CHAMBERS

Global Practice Guides

FinTech

Law & Practice – Australia

Contributed by
Clayton Utz

2018

CHAMBERS AND PARTNERS®

AUSTRALIA

The 'Law & Practice' sections provide easily accessible information on navigating the legal system when conducting business in the jurisdiction. Leading lawyers explain local law and practice at key transactional stages and for crucial aspects of doing business.

Contributed by Clayton Utz ***Authors:*** Ken Saurajen, Walid Sukari, Peter Rugg, Ewan Scobie

Law and Practice

Contributed by Clayton Utz

CONTENTS

Contributed by Clayton Utz ***Authors:*** Ken Saurajen, Walid Sukari, Peter Rugg, Ewan Scobie

Clayton Utz is a first-tier, independent Australian law firm known for its long-standing contribution to the country's legal and commercial landscape, progressive culture and incisive approach to complex legal problems. It is one of Australia's largest full-service law firms, with over 170 partners and 1,400 employees in Sydney, Melbourne, Brisbane, Canberra, Darwin and Perth, offering an integrated suite of high-end legal services to the country's largest and most notable corporations, Commonwealth, State and Territory governments and other entities. The national w Industry Group draws, as needed, on our specialisations across a range of practice areas, including Technology, Banking & Financial Services, Corporate and Regulatory disciplines, and other specialist areas as required from time to time. Its key contributors are as follows: Intellectual Property & Technology Group, Corporate Transactions Group Banking and Financial Services Group.

Authors

Ken Saurajen is an Intellectual Property and Technology Law partner with a formidable reputation for the design and structuring of some of Australia's and the Asia-Pacific region's most difficult and unorthodox TMT transactions. His practice is characterised by creative and innovative contracting styles and the successful execution of landmark projects, often for which little-to-no precedent exists. Ken is particularly renowned for his work in the financial services sector on large-scale IT procurements (for example, core banking, applications development and cloud services), outsourcing and transformation projects, software licensing and telecommunications. His expertise in technology applications and services also extends to many adjacent areas of FinTech industry activity, such as electronic payment systems, banking solutions and superannuation. He is a member of the New South Wales Law Society and a former committee member and treasurer of the NSW Society for Computers and the Law.

Walid Sukari is a special counsel in the Intellectual Property and Technology Law group practising in technology investments and complex IT, intellectual property, media and telecommunications contracting. He also designs, negotiates and advises on contracts relating to intellectual property licencing and outsourcing and is well-regarded for skilfully structuring bespoke and difficult contract documentation and providing reasonable and practical advice to address and mitigate key business risks. His practice also extends to supporting Australian start-up technology companies in relation to their intellectual property protection and compliance issues. Walid is a member of the New South Wales Law Society and the Communications and Media Law Association (CAMLA) and is a former treasurer of the NSW Society for Computers and the Law.

Peter Rugg is a senior associate in the firm's Intellectual Property and Technology Law group with deep experience in TMT-related contracting. Peter's practice spans outsourcing and transformation projects, systems integration, software and data licensing, intellectual property, telecommunications regulation and broader project contracting. His transaction highlights include projects relating to software-as-a-service, business-critical systems integration (including agile development methodologies), electronic payment systems, software and data licensing models, telecommunications services and infrastructure and the commercialisation of new technologies. Peter is a member of the New South Wales Law Society.

Ewan Scobie is a senior lawyer in the firm's Intellectual Property and Technology Law group with expertise in complex technology contracting, privacy regulation, software licensing and telecommunications. Ewan's practice also encompasses commercial and regulatory advice on cross-border issues in highly regulated industries, including with respect to financial services, healthcare and telecommunications. Ewan is a member of the New South Wales Law Society and a member of the Communications, Entertainment and Technology Law Committee of New South Wales Young Lawyers.

1. FinTech Market

1.1 The Development of FinTech Products and Services

Australia is proving itself to be a fertile test bed for innovative commercial applications that lie at the intersection of traditional financial services offerings and new, enabling technology solutions. The market consensus is that good prospects now exist for Australia to see exponential growth in world-leading FinTech solutions, due to the coincidence of a number of critical factors which have created strong conditions for success.

These conditions include:

- the existence of a savvy and discerning consumer base, offering intelligent and rapid market feedback;
- increasingly pragmatic risk appetites, of both Australian corporates and their customers;
- a financially empowered demographic that is culturally disposed to high levels of new technology adoption;
- increasing levels of financial support for promising FinTech ventures; and
- the recent proliferation of co-working and incubation environments.

1.2 The Market for FinTech Products and Services

The conditions described above have contributed to a very optimistic outlook leading some analysts to predict that the total market size of the Australian FinTech sector will grow aggressively, with a report by analysts Frost & Sullivan predicting growth to AUD4.2 billion by 2020 (of which AUD1 billion is expected to be entirely additive to Australia's existing economy).

The observed appetite for new FinTech products and services in Australia has not been confined to particular sub-sectors or activities. The market has seen well-progressed initiatives relating to micro-payments, peer-to-peer transactions, crowdfunding, distributed ledger technologies, smart contracts, new blockchain-enabled security solutions, robotic advice and big data applications.

One source of this interest is, predictably, Australia's quickly growing start-up community, which is finding inspiration in a strongly supportive innovation culture and the precedents of some notable recent successes. Enthusiasm is not confined to the start-up community however, with large corporates also embarking on significant investments in FinTech. Some established financial institutions have undertaken this by way of organic development activities, insourcing their own expertise to develop proprietary technological solutions in exploratory sandboxes or test tube environments. Other financial institutions have chosen to participate through strategic, diversified investments in an array of promising new businesses or purpose-specific joint ventures focused on the exploitation or commercialisation of a particular opportunity.

