Legal 500
Country Comparative Guides 2025

Australia
Fintech

Contributor

Gilbert + Tobin

Peter Reeves

Partner | preeves@gtlaw.com.au

Georgina Willcock

Special Counsel | gwillcock@gtlaw.com.au

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

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

Australia: Fintech

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

There is no single regulator responsible for regulating fintech companies in Australia. The applicable regulators depend on the nature of the services provided, and activities engaged in, by a fintech company. The most commonly relevant regulators are as follows:

The Australian Securities and Investments Commission (**ASIC**) is Australia's integrated corporate, markets, financial services and consumer credit regulator. ASIC administers various legislation including the *Corporations Act 2001* (Cth), the *Australian Securities and Investments Commission Act 2001* (Cth), the *National Consumer Credit Protection Act 2009* (Cth), the *Financial Accountability Regime Act 2023* (Cth), and parts of certain other pieces of legislation such as the *Banking Act 1959* (Cth) and the *Superannuation Industry (Supervision) Act 1993* (Cth). ASIC's responsibilities include licensing, industry supervision and surveillance, administering and enforcing consumer protection provisions including the unfair contracts regimes, and enforcement.

The Australian Prudential Regulation Authority (**APRA**) is Australia's prudential regulator of banks, insurance companies and most superannuation funds. Prudential regulation is concerned with maintaining the safety and soundness of financial institutions, and protecting the interests of depositors, policy holders and superannuation fund members. APRA works closely with ASIC, the Australian Treasury and the Reserve Bank of Australia.

The Australian Competition and Consumer Commission (**ACCC**) is Australia's national competition, consumer, fair trading and product safety regulator. The ACCC administers the *Competition and Consumer Act 2010* (Cth), which covers a range of relationships and responsibilities including product safety and labelling, unfair market practices, price monitoring, industry codes and regulation, and mergers & acquisitions. In the near future, the ACCC's responsibilities will likely expand to administer a new Scams Protection Framework, for which ASIC (and other regulators) will likely also have responsibility.

The Australian Transaction Reports and Analysis Centre (**AUSTRAC**) is Australia's financial intelligence unit and anti-money laundering and counter-terrorism financing (**AML/CTF**) regulator. AUSTRAC's responsibilities include receiving and processing suspicious matter and funds transfer reports in order to assist in detecting and disrupting serious and organised crime.

The Office of the Australian Information Commission (**OAIC**) promotes and upholds privacy and information access rights, including by administering the *Privacy Act 1988* (Cth). The OAIC's regulatory responsibilities are evolving with the development of a consumer data right and a national DigitalID framework.

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

Notwithstanding occasional comments to the contrary, the Australian Government, legislators and regulators are, at best, lethargic when it comes to providing regulatory certainty and paths to market for the digital assets sector. ASIC's recent approach to administering laws that may apply to digital assets businesses has been that of "regulation by enforcement", creating an uncertain and at times hostile environment for digital asset businesses. Due in part to the regulatory treatment, it can be extremely challenging for digital asset fintech businesses to open Australian bank accounts, onboard with established payment rails and to obtain insurance. Proposed reforms are not progressing with pace nor do they contain measures to meaningfully support the Australian digital asset sector.

As at the date of writing, various reforms relevant to the fintech market are underway in Australia. These include reforms to the AML/CTF laws, payment regulation laws and digital asset laws. While none of these present imminent risks per se, it does create an fluid environment that can be challenging to launch new businesses and products with certainty of regulatory outcomes.

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

This depends on the nature of the activities engaged in, and services provided by, the fintech. For example:

- if the fintech is carrying on a business of providing a

financial service (eg, a business of providing financial product advice, dealing in financial products, providing a custodial or depository service or making a market in financial products), the fintech may be required to hold an Australian financial services licence (**AFSL**).
- if the fintech is carrying on a business of engaging in consumer credit activities, the fintech may be required to hold an Australian credit licence (**ACL**).
- if the fintech is operating a financial market, the fintech may be required to hold an Australian market licence.
- if the fintech is carrying on a banking business, the fintech may be required to be an authorised deposit-taking institution.
- if the fintech is providing remittance or digital currency exchange services, the fintech may be required to be registered with AUSTRAC.

