Legal 500
Country Comparative Guides 2025

Singapore
Fintech

Contributor

DREW & NAPIER

Drew & Napier LLC

Chua Tju Liang

Head of blockchain and digital assets practice | tjuliang.chua@drewnapier.com

Ulanda Oon

Senior Associate | ulanda.oon@drewnapier.com

This country-specific Q&A provides an overview of fintech laws and regulations applicable in Singapore.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Singapore: Fintech

1. What are the regulators for fintech companies in your jurisdiction?

The Monetary Authority of Singapore (MAS) is the primary regulator of Singapore's financial services industry, overseeing its financial institutions and sectors such as banking, capital markets and payments.

However, under Singapore's activity-based regulatory regime, certain activities undertaken by fintech companies may fall within the regulatory ambit of other regulatory authorities. For instance, (a) the Personal Data Protection Commission of Singapore (PDPC) regulates the use, collection and management of personal data; (b) the Competition and Consumer Commission of Singapore oversees consumer protection; and (c) the Cybersecurity Agency of Singapore oversees national cybersecurity and regulates critical information infrastructure.

2. Do you foresee any imminent risks to the growth of the fintech market in your jurisdiction?

Rising cybersecurity risks may undermine consumer trust, while rising geopolitical tensions may hinder adoption of fintech products and services, particularly for fintech companies involved in cross-border payments and global trade finance.

To mitigate risks, Singapore's government has launched campaigns to promote cybersecurity awareness, improve digital hygiene, and support regional cross-border cooperation. The MAS enhances digital trade infrastructure and adopts flexible regulations for fintech companies. In 2024, it has committed S$100 million under the Financial Sector Technology and Innovation Scheme 3.0 to advance quantum computing and AI.

3. Are fintechs required to be licensed or registered to operate in your jurisdiction?

Whether a fintech company must be licensed or registered in Singapore depends on its jurisdiction of incorporation, specific business activities and applicable exemptions. Relevant legislation include:

a. Securities and Futures Act (SFA);
b. Banking Act;
c. Financial Advisers Act;
d. Payment Services Act (PSA);
e. Cybersecurity Act;
f. Insurance Act;
g. Moneylenders Act;
h. Commodity Trading Act;
i. Precious Stones and Precious Metals (Prevention of Money Laundering and Terrorism Financing) Act (PSPMA);
j. Financial Services and Markets Act;
k. Trust Companies Act.

Where a fintech company engages in regulated activities under these laws, it may require a licence unless applicable exemptions apply.

4. What is a Regulatory Sandbox and how does it benefit fintech start-ups in your jurisdiction?

The MAS FinTech Regulatory Sandbox (Sandbox) allows financial institutions and fintech companies to experiment with new technologies and develop innovative financial products in a controlled environment within a defined timeframe.

The flexibility afforded by the Sandbox is especially beneficial to start-ups as the MAS may relax specific legal and regulatory requirements during the sandbox period, giving start-ups the runway to refine and test their products without incurring high compliance costs.

5. How do existing securities laws apply to initial coin offerings (ICOs) and other crypto assets, and what steps can companies take to ensure compliance in your jurisdiction?

Companies operating in the crypto-asset space in Singapore will have to consider two regulatory regimes – (a) the PSA regime, which regulates services in "digital payment tokens", and (b) the securities laws regime (principally the SFA). This will primarily be determined by the characteristics of the crypto assets that such companies deal with.

In general, most cryptocurrencies and stablecoins would constitute "digital payment tokens" under the PSA. Broadly speaking, most token issuers, digital asset custody service providers, and cryptocurrency exchanges

would require a licence under the PSA. See the response to Q7 for more details.

If the company deals with crypto assets that constitute capital markets products under the SFA, then the existing securities laws requirements will apply. In such cases, (a) the sale of such tokens will be subject to prospectus requirements unless exemptions apply (e.g. where such sale is to accredited or institutional investors); and (b) related activities pertaining to such sale (e.g. inducing the purchase of such tokens) could require a licence. Additionally, asset-backed tokens which deal with precious stones and metals will fall under the PSPMA. Please refer to the response to Q7 for further details.

Companies should seek legal advice on the characterisation of their tokens prior to finalising the token's functions, its launch or sale in Singapore. This would ensure flexibility to tweak certain functions (if necessary) based on counsel's feedback.