1.3 The Key Market Participants in the Specified Activities

Please see **1.2 The Market for FinTech Products and Services**.

1.4 FinTech Technologies/Companies

Two consistent themes have strongly emerged from recent FinTech initiatives in Australia. The first is a philosophical distinction between mere 'innovation' on the one hand and true 'disruption' on the other. Broadly, the concept is that while innovation entails identifying and implementing novel ways to improve and refine existing products and services within a particular sales channel (effectively, within a single traditional vertical offering), true 'disruption' involves using new technologies to fundamentally shift the core value proposition of existing goods and services between different vertical product and service lines that did not traditionally intersect.

The second theme is a strong consciousness of the imminent disintermediation of a range of service industries and service providers, the strategic significance of which risks becoming heavily diminished as a result of new digital and other technological applications.

While new FinTech technologies have certainly begun to make inroads in specific areas of the Australian financial services markets, this penetration has yet to reach the stage where such entities have fully displaced traditional financial service providers. However, the industry is conscious that the continued growth of disruptive technologies will increase the likelihood of this occurring.

1.5 Partnerships Between Traditional Institutions and FinTech Companies

Please see **1.2 The Market for FinTech Products and Services**.

1.6 Approach to FinTech Innovation

From a policy perspective, Australia is an objectively favourable environment for new FinTech ventures. The trends described above coincide with a re-invigorated policy focus on FinTech innovation and a growing appreciation of the importance of the evolution of Australia's historical economic dependency on resources to the intelligent leveraging of ideas. In this regard, the Australian Federal Government and Treasury has stated its commitment to working with industry, regulators and other market participants in relation to the key factors required to underpin Australia's continued innovation in financial services, with a view to supporting

Australia becoming Asia's leading market for FinTech innovation and investment.

The Australian government's current stated policy priorities from a FinTech perspective include:

- Crowdfunding: The introduction into parliament in 2015 of a crowd-sourced equity funding framework, with the aim of providing eligible Australian companies with easier access to new funding sources. The government conducted FinTech-focused industry consultations to assist it in determining matters such as the assets and turnover threshold for equity crowdfunding eligibility and the appropriate cooling-off period for investors in crowd-sourced equity funded ventures. This culminated in the Corporations Amendment (Crowd-sourced Funding) Act 2017 (Cth), which implemented a framework to provide temporary reporting and corporate governance relief to new public companies eligible for crowdfunding, to facilitate crowd-sourced funding by small unlisted public companies and to allow for ministerial discretion to exempt clearing and settlement facility operators from certain existing licensing regimes.
- Credit reporting: Encouraging the utilisation of comprehensive credit reporting and supporting industry efforts to expand access to and utilisation of reporting data across the economy, to drive innovation in financial services and facilitate development of new P2P products and services.
- Data availability: A focus on improved data availability and the economic benefits of the improved use of data, with a default policy position of open access to non-sensitive public data, with private sector innovation encouraged through the possibility of fee-based, specialised data product offerings. This policy direction is supported by the work of the Australian government's Productivity Commission, which was commissioned to investigate ways to improve the availability and use of both public and private sector data. The Productivity Commission delivered its final public inquiry report on data availability and use to the Australian government on 31 March 2017.
- Regulatory sandboxing: The development of a regulatory environment that delivers consumer confidence without inhibiting opportunities for innovation. In this regard, the Australian government has been working with Australia's chief corporate regulator, the Australian Securities and Investments Commission (ASIC), to develop a 'regulatory sandbox' in which FinTech start-ups can develop new financial products and services and receive greater support for managing regulatory risks during testing phases. Combined with the ability for ASIC to grant waiver relief in particular cases, the Australian government has also stated its commitment to making it easier for start-ups to manage their way through complex financial services regulation.
- Technology neutral regulation: A consistent theme in Australian historical regulatory policy, in relation to the regulation of new technological innovations, developments and solutions generally, has been the recognition of the need to prioritise technology-neutral forms of legislation, so as not to prohibit or stifle new innovations through overly prescriptive or hard-coded technological requirements. This is intended to preserve flexibility and agility for businesses and allow them to quickly adapt their solutions and delivery to changing consumer preferences without unnecessary restrictions.
- Algorithmic and robotic advice: The Australian government has committed to support industry and regulatory bodies on the development of guidance in relation to those compliance obligations which affect digital and automated financial advice. While robo-advice is contemplated generally by existing regulatory guidance, the government is seeking to work with regulators to provide greater clarity in relation to specific issues, including how the 'best interests' duty is fulfilled in the context of robo-advice. On 21 March 2016, ASIC released Consultation Paper 254, addressing the regulation of digital financial product advice.
- Tax treatment of digital currency: The Australian government has acknowledged the potential for effective double taxation on consumers who use digital currencies to purchase goods or services already subject to Australian Goods and Services Tax (GST). As such, it proposes to work with industry to achieve appropriate regulatory reform regarding the treatment of GST in relation to digital currencies.
- Blockchain: Following an intense period of excitement in relation to the potential for blockchain technology to revolutionise a broad range of FinTech-related sectors, industry attention in Australia has since matured into a more measured discussion focused on identifying and testing the realistic and practical applications of distributed ledger technologies to specific product and service functions. Areas of interest have included cybersecurity solutions for financial services transactions, the use of smart contracts and automated settlements. The Australian government has also recognised the potential for blockchain technology to simplify end-to-end market operation and welcomed the Australian Stock Exchange's current exploration of blockchain technology for post-trade equity market functions.
- FinTech in government procurement: The policy priority of exploring new ways to leverage the significant opportunities FinTech offers to meet the Australian government's own procurement and service delivery requirements has also been recognised. Given the significant multi-billion dollar value of Commonwealth government procurement expenditure, the Australian government has acknowledged the significance of 'ProcTech,' being the potential impact of FinTech on government procurement, indicating that: "[t]he Commonwealth will be looking for innovative FinTech solutions to foster diversity, choice and responsiveness in government services" and recognising that ProcTech can "help encourage innovation, entrepreneurship and more efficient investment, providing greater value for taxpayer

