Rajah & Tann (Singapore) are both preeminent legal practices in their respective regions, with extensive experience in the fintech industry. If you have any further inquiries or require any assistance, please do not hesitate to contact us through the contact information provided at the end of this guide.

What is Fintech and its development in Hong Kong and Singapore?

Fintech is the use of digital technology to provide financial services and products. The fintech industry has experienced exponential growth in recent years as a result of advances in technology and changing consumer behaviour. By offering innovative and convenient solutions to meet the evolving needs of consumers, fintech companies are revolutionising the traditional financial services industry.

Hong Kong and Singapore are two leading financial hubs in Asia with thriving fintech ecosystems. Both cities offer a range of government-supported initiatives to encourage fintech innovation, coupled with a supportive regulatory environment, strong financial infrastructure and a highly skilled workforce, making them attractive destinations for fintech businesses. As a result, a growing number of fintech companies have set up in Hong Kong and Singapore in recent years.

What are the benefits of engaging in Fintech business in Hong Kong and Singapore?

Fintech businesses operating in Hong Kong and Singapore can enjoy a number of benefits. These include:

- Access to a large and sophisticated financial market
- Supportive regulatory environment for fintech innovation
- A strong legal and regulatory framework to protect investors and consumers
- Strong government support and initiatives for fintech development
- Access to a highly skilled workforce and talent development initiatives
- Access to a supportive ecosystem of investors, accelerators, and industry associations

Legal Framework and Regulatory Landscape

I. Digital Tokens Issuance / Offering

Overview

Has there been a specific regulation enacted, or are digital tokens regulated through existing legislation?

Hong Kong

No specific regulation has been enacted to regulate digital tokens. Where the tokens involved fall under the definition of "securities" or "futures contracts" under the Securities and Futures Ordinance (**"SFO"**), the securities law in Hong Kong applies. Utilities tokens which are not "securities" or "futures contacts", as defined in the SFO, will not fall under the scope of the SFO.

Singapore

The primary applicable legislation is the Payment Services Act 2019 (**"PSA"**) which regulates services relating to digital payment tokens (**"DPT"**). At present, dealing in DPTs and facilitating the exchange of DPTs is regulated. Amendments to the PSA are incoming that will expand the regulatory scope to include services for custody, transfer and broking of DTPs. Additionally, tokens which bear characteristics of other financial products (such as securities, units in collective investment schemes, derivatives contracts, or commodities) may be separately regulated under other financial regulatory legislation such as the Securities and Futures Act 2001 (**"SFA"**), Commodity Trading Act 1992 (**"CTA"**) or other laws.

Security Tokens

1. What constitute security tokens?

Hong Kong

Tokens which represent (i) ownership interests or rights in companies which allow the token holders to receive dividends or participate in the distribution of the companies' surplus assets upon winding-up or (ii) debentures where the issuing terms of the tokens impose obligations on the issuer to repay token holders their principal (i.e. their investment in the tokens and interest) or (iii) interests in a collective investment scheme where proceeds of tokens are used to make investments which are managed by a scheme operator collectively with an aim to enable token holders to participate in a share of the returns provided by those investments are akin to traditional securities. As such, they may be treated as "securities" and fall under the purview of the Securities and Futures Commission (**"SFC"**) and the provisions of the SFO.

Singapore

"Security tokens" are not regulated per se and are not a defined term under Singapore law, but tokens which have features of traditional "securities" or "units in a collective investment scheme" would be subject to regulation as such under the Securities and Futures Act 2001. The structure and characteristics of, including the rights attached to, the tokens would need to be examined to determine if this is the case.

"Securities" regulated under the SFA would include both equity securities and debt securities; the former would include tokens that represent ownership interests in a company including the right to vote in general meetings or to receive dividends or a share of profits or to participate in the residual assets of the entity upon winding up, while the latter would include tokens that evidence or acknowledge a debt such as tokens that are in the nature of bonds, notes or other debt obligations which are typically characterised by regular interest payments and return of principal upon maturity of the financial product. Tokens where the proceeds thereof are managed collectively by a scheme operator for the purpose of enabling the holders to participate in or receive profits, income, or other payments or returns from such management may be considered "units in a collective investment scheme".

2. Is a licence required for offering or dealing in security tokens?

Hong Kong

Yes, any intermediary who offers, markets or distributes security tokens in Hong Kong must be licensed by the SFC for the Type 1 (dealing in securities) regulated activity. If a person actively markets to the Hong Kong public any services that he provides, and if such services would constitute a regulated activity if provided in Hong Kong, then the person would be regarded as carrying on a business in that regulated activity. Accordingly, a person needs to be appropriately licensed before actively marketing his or her services in Hong Kong, even if the person is based outside Hong Kong. Any marketing, distribution or dealing with security tokens as a business in Hong Kong without a proper licence constitutes a criminal offence, unless an exemption applies[1].

Singapore

Yes, carrying on business in dealing in capital markets products (including "securities" or "units in a collective investment scheme") which includes making or offering to make with any person, or inducing or attempting to induce any person to acquire or dispose of securities, is a regulated activity under the SFA. Such regulated activity is defined widely and would include any solicitation, marketing, or distribution activities relating to the security[2]. Unless exempted, persons who carry on such business require a capital markets services licence to do so. Even if the person conducting the regulated activity is based outside of Singapore, licensing requirements would apply if done partly in and partly outside Singapore, or even wholly outside Singapore if the activity would have a substantial and reasonably foreseeable effect in Singapore. Failure to obtain a licence is an offence punishable by a fine and/or a jail term.

[1]Note that conducting a business of other regulated activities (e.g. advising on security tokens or managing a portfolio of security tokens) in relation to security tokens in Hong Kong will be subject to additional licensing requirements.

[2]Financial advisory activities relating to the security are separately regulated by the Financial Advisers Act 2001 of Singapore (**"FAA"**). Managing a portfolio of security token assets may also be regulated as fund management activity under the SFA.

3. Is registration or authorisation required for offering of security tokens to the public?

Hong Kong

◊ Yes, if security tokens are offered to the Hong Kong public, registration or authorisation requirements under the SFO may be triggered unless an exemption applies.

◊ The offering of security tokens which are akin to shares, debentures or bonds in Hong Kong, is required to comply with the prospectus requirements for offering of shares and debentures under the Companies (Winding Up and Miscellaneous Provisions) Ordinance (Cap. 32) ("CWUMPO"). The prospectus would need to include all relevant information about the security token offering, the issuer, and the underlying assets (if any), as well as details about the issuer's business, financials, management team and risk factors associated with the investment.

◊ Security tokens which are interests in collective investment schemes (i.e. funds) can only be offered to the public in Hong Kong if the collective investment schemes are authorised by the SFC under the SFO.

◊ The SFC issued a Circular on Tokenisation of SFC-authorised Investment Products on 2 November 2023 ("Fund Tokenisation Circular"), which sets out the requirements for tokenised SFC-authorised investment products (including funds). At the initial stage, the SFC is of the view that it is appropriate to allow primary dealing of tokenised SFC-authorised investment products whereas secondary trading would warrant more caution and careful consideration. In general, the underlying product must meet all the applicable product authorisation requirements; product providers are required to comply with certain requirements on the tokenisation arrangement; as part of application, the SFC may require third party audit on the smart contracts and legal opinion to be submitted; offering documents need to be enhanced to set out clearly the tokenisation arrangement, the ownership representation of the tokens and the associated risks; and the product provider need to have least one competent staff member with relevant experience and expertise to operate or supervise the tokenisation arrangement and manage the associated risks. Prior consultation with the SFC would be required for any tokenised investment products.

Singapore

◊ Offers of security tokens to persons in Singapore would be subject to prospectus requirements under the SFA, unless an exemption applies.

◊ The prospectus requirements are found in Part 13 of the SFA and the Securities and Futures (Offers of Investments) (Shares and Debentures) Regulations 2005 (**"SFOISDR"**) or Securities and Futures (Offers of Investments) (Collective Investment Schemes) Regulations 2005. The prospectus is expected to contain all information that investors and their professional advisers would reasonably need to make an informed investment decision, and this general disclosure test is supplemented by detailed checklists in the SFOISDR of information to be provided in the prospectus.