6. What are the key anti-money laundering (AML) and Know Your Customer (KYC) requirements for cryptocurrency exchanges in your jurisdiction, and how can companies implement effective compliance programs to meet these obligations?

Aside from requirements under general law (which apply to all businesses in Singapore) to carry out a reasonable standard of KYC and due diligence on transaction counterparties and customers, regulated cryptocurrency exchanges in Singapore must also satisfy specific AML/KYC obligations under the PSA. These include implementing policies and procedures covering customer due diligence (CDD), transaction-monitoring, suspicious transaction reporting, and record-keeping.

Exchanges must verify user and beneficial owner identities, comply with the travel rule for value transfers, and retain CDD and transaction records for at least five years. Customers and their connected parties must be screened against money laundering and terrorism-financing lists published by the MAS and other authorities.

To ensure compliance, companies should align AML/KYC policies with MAS guidelines (PSN02 and PS-G02), appoint experienced compliance teams, and conduct regular board-level reviews to address evolving risks.

7. How do government regulations requiring licensing or regulatory oversight impact the operations of cryptocurrency and blockchain companies in your jurisdiction, and what strategies can be employed to navigate these varying requirements?

Singapore's legal regime is technology-agnostic in that it does not regulate blockchain or cryptocurrency companies *per se*. Instead, it focuses on regulating specific underlying activities which such companies may conduct.

Generally, companies which carry on a business of providing account issuance, domestic or cross-border money transfers, merchant acquisition, e-money issuance, money-changing or digital payment token (DPT) services in Singapore must obtain a money-changing, standard payment institution or major payment institution licence unless exempted.

To expand, activities regulated as DPT services under the PSA include:

a. dealing in DPTs (e.g. conducting ICOs);
b. facilitating the exchange of DPTs where the service provider either comes into or does not come into possession of the moneys or DPTs involved (e.g. operating a centralized or decentralised exchange, respectively);
c. facilitating the transmission of DPTs from one account to another; and
d. providing custodial services for DPTs.

As such, given that most cryptocurrencies and stablecoins constitute DPTs, many token issuers, digital asset custody service providers and cryptocurrency exchanges require a licence under the PSA.

If a company's activities involve digital assets classified as CMPs under the SFA, licensing may be required. The following is a non-exhaustive list of key SFA-regulated activities that may be applicable:

a. dealing in CMPs;
b. advising on corporate finance;
c. fund management; and
d. providing custodial services.

Digital assets backed by precious stones or metals may also trigger registration requirements under the PSPMA. For instance, the sale or redemption of such asset-backed tokens which allow redemption of such underlying precious stones or metals may fall within the PSPMA's definition of "regulated dealing".

That said, MAS is not looking to regulate all

cryptocurrency and blockchain activities. Companies should engage experienced legal counsel to determine their preferred regulatory approach. Strategies include segregating business functions into different entities or adjusting product and service offerings to ensure compliance or to qualify for exemptions.

8. What measures should cryptocurrency companies take to comply with the governmental guidelines on tax reporting and obligations related to digital assets in your jurisdiction?

Singapore's tax regime, governed by the Income Tax Act and Goods and Services Tax (GST) Act, apply to the use of digital assets. Businesses must report the fair value of digital assets received for goods, services or trading to avoid under-reporting penalties. Singapore has no capital gains tax, and the corporate tax rate is 17%.

For GST-registered businesses, 9% GST applies to goods and services. However, when DPTs (as defined under the GST Act) are used as payment, they are not treated as a supply of services, so GST does not apply. Similarly, exchanges of DPTs for fiat currency or other tokens, and loans or credits involving such tokens, are GST-exempt.

However, uncertainty remains regarding GST applicability to digital assets falling outside the definition of DPTs under the GST Act. Companies should therefore seek professional advice to ensure compliance with evolving tax regulations.

9. How can blockchain companies address data privacy and protection regulations in your jurisdiction, while ensuring transparency and security on decentralized networks?

Singapore's Personal Data Protection Act (PDPA) requires companies to safeguard personal data in their possession or control against unauthorized access, use, disclosure or similar risks. Personal data includes any information identifying an individual, even if inaccurate, and must comply with PDPA requirements (e.g. reasonable security measures). The adequacy of security measures, judged objectively, is key to ensuring compliance.