money and potential savings that can be re-directed into vital services." In this regard, the government has specifically acknowledged opportunities for improvement in payment systems processes (and associated benefits to government agencies and departments), the potential for FinTech services to encourage diversity, choice and responsiveness in public services and the availability of significant cost savings that may be derived from a transition away from manual legacy processes to new technologies.

- Cybersecurity: There is widespread industry acceptance that safe and secure technological conditions are essential for encouraging an environment of IT innovation. Cybersecurity has been identified as a policy priority, with the Australian government supporting the establishment of a Cyber Security Growth Centre to foster engagement between the private sector and research initiatives, increase access to global markets, address cybercrime and investigate opportunities for appropriate regulatory reform.
- Foreign currency settlement infrastructure: In an increasingly global economy, it is important for FinTech start-ups whose ventures involve payment solutions, systems or technologies to have cost-effective access to foreign settlement infrastructure. In this regard, the Australian government has noted that improved access will offer improved opportunities to FinTech businesses and consumers of related products and services.

1.7 Laws or Policy to Encourage Innovation

Please see **1.2 The Market for FinTech Products and Services**.

2. Regulation

2.1 Regulatory Regimes for Specified Activities or FinTech Companies

Australia has a federated system of government involving a Commonwealth (national) government and also individual state and territory governments. As a general rule, both Commonwealth and state or territory laws will apply to conduct in a particular state or territory, although there are specific exceptions.

Generally, there are no headline categories of laws or regulations which purport to apply uniquely to companies which are considered to be FinTech companies. Companies which engage in the Specified Activities or participate in businesses relating to the FinTech sector are subject to the same laws and regulations as may apply to any other entities engaging in broadly similar activities. That said, the laws which tend to be most applicable to the operations of FinTech companies are:

- The national Competition and Consumer Act 2010 (Cth), which is the principal item of legislation governing trade practices. It addresses matters such as anti-competitive practices, the force of industry codes of conduct, enforcement and remedies, processes for authorisations and notifications of conduct, price monitoring and telecommunications-specific anti-competitive conduct;
- The national Competition and Consumer Act 2010 (Cth) also incorporates the Australian Consumer Law, which regulates fair trading, competition and consumer protection and works in tandem with the Fair Trading Acts of individual states and territories. This deals with matters such as misleading or deceptive conduct engaged in by corporations, anti-competitive conduct, unfair trade practices, unconscionable conduct, statutory conditions or warranties attached to goods and services, product safety, manufacturer liability and representations as to country of origin;
- There is no general common law right to personal privacy in Australia. However, the Privacy Act 1988 (Cth) is national legislation which regulates the collection, use and handling of information that is considered personal information. Refer to **5.1 Data Privacy and Cybersecurity Regulatory Regimes** for a fuller description of Australia's laws as they relate to personal information;
- Australia has a single, national regime for the regulation of consumer credit and a National Credit Code implemented by the National Consumer Credit Protection Act 2009 (Cth), which has replaced the prior system of state and territory-based consumer credit codes. FinTechs supporting peer-to-peer lending initiatives need to be mindful of the requirements of the Act if their products and services involve the provision of credit or the making of credit contracts where an associated fee is charged;
- Some FinTech ventures and initiatives are increasingly focused on providing a strategic market alternative for services traditionally performed by established banks and financial institutions. Banking activities are carefully regulated in Australia and the Banking Act 1959 (Cth) prohibits a corporation from carrying on any banking business in Australia unless specific conditions are met. While 'banking business' is defined in the Act, the issue of whether an entity is carrying on banking business can still require a careful analysis depending on the activities to be conducted; and
- In Australia, persons providing financial product advice are required to be licensed for the conduct of a financial services business. Activities that may be considered conducting a financial services business include giving recommendations about which financial products to purchase, trading in shares on behalf of a client, quoting prices for the trading of financial products and operating a registered managed investments scheme (which would also need to be separately registered). Obtaining an Australian Financial Services Licence (AFSL) under the Corporations Act 2001 (Cth) authorises its holder and its representatives to provide financial services to clients. While there is great interest in the potential for algorithmic and robotic advice

to disintermediate traditional advisory services, FinTech ventures whose activities may involve conducting a financial services business should consider the applicability of AFSL licensing requirements.