◊ Where the tokens are collective investment schemes (**"CIS"**), such schemes must be authorised or recognised by the Monetary Authority of Singapore (**"MAS"**) before they may be offered to the public.

4. Is there any safe harbour or exemption applicable to offering of security tokens?

Hong Kong

◊ The offering of security tokens will be exempted from the prospectus requirement and authorisation if any of the following exemptions applies.

◊ **Professional Investor Exemption:** Security token offerings targeted exclusively at professional investors would be exempt from complying with the offering requirements stated above. "Professional investors", as defined in the SFO, include various institutional investors; trust corporations with at least HK$40 million in assets; and individuals, corporations and partnerships with investment portfolios of at least HK$8 million.

◊ **Private Placement Exemption:** This exemption is for cases where information is distributed in a manner that does not constitute an offer to the public and therefore does not fall within the prohibition contained in the SFO or the definition of "prospectus" in the CWUMPO. For example, it is generally accepted as market practice that an offer to not more than 50 offerees (not actual subscribers) who do not qualify as professional investors, will not be regarded as being made to the public.

Singapore

The offering of tokens which fall within the definition of securities or units in a collective investment scheme under the SFA may be exempted from the prospectus registration requirements under certain safe harbour exemptions, some of which would include:

◊ **Small Offers Exemption:** Offers where the total amount raised within a period of 12 months does not exceed S$5 million (or its equivalent in foreign currency).

◊ **Private Placement Exemption:** Offers which are made to no more than 50 persons within any period of 12 months. The limit of 50 persons refers to the number of persons offered, and is not based on the number of persons accepting the offer.

◊ **Offers made to Accredited Investors and Institutional Investors:** Offers made to institutional investors (as defined under the SFA) and accredited investors are not subject to the prospectus registration requirements.

The prospectus exemptions (save for offers to institutional investors only) are subject to various conditions, including that the offers not be accompanied by any advertisement, and no selling or promotional expenses are incurred in relation to the offer, and resale restrictions.

Offers of "security tokens" that are units in a collective investment scheme to accredited investors would also need to be notified to MAS and entered into the MAS' list of restricted schemes, amongst other requirements.

Non-Securities Token e.g. Stablecoins, Utility Tokens, NFTs

1. Are stablecoins regulated?

Hong Kong

◊ Stablecoins are currently not regulated in Hong Kong but the Hong Kong Monetary Authority (**"HKMA"**) and the Financial Services and Treasury Bureau (**"FSTB"**) recently announced a proposal to require issuers of fiat-referenced stablecoins in Hong Kong to submit to a licensing regime[3].

◊ Under the proposal, issuers of such stablecoins must meet a set of conditions before being issued a licence – such conditions include requirements as regards management of reserves, a stabilisation mechanism, and redemptions by users. In particular, issuers will be required to ensure that the value of the reserve assets backing the stablecoin in question is at least equal to the par value of the stablecoins in circulation, and be of high quality and liquidity. Reserve assets must be segregated from an issuer's other assets, and the issuer should have adequate risk management and controls to ensure proper management of any investment activities relating to the reserve assets.

◊ Other requirements include restrictions on other business activities, and other requirements on financial resources, disclosure, governance, systems and management. It will be an offence to issue such stablecoins without a licence from the HKMA.

◊ It is also proposed that the HKMA will have the power to adjust and modify the regulatory regime for stablecoins as necessary, in order to allow regulators to address any emerging risks and new types of stablecoins as necessary.

Singapore

◊ The MAS has stated that stablecoins, being crypto-assets that aim to maintain a stable value relative to a specified asset, are currently treated as DPTs under the PSA. Entities that provide the service of dealing in and/or facilitating the exchange of stablecoins would fall within the scope of regulated DPT services that attract licensing requirements.

◊ The MAS has proposed to introduce a new regulated payment service under the PSA, "stablecoin issuance service", that would capture issuers of single currency pegged stablecoins (**"SCS"**) denominated in SGD or G10 currencies in Singapore (**"SCS Framework"**). All stablecoins (whether or not SCS) would also continue to be considered DPTs and providers of DPT services would continue to be subject to the existing DPT regulatory regime. Under the SCS Framework, SCS issuers would be subject to various requirements including:

- Hold the reserve assets only in asset classes with very low risk, and in segregated account accounts separate from its own assets;
- conduct independent attestations of their reserve assets on a monthly basis;
- allow for redemption of SCS within 5 business days.

[3] See HKMA and FSTB's Legislative Proposal to Implement the Regulatory Regime for Stablecoin Issuers in Hong Kong: https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2023/20231227e4a1.pdf

Hong Kong (cont.)

- Certain other products with similar structures and/or nature, such as stored value facilities, will be excluded from the definitions of a fiat-referenced stablecoin (and in any event stored value facilities are regulated separately under their own regime).

- Only fiat-referenced stablecoins issued by licensed issuers, authorized institutions, licensed corporations and licensed virtual asset service providers (**"VASPs"**) can offer such stablecoins to the general public in Hong Kong. A stablecoin not licensed by the HKMA can only be offered by authorized institutions, licensed corporations, and licensed VASPs to professional investors.

- The proposals are subject to a public consultation period ending on 29 February 2024, and as such the specific details of the proposed regulatory regime are still subject to further amendments. Cryptocurrency businesses and other related businesses should consider whether their business models may be caught by the proposed regulations – in particular, the intention to regulate wallets in relation to stablecoins could capture cryptocurrency wallets generally.

2. Are utilities tokens and non-fungible tokens (“NFTs”) regulated?

Hong Kong

◊ Utility tokens that are genuinely non-securities and non-payment-related stablecoins and NFTs that are genuinely digital representations of a collectible (e.g. artwork, music or video) are currently not subject to the SFC’s or HKMA’s regulatory regimes.

◊ However, fractionalised or fungible NFTs which are structured as interests in a collective investment scheme may be treated as “securities” and hence, may trigger the licensing and authorisation requirements set out above.

Singapore

The terms “utility token” and “non-fungible token” are not defined terms under Singapore law. Depending on their nature and characteristics, such tokens may be considered digital payment tokens, and/or other traditional financial products such as securities, debentures, units in collective investment schemes, or derivative contracts. NFTs or utility tokens that do not fall within any of these aforementioned regulated categories would not be subject to regulation under Singapore law.

II. Virtual Assets ("VA")[4] Exchanges

1. Is VA exchange regulated?

Hong Kong

In Hong Kong, the operators of VA exchanges that match VAs for clients and take custody of client assets (fiat currencies and VAs), must be licensed by the SFC as virtual asset service providers (**"VASPs"**) under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (**"AMLO"**) and for Type 1 (dealing in securities) and Type 7 (providing automated trading services) regulated activities under the SFO.

Singapore

In Singapore, persons who facilitate the exchange of digital payment tokens are required to be licensed by the MAS as payment services providers under the PSA. The term "facilitating the exchange of digital payment tokens" generally means establishing or operating a digital payment token exchange where offers to buy and sell digital payment tokens for money or digital payment tokens are made.

The provision of a place or facility on which security tokens may be secondarily traded on a centralized basis may constitute the operation of an organised market, which may require a licence as an approved exchange or a recognised market operator under the SFA.

[4] VAs refer to digital representations of value which may be in the form of digital tokens (e.g. utility tokens, stablecoins, security-backed tokens, or asset-backed tokens) or any other virtual commodities, crypto assets or other assets of essentially the same nature, irrespective of whether or not they amount to "securities" or "futures contracts" as defined under the SFO, but exclude digital representations of fiat currencies issued by central banks.

2. What are the key eligibility requirements to be a licensed VA exchange?

Hong Kong

- **Incorporation and Registration:** The first step to becoming a VASP in Hong Kong involves incorporating and registering the business as a company (or registered non-Hong Kong company) under the Companies Ordinance.