Additionally, if the fintech is carrying on a business of any kind in Australia, the business must register with ASIC as a foreign company.

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

A regulatory sandbox is a framework established by a regulator which allows fintech start-ups and other innovators to conduct live experiments in a controlled environment, under regulatory supervision. Essentially, permitting Fintechs to operate small-scale financial services or credit activities as pilot products or short-term projects, without having to adhere to stringent licensing requirements. However, participation in the regulatory sandbox is subject to strict eligibility criteria, notably that there must be a net benefit to the public, the product or service must be new and innovative, and only certain kinds of businesses, products and services are eligible.

Next year will mark ten years since ASIC established the fintech regulatory sandbox. This framework allows eligible businesses to test specific financial services and products, as well as engage in credit activities, without the requirement to hold an AFS licence or an ACL. In 2020, a new 'enhanced regulatory sandbox' was established by the Australian Government, to increase the testing period to a maximum of 24 months, and to widen the scope of permissible testing to encompass a more extensive range of financial services and credit activities. ASIC is engaged in an enhanced cooperation agreement with the United Kingdom's Financial Conduct Authority. This agreement facilitates the mutual referral of innovative businesses to each other's regulatory sandboxes, benefitting fintech start-ups through enhanced cross-border collaboration.

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?

Existing securities laws will apply to ICOs and other crypto assets where the offering constitutes the provision of a financial service. Issuers and other service providers (eg, promoters; asset holders) may be required to hold an AFSL or be able to rely on an exemption, as well as comply with applicable conduct and disclosure obligations.

ASIC has released Information Sheet 225: Crypto-assets. This information sheet sets out guidance and ASIC's expectations regarding raising funds through an ICO and engaging in other crypto related activities. In December 2024, ASIC published a Consultation Paper proposing updates to this information sheet. The consultation paper includes a number of "worked examples" of crypto asset related activities and ASIC's views on whether these activities involve the provision of a regulated service. The consultation process will close at the end of February 2025.

Even if a crypto asset is not a financial product, it is still subject to regulatory oversight in Australia. This includes under the Australian consumer law (**ACL**), which contains consumer protection provisions that include a prohibition on misleading or deceptive conduct and restrictions on referral selling arrangements.

The AML/CTF Act will apply to operators of digital currency exchange services. From July 2026, the AML/CTF Act will apply to other virtual asset service providers, including on and off ramp providers, transferors of virtual assets, providers of asset holding or administration services and providers of offer or sale services.

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?

If an entity provides a designated service in Australia and has a geographical connection to Australia, the entity is a reporting entity and has obligations under the AML/CTF Act. These obligations include to:

- enrol (and, if required, register) with AUSTRAC;
- adopt and maintain a compliant AML/CTF Program that includes risk based procedures for carrying out customer due diligence and a program for monitoring transactions;
- report suspicious matters and international funds transfer instructions to AUSTRAC, as well as an annual compliance report; and
- record keeping requirements.

In relation to KYC, the obligations are generally risk based and require that the reporting entity take reasonable steps to identify and verify the identity of the customer, to determine that the customer is who they say they are and to identify beneficial owners. Additional KYC requirements may apply in relation to high risk customers, jurisdictions, designated services or delivery channels.

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?

This depends on the nature of the activities engaged in, and services provided by, the fintech. Refer to the response to questions 3 and 5 above, and 11 and 12 below.

As a general comment, we note that there are various legislative and regulatory reforms underway and matters before Australian courts, the outcomes of which will impact the operations of cryptocurrency and blockchain business in Australia.

We recommend a fintech work with local counsel to determine and understand the legal and regulatory landscape that is applicable to the proposed offering. This work should include operational and tax efficient structuring advice, as well as identifying any applicable licensing, registration, approval or exemption requirements. Conduct and disclosure requirements will generally flow from any required licenses, registrations, approvals or 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?

