International
Comparative
Legal Guides

Practical cross-border insights into fintech law

Fintech 2023

Seventh Edition

Contributing Editors:
Rob Sumroy & James Cook
Slaughter and May

ICLG.com

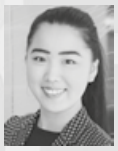
Expert Analysis Chapter

Q&A Chapters

Q&A Chapters Continued

Australia


Peter Reeves


Emily Shen


Meg Dalco

Gilbert + Tobin

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and the state of the development of the market, including in response to the COVID-19 pandemic and ESG (Environmental, Social and Governance) objectives. Are there any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications)?

The COVID-19 pandemic has been the defining feature of the Australian landscape over the last few years, which has resulted in some instability in the market. There has been a focus on fintech and the rapid digital evolution of the financial sector, with many fintech businesses developing and refining product and service offerings to better meet shifting consumer preferences and reflect innovations and opportunities created by technology.

As of 2023, the pace of fintech creation, development and adoption has been propelled by a broadening of product offerings by the Australian fintech community and assisted by the maturing of the Australian policy and regulatory approach. While previous fintech offerings were limited to operating on the periphery of traditional financial services (including lending, personal finance and asset management), the sector has now moved to disrupt the core product offering of many Australian institutional financial service providers, including payments, wallets, supply chain, wealth and investment, data and analytics and decentralised finance. In the data and investment sector in particular, there have been opportunities for fintechs to assist businesses with growing investor preferences for sustainable investing by collating and analysing Environmental, Social and Governance (**ESG**) data.

Though the fintech sector continued to sustain growth overall in 2022, there have been some concerns regarding the possibility of a recession due to uncertainties relating to the Russia-Ukraine conflict, rising interest rates and continued issues with global supply chains. 2022 saw the total number of deals decrease, indicating a shift in investor attitude towards targeted fintech investments. However, experts have indicated that the slowdown of growth in the fintech sector is relative to what was seen in 2019 and 2020 (indicating that it is still growing at reasonable levels), and previous record investments have maintained long-term investor confidence, demonstrating that the current downturn in the fintech sector is likely a short-term issue. Regulators and the Government face the challenge of adapting and aligning existing financial regulation to new products and services, balancing innovation with consumer protection. Regulators such as the Australian Securities and Investments Commission (**ASIC**), Australian Prudential Regulation Authority (**APRA**) and Australian Transaction Reports and Analysis Centre (**AUSTRAC**) have become more proactive on licensing, conduct and disclosure and have taken a more rigorous approach to enforcement. In particular, ASIC has become significantly more active in enforcing disclosure issues with respect to design and distribution obligations, and crypto assets (see question 3.3).

Australia's current financial services policy and regulatory context is still largely informed by the findings of the 2017–2019 Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (**Royal Commission**), the outcome of which was a series of recommendations for regulatory reform, focusing on matters such as prioritising the interests of consumers, overhauling conflicted remuneration structures and changing the way add-on products are distributed. A raft of legislative changes followed (or are expected to follow) to implement these recommendations and fintechs – particularly those that are motivated to provide financial services in a way that is more convenient, personalised and simplified for consumers – will be well placed to adapt to these changes, and seize the opportunity presented by the current public sentiment of dissatisfaction with traditional providers. As part of the Government's response to the Royal Commission, the Australian Law Reform Commission (**ALRC**) conducted an inquiry into simplifying Australia's financial services regulatory framework to make it "more adaptive, efficient and navigable for consumers and regulated entities". The ALRC has agreed to provide interim reports on three areas, being the design and use of definitions in corporations and financial services legislation, the regulatory design and hierarchy of laws, and the potential to reframe or restructure Chapter 7 of the *Corporations Act 2001* (Cth) (**Corporations Act**) (i.e. the overarching financial services laws). The first interim report on definitions and the second interim report on regulatory design and legislative hierarchy have both been released. The third and final interim report on potential reframing or restructuring of Chapter 7 of the Corporations Act is expected to be released on 25 August 2023. A consolidated final report is due 30 November 2023.

However, regulators and legislators are also looking beyond the findings of the Royal Commission as the financial services sector adapts.

There has been a raft of targeted reviews in this space, including the Council of Financial Regulators' (**CFR**) Stored Value Facility Review, the Treasury Payments System Review, the Senate Select Committee on Australia as a Technology and Financial Centre and the Parliamentary Joint Committee Inquiry into Mobile Payments and Digital Wallets. More recently:

- on 23 December 2022, the Australian Treasury (**Treasury**) closed its consultation on regulating buy now, pay later (**BNPL**) arrangements, with the intention of reducing the potential for consumer harm;
- on 3 February 2023, the Treasury released its highly anticipated consultation paper on "token mapping", a foundational step in the Government's intended plans to regulate the crypto sector;
- the Treasury closed a consultation on 6 February 2023 with respect to the Government's Strategic Plan for the Payments System, which sets a reform agenda including but not limited to updating the *Payment Systems (Regulation) Act 1998* (Cth) (**PSRA**) to capture the full suite of payment entities and systems, and implementing a tiered licensing framework for payment service providers;
- on 8 February 2023, the Government released the final report from the Quality of Advice Review, which sets out key recommendations with respect to the regulation of general and personal advice;
- on 16 February 2023, the Attorney-General released the detailed Privacy Act Review Report, providing 116 proposals at a principal level on how the *Privacy Act 1998 (Cth)* (**Privacy Act**) can be uplifted to best fit the consumer privacy needs; and
- on 20 April 2023, the Attorney-General released its proposed reforms to the *Anti-Money Laundering/Counter-Terrorism Financing Act 2006* (**AML/CTF Act**), with consultation open until 16 June 2023.