- **Fit and Proper Criteria:** When assessing the fitness and propriety of the individuals to be licensed by the SFC (including two responsible officers, one of whom must be an executive director), directors, managers, and substantial shareholders, the SFC will consider:

  i) educational or other qualifications or experience, having regard to the nature of the functions he or she will perform;
  ii) ability to carry on the regulated activity under the SFO competently, honestly and fairly; and
  iii) reputation, character, reliability and financial integrity.

- **External assessment:** A VASP applicant must engage an external assessor to assess its proposed business activity and prepare two external assessment reports. The Phase 1 report covers the applicant's structure, governance, operations, and systems. The Phase 2 report covers the assessor's review and assessment of the applicant's adoption of its policies, procedures, systems, and controls.

- **Governance:** VASPs are required to have in place a token admission and review committee.

- **Insurance:** The compensation arrangement needs to cover potential losses of 50% of client VAs held in cold storage and 100% of client VAs held in hot and other storage. The arrangement may include any or a combination of i) third-party insurance; ii) funds of the VASP or any of its group companies; and iii) a bank guarantee provided by a Hong Kong authorised financial institution (i.e. a bank).

Singapore

- **Incorporation:** be incorporated or have a permanent place of business or a registered office in Singapore;

- **Opening hours:** have one person in Singapore for fixed hours to respond to and address complaints and queries;

- **Directorships:** either (i) have at least one executive director who is either a Singapore Citizen or Permanent Resident, or (ii) at least one executive director who is an Employment Pass holder and a non-executive director who is a Singapore Citizen or Permanent Resident;

- **Experience of Directors:** the executive directors and CEO must have sufficient experience in operating a payment services business;

- **Base Capital:** have a base capital of S$250,000 (for major payment institution) or S$100,000 (for standard payment institution);

- **Security:** for major payment institution only, provide security of S$100,000 or S$200,000 (depending on expected volume of transactions) prior to commencing business, in the form of either a cash deposit with MAS or a bank guarantee;

- **Fit and Proper Requirements:** the officers, employees, representatives and substantial shareholders must fulfil the fit and proper requirements;

- **Internal Policies and Risk Management:** have in place compliance and audit arrangements, technology risk and cybersecurity measures and AML/CTF policies that are commensurate with the level of risk;

Hong Kong (cont.)

◊ **Financial strength:** A VA trading platform operator licensed for Type 1 (and Type 7) regulated activities must maintain at all times a minimum paid-up share capital of HK$5,000,000 and liquid capital of not less than HK$3,000,000 (or at least 5% of its adjusted liabilities, whichever is higher).

◊ **AML/CFT:** A VASP must comply with the "travel rule" so that when it acts as an ordering institution, it obtains, records and submits required information about the originator and recipient to the beneficiary institution and when it acts as a beneficiary institution, it obtains and records the required information submitted by the ordering institution or intermediary institution.

Singapore (cont.)

◊ **Legal Opinions:** provide a legal opinion containing a risk assessment and regulatory characterisation (whether it is regulated under SFA as a capital markets product or the PSA as a DPT) of each of the tokens listed on the exchange, and provide a full list of digital tokens (including tokens that are not DPTs) that the applicant will be supporting to the MAS;

◊ **AML/CFT:** VASPs must comply with the "travel rule" to, as the ordering institution, obtain, record and submit the required information of the originator and recipient to the beneficiary institution, and as the beneficiary institution, obtain and record the required information submitted by the ordering institution or intermediary institution;

◊ **Letter of Responsibility / Letter of Undertaking:** a letter of responsibility or letter of undertaking may be required from the applicant's parent entity or related company, amongst other factors the MAS may take into consideration including the track record and financial condition of the applicant, its holding company or related corporations (where applicable), and the operational readiness of the applicant.

III. Money Service Operator

My proposed business may involve the transfer of money across jurisdictions, or the changing of money from one currency to another. Does this trigger any licensing requirements?

Hong Kong

◊ Under the AMLO, money service operators operating in Hong Kong must obtain a licence before conducting any money service business in Hong Kong. Two types of "money service" are regulated under the AMLO, namely:

- money changing services – the exchange of currencies, but excluding any such service operating within the premises of a hotel, or any service consisting solely of transactions for the purchase of non-Hong Kong currencies in exchange for Hong Kong currency; and
- remittance services –sending/receiving or arranging for the sending/receiving of money into and out of Hong Kong, or arranging for the receipt of money in a place outside of Hong Kong.

◊ Under the AMLO, a person who operates a money service without a licence commits an offence. A person who intends to operate a money service must make an application to Hong Kong's Customs and Excise Department. Certain criteria need to be met before a licence is granted, including whether the directors and ultimate owners of the applicant are fit and proper, review of business plans and the anti-money laundering policy of the applicant, inspection of the applicant's proposed premises to operate its business, and so forth.

◊ Companies whose business model involves some element of remittance or money changing should seek legal advice as to whether or not a money service operator's licence is required.

Singapore

Where money transfers are involved, the relevant regulated payment services are "domestic money transfer service" (**"DMT"**) and "cross-border money transfer service" (**"CMT"**) where:

- DMT means the service of accepting money for the purpose of executing, or arranging for the execution of payment transactions between payers and payees who are both in Singapore; and

- CMT means a service of accepting money in Singapore, whether as principal or agent, for the purpose of transmitting, or arranging for the transmission of, the money to any person outside Singapore or any service of receiving any money from outside Singapore for, or arranging for the receipt of any money from outside Singapore by, any person in Singapore, whether as principal or as agent.

Where the money transfer service provider also issues payment accounts or e-money, the regulated payment services of "account issuance service" and "e-money issuance service" would also be attracted.

Money changing services (i.e. the service of buying or selling foreign currency notes) is also a regulated payment service.

All of the foregoing would attract licensing requirements under the PSA.

Data Protection and Privacy

1. Are there dedicated data protection laws?

Hong Kong

Hong Kong's principal data protection law is the Personal Data (Privacy) Ordinance (**"PDPO"**). The main requirements that must be observed by data users are specified in the 6 data protection principles (**"DPP"**) which outline how data users should collect, handle and use personal data. In summary:

◊ DPP1 requires personal data to be collected for a lawful purpose, collection of data not to be excessive and collected by lawful and fair means, and sets out the information data users should inform data subjects about their collection and use of their data.

◊ DPP2 requires data users to ensure personal data are accurate and not kept longer than necessary.

◊ DPP3 prohibits the use of personal data for any new purpose without first obtaining the data subject's express and voluntary consent.

◊ DPP4 requires data users to ensure security of personal data.

◊ DPP5 obliges data users to disclose their personal data policies and practices, the kinds of personal data held and their main use purposes.

◊ DPP6 provides for data subjects' data access and correction rights.

There are also requirements relating to the use and provision of personal data for direct marketing purposes, and anti-doxxing provisions.

The Privacy Commissioner for Personal Data (**"PCPD"**) is responsible for overseeing the implementation of and compliance with the PDPO.

Singapore

Protection of personal data in Singapore is governed by the Personal Data Protection Act 2012 (**"PDPA"**) and subsidiary legislation, which collectively outline how organisations should collect, use, process and disclose personal data, as specified in 11 broad obligations:

◊ Consent Obligation: Organisations must obtain the consent of individuals before collecting, using or disclosing their personal data.