Income Tax

As of 1 January 2025, there are no specific tax reporting or other tax-related obligations applicable to digital assets.

From an income tax perspective, Australian tax resident cryptocurrency companies are generally taxable in Australia on all worldwide income (although exemptions and tax credits may be available in respect of foreign sourced income). Conversely, non-Australian tax resident cryptocurrency companies are generally only subject to income tax in Australia on “Australian sourced” income. The source of income is generally fact-dependent although in certain circumstances, Australian domestic tax law or an applicable tax treaty may impact this position.

Relevantly:

- if a non-Australian incorporated cryptocurrency company has board members, board meetings or key decisions makers physically located in Australia, care should be taken to ensure the company is not treated as an Australian tax resident (e.g., by virtue of the company's central management and control being in Australia); and
- if a non-Australian tax resident cryptocurrency company has a presence in Australia (e.g., a fixed place of business such as an office, or employees located in Australia), care should be taken to ensure this does not give rise to Australian sourced income via an Australian permanent establishment.

Protocols can be implemented to mitigate each of the above risks.

Having regard to the above, it is important for cryptocurrency companies to consider their residency for Australian tax purposes as this will determine whether they are subject to Australian corporate tax on income from worldwide sources or only on Australian-sourced income.

From an Australian income tax perspective:

- digital assets are not treated as “money”, but rather are capital gains tax assets;
- gains on the disposal of digital assets may be taxed on “revenue” account (i.e., akin to ordinary income) or on “capital” account (which may give rise to concessional tax outcomes). The distinction between revenue and capital gains depends on various factors such as whether the taxpayer is a trader, for what purpose digital assets were acquired (e.g. for disposal at a profit in the short-term, or to hold long-term), and

the ability to derive an income stream from the digital assets (e.g., from staking); and
- rewards for staking digital assets are generally treated as ordinary income.

Although there is no specific tax law governing the tax treatment of digital assets and cryptocurrency, the Australian Taxation Office (**ATO**) has issued guidance on a range of issues including the above and other transactions such as lending and borrowing with decentralised finance protocols, the supply of cryptocurrency to liquidity pools and the wrapping of tokens. Where taxpayers enters into transactions involving the acquisition or disposal of digital assets or cryptocurrency, the ATO requires the keeping of records to evidence the calculation of capital gains and losses including dates and Australian dollar values of transactions. Companies which transact in cryptocurrency should review the ATO guidance and ensure they are aware of the ATO's views on the tax treatment of various transactions involving cryptocurrency as well as the ATO's record keeping requirements.

Goods and services tax

The treatment of digital assets for Australian goods and services tax (GST) purposes depends on, in addition to other factors, the nature of the digital asset in question.

The sale or purchase of cryptocurrency which is a "digital currency" (as defined) is not subject to GST in Australia. A "digital currency" is, for GST purposes, a digital unit of value that:

- is fully interchangeable with the same digital currency;
- can be provided as payment;
- is available to the public free of any substantial restrictions;
- is either:
- not denominated in any country's currency; or
- denominated in a currency that is not issued by, or under the authority of, an Australian or foreign government;
- does not have a value that is derived from or is dependent on anything else; and
- does not give an entitlement to receive something else unless it is incidental to holding it or using it as payment.

Examples of digital currency include Bitcoin, Ethereum and Litecoin.The supply of a digital currency (as defined) in exchange for money or other digital currency is either an input taxed financial supply (if supplied to an Australian resident located in Australia) or a GST-free supply (if supplied to a non-resident who is not located in Australia). As such, the suppliers of cryptocurrency are not required to remit GST to the ATO on the supply of cryptocurrency, but may also be restricted from claiming input tax credits on the GST charged on costs that relate to these supplies.