For the past few years there has been sustained attention on blockchain technology and a growth in interest in the technology by established businesses in the financial services sector. In particular, there has been growing interest in how decentralisation and new governance models such as decentralised autonomous organisations (**DAOs**) can exist and be regulated. It is expected that further clarity on the application of the Australian regulatory regime to such models will come in due course – the Senate Select Committee on Australia as a Technology and Financial Centre recommended the introduction of a new DAO legal entity in Australian corporate law and this recommendation has been agreed to by the Government.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

At the time of writing, there have not been any prohibitions or restrictions on specific fintech business types. Cryptocurrency-based businesses are permitted in Australia, provided such businesses comply with applicable laws (including financial services and consumer laws).

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Equity funding

Businesses can raise equity using traditional private and public fundraising methods (e.g. private placement, initial public offering (**IPO**), and seed and venture capital strategies), through grants and initiatives offered by Government and State/Territory agencies, and through crowdfunding.

In late 2017, a regulatory framework was introduced for crowd-sourced equity funding (**CSEF**) by public companies from retail investors. While reducing the regulatory barriers to investing in small and start-up businesses, the framework also created certain licensing and disclosure obligations for CSEF intermediaries (i.e. persons listing CSEF offers for public companies). This regime was extended in 2018 to also apply to proprietary companies. While there are a range of reporting requirements imposed on proprietary companies engaging in crowdfunding, there are also a number of concessions made with respect to restrictions that would otherwise apply to their fundraising activities.

Under the CSEF framework, there are exemptions for persons operating markets and clearing and settlement (**CS**) facilities from the licensing regimes that would otherwise be applicable to those facilities. These additional exemptions provide a means by which a person operating a platform for secondary trading can seek an exemption with tailored conditions from more onerous licensing requirements.

ASIC has released *Regulatory Guides 261 Crowd-sourced funding: Guide for Companies* and *262 Crowd-sourced funding: Guide for intermediaries* to assist companies seeking to raise funds through CSEF and intermediaries seeking to provide CSEF services, respectively.

Debt funding

There have been calls to extend the existing crowdfunding framework to debt funding, and the Government has previously indicated that it intends to consult on this. Debt financing is less common than equity financing in the Australian fintech sector; however, businesses can approach financial institutions, suppliers and finance companies in relation to debt finance.

Asia Region Funds Passport and Corporate Collective Investment Vehicles

The Asia Region Funds Passport (**Passport**) was introduced in 2018 and is a region-wide initiative designed to facilitate the offer of interests in certain collective investment schemes (**CIS**), established in Passport member economies to investors in other Passport member economies. It aims to provide Australian fund managers and operators with greater access to economies in the Asia-Pacific region by reducing regulatory hurdles.

On 10 February 2022, the Government passed the *Corporate Collective Investment Framework and Other Measures Bill 2021* (Cth), which introduced a new type of corporate fund vehicle known as a "corporate collective investment vehicle" (**CCIV**) from 1 July 2022. The policy behind the CCIV regime was to introduce a new type of investment vehicle which is attractive to foreign investors, thereby improving the competitiveness of Australia's managed funds industry. It is intended to complement the Passport by making Australian funds more accessible to foreign investors.

The Australian funds market is dominated by unit trusts, a structure that historically has been unfamiliar to many offshore jurisdictions where corporate and limited partnership investment vehicles are the norm throughout the Asia-Pacific region. The CCIV will provide an internationally recognised investment vehicle which will be able to be more readily marketed to foreign investors (including through the Passport).

There are concerns that the reforms will add extra complexity, given the far-reaching potential changes to corporate, partnership and tax laws. However, the enactment of the Passport and the CCIV may lead to new financing opportunities for fintech businesses.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Incentives for investors

(1) **Early stage innovation company incentives**
Incentives are available for eligible investments made in start-ups known as Early Stage Innovation Companies (**ESICs**), which are generally newly incorporated entities with low income and expenses.
Investments of less than 30% of the equity in an ESIC would generally qualify for a 20% non-refundable carry forward tax offset (capped at AUD 200,000 per investor and their affiliates combined in each income year, including any offsets carried forward from the prior year's investment) and a 10-year tax exemption on any capital gains arising on disposal of the investment (provided they are held for at least one year but less than 10 years).

(2) **Eligible venture capital limited partnerships**
Fintech investment vehicles may be structured as venture capital limited partnerships (**VCLPs**) or early stage venture capital limited partnerships (**ESVCLPs**), and receive favourable tax treatment for eligible venture capital investments.
For VCLPs, benefits include tax exemptions for foreign investors (limited partners) on their share of any revenue or capital gains made on disposal of the investment by the VCLP, and concessional treatment of the fund manager's carried interest in the VCLP. For ESVCLPs, the income tax exemption for VCLPs is extended to both resident and non-resident investors, plus investors obtain a 10% carry forward non-refundable tax offset for new capital invested in the ESVCLP.

Incentives for fintechs

The Research & Development (**R&D**) Tax Incentive programme is available for entities incurring eligible expenditure on R&D activities, which includes certain software R&D activities commonly conducted by fintechs. Claimants under the R&D Tax Incentive programme may be eligible for one of the following incentives:

(a) *Small businesses (less than AUD 20 million aggregated turnover)*: a refundable offset of 18.5% above the claimant's corporate tax rate, which is 25% (if the claimant is eligible for the lower corporate tax rate), providing a total 43.5% refundable tax offset; or

(b) *Other businesses (aggregated turnover of AUD 20 million or more)*: a non-refundable tax offset of the claimant's corporate tax rate, plus an incremental premium of either 8.5% (for R&D expenditure between 0% and 2% R&D intensity) or 16.5% (for R&D expenditure above 2% R&D intensity). A claimant's incremental premium is based on its R&D intensity, which is the proportion of the claimant's eligible R&D expenditure as a percentage of total business expenditure.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The ASX sets out 20 conditions to be satisfied in its Listing Rules. Briefly, these include the entity having at least 300 non-affiliated security holders each holding the value of at least AUD 2,000, and the entity satisfying either the profit test or the assets test (which requires particular financial thresholds to be met).