2.2 Regulatory or Governmental Agencies for Specified Activities or FinTech Companies

Each of the Commonwealth Acts referred to above are administered by a national regulator which is statutorily appointed to exercise powers in respect of the enforcement and administration of that Act, as follows:

- Competition and Consumer Act 2010 (Cth) and Australian Consumer Law - Australian Competition and Consumer Commission
- Privacy Act 1988 (Cth) - Office of the Australian Information Commissioner
- National Consumer Credit Protection Act 2009 (Cth)- Australian Securities and Investments Commission
- Banking Act 1959 (Cth) - Australian Prudential Regulation Authority
- Australian Financial Services Licences issued under the Corporations Act 2001 (Cth) - Australian Securities and Investments Commission

As indicated above, none of this legislation is uniquely targeted to FinTech companies. They apply to any entity which engages in conduct which those laws purport to regulate. Generally, the approach taken by the above regulators may be both proactive and responsive. These regulators may issue guidance notes or information circulars, to provide direction to the market in relation to the attitude it is likely to take to certain types of conduct or the enforcement of particular legislation. A regulator may initiate its own investigations or conduct audits into activities which it considers to be of regulatory or prudential concern. Alternatively, a regulator may investigate conduct in response to complaints it receives regarding alleged instances of specific conduct.

2.3 "Sandbox" or Other Regulatory "Neutral Zones"

In February 2017, Australia's chief corporate regulator, ASIC, established a "world-first class waiver" specifically designed to allow eligible FinTech business to test certain services for up to a year without the need to obtain an AFSL or credit licence. This contributes to an overall regulatory sandbox framework comprising three options for relief:

- Falling within existing statutory exemptions or leveraging flexibility within the current legal framework (for example, structuring arrangements in such a way as to qualify for existing relief, such as acting as a representative on behalf of another licensed party);
- Seeking individual relief from ASIC on a case-by-case basis; or
- Relying on the new FinTech licensing exemption for the testing of new products and services.

The waiver is implemented by way of ASIC Corporations (Concept Validation Licensing Exemption) Instrument 2016/1175 and ASIC Credit (Concept Validation Licensing Exemption) Instrument 2016/1176.

The FinTech licensing exemption applies to specific types of financial services and credit services and is designed to reduce the regulatory burden on new FinTech businesses in their testing phase for those services, allow greater scope for concept validation and provide relief from some of the key barriers to FinTech innovation in Australia. It has been welcomed by the Australian government, which has stated that it is "continuing to look at options to create a second stage legislative sandbox that provides further exemptions for start-up issuers of financial products and services."

While there is no application process for relief, a person seeking to rely on the FinTech licensing exemption must notify ASIC before it begins relying on the exemption and provide certain required information. That person must also advise its clients or potential clients that it is relying on the exemption and does not have the relevant licence. Importantly, the exemption does not displace the need to comply with other laws or regulatory requirements that may be relevant to a FinTech venture's business model, such as anti-money laundering or the requirements relating to the provision of tax agent services.

The national regulatory sandbox initiatives work together with any innovation initiatives of individual Australian states and territories. For example, the New South Wales (NSW) government is proposing its own regulatory sandbox to accelerate innovation in that state. That sandbox will be applications-based, with the NSW government having received submissions from interested parties in late 2016.

2.4 Change of Control Approval Requirements

There are no specific mandatory change of control requirements or processes targeted at FinTech companies.

2.5 Recent Developments or Notable Proposed/ Forthcoming Regulatory Changes

Please see **1.6 Approach to FinTech Innovation** and **2.4 Change of Control Approval Requirements**.

2.6 Burden of Regulatory Framework and Protection of Customers

Australia has a robust, comprehensive and mature legislative framework governing the supply of financial products and services. In large part, it is this stable framework which can be credited for a long history of consumer confidence in the existence of certain and predictable regulatory conditions

and an expectation of vigilant enforcement. In any jurisdiction, the rapid development of new technologies will always pose fresh challenges for existing regulatory frameworks which did not contemplate those technologies at the time of their inception. While lawmaking is necessarily reactive in this sense, the formal recognition of the policy priorities described in **1.6 Approach to FinTech Innovation** demonstrate an appropriate awareness of the need to strike a balance between preserving consumer confidence in appropriate safeguards and the encouragement and facilitation of innovation in new FinTech activities.

2.7 Regulatory Impediments to FinTech Innovation at Traditional Financial Institutions

As described in **2.1 Regulatory Regimes For Specified Activities or FinTech Companies** and **2.2 Regulatory or Governmental Agencies For Specified Activities or FinTech Companies**, there are various activities that may be engaged in by FinTech ventures, as with any other venture, that could potentially require certain licences or authorisations, depending on the scope of anticipated activities. For instance, carrying on a banking business requires a banking licence under the Banking Act 1959 (Cth), the provision of consumer credit requires a national credit licence under the National Consumer Credit Protection Act 2009 (Cth) and the conduct of a financial services business requires an AFSL under the Corporations Act 2001 (Cth). As such, it could be argued that established entities who are existing holders of relevant licences enjoy an immediate advantage from a compliance perspective and enjoy some short-term protection from new ventures which are unable to compete because they lack the appropriate permissions. Policy initiatives adopted to promote innovation (such as the regulatory sandboxing for testing purposes described in **2.4 Change of Control Approval Requirements**) will go some way to alleviating disincentives to entry. However, it is likely that, for good prudential reason, licensing requirements will remain in respect of certain activities in the financial services sector.

2.8 Regulatory Regime's Approach to Consumers and Small Business Customers

Regulation of financial markets is generally shared between ASIC and APRA. The Australian financial services regulatory regime is broadly focused on ensuring that a healthy governance framework exists to support the integrity of dealings by multiple stakeholders in financial services sector transactions. Maintaining the confidence of consumers, small businesses and larger corporations in the integrity of regulation and enforcement is a key component of this. In respect of trade and commerce generally (as distinct from regulation that is specific to financial services) consumers and small business customers do enjoy certain protections under specific regulatory regimes, including under the Australian Consumer Law and Corporations Act 2001 (Cth).