The PDPC advises against storing personal data on permissionless blockchains in any form, as on-chain data permanence poses compliance risks. However, emerging technologies like zero-knowledge proofs may offer solutions by enabling credential verification without exposing personal data, supporting PDPA-compliant blockchain applications.

10. How do immigration policies, such as the U.S.'s H-1B and L-1 visas, impact the ability of fintech companies to hire international talent in your jurisdiction?

Singapore has put in place a number of immigration policies which aim to attract global talent and fortify its status as a fintech hub.

Foreign employees generally require a work pass. In line with Singapore's policy to appeal to international talent, there are a number of work passes which foreign employees may apply for:

- Employment Pass – for professionals, managers, and executives. Applicants must meet a salary benchmark (from S$6,200 for the financial services sector) and score at least 40 points under the COMPASS system, which evaluates salary norms, qualifications, diversity, local employment support, skill shortages, and government partnership initiatives. COMPASS-exemptions apply for fixed monthly salaries above S$22,500, or for specific roles (e.g. short-term positions, intra-corporate transferees).
- Tech.Pass – for established tech entrepreneurs, leaders, and experts. Eligibility requires meeting two of the following criteria: a last-drawn monthly salary of at least S$22,500, five years in a leading role at a tech company valued at US$500 million or with US$30 million funding, or five years contributing to a tech product with at least 100,000 monthly users or US$100 million annual revenue. Holders can start companies, work for multiple employers and sponsor family members. The pass is valid for two years, renewable for another two upon meeting criteria.
- EntrePass – for foreign entrepreneurs starting venture-backed or tech-focused businesses in Singapore. Applicants must have, or plan to establish a private limited company with at least 30% ownership, or a business backed by venture-funding or which owns innovative technologies. Additionally, they must also meet at least one of the following criteria: raise at least S$100,000 from a single funding round from investors for any past or current business, founded and sold a business that is venture-backed or owns innovative technologies, the business is or will be supported by an incubator or accelerator that is either government recognised or internationally renowned, hold intellectual property (IP) providing a significant competitive advantage, have a relevant ongoing research collaboration in Singapore with an

institute of higher learning or research institution. The pass is valid for up to one year, renewable for two years and allows family sponsorship if business spending and local job-creation requirements are met.

11. What are the key regulatory and compliance requirements that a fintech must address when entering the market in your jurisdiction, and how can the company ensure adherence to all applicable laws and regulations?

See response to Q3.

12. How should a fintech approach market entry strategy in your jurisdiction, considering factors such as target customer demographics, competitive landscape, and potential partnerships with banking and other financial institutions?

When entering the Singapore market, fintech companies should obtain legal advice on applicable solicitation or marketing restrictions pertaining to their products or services, as these may limit the fintech company's potential reach. For instance, the MAS has issued guidelines to regulated payment service providers, prohibiting such entities from promoting DPT services in public areas in Singapore.

In terms of customer demographics in the financial services sector, Singapore has more regulatory safeguards for retail customers than for accredited or institutional clients. Fintech companies targeting the latter may benefit from licensing exemptions.

Additionally, fintech companies may consider exploring partnerships with licensed banks and financial institutions. Collaborating with these entities can allow a fintech company to offer regulated services without needing to obtain its own licence.

13. What are the primary financial and operational risks associated with entering the market in your jurisdiction, and how can the fintech effectively mitigate these risks to ensure a smooth transition and sustainable growth?

Entering the Singapore market poses financial risks such as high setup costs for infrastructure, manpower, and regulatory compliance. Additionally, established competitors and marketing restrictions may hinder market penetration and delay revenue generation. To mitigate these risks, fintech companies should adopt a phased approach, initially targeting a narrow client base. This strategy helps manage regulatory compliance costs and assess product interest before the company decides to expand its offering to a broader retail market.

14. Does your jurisdiction allow certain business functions to be outsourced to an offshore location?

That depends on the type of business function to be outsourced offshore and whether the fintech company is a regulated entity.

If the fintech company is not a regulated financial institution, there are generally no specific outsourcing restrictions under Singapore law. However, if the company is a regulated financial institution in Singapore, it must adhere to MAS' outsourcing guidelines. These include requirements for risk-management, oversight of current and future outsourcing arrangements, service provider evaluation, business continuity plans and cloud computing usage.