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

There have been a number of IPOs including that of Butn, which operates a payments and funding solution for organisations, Beforepay, an app providing "pay on demand" services, and Halo Technologies Holdings, a fintech company specialising in providing technology solutions for all different types of investors, streamlining its services into one application.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Broadly, the regulatory framework that applies to fintech businesses includes financial services and consumer credit licensing, registration and disclosure obligations, consumer law requirements, privacy and anti-money laundering and counter-terrorism financing (**AML/CTF**) requirements.

Licensing obligations apply to entities that carry on a financial services business in Australia or engage in consumer credit activities. The definitions of *financial service* and *financial product* are broad, and will generally capture any investment or wealth management business, payment service (e.g. non-cash payment facility), advisory business (including robo-advice), trading platform, and crowdfunding platform, triggering the requirement to hold an Australian financial services licence (**AFSL**) or be entitled to rely on an exemption. Similarly, engaging in peer-to-peer lending activities will generally constitute consumer credit activities and trigger the requirement to hold an Australian credit licence (**ACL**) or be entitled to rely on an exemption.

Fintech businesses may also need to hold an Australian market licence where they operate a facility through which offers to buy and sell financial products are regularly made and accepted (e.g. an exchange). If an entity operates a CS mechanism which enables parties transacting in financial products to meet obligations to each other, the entity must hold a CS facility licence or otherwise be exempt.

The *Australian Consumer Law* applies to all Australian businesses that engage or contract with consumers. Obligations include a general prohibition on misleading and deceptive conduct, false or misleading representations, unconscionable conduct and unfair contract terms in relation to the offer of services or products. In 2018, ASIC received a delegation of power from the Australian Competition and Consumer Commission (**ACCC**), enabling it to take action where there is potential misleading and deceptive conduct associated with crypto assets.

The *Australian Securities and Investments Commission Act 2001* (Cth) (**ASIC Act**) generally reflects the consumer protections under the *Australian Consumer Law* and is applicable to the provision of financial services and products.

The AML/CTF Act applies to entities that provide "designated services" with an Australian connection. Generally, the AML/CTF Act applies to any entity that engages in financial services or credit (consumer or business) activities in Australia. Obligations include enrolment with AUSTRAC, reporting and customer due diligence.

The *Banking Act 1959* (Cth) regulates those engaged in the business of banking to be authorised by APRA (i.e. be an "authorised deposit-taking institution" or **ADI**) before engaging in such business. It also contains the Banking Executive Accountability Regime (**BEAR**), which is also administered by APRA and

establishes, among other things, accountability obligations for ADIs and their senior executives and directors, and deferred remuneration, key personnel and notification obligations for ADIs.

The PSRA regulates purchased payment facility providers in relation to stored value facilities. Generally, such holders of stored value must be an ADI or be exempt from the requirement. The RBA is currently reviewing the regulatory framework for retail payments and released its conclusions paper on 22 October 2021. The new policy actions coming from the review generally relate to dual-network debit cards and least-cost routing of debit transactions, interchange fees and scheme fees.

The *Financial Sector Collection of Data Act 2001* (Cth) (**FSCODA**) is designed to assist APRA in the collection of information relevant to financial sector entities. FSCODA generally applies to any corporation engaging in the provision of finance in the course of carrying on business in Australia, and APRA collects data from registered financial corporations under FSCODA. Generally, registered financial corporations with assets greater than AUD 50 million need to regularly report to APRA statements of financial position.

The *Financial Sector (Shareholdings) Act 1998* (Cth) creates an ownership limit of 20% in a financial sector company without approval from the Treasurer.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

At the time of writing, there are no laws in Australia that have been implemented to specifically regulate cryptocurrencies or cryptoassets. Generally, the predominant focus on the regulation of cryptocurrencies has revolved around its application to the established regulatory frameworks (e.g. financial services and consumer credit).

Currently, the only formal monitoring of cryptocurrency activity in Australia is in relation to AML/CTF (see question 4.5). However, there have been numerous Government reviews that are ongoing or have recently been completed in connection with how cryptocurrency and cryptocurrency-adjacent services should be regulated (see question 1.1). In particular, the Government has released a consultation on token mapping, which seeks to identify the key activities and functions of crypto assets and map them against existing regulatory frameworks. The paper proposes a high-level taxonomy of four product types categorised under two kinds of token systems:

- intermediated token systems (i.e. systems involving a promise or arrangement for functions to be performed by intermediaries or agents): crypto asset services (i.e. token systems that accept crypto tokens as part of performing a function under a legal agreement or other arrangement) and intermediated crypto assets (i.e. a crypto token linked to an asset including but not limited to rights, licences, currency or goods and services); and
- public token systems (i.e. systems that involve functions ensured by a crypto network directly): network tokens (i.e. tokens created as part of a network's consensus mechanism that are used for various functions); and public smart contracts (i.e. smart contracts that are created for the purpose of enabling unknown parties to enter transactional relationships).

The consultation closed on 3 March 2023. The Government has indicated that it will release a licensing and custody paper for crypto asset service providers in mid-2023. It is expected that the recommendations from these reviews will have significant effects on the current regulatory regimes relevant to cryptocurrency.