2.9 Outreach by Regulators or Government Authorities to Engage with FinTech Innovators

In addition to the Australian government policy priorities described in **1.6 Approach to FinTech Innovation**, various consultation frameworks have been established to allow for closer engagement with industry and ongoing alignment with FinTech innovators. A key initiative in this regard is ASIC's establishment of an Innovation Hub to provide information and access to informal assistance to eligible start-ups. The Innovation Hub is intended to enable such businesses to request informal guidance from ASIC on licensing requirements and key regulatory issues and help them understand their options and prepare applications for any relevant licences or waivers.

Through the Innovation Hub, ASIC proposes to engage with the FinTech community through industry events at hubs and co-working spaces; offer eligible businesses a designated contact to help them navigate regulatory requirements; provide relevant information; address innovation issues through Innovation Hub task forces having senior ASIC representation; and inform its own regulatory focus through consultation with FinTech industry experts on its Digital Finance Advisory Committee. ASIC has stated that it also proposes to meet regularly with international counterparts to exchange comparative learnings on innovation developments and policy with other jurisdictions.

Other regulatory authorities have also participated in industry engagement initiatives. Examples include APRA's participation in ASIC's Digital Finance Advisory Committee and the work of the Australian Transaction Reports and Analysis Centre (AUSTRAC) in engaging and collaborating with FinTech start-ups involved in the digital transformation of financial services and payments, with a view to ultimately moderating the regulatory burden for business engaging in those activities.

2.10 Unregulated Specified Activities

Because of the responsive nature of regulatory evolution, Australia does not at this stage have specific legislation targeted at every type of Specified Activity. For example, there is no purpose-specific legislation dealing with robo-advice, blockchain solutions or digital currencies. However, existing laws (which, in keeping with Australia's historical legislative approach, are largely technology-neutral) will automatically apply to the deployment of new technologies, until such time as policy observations identify a need for reform and design and implement the appropriate legislation.

2.11 Foreign FinTech Companies

In relation to their activities, foreign FinTech companies (or local subsidiaries of foreign FinTech companies) are subject to the same laws and requirements for doing business in Australia as any other entity. Some requirements which are

likely to be most relevant to the operations of foreign FinTech companies are:

- Foreign company registration: Any foreign business proposing to conduct business in Australia must, under the Corporations Act 2001 (Cth), register as a foreign corporation with ASIC. Alternatively, a foreign corporation may establish a local Australian subsidiary to undertake any relevant activities, this entity must comply with statutory incorporation and ongoing corporations law requirements.
- Australian financial services licensing: As discussed above in **2.1 Regulatory Regimes For Specified Activities or FinTech Companies**, a foreign company (like an Australian company) generally requires an AFSL to carry on a business of providing financial services in Australia, unless an exemption applies.
- Banking business: Any foreign company, or local subsidiary of such a company, engaging in banking business in Australia must be authorised to do so by APRA. A foreign company proposing to conduct such business would need to apply to APRA and provide information as to various matters required to inform APRA's assessment, such as capital, ownership, management, risk management and internal control systems, information and accounting systems, external and internal audit arrangements and supervision by its home supervisor. The Banking Act 1959 (Cth) also prevents foreign banks from establishing offices (as distinct from regulated Australian subsidiaries) in Australia without the consent of APRA.
- Tax requirements: The local subsidiary of any foreign company will need to comply with standard Australian taxation registration and lodgement requirements, such as obtaining an Australian Business Number (ABN), tax file number (TFN) and goods and services tax registrations. That entity will also need to attend to lodgement of Australian income tax returns, business activity statements and fringe benefits tax returns (as applicable).
- Specific reporting obligations: The Financial Sector (Collection of Data) Act 2001 (Cth) requires certain corporations to register with APRA and periodically report to it on particular matters.

Other laws may apply depending on the type and nature of the activities proposed to be conducted in Australia.

2.12 Regulatory Enforcement Actions Against FinTech Companies

There have not been any notable enforcement actions brought by regulators which have uniquely targeted the activities of FinTech ventures in Australia.

2.13 "Shadow Banking"

While Australia does not currently have any shadow banking-specific regulations, Australia's regulators are sensitive to the potential for shadow banking to introduce systemic risk into the Australian financial system and have undertaken reviews into various aspects of the shadow banking sector. This has included:

- Regular reviews of shadow banking risks undertaken by the Council of Financial Regulators and annual reporting by the Reserve Bank of Australia (RBA) to that Council on high-level developments in shadow banking;
- Targeted reviews into possible systemic risk by ASIC;
- The development of a discussion paper in April 2014 by APRA, aimed at simplification of the prudential framework for securitisation (having regard to lessons from the global financial crisis); and
- Changes to the Banking Act 1959 (Cth) Exemption Order applicable to registered financial corporations, to strengthen regulation of the issue of debentures to retail clients by finance companies.

The RBA has expressed a view that regulations need to be proportionate to the risks involved, and the relatively small scale of shadow banking activities in Australia and their minimal links to the regular banking system means that the risks presented by such activities to the Australian financial system are minimal. Australian regulators are continuing to monitor shadow banking developments and exercising ongoing vigilance, with appropriate regard to international reforms.

3. Form of Legal Entity

3.1 Potential Forms of Charter

The three most common legal structures in Australia are sole traders, partnerships and companies. A company will include an incorporated joint venture. Anecdotally, while some FinTech start-ups pursue their ventures as a sole trader, many establish a company structure in recognition of the benefits of incorporating and operating through a limited liability vehicle. Unlike a partnership, a company is also recognised as a separate legal entity capable of enforcing rights in its own name (and having rights enforced against it). Tax requirements also differ depending on the form of entity adopted.