15. What strategies can fintech companies use to effectively protect their proprietary algorithms and software in your jurisdiction, and how does patent eligibility apply to fintech innovations?

Singapore has a robust IP protection regime conducive to fintech innovation. Proprietary algorithms and software can be protected via three main methods, with each its advantages and disadvantages:

a. Patent protection – Patents provide exclusive rights for up to 20 years, allowing holders to make, sell, or use their invention. However, patent applicants must publicly disclose the details of their invention, which may include specific algorithms or training data sets, which could expose the technology to competitors.
b. Copyright protection – Copyright automatically protects original works in tangible form (e.g. algorithms, software, source codes). No registration is required, but the work must be original to qualify for exclusive control over its use.
c. Law of confidence – Apart from contractual duties of confidence, an obligation of confidence *vis-à-vis* confidential information may be imposed in equity under Singapore law. Companies can seek relief if confidential information is wrongfully accessed or exploited, ensuring secure use of proprietary data.

16. How can a fintech company safeguard its trademarks and service marks to protect its brand identity in your jurisdiction?

Singapore's trade mark registration regime grants registrants exclusive rights to use (and authorise others to use) the trade mark in relation to the goods or services for which it has been registered. As the mark's proprietor, the registrant can seek remedies for infringement of its trade mark under the Trade Marks Act 1998, including:

a. injunctions (subject to such terms as the court may deem fit);
b. damages;
c. account of profits; and
d. statutory damages for counterfeit marks.

Registered trade marks are protected for 10 years from the date of filing and can be renewed upon expiry.

Unregistered trade marks may also be protected under the law of passing off. To succeed, the plaintiff must establish goodwill in their goods or services, show that the defendant misrepresented their goods or services as those of the plaintiff, and prove that this misrepresentation has caused or is likely to cause harm to the plaintiff's goodwill.

17. What are the legal implications of using open-source software in fintech products in your jurisdiction, and how can companies ensure compliance with open-source licensing agreements?

The use of open-source software in fintech products is governed by the terms of the open-source license. Unauthorized use, or uses beyond the scope of licence permissions may breach the license and result in copyright or patent infringement. To ensure compliance, companies must use the software within the permitted scope of the license and adhere to any requirements, such as contributing modified works back to the open-source community under the same terms.

18. How can fintech startups navigate the complexities of intellectual property ownership when collaborating with third-party developers or entering into partnerships?

Fintech startups should ensure that agreements with third-party contractors expressly set out the treatment of IP developed during the course of the collaboration, whether any licences for use of such IP and non-competes are required, and consider matters dealing with moral rights. Furthermore, non-disclosure agreements and confidentiality clauses should be incorporated in the agreements with such contractors.

Additionally, where the collaboration involves parties in multiple jurisdictions, fintech startups should examine whether the IP law regimes in such jurisdictions are registration-based or well developed and consider the need for additional contractual protections.

19. What steps should fintech companies take to prevent and address potential IP infringements, such as unauthorized use of their technology or brand by competitors?

Fintech companies should first ensure that their IP is protected by the legal regime – refer to the response to Q15, Q16 and Q18 above. This provides the basis for which relief can be granted in respect of IP infringements.

From a preventative point of view, fintech companies can adopt technical safeguards to prevent competitors from copying or reverse-engineering proprietary software or algorithms. Strategies include keeping core algorithm logic on company servers to limit IP exposure, using virtual environments to isolate execution of sensitive algorithms, and implementing runtime integrity checks for tamper detection.

20. What are the legal obligations of fintechs regarding the transparency and fairness of AI algorithms, especially in credit scoring and lending decisions? How can companies demonstrate that their AI systems do not result in biased or discriminatory outcomes?

While Singapore's regulatory authorities have published several whitepapers and guidelines on AI-use in operations, these are not legally binding on fintech companies generally.

However, where a fintech is a regulated financial institution, MAS expects such companies to apply the Fairness, Ethics, Accountability and Transparency Principles (FEAT Principles) when using AI and data analytics (AIDA) for decision-making in providing financial products and services. The FEAT Principles were co-created by MAS and the financial industry to promote ethical AIDA deployment.