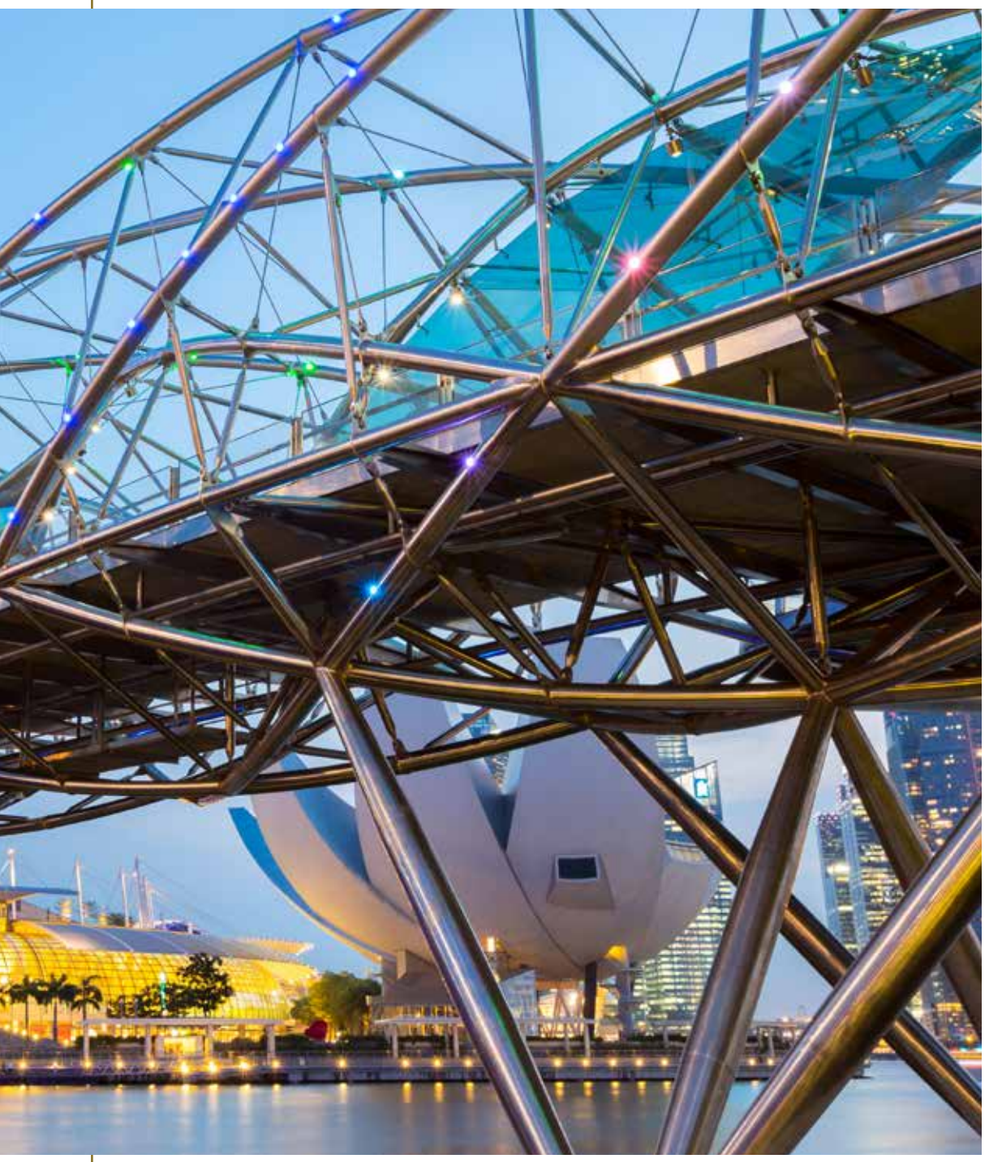
◊ Purpose Limitation Obligation: Organisations may collect, use or disclose personal data only for reasonable purposes explicitly communicated.

◊ Notification Obligation: Individuals must be informed about the purposes of data collection, use, or disclosure.

◊ Access and Correction Obligations: Individuals have the right to request access and correction of their personal data.

◊ Accuracy Obligation: Organisations must make reasonable efforts to ensure personal data are accurate.

◊ Protection Obligation: Organisations must implement security measures to protect personal data and storage media from unauthorised access, disclosure, alteration, loss and destruction.



Singapore (cont.)

◊ Retention Limitation Obligation: Personal data should only be retained for as long as necessary to fulfil the purposes of collection.

◊ Transfer Limitation Obligation: Transfer of personal data outside Singapore is restricted unless the receiving jurisdiction ensures a comparable level of protection.

◊ Accountability Obligation: An organisation must demonstrate compliance with the PDPA.

◊ Data Breach Notification Obligation: An organisation must notify the regulator and/or affected individuals, if it has suffered a data breach that is likely to result in significant harm or be of significant scale. Where an organisation has reason to believe that a data breach affecting personal data in the organisation's possession or control has occurred, it must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach meets any of the notification thresholds, and this assessment should not exceed 30 calendar days. Once the organisation has ascertained that the breach is notifiable, it should make the data breach notification within 3 calendar days of its determination.

◊ Data Portability Obligation: Organisations are required to transmit an individual's data that is in the organisation's possession or under its control, to another organisation in a commonly used machine-readable format, if the individual makes such a request. However, this obligation has not yet taken effect.

The PDPA also establishes obligations relating to a do-not-call registry.

2. Is there any specific restriction on cross-border transfer of personal data?

Hong Kong

There are provisions prohibiting transfer of personal data to places outside of Hong Kong unless specified circumstances are satisfied. However these provisions have not yet come into operation. That said, the general requirements of the PDPO should be complied with in cross-border data transfers. The PCPD's recommended model contractual clauses for cross-border data transfer may be voluntarily incorporated into commercial agreements between data transferors and transferees.

Singapore

- Under the Transfer Limitation Obligation, an organisation may transfer personal data overseas if it has taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations or specified certifications to provide the transferred personal data a standard of protection that is comparable to that under the PDPA. Such legally enforceable obligations include obligations that may arise under a law, contract, binding corporate rules or some other legally binding instrument.

- Additionally, there are certain circumstances where an organisation could be permitted to transfer personal data even if they are unable to rely on legally enforceable obligations as stated above (though as good practice, organisations should seek to rely on legally enforceable obligations). These circumstances include cases where the transfer of the individual's personal data is reasonably necessary for the conclusion or performance of a contract between the organisation and the individual, where it is necessary in the vital interests of the individuals or in the national interest, where the individual whose personal data is to be transferred grants their consent for the transfer of personal data having been informed of how their data will be protected in the destination country, or where the personal data is publicly available in Singapore.

3. Are businesses legally required to notify any authorities of data breaches?

Hong Kong

There is no statutory requirement of notification. The company should assess the circumstances of the data breach and its impact to decide if a notification is needed. If the data breach is likely to result in a real risk of harm to affected data subjects, the company should consider notifying the PCPD, the affected data subjects and other relevant parties as soon as practicable.

Singapore

An organisation must notify the regulator, the Personal Data Protection Commission (PDPC) and/or affected individuals, if it has suffered a data breach that results in or is likely to result in significant harm, or that is or is likely to be of a significant scale. Where the number of individuals impacted are 500 or more, this is deemed to be of significant scale. Where an organisation has reason to believe that a data breach affecting personal data in the organisation's possession or control has occurred, it must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach meets any of the notification thresholds, and this assessment should not exceed 30 calendar days. Once the organisation has ascertained that the breach is notifiable, it should make the data breach notification within 3 calendar days of its determination.

Cybersecurity

What are the laws governing cybersecurity?

Hong Kong

Cybersecurity is an issue in Hong Kong given the significant increase in cybercrime cases in recent years, particularly since the Covid-19 pandemic. Such offences, which typically involve someone using a computer or other networked device for improper means, often involve email frauds, love scams or identity theft.

There is currently no single overarching piece of Hong Kong legislation which deals comprehensively with cybercrime and attempts to bolster cybersecurity. Nevertheless, there are some provisions in Hong Kong legislation which deal with, and offer some protection against, cybercrime, as follows:

- Section 60 of the Crimes Ordinance (Cap. 200): this provision makes it a criminal offence to destroy or damage property belonging to another without lawful excuse. The term "destroy or damage" includes the misuse of a computer.

- Section 161 of the Crimes Ordinance: this is a blanket provision which prohibits anyone from obtaining access to a computer with criminal or dishonest intent.

- Section 27A of the Telecommunications Ordinance (Cap. 106): this provision prohibits anyone from knowingly causing a computer to perform any function to obtain unauthorised access to any program or data held in a computer.

Singapore

The Protection Obligation imposed by the PDPA requires organisations to implement security measures to protect personal data and storage media from unauthorised access, disclosure, alteration, loss and destruction.

Aside from the PDPA, laws addressing cybersecurity in Singapore include the Cybersecurity Act 2018 (**"CSA"**) and Computer Misuse Act 1993 (**"CMA"**).