On 29 March 2023, Senator Andrew Bragg introduced a private members bill, *Digital Assets (Market Regulation) Bill 2023* (**Digital Assets Bill**), which proposes to regulate digital assets, including by introducing licensing requirements for digital asset exchanges, digital asset custody service providers and stablecoin issuers. The Digital Assets Bill also proposes to introduce disclosure requirements for facilitators of central bank digital currencies in Australia. The proposed licensing framework appears to draw on the processes and requirements that already exist for AFSL and ACL holders. While the Digital Assets Bill represents a tangible attempt at specific legislation in the crypto space, the Digital Assets Bill was not introduced by the current Government and is a private member's bill that has the capacity to become law if passed by both houses. The Digital Assets Bill follows a similar bill introduced by Senator Bragg in 2022.

From a regulatory guidance perspective, ASIC has released INFO 225 *Crypto-assets* (**INFO 225**) to assist businesses involved with cryptocurrency or providing cryptocurrency-adjacent services. INFO 225 covers regulatory considerations for cryptocurrency offerings, misleading and deceptive conduct, trading platforms and cryptocurrency offered via a regulated investment vehicle.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

Regulators in Australia have generally been receptive to the entrance of fintechs and technology-focused businesses. The financial services regulatory regime adopts a technology-neutral approach, whereby services will be regulated equally, irrespective of the method of delivery. However, further concessions have been made by regulators in order to support technologically-focused start-ups entering the market and numerous reviews are ongoing or have recently been completed in connection with how cryptocurrency, payments and stored value should be regulated (see question 1.1).

ASIC has made certain class orders establishing a fintech licensing exemption and released *Regulatory Guide 257*, which detailed ASIC's framework for fintech businesses to test certain financial services, financial products and credit activities without holding an AFSL or ACL by relying on the class orders (referred to as the regulatory sandbox). ASIC has since withdrawn this regulatory guide and now guides participants to Information Sheet 248, the "enhanced regulatory sandbox".

This enhanced regulatory sandbox allows for testing of a broader range of financial services and credit activities for a longer duration. There are strict eligibility requirements for both the type of businesses who can enter the regulatory sandbox and the products and services that qualify for the licensing exemption. Once a fintech business accesses the regulatory sandbox, there are restrictions on how many persons can be provided with a financial product or service and caps on the value of the financial products or services which can be provided.

Regulators have also committed to helping fintech businesses more broadly by streamlining access and offering informal guidance to enhance regulatory understanding. Both ASIC and AUSTRAC have established Innovation Hubs to assist start-ups in navigating the Australian regulatory regime. AUSTRAC's Fintel Alliance has an Innovation Hub targeted at combatting money laundering and terrorism financing and improving the fintech sector's relationship with the Government and regulators. The Innovation Hub also assesses the impact of emerging technologies such as blockchain and cryptocurrency.

ASIC has also entered into a number of cooperation agreements with overseas regulators under which there is a cross-sharing of information on fintech market trends, encouraging referrals of fintech companies and sharing insights from proofs of concepts and innovation competitions. It is also the intention of a number of these agreements to further understand the approach to regulation of fintech businesses in other jurisdictions, in an attempt to better align the treatment of these businesses across jurisdictions.

It is of note, however, that ASIC has been substantially more active with respect to its investigations and enforcement. Between July and March 2023:

- ASIC issued 24 design and distribution obligation stop orders to prevent consumers and investors being targeted by products inappropriate to their objectives, financial situation and needs; and
- ASIC commenced three civil actions in the Federal Court for alleged breaches of financial services laws with respect to different crypto asset offerings, targeting a payments facility (and associated token) and two providers that offered products permitting users to earn returns under loan arrangements.

ASIC has announced that, throughout 2023, it will target sustainable finance practices and disclosure of climate risks, financial scams, cyber and operational resilience, and investor harms involving crypto assets. Fintech providers and technology-driven new entrants must be cognisant of their financial services obligations when entering the Australian market to ensure adherence to financial services laws.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Regulatory hurdles include registering with ASIC in order to carry on a business in Australia (generally satisfied by incorporating a local subsidiary or registering a branch office), satisfying applicable licensing, registration and disclosure requirements if providing financial services or engaging in consumer credit activities in Australia (or qualifying to rely on an exemption to such requirements), privacy, and complying with the AML/CTF regime. Broadly, these regulatory hurdles are determined by the extent to which the provider wishes to establish an Australian presence, the types of financial products and services provided, and the type of Australian investors targeted.

In the past, it has been common for foreign financial services providers (**FFSPs**) to provide financial services to wholesale clients in Australia by relying on ASIC's "passport" or "limited connection" relief from the requirement to hold an AFSL. In March 2020, ASIC repealed both passport and limited connection relief and announced the implementation of a new foreign AFSL regime and funds management relief. FFSPs currently relying on passport relief or limited connection relief may do so until 31 March 2024.

As part of the 2021–2022 Budget, the Government announced its intention to "restore previously well-established regulatory relief for foreign financial service providers". On 17 February 2022, the Government introduced the Treasury Laws Amendment (Streamlining and Improving Economic Outcomes for Australians) Bill 2022, which seeks to introduce:

- the comparable regulator exemption, which exempts FFSPs authorised to provide financial services in a comparable regime from the requirement to be licensed when dealing with wholesale clients;
- the professional investor exemption, which exempts FFSPs that provide financial services from outside Australia to professional investors from the requirement to be licensed in Australia; and
- an exemption from the fit and proper person assessment to fast track the AFSL process for FFSPs authorised to provide financial services in a comparable regulatory regime.