Broadly, the FEAT Principles cover:

- Fairness: AIDA decisions should not unjustifiably disadvantage individuals or groups. Data and models used in AIDA decisions should be regularly reviewed for accuracy, relevance and bias.
- Ethics: AIDA use must align with ethical standards, and codes of conduct.
- Accountability: AIDA usage must be approved by appropriate internal authorities, while data subjects should have ways to inquire, appeal and request reviews of AIDA decisions.
- Transparency: AIDA use should be proactively disclosed to data subjects, with clear explanations of data usage and decision impacts.

Fintech companies using AIDA should establish internal governance frameworks to ensure appropriate justifications for AIDA-driven decisions (including specific data attributes), particularly in credit scoring and lending. Notably, fintech companies which are regulated financial institutions are required to adhere to existing complaints management processes which are mandated by MAS notices and guidelines, and other legal obligations set out in the respective legislation. The FEAT Principles do not displace those obligations, but instead add colour to MAS' expectations of AIDA use.

To minimize AIDA-related bias or discriminatory outcomes, fintech companies may utilize the FEAT Principles Assessment Methodology and open-source toolkit ("**Veritas Documents**") developed as part of MAS' Veritas Initiative. The Veritas Documents aim to facilitate the systematic adoption of the FEAT Principles by financial institutions.

21. What are the IP considerations for fintech companies developing proprietary AI models? How can they protect their AI technologies and data sets from infringement, and what are the implications of using third-party AI tools?

See responses to Q15, 17, 18 and 19.

22. What specific financial regulations must fintechs adhere to when deploying AI solutions, and how can they ensure their AI applications comply with existing financial laws and regulations? Are there specific frameworks or guidelines provided by financial regulatory bodies regarding AI?

See response to Q20.

Fintech companies may refer to the PDPC's Model Artificial Intelligence Governance Framework which, while not legally binding on companies, outlines best practices for responsible AI deployment.

Given Singapore's technology-agnostic approach to financial services legislation and regulation (which prioritises regulating the impact of AI-deployment on consumers/businesses rather than AI *per se*), entities deploying AI should be aware that they may remain responsible for the outcomes arising from their AI use.

23. What risk management strategies should fintech companies adopt to mitigate potential legal liabilities associated with AI technologies?

The MAS published an Artificial Intelligence Model Risk Management Paper which sets out good practices for AI risk-management by banks and other financial institutions, focusing on risk-management strategies in several key areas, including AI governance, deployment and development. These practices include:

- implementing clear policies articulating FEAT Principles in AI deployment;
- developing comprehensive incident response plans to address potential AI-related issues; and
- ensuring careful negotiation of contracts with external service providers to appropriately address AI-related performance risks and allocate liability.

24. Are there any strong examples of disruption through fintech in your jurisdiction?

Robo-advisors revolutionize Singapore's investment sector by offering AI-driven, low-cost, automated financial advice through platforms like StashAway, Syfe, and Endowus. They eliminate traditional barriers like high fees and capital requirements, making wealth management accessible to retail investors, allowing alignment with individual goals, and driving innovation in the financial services industry.

Similarly, the InsurTech space has seen a rising utilisation of AI-driven tools and machine learning, particularly in the areas of fraud detection, claims processing and underwriting policies. Examples include Prudential's use of domain-specific GenAI models to automate the processing of policy documents, and FWD Group's launch of "FWD Brain", a centralised in-house platform which hosts AI models and outputs to deliver

personalised recommendations to customers.

25. Which areas of fintech are attracting investment in your jurisdiction, and at what level (Series A, Series B, etc.)?

Fintech investments in Singapore target digital banking, blockchain, decentralised finance, and asset tokenization.

This interest is fuelled by the introduction of digital bank licenses which liberalise Singapore's financial industry, coupled with the MAS' initiatives to promote blockchain innovation. The MAS is actively collaborating with global industry associations and financial institutions to enhance the commercial viability and explore the integration of these technologies into traditional finance.

Investments in these fintech areas are primarily in early-stage financing.

Contributors

Chua Tju Liang
Head of blockchain and digital assets practice
tjuliang.chua@drewnapier.com

Ulanda Oon
Senior Associate
ulanda.oon@drewnapier.com