The CSA empowers the Cyber Security Agency to designate computers or computer systems necessary for the continuous delivery of an essential service as a Critical Information Infrastructure (**"CII"**). Owners of the CII will be subject to statutory obligations under the CS Act, including furnishing primarily technical information, complying with codes of practice and standards of performance, complying with written directions, informing the CSA of the change in ownership, reporting cybersecurity incidents, conducting cybersecurity audits and risk assessments, and participating in cybersecurity exercises. The CSA also establishes a light-touch licensing framework for cybersecurity service providers. Finally, the CSA empowers the relevant authorities to investigate cybersecurity threats or incidents for the purposes of assessing its impact (or potential impact), preventing any or further harm from arising, or preventing a further cybersecurity incident from arising. As part of the investigation, persons and organisations must comply and assist with such investigations.

Hong Kong (cont.)

Whilst there is no designated authority in Hong Kong that handles all cybercrime related offences, the Hong Kong Police have established a Cyber Security and Technology Crime Bureau to handle cybercrime issues and carry out relevant investigations. The Hong Kong Computer Emergency Response Team Coordination Centre also provides advice on preventative measures against cybersecurity threats.

In July 2022, the Law Reform Commission published a consultation paper seeking public feedback on Cyber-Dependent Crimes and Jurisdictional Issues. The consultation paper contains proposals for law reform in Hong Kong, including enacting a new piece of legislation to cover the different types of cybercrime and to govern their jurisdictional implications. The consultation period ended in October 2022, and the Government's response in this area is awaited.

Singapore (cont.)

The CMA addresses cybercrimes and applies to any person regardless of nationality or geographical location so long as the accused party, computer programme in question or data was in Singapore at the time of the offence, or the offence causes or creates a significant risk of serious harm in Singapore. The CMA criminalises unauthorised access or modification of computer material and governs the investigation and prosecution of cybercrime perpetrators. It also criminalises offences such as hacking into a computer system and denial of service attacks. Under section 39 of the Criminal Procedure Code 2010, law enforcement may order persons in organisations to assist in providing computer access for the purposes of investigations under to the CMA.

Aside from the above, there are also sector-specific cybersecurity requirements imposed by certain regulators in industries such as healthcare, telecommunications, and financial services.

Intellectual Property

1. What fintech inventions may be patentable under patent law?

Hong Kong

◊ Patents are crucial assets of fintech companies. In the fintech industry, many inventions are software or computer implemented inventions. The patentability of software and computer-implemented inventions is a critical issue to consider when seeking patent protection. The requirements for patentability under section 9A of the Hong Kong Patents Ordinance (Cap. 514) closely mirror its equivalent under the Patents Act 1977 in the UK –an invention is patentable if it is new, involves an inventive step and is susceptible of industrial application. However, non-patentable subject matter includes the following categories: (a) discoveries, scientific theories, or mathematical methods; (b) aesthetic creations; (c) schemes, rules, or methods for a mental act, playing a game or doing business operations, as well as computer programs; and (d) presentations of information.

◊ When it comes to software and business methods, the crucial question is whether the invention makes a technical contribution to the prior art. It is expected that Hong Kong courts will follow an approach similar the courts in the UK in scrutinising the technical effect claimed by the invention.

◊ Fintech inventions in the emerging fields of blockchain, metaverse, Web 3.0 and Artificial Intelligence can also form patentable subject matter provided that the aforesaid requirements of patentability are satisfied. Whilst fintech inventions may make use of software and business methods for providing innovative solutions, businesses wishing to patent their inventions should make sure that such inventions are not business methods and solve technical problems and provide technical effects, so as to qualify as patentable subject matter.

◊ Short-term patent applications in Hong Kong are filed directly at the Hong Kong Patent's Registry and are only examined for formal matters and not for patentability. It is possible to obtain a patent in Hong Kong without a determination as to whether it relates to patentable subject matter if a short-term patent is filed.

◊ The National Intellectual Property Administration of the People's Republic of China (**"CNIPA"**) demonstrates a greater degree of flexibility when it comes to business method inventions. Additionally, it is feasible to secure patents for business method subject matters by re-registering PRC patents that have been granted in China.

Singapore

◊ The criteria for patentability of an invention under the Singapore Patents Act 1994 broadly include (a) qualification as patentable subject-matter, (b) novelty, (c) non-obviousness / inventive step, (d) industrial applicability, and (e) sufficiency.

◊ Recognising the need to afford Fintech (and other technology) organisations quick and effective intellectual property protection, the Intellectual Property Office of Singapore (**"IPOS"**) launched the SG IP Fast Track Programme (**"SG IP FAST"**) in 2020, allowing patent applications in all technology fields to be processed on an accelerated basis. The objective of SG IP FAST is to provide early certainty to applicants in any technology field and facilitate utilisation of the Singapore examination report or registration to accelerate their IP applications overseas. IPOS states that straightforward patent applications filed under this route can be granted in as fast as six months, while non-straightforward patent applications can be granted in as fast as nine months.

◊ Although there was previously uncertainty on whether business methods were patentable subject matter, the prevailing view now is that business methods are patentable.

◊ Mathematical methods (including algorithms) in themselves are not considered to be inventions and are therefore not patentable. However, the application of a machine learning method to solve a specific problem in a way that goes beyond the underlying mathematical method could be regarded as an invention and can be included in a patent application.

◊ Fintech organisations seeking to protect computer programmes or software can do so through patent law if the software is characterised by its technical features and function, rather than its source code. One practical difficulty in obtaining a patent for software programs with incremental differences from existing prior art is that such software may be obvious to persons skilled in the art, rendering it difficult to satisfy the inventive step requirement.

2. How to obtain patent protection for software?

Hong Kong

◊ There are three types of patents in Hong Kong: (i) short-term patents which are only subject to formality examination that requires the submission of, amongst other things, a search report on the prior art in relation to the invention; (ii) re-registration of standard patents which are based on the corresponding PRC, UK or EU (designating UK) patents (including designated patents of PRC, UK or EU through PCT applications) whereas the foreign patent office may adopt a more generous approach to the patentability issue; and (iii) original grant standard patents (**"OGP"**) which are substantively examined by the Hong Kong Intellectual Property Department. The term is 20 years for a standard patent, and 8 years for a short-term patent, both counting from the filing date.

◊ As filing strategy can make a difference in patenting software and computer implemented inventions, depending on the jurisdictions of interest, the applicant may adopt a combined approach, pursuing both the re-registration route based on a foreign application or an OGP and the local route of a short-term patent which may also help secure interim protection before grant of a standard patent.

Singapore

◊ The applicant can (i) submit a domestic patent application to IPOS, or (ii) file an international Patent Cooperation Treaty (**"PCT"**) application for multiple designated countries without the need to file separate applications in the designated countries. A PCT application has two phases, the international phase and national phase. Patents granted in Singapore confer rights on the owner to prevent others from exploiting the invention without consent during the patent term, which is 20 years from filing date.

◊ The advantages of a PCT application include cost savings, the benefit of an International Search Report (which assesses prior art in relation to inventions), and overall flexibility. On the other hand, PCT applications could still entail higher overall costs at the respective national phases. Failures to meet deadlines during the national phase can also lead to abandonment of applications.

3. Are there any subsidies for obtaining patent protection?

Hong Kong

◊ It is worth noting that the Hong Kong Government offers a patent application grant, which is a funding scheme to assist Hong Kong companies and residents to obtain a first patent for their invention, within or outside Hong Kong. A successful applicant will be entitled to a grant of up to HK$250,000 or 90% of the direct costs of the application (whichever is lower). Further details on the scheme are available at *https://www.itf.gov.hk/en/funding-programmes/fostering-culture/pag/index.html.*

◊ An R&D tax deduction system is available in Hong Kong effective from April 1, 2018. This system allows for deductions on qualifying expenses or payments related to research and development. There are two categories of qualifying R&D expenses: Type A and Type B. Type A expenses, which refer to R&D expenses excluding Type B expenses, are eligible for a 100% deduction under certain conditions. Type B expenses, which include costs associated with generating Intellectual Property, are eligible for a 300% deduction on the first HKD 2 million of expenses and a 200% deduction on the remaining amount. There is no limit on the portion of expenses eligible for the 200% deduction.