In relation to each of these legal structures:

- Sole trader: A sole trader is an individual who chooses to operate a business in his or her own personal capacity. The sole trader is personally liable for any business-related liabilities or debts. Typically, this is the most straightforward and least costly business structure. For tax reasons, sole traders will usually need to register for an ABN and also register for GST if the business is likely to earn revenue over AUD75,000 in a financial year.

- Partnership: This is a group or association of individuals who run a business together with liabilities, with income distributed among that group or association. A partnership is generally inexpensive to establish. Notably, while a partnership is not a separate legal entity, it must have its own TFN and lodge an annual partnership tax return. The partnership must also be registered for GST if its annual revenue is AUD75,000 or more.
- Company: A company is a distinct legal entity, owned by its shareholders and run by individuals who manage its affairs (the directors), regulated by ASIC under the Corporations Act 2001 (Cth). A company has higher establishment and ongoing administration costs than sole traders and partnerships and is also subject to statutory reporting requirements. Those reporting requirements vary depending on whether the company is a private (proprietary limited) or public company (limited). Shareholders and directors are generally not responsible for the liabilities of the company (subject to some exceptions where directors may be legally liable under the Corporations Act 2001 (Cth)). A company must be registered for GST if its annual revenue is AUD75,000 or more, must lodge an annual company tax return and pays tax at the company tax rate (which is historically lower than Australia's personal tax rate).

Sometimes a more complex corporate structure will involve a trust. A trustinvolves a trustee, which may be an individual or corporate entity, holding assets for the benefit of a group of persons or corporate entities. A trustee must not use trust property for its own purposes, but must only use trust property for the benefit of trust beneficiaries. The establishment of a trust may be done relatively quickly under a trust deed, however trusts are subject to complex laws (particularly regarding taxation).

3.2 Key Differences in Form

The following sets out some advantages and disadvantages of the legal structures most likely to be adopted by FinTechs in Australia. As noted in **3.1 Potential Forms of Charter**, FinTech start-ups generally initially operate as sole traders or companies (simple private companies), noting that operation as a company offers the protection of limited liability. Start-up ventures should consult with their local legal representative and tax consultants to determine the most appropriate corporate structure for their business.

Sole Trader

Advantages

- inexpensive establishment and administration costs
- all profits retained
- winding-up business simplified
- privacy of business affairs maximised

Disadvantages

- unlimited personal liability
- finance and capital raising may be more difficult
- taxed as an individual

Partnership

Advantages

- relatively low establishment costs
- potentially, greater financing and borrowing capacity than a sole trader
- possibility of income splitting and obtaining tax savings
- maintain privacy of business affairs
- less external regulation than a company

Disadvantages

- unlimited joint and several partner liability for business debts
- each partner is an authorised agent of the partnership liable for the actions of other partners

Company

Advantages

- liability for shareholders is limited
- transfer of ownership is possible by selling shares
- company tax is preferable to income tax (applicable to sole traders and partners)
- access to financing

Disadvantages

- expensive to establish and administer
- additional reporting requirements
- where the company is listed on a stock exchange, its financial affairs are public;
- if directors fail to meet their legal obligations, they may be held personally liable for company debts or be liable to pay pecuniary penalties.

3.3 Recent Legal Changes

There have been no recent legal changes that have altered the desirability or selection of a legal entity.

4. Legal Infrastructure (Non-regulatory)

4.1 Desirable Changes to Facilitate Specified Activities

There are a range of new FinTech activities that have been identified as policy priorities by the Australian government, as further described in **1.6 Approach to FinTech Innovation**. Such policy support and initiatives may lead to future legal reform, although no such non-regulatory reform appears to be currently contemplated.

4.2 Access to Real-Time Gross Settlement Systems

Real-Time Gross Settlement (RTGS) systems are part of the Reserve Bank of Australia's Information and Transfer Sys-

tem (RITS). Access to RTGS systems is therefore conditional on RBA approval. FinTech companies may apply for RITS membership and seek approval to use RTGS systems. RITS membership categories include banks, other holders of exchange settlement accounts (ESAs) and non-ESA holders.

Although any person can apply for RITS membership, RBA approval may be conditional on other factors and membership will require compliance with the RBA's RITS Regulations. In practice, given the steps surrounding the approval and maintenance of RITS memberships, FinTech ventures may wish to consider the approach of accessing RTGS systems through existing financial institutions that have already received RBA approval.

4.3 Special Insolvency Regimes

There are no notable insolvency, administration or other like laws or regulations which regulate FinTech companies differently to other Australian financial institutions.

4.4 Electronic Signatures

In the majority of instances, Australian common law does not mandate any formal signing requirements to form a legally enforceable agreement between private parties. Therefore, a duly applied digital or electronic signature can be used (and relied on) to demonstrate an objective intention to create binding legal relations. Slightly different factual or evidentiary issues of proof and reliability may arise with an agreement signed electronically or digitally as compared to a paper signature. However, the underlying principles of proof are the same and physical signatures are equally not immune from analogous evidentiary challenges, notwithstanding that the facts by which signature is proven may differ.