However, this Bill lapsed as a result of a change in Government and there have been no public announcements regarding the future of FFSP regulation in Australia by the new Government. It is generally expected that some form of comparable jurisdiction relief will be reintroduced, however the timing and the form of such relief remain uncertain.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The Privacy Act

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 AUD 3 million. In some instances, the Privacy Act will apply to businesses (e.g. credit providers and credit reporting bodies) regardless of turnover.

The Privacy Act includes 13 Australian Privacy Principles (**APPs**), which impose obligations on the collection, use, disclosure, retention and destruction of personal information.

The Privacy Act includes a Notifiable Data Breaches (**NDB**) scheme. 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 (**OAIC**) in the event of a data breach (i.e. unauthorised access to or disclosure of information, or loss of information which may amount in unauthorised access or disclosure) which is likely to result in serious harm to those individuals.

It should be noted that in December 2019, the Attorney-General announced that the Commonwealth Government would conduct a review of the Privacy Act. The review forms part of the Commonwealth Government's response to the ACCC's Digital Platforms Inquiry, with the aim to investigate the effectiveness of Australia's current privacy regime. Following the release of the Issues Paper in October 2020 and a Discussion Paper in October 2021, on 16 February 2023 the Attorney-General released the *Privacy Act Review Report* (**Privacy Report**). The Privacy Report details 116 proposals at a principles level but does not provide an exposure draft of any reform legislation. It is expected that many of the proposals are likely to be subject to further consultation. The Government sought feedback on the Privacy Report and consultation closed 31 March 2023. At the time of writing, it is expected that the Government will formally respond to the Report, indicating which of the 116 proposals will be implemented in amending legislation.

Consumer data right and access

In response to the Productivity Commissions' report on Data Availability and Use, the Government is implementing the national consumer data right (**CDR**) framework which will give customers a right to share their data with accredited service providers (including banks, comparison services, fintechs or third parties), encouraging the flow of information in the economy and competition within the market.

The banking sector was the first sector to be subject to the CDR framework under the "Open Banking" regime. Under this framework, consumers are able to exercise greater access and control over their personal banking data as well as data connected to home loans, personal loans, overdrafts, and business finance. These sharing arrangements are intended to facilitate easier swapping of service providers, enhancement of customer experience based on personal and aggregated data, and more personalised offerings.

In November 2022, the Government introduced a Bill into Parliament which would implement action initiation (also known as "write access") under the Open Banking regime. The legislation will allow consumers to instruct accredited action initiators to initiate actions such as payments on their behalf.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Yes, the Privacy Act has extra-territorial operation and extends to acts undertaken outside Australia and its external territories in respect of entities that have an "Australian link". That is, where the entity is an Australian citizen or otherwise established in Australia or "carries on business" in Australia.

Under the framework for cross-border disclosure of personal information, APP entities must take reasonable steps to ensure that overseas recipients handle personal information in accordance with the APPs, and the APP entity is accountable if the overseas recipient mishandles the information.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The Privacy Act confers on the OAIC a variety of investigative and enforcement powers to use in cases where a privacy breach has occurred, but it is largely a complaints-based regime. The enforcement regime includes the power for the OAIC to:

- investigate a matter following a complaint made by an individual or on the OAIC's own initiative;
- make a determination requiring the payment of compensation or other remedies, such as the provision of access or the issuance of an apology;
- require enforceable undertakings;
- seek an injunction; and
- seek civil penalties, which may be the greater of:
  - AUD 50 million; and
  - three times the benefit directly or indirectly obtained from the contravention, if this can be determined by a court, or 30% of turnover during the breach period, if the benefit cannot be determined by a court.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Cyber security regulation has been a key focus of regulators and the government given the recent high-profile cyber-attacks and the interplay between financial services, financial products and new technologies. However, there are no specific, standalone mandatory cyber security laws or regulations which would apply to fintech businesses.

In August 2020, the Commonwealth Government released its Cyber Security Strategy 2020, which will invest AUD 1.67 billion over 10 years in a tripartite approach to protecting, improving and enforcing Australia's cyber resilience. This will be delivered through action by governments, businesses and the community. The Government has also established an Industry Advisory Committee to shape the delivery of short- and longer-term actions as set out in its strategy. Following a number of high-profile cyber-attacks, the Commonwealth Government announced in December 2022 that it will develop a 2023–2030 Australian Cyber Security Strategy, with the aim of strengthening Australia's resilience and ability to respond to cyber threats. The Government has appointed an Expert Advisory Board to assist with the development of the updated Cyber Security Strategy.

ASIC provides a number of resources to help firms improve their cyber resilience, including reports, articles and practice guides. ASIC has previously provided guidance regarding cyber security in *Report 429 Cyber Resilience – Health Check* and *Report 555: Cyber resilience of firms in Australia's financial market*. In these reports, ASIC examined and provided examples of good practices identified across the financial services industry and questions board members and senior management of financial organisations should ask when considering their cyber resilience. ASIC's *Regulatory Guide 255* also sets out the standards and frameworks against which providers of digital advice should test their information security arrangements, and nominated frameworks setting out relevant compliance measures which should be put in place where cloud computing is relied upon.

In December 2019, ASIC released the first report into the cyber resilience of firms in Australia's financial markets (REP 651). ASIC has since released an updated report for 2020–2021 (REP 716). The reports identify key trends in cyber resilience practices and highlights existing good practices and areas for improvement. REP 651 identified investment, education, acquisition and retention of skilled resources, and strong leadership from senior management as being core factors to maintaining strong cyber resilience. However, ASIC expressed concern towards the trend of outsourcing non-core functions to third-party providers, as this created difficulty when managing cyber security risks in a business' supply chain. In the December 2021 report, ASIC notes a general improvement in cyber reliance but states that there were no material improvements in supply chain risk management and encourages firms to consider supply chain risk management as an ongoing priority.