Otherwise, the normal GST rules apply to using digital currency to pay for goods and services as if the digital currency is money but the remittance of GST to the ATO on any taxable supply of goods or services must be in Australian currency. Generally, whether GST is payable on a supply of goods and services depends on a number of factors, including whether the supplier is registered (or required to register because it has a GST turnover of A$75,000 or more) for GST and whether the supply is made in the course or furtherance of an enterprise. In this regard, the scope of carrying on an "enterprise" is broader than carrying on a "business", and includes an activity, or a series of activities, in the form of business or in the form of an adventure or concern in the nature of trade.

For other cryptocurrencies which are not digital currency, such as a non-fungible token (NFT), a stablecoin pegged to the value of some other asset, or certain initial coin offerings, the GST treatment can be more complex and may depend on the specific characteristics and use of the asset. In general, the domestic supply of an NFT is a taxable supply and a stablecoin is an input taxed financial supply.

It is important to note that the tax treatment of digital assets in Australia is nuanced and subject to change, especially as the digital asset landscape continues to evolve.

Crypto Asset Reporting Framework

The OECD has developed a Crypto Asset Reporting Framework (**CARF**) with related amendments to the Common Reporting Standard. The OECD CARF is a new tax transparency framework which provides an international standard for the automatic exchange of crypto related account information between tax authorities. Australia has signalled an intention to implement the CARF by 2027, however the way in which this will occur has not yet been determined. Consultation is ongoing.

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

In Australia, the *Privacy Act 1988* (Cth) (**Privacy Act**) regulates the handling of personal information by Government agencies and private sector organisations with an aggregate group revenue of at least A$3 million with a jurisdictional link to Australia. In some instances, the Privacy Act will apply to businesses (eg, credit providers and credit reporting bodies) regardless of turnover. The Privacy Act includes 13 Australian Privacy Principles, which impose obligations on the collection, use, disclosure, retention and destruction of personal information. Relevantly, before entities collect personal information, they must disclose the way in which this data will be used, the purposes for which it will be used and third parties to which it is likely to be disclosed. This is the basis on which individuals provide consent for their personal information to be collected, used and disclosed. Note, Australia's privacy legislation is currently the subject of reform and it is anticipated that there will be significant changes in this space.

Blockchain arrangements can be structured in various ways, from information being readily visible to all participants on a network, to closed networks where information is limited to specific participants in specific instances. Therefore, entities wishing to collect and use personal information through blockchain implementations must ensure that they have gained appropriate consents for the contemplated use and disclosure.

The Notifiable Data Breaches (**NDB**) scheme was implemented in 2018. The NDB scheme mandates that entities regulated under the Privacy Act are required to notify any affected individuals and the Office of the Australian Information Commissioner in the event of a data breach (ie, unauthorised access to or disclosure of information) which is likely to result in serious harm to those individuals. The NDB scheme applies to agencies and organisations that the Privacy Act requires to take steps to secure certain categories of personal information. Therefore, entities will also need to ensure that any blockchain implementations are sufficiently protected from security issues such as unauthorised access and operational failure, and in the case of a data breach, ensure that they have adequate processes in place to comply with the NDB scheme.

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?

Migrants require working visas from the Department of Home Affairs (**DOHA**) to work in Australia, and each type has its own eligibility requirements. Businesses can nominate or sponsor such visas.

The Temporary Skill Shortage (subclass 482) visa (TSS visa) is the most common form of employer-sponsored visa for immigration to Australia. To be eligible for the TSS visa, an applicant's occupation must:

- be on the short-term skilled occupations list, with a maximum visa period of two years, or up to four years if an International Trade Obligation applies (Hong Kong passport holders are eligible for up to five years), with an option to apply for permanent residency subject to eligibility requirements;
- be on the medium-and long-term strategy skills list or the regional occupational list, with a maximum period of four years (or five years for Hong Kong passport holders) and an option to apply for permanent residency, subject to eligibility requirements; or
- have an employer that has a labour agreement with the Australian Government in effect, with a maximum period of up to four years (or five years for Hong Kong passport holders).