Requirements in relation to the proper execution of deeds are more prescriptive. Both the common law and certain statutes impose requirements for valid execution of deeds which are more difficult to achieve digitally or electronically. Relevant statutes include the Conveyancing Act 1919 (NSW) (for individuals) and the Corporations Act 2001 (Cth). Specifically:

- Deeds under common law: The traditional requirements for creating a legally enforceable deed under common law are relatively strict and very focused on requirements of physical form. They require a document to be written on vellum, parchment or paper and to be signed, sealed and delivered. It would be difficult for an electronic or digital form of signing or execution to satisfy these physical requirements.
- Deeds under the Conveyancing Act 1919 (NSW): Section 38 of the Conveyancing Act requires every deed, whether or not affecting property, to be signed as well as sealed, and attested by at least one witness.
- Execution of documents by a company under Section 127(1) of the Corporations Act 2001 (Cth): Corporations law is expressly excluded from the benefit of the provisions in the Electronic Transactions Act 1999 (Cth).

A deed that fails the requirements for valid execution as a deed will often (subject to the existence of valuable consideration) still take effect as an agreement. However, it is prudent for parties to consider maintaining a practice of physical (paper) execution for instruments where it is essential that those instruments take effect as deeds. For example, where there is questionable consideration or where there is a special requirement for the particular subject matter to be recorded in a deed.

Australia does have Electronics Transactions legislation (both at a Commonwealth and individual state and territory level, all of which are substantially similar). This legislation is frequently misunderstood as strictly mandating the minimum requirements for a legally effective electronic or digital signature between private contracting parties. This is not the case. The fundamental premise of the various Electronic Transactions Acts in relation to signatures is effectively to provide that where a legal requirement exists (under a Commonwealth, state or territory law, as applicable) for a person to provide a signature, that requirement will be taken to have been met, notwithstanding it being done electronically, provided some basic tests are met.

These tests are (for Commonwealth legal requirements, as an illustration):

- method of identification and intention of signatory: A method must be used to identify the person and to indicate the person's intention in respect of the information communicated;
- reliability of method: The method must be reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in light of all the circumstances;
- IT requirements: If the signature is required to be given to a Commonwealth entity, any method of identification in the first point above is in accordance with the particular IT requirements of that Commonwealth entity; and
- consent: If the signature is required to be given to a person who is not a Commonwealth entity, the person to whom the signature is required to be given consents to that requirement being met by way of the use of the method.

4.5 Standards for Proving Identity in Electronic Transactions

There are no specific technical standards for proving identity in electronic transactions. However, as a matter of good practice, entities are increasingly being encouraged to utilise purpose-built signature technologies (digital signatures)

which provide a greater level of sophistication and security than a mere electronic representation.

The term 'electronic signatures' is generally used in a different way from digital signatures, as it can mean simply any representation of a signature or expression of intent to be bound that is in electronic form - such as typing a name or a graphic of a handwritten signature. Digital signatures are a subset of electronic signatures and usually refer to a purpose-specific signature technology with a greater level of sophistication and security than a mere electronic representation.

The chosen digital signature solution should ideally:

- enable clear identification of the signatory and require authentication of the signatory as a precondition to digitally or electronically signing a document;
- preserve the form of the document immediately following signing and protect it against unauthorised changes or amendments;
- appropriately archive and record the making of the signature; andImplement appropriate certification processes to ensure the signature can only be applied by an authorised person and is not tampered with.

These features are not exhaustive (or determinative) but, in the event of a dispute, would assist a party in demonstrating the robustness and reliability of its chosen digital or electronic signature process.

5. Data Privacy and Cybersecurity

5.1 Data Privacy and Cybersecurity Regulatory Regimes

Data Privacy

Australia's Privacy Act 1988 (Cth) regulates the collection, use and handling of information that is considered personal information. Personal information is defined as "information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable." This means that entities regulated by the Act must comply with its requirements if they are collecting, using or disclosing information (for example, about their customers) relating to an individual's name, address, contact details, date of birth, financial or medical details or any other personally identifying information, including any notes or comments about that individual.

The Act applies to most Australian government agencies, all private sector and not-for-profit entities with an annual turnover in excess of AUD3 million and private health service providers. It also applies to some types of small businesses that provide certain types of services.

The Act implements 13 Australian Privacy Principles, or APPs, which cover matters such as how personal information can be used; offshore transfer of personal information; direct marketing; keeping personal information secure and maintaining its quality; the right of individuals to access and correct their personal information; and maintaining a privacy policy and how personal information should be managed. Higher standards apply for dealings with sensitive information, being certain types of personal information (health, race, ethnicity, sexual preference, religious belief or political opinion).

The Act also regulates the privacy aspects of health and medical research and Australia's consumer credit reporting system (which may be relevant to P2P lending, consumer lending and other activities relevant to FinTech ventures). It also, together with the Privacy (Tax File Number) Rule 2015 issued under it,addresses collection, storage, use, disclosure, security and disposal of TFNs and related information.

In addition to the Privacy Act, some sector-specific laws also exist which are relevant to data privacy and dealing with personal information. These include:

- The Telecommunications Act 1997 (Cth) and Telecommunications (Interception and Access) Act 1979 which addresses the retention of personal information by telecommunications carriers and carriage service-providers, and regulates how law enforcement agencies may access that information;
- The Spam Act 2003 (Cth), which prohibits the sending of unsolicited commercial electronic messages (including emails);
- The Do Not Call Register Act 2006 (Cth), which establishes a secure database which individuals and organisations can register their telephone numbers with, to prohibit telemarketers from calling those numbers;
- The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Anti-Money Laundering and Counter-Terrorism Financing Rules also impose certain obligations on participants in the financial sector who provide particular types of services (such as money transfers and gambling-related services). These include obligations to collect and verify 'know your customer' (KYC) information about the identity of a customer.