Singapore

Local Singapore companies may apply for the Enterprise Development Grant, administered by Enterprise SG, to defray costs for projects that help companies upgrade and innovate, including those that are patent-related (see *https://www.enterprisesg.gov.sg/financial-support/enterprise-development-grant*).

Companies looking to market products in a new overseas market can apply for a Market Readiness Assistance Grant, which can be used to defray patent-related costs (see *https://www.enterprisesg.gov.sg/financial-support/market-readiness-assistance-grant*).

The Enterprise Innovation Scheme, administered by the Inland Revenue Authority of Singapore, allows eligible companies to obtain tax deductions / allowances on qualifying expenditure, including registration of patents and/or acquisition and licensing of patent rights (see *https://www.iras.gov.sg/schemes/disbursement-schemes/enterprise-innovation-scheme-(eis)*).

4. What other mechanism may be available to protect IP rights in software?

Hong Kong

◊ Apart from patent law which protects software's technical features, other individual elements contained in software can also be protected as copyrighted work, trade marks, trade secrets and/or registered designs, provided that the specific requirements of the relevant bodies of law are fulfilled. In Hong Kong, copyright subsists in original works and automatically arises at the time of creation without registration. This could extend to various elements in software such as its source codes, visual features, UI designs, logos, text, audio, video and other original content. For example, the source code, where originally developed, can be protected as literary work under copyright law. In addition, in certain circumstances source code is also protectable as a trade secret (confidential information) by Hong Kong common law, where the source code is not known to the public, has commercial value and corresponding protective measures have been taken to secure its confidentiality.

◊ Other elements such as the name and logo of the software can give rise to trade mark rights where they are used in a trade or registered as trade marks. UI design may qualify as copyrighted artistic work if sufficiently original. It is also possible for UI design to be registered as registered design in Hong Kong provided that the application meets certain requirements. UI design is registrable as registered design if it has features of shape, configuration, pattern or ornament which appeal to the eye and are not solely dictated by function, the features are applied to an article of manufacture, and the design is new as of the date of filing the application (or any priority date, if claimed).

Singapore

◊ Copyright is an important area of intellectual property law that Fintech organisations rely on to protect software and computer programmes. Computer programmes are protected by copyright as a literary work under the Copyright Act 2021. Copyright in Singapore is non-registrable and arises at the point of creation. Any computer programme or software that is characterised by source code enjoys copyright protection.

◊ The protection of confidential information is also of importance to Fintech organisations. Where (a) information is of a confidential nature (e.g., the information is clearly designated as a secret) and (b) such information has either been imparted in circumstances importing an obligation of confidence or has been accessed or acquired without the owner's knowledge or consent, then a rebuttable presumption of breach of confidence arises. The party-in-breach has the onus of showing how receipt of the confidential information does not undermine the organisation's interest in avoiding wrongful loss caused by loss of the information's confidential character. As long as this information retains its confidential character, the obligation of confidence applies continuously.

◊ Other aspects such as name and logo of the software may give rise to trade mark rights, whether registered or otherwise.

5. What are the common IP challenges faced by fintech businesses and how to avoid them?

Hong Kong

◊ In developing and protecting their IP assets, fintech operators are faced with the challenges of safeguarding themselves against third parties' infringements as well as avoiding infringing others' rights. As a general rule, businesses should ensure, by way of e.g., contracts and IP policies, that third parties' content is not used without authorisation. In certain circumstances, e.g., before launch of products, availability searches and freedom-to-operate searches are also advisable for clearance of infringement risks of trade marks, patents and/or registered designs. To ensure the effective protection of intellectual property rights and facilitate future enforcement, it is essential to file registrations promptly and proactively for appropriate IP protection, such as trademarks, registered designs, and patents.

◊ The recent Copyright (Amendment) Ordinance, which came into effect on 1 May 2023, introduces safe harbour provisions to limit liability of online service providers in respect of copyright infringement taking place on their platforms. A platform will be excused from liability for damages if the prescribed conditions are fulfilled, including to take reasonable steps to limit/stop the infringement as soon as practicable following receipt of notice or becoming aware of the infringement. Nevertheless, a platform is not required to monitor its service or actively detect infringing activities. A Code of Practice has also been issued for practical guidance on the recommended procedures that qualify for the safe harbour provisions.

Singapore

◊ Fintech businesses often rely on partnerships and use of third-party technologies, which may raise challenges in relation to licensing agreements. This requires contractual clarity in matters of IP ownership and the scope of license.

◊ As Fintech is a highly competitive industry, competitors both locally and overseas may attempt to replicate Fintech innovations. This requires a coordinated international IP strategy and awareness of IP laws in multiple target markets.

◊ Finally, the high employee turnover and mobility of tech talent poses IP challenges. These can be mitigated through the inclusion of non-compete, non-disclosure, confidential information, and intellectual property, and indemnification clauses in employment agreements that should be entered into at the point of employment.

Anti-Money Laundering

1. What are requirements in relation to anti-money laundering?

Hong Kong

◊ Hong Kong's requirements in relation to anti-money laundering and counter-terrorist financing (**"AML/CFT"**) are mostly to be found in the AMLO and specific guidelines issued by regulators of entities that are subject to the requirements of the AMLO.

◊ Financial institutions (banks, companies regulated by the SFC, insurers, money service operators, issuers of stored value facilities, VASPs, etc.) and designated non-financial businesses and professions (accountants, estate agents, legal professionals, trust and company services providers, and precious metal and stones dealers) are regulated under the AMLO. Other regulated entities may be subject to similar requirements by virtue of licensing or regulatory requirements imposed by those entities' regulators (e.g. money lenders - although not "financial institutions" under the AMLO, they are subject to similar requirements by virtue of their licensing conditions).

◊ There are two main requirements under the AMLO.
- Customer due diligence
- Record keeping

Singapore

◊ Singapore's legal regime in relation to AML/CFT is primarily set out under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (**"CDSA"**), and the Terrorism (Suppression of Financing) Act 2002 (**"TSFA"**). These are general laws that would apply generally in Singapore whether to financial institutions or non-financial institutions.

◊ Financial institutions are required to comply with additional AML/CFT measures which are set out in other pieces of legislation and the guidelines, notices and circulars issued by the MAS. The measures generally include:
- Customer due diligence (identification and verification of customer's identity);
- Transaction monitoring;
- Sanctions screening
- Record keeping
- Reporting of suspicious transactions

◊ There are also sanctions requirements imposed under subsidiary legislation under the Financial Services and Markets Act 2022 and United Nations Act 2001 (applicable to financial institutions and non-financial institutions respectively) that are intended to effect the sanctions imposed by the UN Security Council.

2. What are the requirements in relation to KYC?

Hong Kong

- Entities that are subject to the AMLO or other requirements as regards AML/CFT (**"Covered Entities"**) are required to conduct KYC checks and obtain further information about their customers to ensure that any business relationship (and any transactions from it) is not a money laundering risk.
- In general, a Covered Entity will be required to identify the customer in question and any beneficial owners, verify said identities, and where necessary, obtain further information about the purpose and intended nature of the business relationship.
- Certain classes of persons (such as politically exposed persons) are subject to additional measures.

Singapore

- Financial institutions that are subject to additional AML/CFT measures as mentioned above in question 7.1 would be subject to requirements to conduct customer due diligence on persons they enter into business relationships with or conduct transactions for, including to obtain certain identification information about their customers and their beneficial owners, verify such information, as well as obtain information on the purpose and nature of the business relationship.
- Enhanced customer due diligence requirements would apply to politically exposed persons as well as persons from higher-risk AML/CFT jurisdictions.