The DOHA has created a Global Business & Talent Attraction Taskforce to attract high value businesses and individuals to Australia. The Taskforce facilitates the Global Talent Visa program and Global Talent Employer Sponsored program. To be invited to apply for a visa under the Global Talent Visa program, a candidate must be highly skilled in one of the ten target sectors (including digitech and financial services and fintech) and be able to attract a salary that meets the high income threshold.

Government is working to fill gaps in access to talent and in the recent budget, announced its commitment to create 1.2 million tech-related jobs by 2030 and deliver programs to support tech skills and innovation in Australia (including in the areas of artificial intelligence and quantum technologies) over the next financial year.

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?

Broadly, fintechs should consider (and potentially seek advice from local counsel) on Australian corporate registration, licensing / approval requirements, restrictions on ownership (eg, foreign ownership restrictions), consumer protection requirements, privacy and data protection requirements, and taxation.

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?

We recommend a fintech work with local counsel to determine and understand the legal and regulatory landscape that is applicable to the proposed offering. This work should include operational and tax efficient structuring advice, as well as identifying any applicable licensing, registration, approval or exemption requirements. Conduct and disclosure requirements will generally flow from any required licenses, registrations, approvals or exemptions.

Assessment of target customer demographics will form part of this exercise, due to Australia's consumer-centric approach to product design and distribution. Local counsel can assist with understanding the competitive landscape (including any competition analysis required from the perspective of relevant law), and can facilitate arrangements with local banking and financial institutions.

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?

This depends on the nature of the fintech and the services provided by the fintech. If the fintech is the provider of a regulated service such as a financial, consumer credit or banking service, the fintech will likely have regulatory capital requirements to support financial stability and consumer outcomes. Similarly, a provider of a regulated service will likely have licensing, conduct and disclosure requirements that will need to be integrated into operations and generally require some level of onshore human, financial and technological resourcing.

We recommend seeking local advice to understand the applicable risks.

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

This depends on the nature of the fintech and the services provided by the fintech. Generally, unless the fintech is APRA regulated, there is no legal or regulatory restriction on outsourcing to an offshore location. However, depending on the nature of the business, Australian consumers may expect certain functions remain onshore.

If the fintech is APRA regulated, there is an APRA approval process for an outsourcing of a material business activity to an offshore service provider.

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?

In Australia, it is challenging to secure patent protection for fintech innovations. There is uncertainty as to whether an invention that uses or features computer software or hardware will be patentable subject matter under the *Patents Act 1990* (Cth) and courts will likely consider this issue on a case-by-case basis. Generally, a mere scheme, plan or discovery, or mere abstract ideas or information are not patentable subject matter.

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

There are multiple layers of protection available to fintechs in Australia in respect of intellectual property (**IP**). Key forms of protection are outlined below. Sophisticated fintechs have a strategy that leverages many, if not all of these:

Copyright: Copyright legislation in Australia protects many aspects of fintech innovation, including source code, visual features, application programming interface structures, and other works. Copyright arises automatically on creation of an original work. An important limitation is that it protects the material expression of an idea, rather than the idea itself. Human authorship is also required for copyright to subsist.

Confidential information: Trade secrets and know-how are particularly valuable in the fintech space, given the difficulties in securing patent protection for software. Confidential information is protected under common law. There is no statutory trade secrets regime. This means that robust contractual and practical protections in respect of confidential information are essential.

Trade marks: Establishing a unique brand and building goodwill in that brand is a key strategy for protection of

fintech innovation in Australia, given the limitations of the other forms of protection. Australia recognises registered and unregistered trade mark rights, however registered trade marks are significantly simpler to enforce and commercialise.

Contractual protections (third party creation of IP): Where IP is created for a fintech by a third party, it is important to consider whether there is an effective assignment of the IP created by the third party and whether all of the relevant IP is captured within the agreement (e.g. including where any improvements to a fintech business' intellectual property are made by the third party). Australia does not have a 'work made for hire' regime, so contractual assignment provisions are essential.