Australia has ratified the Council of Europe Convention on Cybercrime (the Budapest Convention), which codifies what constitutes a criminal offence in cyber space and streamlines international cyber crime cooperation between signatory states. Australia's accession was reflected in the passing of the *Cybercrime Legislation Amendment Act 2011* (Cth).

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The AML/CTF Act applies to entities that provide "designated services" with an Australian connection. Fintech business will often have obligations under the AML/CTF Act as financial services and lending businesses typically involve the provision of designated services. Obligations include:

- enrolling with AUSTRAC;
- conducting due diligence on customers prior to providing any designated services;
- adopting and maintaining an AML/CTF programme; and
- reporting annually to AUSTRAC and as required on the occurrence of a suspicious matter, a transfer of currency with a value of AUD 10,000 or more, and all international funds instructions.

Digital currency exchange providers also have obligations under the AML/CTF Act and must register with AUSTRAC or

face a penalty of up to two years' imprisonment or a fine of up to AUD 137,500 (or both) for failing to register. Digital currency exchange providers must renew registration every three years. Exchange operators are required to keep certain records relating to customer identification and transactions for up to seven years.

On 20 April 2023, the Attorney-General released its proposed reforms to the AML/CTF Act. The reform package accepts all recommendations made by the Senate Legal and Constitutional Affairs Reference Committee Inquiry into the Adequacy and Efficacy of Australia's AML/CTF Regime, now proposing to extend the AML/CTF Act to "tranche-two entities" for the first time. These reforms would result in lawyers, accountants, trust and company service providers, real estate agents and dealers in precious metals and stones becoming in scope for the operation of the AML/CTF Act. The proposed model also suggests expanding the regulation of digital currency exchanges from the types of services currently regulated (that being the exchange of cryptocurrency for fiat currency and *vice versa*) to include:

- exchanges between one or more other forms of digital currency;
- transfers of digital currency on behalf of a customer;
- safekeeping or administration of digital currency; and
- provision of financial services related to an issuer's offer and/or sale of a digital currency (e.g. Initial Coin Offerings where start-up companies sell investors a new digital token or cryptocurrency to raise money for projects).

The consultation also proposes expanding the travel rule to remittance service providers and digital currency exchange providers, in line with international standards.

Consultation on the reforms closes on 16 June 2023, and a second consultation paper is expected.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction (for example, AI)?

An entity that conducts any "banking business", such as taking deposits (other than as part-payment for identified goods or services) or making advances of money, must be licensed as an ADI. For locally incorporated entities, APRA offers a restricted pathway to becoming an ADI, known as a restricted ADI (**RADI**) licence. Becoming a RADI may be appealing to new entrants that do not have the resources and capabilities to establish an ADI and need time to develop these resources and capabilities. The restricted pathway allows entrants to conduct limited banking business as a RADI for a maximum of two years, before needing to meet the requirements of the full prudential framework and applying for an ADI licence. The initial conditions on a RADI licence are more restricted than those of a full ADI licence, reflecting the restricted range of activities permitted under the licence. This pathway can assist entrants in seeking the investment required to operationalise the business while progressing compliance with the full prudential framework and an ADI licence application. Entrants that cannot meet the requirements of an ADI are expected to exit banking business. Generally, APRA will subject new ADIs and RADIs to greater prudential supervision than established ADIs in the initial years of being licenced. This includes APRA accounting for the heightened risk profile of new ADIs and RADIs by adopting adjusted capital requirements, contingency planning and deposit restrictions. For new ADIs, APRA will assess the sustainability and track record of the new ADI when determining whether the ADI is established and these adjustments are no longer necessary.

Australia's approach to regulating artificial intelligence (**AI**) has generally been a soft-law, principles-based approach. This approach has led to the development of a set of eight voluntary principles by the Australian Government Department of Industry, Science and Resources (**AI Ethics Principles**). The AI Ethics Principles are designed to be utilised by participants when developing, designing, integrating or implementing AI systems to achieve safer, more reliable outcomes. The AI Ethics Principles are part of a larger AI Ethics Framework which is holistically aimed at assisting businesses and governments to responsibly develop and implement AI – known as the AI Action Plan. The AI Action Plan has not been developed in isolation but is to be employed alongside other AI initiatives (such as the Australian Human Rights Commission's Human Rights and Technology Project and the OECD's Principles on AI). Although there are legal regimes that impact how AI is used in the Australian landscape (for example, the privacy regime), there are currently no current laws or regulations that apply specifically to AI in Australia, and it is not anticipated that Australia will move away from the current approach.

Fintech businesses are subject to the prohibitions laid out in the *Australian Consumer Law*, which is administered by the ACCC. Broadly, this includes prohibitions on misleading and deceptive conduct, false or misleading representations, unconscionable conduct and unfair contract terms. While the *Australian Consumer Law* does not apply to financial products or services, many of these protections are enforced by ASIC either through mirrored provisions in the ASIC Act or through delegated powers.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The hiring and dismissal of staff in Australia is governed under the *Fair Work Act 2009* (Cth) (**Fair Work Act**). In relation to hiring, minimum terms and conditions of employment for most employees (including professionals) are governed by modern awards, which sit on top of the National Employment Standards. However, modern awards do not apply to employees earning over a threshold of AUD 162,000 (from 1 July 2022, threshold indexed annually), provided their earnings are guaranteed by written agreement with their employer.

To terminate an employee's employment, an employer must give an employee written notice of the last day of employment. There are minimum notice periods dependent on the employee's period of continuous service, although the employee's award, employment contract, enterprise agreement or other registered agreement could set out longer minimum notice periods. Notice can be paid out rather than worked; however, the amount paid to the employee must equal the full amount the employee would have been paid if they worked until the end of the notice period.