3. Do entities need to maintain records of their transactions?

Hong Kong

- Covered Entities are required to keep records of the customer due diligence (**"CDD"**) they conduct, as well as transaction records and other records that are necessary to meet the regulatory requirements for AML/CFT.
- In essence, there should be a paper trail for any funds in relation to a customer that may be moving through the Covered Entity, and all information relating to the CDD and transaction records should be readily available for the entity and the relevant regulator's review.
- Records pertaining to CDD and transactions should be kept for a period of at least five years from when the business relationship ends, or after the relevant transaction completes.

Singapore

Financial institutions that are subject to additional AML/CFT measures as mentioned above in question 7.1 would be subject to record-keeping requirements, to maintain and retain for at least 5 years (following the termination of business relations with the customer or execution of relevant transaction) the customer due diligence information they have obtained (see question 7.2 above), as well as data, information and documents that would enable any individual transaction undertaken for a customer to be reconstructed (including amount and type of currency involved).

Records should also be kept of data, information and documents that would allow the relevant regulatory authorities to assess the financial institution's compliance with the appliable AML/CFT requirements as well as satisfy information requests within a reasonable or required time.

Setting up Business in Hong Kong and Singapore

1. What are the requirements to incorporate a private company?

Hong Kong

A common vehicle for a business is a private company limited by shares. The incorporation of a private company in Hong Kong requires at least 1 shareholder; there is no requirement that a shareholder be resident in Hong Kong and any legal entity can be a shareholder. There is no minimum share capital required. The company must have a registered office in Hong Kong. It must have at least 1 individual director, who need not be resident in Hong Kong. It must also have a company secretary who or which is resident in Hong Kong. Every business in Hong Kong must register with the Business Registration Office.

Singapore

The most common business vehicle in Singapore is a private company limited by shares.

A private company must have at least one shareholder subscribing for one share, at least one director and secretary ordinarily resident in Singapore, and a physical registered office address in Singapore. It must not have more than 50 shareholders (counting joint shareholders as one person and not counting any employee shareholders).

There are no foreign ownership restrictions and minimum capital requirements except in certain limited circumstances.

Companies in Singapore are regulated by the Accounting and Corporate Regulatory Authority.

2. Why should you start a business in Hong Kong/ Singapore?

Hong Kong

Hong Kong is characterised by a high degree of internationalisation, a business-friendly environment, open and fair competition, free flow of information, a well-established and comprehensive financial network, a superb network of transport and telecommunications infrastructure, sophisticated support services and a well-educated workforce complemented by a pool of efficient entrepreneurs. It also has a substantial amount of foreign exchange reserves, a fully convertible and stable currency, no exchange controls and a relatively simple tax system with tax being levied at a low rate.

Singapore

According to the Economist Intelligence Unit, Singapore has been ranked the world's best business environment for 15 consecutive years. Several contributing factors are the favourable taxation system, well-established banking facilities and financial institutions, ease of obtaining investment capital, a highly-skilled workforce, supportive government policies, and well-developed infrastructure.

3. Are there any Government initiatives to support Fintech businesses?

Hong Kong

Examples of government financial incentives and support for research and development (**"R&D"**) include:

- A HK$2 billion Innovation and Technology Venture Fund was set up to attract funds to co-invest in local innovation and technology (**"I&T"**) start-ups.
- A HK$5 billion Strategic Tech Fund was set up to invest in mid-stage I&T start-ups from around the world to enrich the I&T ecosystem in Hong Kong.
- The Hong Kong Science and Technology Parks Corporation implemented the "HKSTP venture fund" which assists start-ups at early stages as well as helps start-ups further their business and fast-track their global expansion.
- The Hong Kong- Shenzhen Innovation and Technology Park will be developed as a key base for co-operation in scientific research. The Park focuses on six R&D areas – healthcare technologies, big data and artificial intelligence, robotics, new material, microelectronics and financial technology.
- The Enhanced Tax Deduction for R&D Expenditures and the Research and Development Cash Rebate Scheme were implemented to encourage R&D and investments and promote technological innovation in Hong Kong.

Singapore

Under the Financial Sector Technology and Innovation Scheme (**"FSTI 3.0"**), MAS has committed up to S$150 million over three years to provide support for innovation in the financial sector, including:

- The Centre of Excellence Grant to co-fund manpower expenses and rental expenses for financial institutions, corporate venture capital entities and global technology companies intending to set up a Centre of Excellence in Singapore;
- The Industry-wide Technological Infrastructure or Utility Project Grant to co-fund manpower expenses for projects which aim to improve productivity, efficiency, or build technology and infrastructure in the financial sector;
- The Innovation Acceleration Track to support businesses engaging in experimentation and development of nascent technologies in the financial services sector, by reimbursing up to 50% of manpower costs, professional services costs and equipment, hardware, data or software costs, up to a cap of S$400,000;
- The Artificial Intelligence and Data Analytics (**"AIDA"**) Grant which is aimed at providing support for financial institutions, FinTechs or Industry Consortiums who focus on AIDA adoption, by co-funding up to 30% of qualifying expenses, up to a cap of S$500,000;
- The Environmental, Social and Governance (**"ESG"**) Grant catered to Singapore-based financial institutions which demonstrate use of technology to address their business needs in ESG data and infrastructure. MAS will fund up to 50% of qualifying expenses, up to a cap of S$500,000 and limited to a funding duration of up to 18 months; and
- The Regulatory Technology Grant which provides funding to financial institutions undertaking projects which utilise technology to enhance efficiency of risk management and compliance functions. MAS will provide funding of up to 30% of qualifying expenses which will be capped at S$100,000 and limited to an 18 month funding duration.

Enterprise Singapore, a statutory board under Singapore's Ministry of Trade and Industry, further provides grants to qualifying businesses such as the Enterprise Development Grant and provides access to funding through the Enterprise Financing Scheme.

Talent and Workforce Development

1. How to obtain work visa/permits?

Hong Kong

◊ Generally, unless a person has the right of abode, right to land, or right of unconditional stay in Hong Kong, he/she requires a visa in order to work in Hong Kong, whether under an employment, secondment, or some other arrangement. Without such permissions, both the employer and the employee will be criminally liable.

◊ Employees may, with the sponsorship of a Hong Kong entity, apply for an employment visa under the Admission Scheme for Mainland Talents and Professionals (for Mainland residents) or the General Employment Policy (for other foreign nationals). To be eligible for a visa under either scheme, broadly speaking, the Immigration Department must be satisfied that the applicant has a good educational background, normally a first (i.e. bachelor's) degree in the relevant field, but in special circumstances, good technical qualifications, proven professional abilities and/or relevant experience and achievements supported by documentary evidence may also be accepted; the applicant possesses special skills, knowledge or experience of value to and not readily available in Hong Kong; and the remuneration package is broadly commensurate with the prevailing market level for similar positions in Hong Kong. The entry visa for employment is typically valid for two years, and must be renewed if the employee is to continue to work in Hong Kong after the visa's expiration.

Although there may be other visa schemes which an employee may apply for, employers typically prefer the above scheme as it ties the employee to the employer.

Singapore

Generally, foreigners who wish to work in Singapore are required to apply for a work pass with the Ministry of Manpower (**"MOM"**). Singapore citizens and permanent residents are not required to obtain such work passes and may freely work for any organisations in Singapore without the need for a work pass.

Foreigners applying for work passes would be required to meet certain salary requirements. Information about the various types of work passes available to a foreigner intending to work in Singapore is set out in the MOM website at mom.gov.sg. Some key examples are set out below:

i. Employment Pass – for professionals, managers, executives or specialists who have a job offer in Singapore and earn a fixed monthly salary of at least S$5,000, depending on their qualifications and experience and possess certain recognised qualifications. A different set of criteria applies to professionals, managers, executives or specialists in the financial services sector;

ii. Personalised Employment Pass (**"PEP"**) – for overseas foreign professionals whose last drawn fixed monthly salary overseas was at least S$$22,500. A PEP holder has greater job flexibility, for example, they are not required to re-apply for a new pass when they change jobs. A notification to the MOM of the change suffices.

iii. EntrePass – for foreign entrepreneurs who are keen to operate a business in Singapore that is venture-backed or possesses innovative technologies. Detailed information about the eligibility requirements for an EntrePass and resources about joining the EntrePass programme is available on the StartUp SG website at startupsg.gov.sg.