Employee created intellectual property: By default, IP created by employees is owned by the employer, where the creation of IP is within the scope of their engagement. However, to avoid disputes about ownership, it is important to ensure that employment agreements contain adequate assignment provisions.

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?

If the fintech company makes its own open-source software available to third parties:

- There is a risk that another person may use that open-source software to develop another product or service, notwithstanding any restrictions in the open-source licensing agreement. In our experience, it is difficult to enforce contraventions of terms that restrict use of open-source software.
- The terms of the licensing agreement should contain appropriate limitations on liabilities and disclaimers on fitness and propriety (to the maximum extent permitted by law).

If the fintech company is the consumer / user of open-source software, the fintech company should:

- Ensure that it complies with the terms of the licensing agreement, particularly insofar as terms restrict the fintech's ability to use, modify or redistribute the software.
- Undertake due diligence testing on the code to ensure it is fit for purpose (especially in relation to security vulnerabilities).
- Undertake due diligence to identify any third party IP risks in using the software.

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

A fintech startup should develop a confidentiality / non-disclosure agreement that can be agreed with counterparties prior to entering into commercial or legal discussions.

We recommend seeking local legal advice to assist in negotiating any IP licence terms or terms of use.

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?

Refer to the protections set out in question 16.

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?

There are no specific laws applicable to the use, development and adoption of AI or machine learning in Australia. However, other data protections apply (e.g. Privacy Act requirements apply to AI technologies that use personal information). Importantly, the Privacy Act does not contain a specific principle related to automated decision making (such as is available under the General Data Protection Regulation) however, privacy reforms may introduce a similar principle in the future.

Fintechs should consider any discrimination or biases that may arise from their use of AI and monitor their AI products to ensure discriminatory outcomes are not experienced. Further, where AI solutions are implemented to provide financial services or undertake credit activities, the business must train and monitor its AI solution to comply with the applicable laws and ensure there are no negative consumer outcomes.

If a fintech is regulated (eg, as an AFSL holder because it carries on a business of providing financial services), the fintech must ensure its use of AI is consistent with its

regulatory obligations.

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?

Regarding protecting AI technologies, refer to the response to question 16.

Regarding the use of third-party AI tools, use will be governed by the terms of agreement with the AI service provider. This will likely limit the user's rights to develop, modify or improve the AI, and will generally restrict any ownership interests in the AI.

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?

Whilst not currently a legal requirement for the private sector, the Government has designed 8 AI Ethics Principles, which provide a voluntary framework designed to complement (but not substitute) current AI practices. It has also hosted two consultations relating to the identifying the risks and responsible use of AI including one which concluded in May 2022 and one which concluded in August 2023.

More specifically, Australian regulators had made statements expressing general support for the use of AI but reminding the regulated population to be mindful of obligations.

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

This depends on the nature of the business and the way that AI is deployed by the fintech. At a minimum, the fintech should apply its risk management methodology to identify, assess, mitigate and monitor the risks associated with the use of any AI technologies. Effective risk management may require additional human resources with specific expertise in AI technologies, and disclosure of risks to clients.

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

Australia has a very active and innovative payments sector, with lots of businesses looking to make non-cash payments more affordable, accessible and fast. An evolving regulatory landscape makes these offerings complex but also creates opportunities for disruption.

Fintech disruption in offerings related to cost of living and housing affordability are particularly prevalent. There are various successful operators of fractionalised and tokenised property investment or ownership models, and various providers of fast and convenient liquidity for specific purposes such as funding deposits or bridging finance.

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

Most areas of fintech are attractive to investors in Australia. Payment service providers, fractionalised or tokenised investment models and consumer credit offerings are particularly attractive. Investment occurs at all levels, however we see Series B onwards as the more common level.

Contributors

Peter Reeves
Partner
preeves@gtlaw.com.au

Georgina Willcock
Special Counsel
gwillcock@gtlaw.com.au