For serious misconduct, employers do not need to provide a notice of termination; however, the employee must be paid all outstanding entitlements such as payment for time worked or annual leave.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Under the Fair Work Act, minimum entitlements for employees are set out under modern awards and include terms and conditions such as minimum rates of pay and overtime.

Australia also has 11 National Employment Standards. These include maximum weekly hours, requests for flexible working arrangements, parental leave and related entitlements, annual

leave, long service leave, sick leave, compassionate leave, public holidays, notice of termination and redundancy pay, and a fair work information statement.

The Fair Work Act also has some general protection provisions governing a person's workplace rights, freedom of association and workplace discrimination, with remedies available to employees if these provisions are contravened.

The Government recently passed the *Fair Work Legislation Amendment (Secure Jobs, Better Pay) Act 2022*, which came into effect in December 2022. This legislation includes a raft of reforms targeting pay secrecy and gender equality, and provides amendments to the operation of bargaining and enterprise agreements. Notably, since 7 March 2023, sexual harassment in connection to work has been prohibited.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

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

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

- have an occupation that is 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 to stay up to five years), with an option to apply for permanent residency subject to eligibility requirements;
- have an occupation that is 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).

Migrants can also apply for the Business Innovation and Investment (Provisional) visa (subclass 188) or associated Business Innovation and Investment (Permanent) visa (subclass 888), which are for people who wish to operate a new or existing business in Australia, conduct business and investment activity in Australia or undertake an entrepreneurial activity in Australia. Further, DOHA has created a Global Business & Talent Attraction Taskforce to attract high-value businesses and individuals to Australia (along with their ideas, networks and capital). The Taskforce facilitates the Global Talent Visa programme and Global Talent Employer Sponsored programme. To be invited to apply for a visa under the Global Talent Visa programme, a candidate must be highly skilled in one of the 10 target sectors (including digitech, blockchain and digital ledger technologies, and financial services and fintech) and be able to attract a salary that meets the high-income threshold (as of 1 July 2022, the high-income threshold is AUD 161,000).

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Patent protection is available for certain types of innovations and inventions in Australia. A standard patent provides long-term protection and control over a device, substance, method or process, lasting for up to 20 years from the filing date. The requirements for a standard patent include:

- an invention or technology must be "patentable" (e.g. new products or processes), as not all inventions are able to be protected by patent registration. For example, the High Court of Australia recently held that only software which creates an "artificial state of affairs" and a "useful result" can be protected by patent registration (see *Aristocrat Technologies Australia Pty Ltd v Commissioner of Patents* [2022] HCA 29);
- the invention must be new (i.e. you cannot patent something that is already publicly known). For this reason, it is critical to sign confidentiality agreements before discussing the invention with any third parties;
- there must be an inventive step. This means if the invention is "obvious" to a skilled person, then the invention cannot be protected by patent registration; and
- the invention must have "utility". This does not mean the invention must be useful, but rather the invention must be capable of being made in accordance with the claims and information in the patent specification.

Previously, inventions could be patented under an innovation patent (targeted at inventions with short market lives); however, these can no longer be applied for. Pre-existing innovation patents are still enforceable.

In Australia, provisional applications can also be filed as an inexpensive method of signalling an intention to file a full patent application in the future, providing applicants with the priority date from the date the provisional application was filed. However, filing the provisional application alone does not provide the applicant with patent protection, but does give the applicant filing a 12-month period to decide whether to proceed with a standard patent application.

Design protection is available, for any design that is both new and distinctive. Where patent registration protects an invention or process, design protection grants an applicant monopoly over the visual features of a product (which include the shape, configuration, pattern and ornamentation) for a maximum period of up to 10 years.

An Australian patent or design only provides protection in Australia. To obtain patent protection abroad, the applicant will need to file separate patent applications in each country or file a single international application under the Patent Cooperation Treaty (**PCT**), which gives the application effect in 155 countries including Australia. PCT applications based on a provisional application must be carried out within 12 months of filing the provisional application.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Broadly, the person or business that has developed intellectual property (**IP**) generally owns that IP, subject to any existing or competing rights. In an employment context, the employer generally owns new IP rights developed in the course of employment, unless the terms of employment contain an effective assignment of such rights to the employee. Contractors, advisors and consultants generally own new IP rights developed in the course of engagement, unless the terms of engagement contain an effective assignment of such rights to the company by whom they are engaged.

Under the *Copyright Act 1968* (Cth) (**Copyright Act**), creators of copyright works such as literary works (including software)

also retain moral rights in the work (for example, the right to be named as author), unless these rights are effectively assigned in writing. Moral rights are considered under the Copyright Act and are rights that automatically arise when someone creates work (e.g. art, music, writing, etc.), and include: (i) the right to be identified as the creator or author of a work (e.g. art, music, writing, etc.); (ii) the right not to have others being credited as the creator; and (iii) the right to not have their work used in a way that hurts their reputation. Moral rights cannot be sold or given away, so "waivers and consents" from the creators are needed in relation to these rights when the works are used by third parties. In Australia, only moral rights consents are effective at law, so the creator needs to agree to someone else using their works without referencing them (for example) in order to mitigate the risk of moral rights infringement claims.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Options available to protect or enforce IP rights depend on the type of IP. As an example, software (including source code) is automatically protected under the Copyright Act. An owner may also apply to IP Australia, the Government body administering IP rights and legislation, for software to be registered under the *Designs Act 2003* (Cth) (for example, visual elements of the user interface) or patented under the *Patents Act 1967* (Cth). Software can also be protected contractually through confidentiality agreements between parties.