Singapore (cont.)

iv. S Pass – for skilled workers who earn a fixed monthly salary of at least S$3,000. MOM has announced that it will continue to raise the qualifying salaries and levies for S Pass holders. The qualifying salaries for S Pass holders in the financial services sector are higher. In addition to the requirements on qualifying salaries, S Pass holders must also satisfy requirements on educational qualifications and relevant work experience; and

v. Work Permit – for foreign workers from approved source countries working in the construction, manufacturing, marine, process or services sector.

There are certain restrictions on the number of foreigners that a company may employ, depending on the class of worker or the industry in which he is employed. For example, the number of foreigners holding S-Passes that a company can employ is currently capped at 10% of the company's total workforce in the services sector and 15% in the construction, manufacturing, marine shipyard and process sectors.

Employers are also expected to adhere to the Fair Consideration Framework (which sets out guidelines for hiring of employees) when hiring foreign employees.

2. What are the laws in relation to employee conduct?

Hong Kong

◊ Hong Kong has numerous laws governing workplace relations and behaviour, such as the four ordinances prohibiting discriminatory behaviour on the grounds of gender, marital, pregnancy or breastfeeding status, disability, race, and family status; the Prevention of Bribery Ordinance which forbids employees from soliciting or accepting bribes; and the Competition Ordinance under which anti-competitive conduct (such as agreeing with a competitor business to fix prices, restrict output share markets, and/or rig bids) is prohibited. Violation of such laws may lead to civil and/or criminal consequences.

◊ As an employer is generally vicariously liable for its employees' conduct if the relevant act is closely connected with the employment, to minimise the chances of violation, protect company reputation, and strengthen a culture of compliance, Hong Kong employers typically adopt employee handbooks and policies (such as policies on conflict of interests, data privacy, anti-discrimination, whistleblowing, and disciplinary procedures) even though they are not legally required, and conduct regular compliance training for their employees, to ensure that employees are aware of and uphold the standard of conduct that is expected from them.

Singapore

Under Singapore law, the employer-employee relationship is regulated by a mixture of statutory law and common law. In particular, the Employment Act 1968 (**"EA"**) is the main piece of employment legislation that regulates employer-employee relations in Singapore. Pursuant to the EA, employers are required to provide their employees with certain minimum statutory entitlements in relation to certain key aspects of the employment relationship (such as salary payments and leave entitlements).

There are also guidelines and advisories issued by the Tripartite Alliance for Fair & Progressive Employment Practices that supplement the employment laws in Singapore and set out the policies that employers should adopt to promote fair and responsible employment practices.

Subject to the above, employers are free to negotiate the employer-employee relationship by way of contract. Singapore companies also typically adopt employee handbooks and policies even though they are not strictly required.

Way Forward

The fintech industry is currently experiencing tremendous growth opportunities globally. However, navigating the legal and regulatory landscape of a foreign jurisdiction can be challenging. This guide provides a comparative overview of the legal and regulatory aspects that fintech companies should consider when setting up a business in Hong Kong and Singapore.

Before venturing into a new jurisdiction, fintech companies should seek professional legal advice to ensure they understand the local legal and regulatory requirements, and if they decide to set up a business in the jurisdiction, to ensure they comply with the relevant local laws and regulations. Fintech companies may also consider participating in accelerator programs or other government initiatives that can provide guidance and support for their businesses.

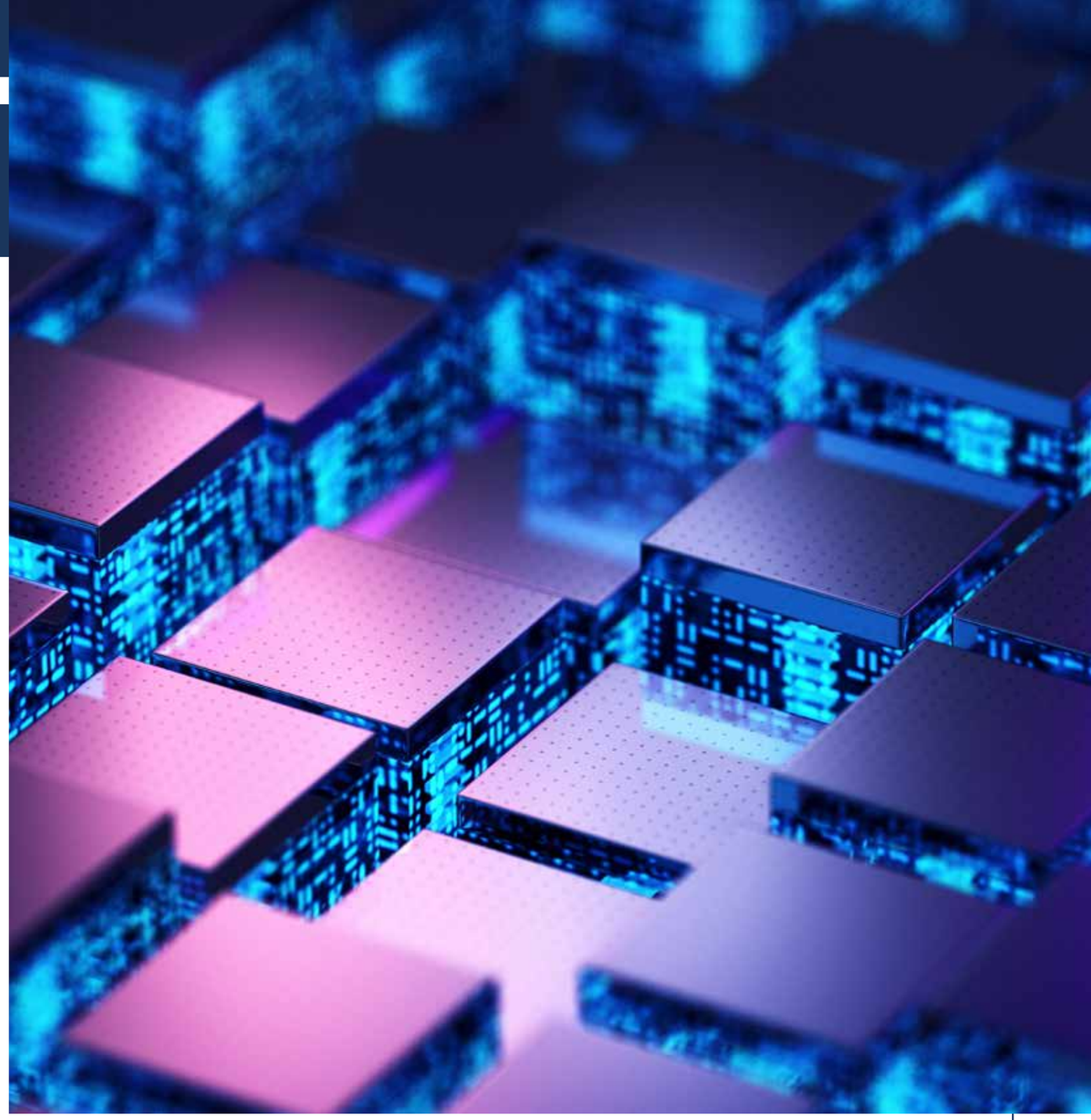
Key Contacts

◊ **Machiuanna Chu**
Partner,
Corporate Commercial
Deacons
E: machiuanna.chu@deacons.com

◊ **Regina Liew**
Head,
Financial Institutions Group
RAJAH & TANN ASIA
E: regina.liew@rajahtann.com

◊ **Isabella Wong**
Partner,
Financial Services
Deacons
E: isabellahm.wong@deacons.com

◊ **Samuel Lim**
Partner,
Financial Institutions Group
RAJAH & TANN ASIA
E: samuel.lim@rajahtann.com



DEACONS 的近律師行 | RAJAH & TANN ASIA

CONTACT US

Deacons
5th Floor, Alexandra House, 18 Chater Road, Central, Hong Kong

Rajah & Tann
9 Straits View #06-07, Marina One West Tower, Singapore, 018937, SG