A standard or provisional patent registration can also protect or enforce IP rights in Australia. Australia is also a party to the PCT, administered by the World Intellectual Property Organization. A PCT application is automatically registered as a standard patent application within Australia; however, the power to successfully grant patent rights remains with IP Australia.

Similarly, the owner of a trade mark registration can enforce their rights against third parties using substantially identical or deceptively similar trade marks for goods and services protected by the registration.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

In Australia, there are generally five approaches to commercialising IP. These are:

- *Assignment*: An outright sale of IP, transferring ownership to another person without imposing any performance obligations. However, there are some limitations to be considered in the context of assignments. For example, the assignment of an unregistered mark is only valid when there is also an assignment of the goodwill in the business (see *Kraft Foods Group Brands LLC v Bega Cheese Limited* [2020] FCAFC 65).
- *Direct in-house use of IP*: Owners of IP may commercialise the IP within an existing entity already in their control. This is generally common if the IP was originally created in-house or was acquired as described above.
- *Licensing*: Permission is granted for IP to be used on agreed terms and conditions. There are three types of licence (exclusive licence, non-exclusive licence and sole licence) and each comes with conditions. Similarly to assignments, there are certain limitations to licensing IP. For example, unregistered trade marks cannot be validly licensed (see *Kraft Foods Group Brands LLC v Bega Cheese Limited* [2020] FCAFC 65).
- *Franchising*: A method of distributing goods and services, where one party (franchisor) grants another party (franchisee) the right to use its trade mark or trade name as well as the use of its business systems and processes in return for payment and royalties. These licensed rights are used by the franchisee to provide goods or services to agreed specifications controlled by the franchisor.
- *Start-up or spin-off*: Where a separate company (either new (start-up) or partitioning from an existing company (spin-off)) is established to bring a technology developed by a parent company to the market. IP activities to be carried out for spin-offs include due diligence, confidentiality, employment contracts, assignment agreements and licence agreements.

Broadly, a business can only exploit or monetise IP that the business in fact owns or is entitled to use. Restrictions apply to the use of IP that infringes existing brands, and remedies (typically injunctions and damages) are available where the use of IP infringes the rights of another business.

Peter Reeves is a partner at Gilbert + Tobin and leads the Fintech + Web3 practice. He is an expert and market-leading practitioner in fintech and financial services regulation. Peter advises domestic and offshore corporates, financial institutions, funds, managers and other market participants in relation to establishing, structuring and operating financial services sector businesses in Australia. He also advises across a range of issues relevant to the fintech and digital sectors, including platform structuring and establishment, payments, blockchain solutions and digital asset strategies. *Chambers and Partners 2023* ranks Peter in Band 1 for Fintech and Peter is also ranked by *Chambers and Partners 2023* for Financial Services Regulation. Peter is recognised by *The Legal 500 2023* as a Leading Individual for Fintech and Financial Services Regulatory, *Best Lawyers 2023* in the area of Funds Management and as a top practitioner at the 2022 FT Innovative Awards.

Gilbert + Tobin
Level 35, Tower 2, International Towers
200 Barangaroo Avenue
Barangaroo
NSW 2000
Australia

Tel: +61 2 9263 4290
Email: preeves@gtlaw.com.au
URL: www.gtlaw.com.au

Emily Shen is a lawyer in Gilbert + Tobin's Fintech + Web3 team with a focus on fintech, crypto assets and financial services. In particular, she has specialist experience advising in relation to platform structuring and establishment, payments and stored value, crypto assets and adjacent services (including decentralised finance, digital currency exchanges and wallets), financial services regulation, consumer credit and BNPL, funds establishment and management, and AML and CTF matters.

Gilbert + Tobin
Level 35, Tower 2, International Towers
200 Barangaroo Avenue
Barangaroo
NSW 2000
Australia

Tel: +61 2 9263 4402
Email: eshen@gtlaw.com.au
URL: www.gtlaw.com.au

Meg Dalco is a lawyer at Gilbert + Tobin in the Fintech + Web3 team with a background in financial service regulation, focusing on fintech, web3 and cryptocurrency. Meg has advised major Australian banks, foreign banks, regional Australian banks, insurance companies, wealth managers, fintechs and payment providers on financial services regulatory requirements and changing regulatory landscapes, obligations management and other drafting and statutory issues. Her advice focuses on matters relating to AFS licensing, credit regulation, AML/CTF, payments systems and purchased payment facility regulations.

Gilbert + Tobin
Level 35, Tower 2, International Towers
200 Barangaroo Avenue
Barangaroo
NSW 2000
Australia

Tel: +61 2 9072 5029
Email: mdalco@gtlaw.com.au
URL: www.gtlaw.com.au

Established in 1988, Gilbert + Tobin is a leading independent corporate law firm and a key player in the Australian legal market. From our Sydney, Melbourne and Perth offices, we provide innovative, relevant and commercial legal solutions to major corporate and Government clients across Australia and internationally, particularly in the Asia-Pacific region.

With a focus on dynamic and evolving market sectors, we work on transactions and cases that define and direct the market. Gilbert + Tobin has become the legal adviser of choice for industry leaders who value our entrepreneurial culture and determination to succeed.

Gilbert + Tobin's reputation for expert advice extends across a broad range of practice areas and is built around an ability to execute with innovation, excellence, agility and deep industry knowledge. We do not just deliver on the *status quo* – we work closely with our clients to identify how their contracting and business processes need to transform and work differently. We advise at the innovative end of the spectrum and our fintech team is comprised of market-leading practitioners who provide clients with the full suite of financial services regulation and commercial advice.

www.gtlaw.com.au

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group