The Australian government recently passed new legislation implementing mandatory reporting of data breaches. The Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) will come into effect in 2018, requiring entities who are regulated under the Privacy Act 1988 (Cth) to advise both the Office of the Australian Information Commissioner, and

also any affected individuals, of any unauthorised access to or disclosure of information of those individuals that would be likely to result in serious harm to them.

Individual Australian states and territories also have similar (although not identical) laws in place relevant to the management of personal information. The Privacy Act 1988 (Cth) expressly provides that the laws of states and territories is capable of operating concurrently with national legislation with respect to the collection, holding, use, correction or disclosure of personal information. For example, the Privacy and Personal Information Protection Act 1998 (NSW) addresses how NSW government agencies collect, use and disclose personal information. That Act is administered by the NSW Information Privacy Commissioner. It contains Information Protection Principles which are conceptually aligned with the national Australian Privacy Principles implemented by the Privacy Act 1988 (Cth). A state or territory may also have sector-specific laws, such as the Health Records and Information Privacy Act 2002 (NSW) in NSW, which sets out certain Health Privacy Principles that NSW government agencies must comply with when handling personal health information.

Cybersecurity
Discussion about cybersecurity in Australia has revolved around both the obligations of private organisations to secure their customers' information against cyber attacks and other cybercrime activities generally.

Australian law is not technologically prescriptive as to the type or level of protection a private organisation must deploy in relation to their information technology systems. There are, however, certain industry and sector-specific guidelines that private FinTech organisations may be required to comply with or which offer guidance in relation to what applicable regulators view as best industry or sector practice. For example, in relation to the banking and finance sector, APRA has issued Prudential Practice Guide - CPG 235 (Managing Data Risk) and Prudential Practice Guide - PPG 235 (Management of security risk in information and information technology). These are designed to guide regulated entities in managing their information technology security risk and elaborate on the steps they should take to protect the personal information of their customers.

Regulation of cybercriminal activities occurs at both a national and individual state and territory level. At a national level, the Commonwealth enacted a range of cybercrime offences in the Criminal Code Act 1995 (Cth) which took effect on 1 March 2013. The Federal Attorney-General has noted that these offences are consistent with those required by the Council of Europe Convention on Cybercrime and are expressed in technology-neutral terms, to cater for technological evolution. Key provisions include offences criminalising the misuse of telecommunications networks; carriage services and computer systems; the ability of law enforcement agencies to require the preservation of certain types of communications; and the ability to access stored communications pursuant to a warrant.

5.2 Recent and Significant Data Privacy Breaches
There have not been any widely publicised recent major data privacy breaches uniquely involving FinTech companies in Australia.

5.3 Companies Utilising Public Key Infrastructures or Other Encryption Systems
While no specific legislation in relation to public key infrastructures (PKI) exists in Australia, the Commonwealth Government has developed the Gatekeeper PKI Framework (PKI Framework). The PKI Framework is essentially an accreditation programme that is stated to be a "whole-of-government suite of policies, standards and procedures" governing the use of digital certificates, to be used for the authentication by Commonwealth government agencies of individuals, organisations and network-protection equipment.

While the Commonwealth Government does not mandate the use of PKI for the authentication of private online transactions or the use of PKI for authentication purposes by private parties, Commonwealth agencies wishing to use digital certificates to authenticate their clients must use digital keys and certificates which have been issued by service providers accredited under the Gatekeeper PKI Framework.

In its current form, the PKI Framework will only be relevant to FinTech companies that seek to be a provider to Commonwealth government agencies of digital keys and certificates, as such companies will need to be accredited to do so under that framework.

5.4 Biometric Data
The collection of biometric data at Australia's borders is regulated under the Migration Act 1958 (Cth), as amended by the Migration Amendment (Strengthening Biometrics Integrity) Bill 2015 (Cth). Under the amended Act, the government has the power to collect various personal identifiers from both citizens and non-citizens at the Australian border. These identifiers may include biometric data, such as through facial recognition systems and fingerprints. The Act also specifies the circumstances in which such information may be collected, the location of collection and the manner in which personal identifiers should be provided. It also establishes a clear process for the storage and management of that information.

The Office of the Australian Information Commissioner has also noted that biometric information used for the purpose

of automated biometric verification or biometric identification may also be sensitive information for the purposes of the Privacy Act 1988 (Cth), noting that such biometric information may include facial features, fingerprints, palm, iris, voice or signature. As described in **2.1 Regulatory Regimes For Specified Activities or FinTech Companies**, higher standards and additional obligations apply for dealings with sensitive information under the Privacy Act.

6. Intellectual Property

6.1 Intellectual Property Protection Regime

Australia recognises a range of different intellectual property rights, including copyright, patents, designs, trade marks, plant breeder rights and circuit layouts. It also recognises other associated rights, such as moral (attribution) rights and the right to have confidential information kept confidential.

Based on recent industry experience, the intellectual property created by Australian FinTech ventures are most likely to take the form of copyright, trade marks or patent rights. Most new intech businesses are focused on the development of original software tools, solutions and applications, which are protected under Australian copyright law as a computer program.

Copyright

Many software-based FinTech-related technologies would qualify for protection as a computer program as that term is defined under the Copyright Act 1968 (Cth). A computer program is defined as a set of statements or instructions used directly or indirectly in a computer in order to bring about a certain result.

The fundamental tenant of Australian copyright law is that it does not protect ideas, concepts or methods, but only the expression of those ideas, concepts or methods in a material form. There is no application or registration process and copyright protection arises automatically on the coming into existence of that expression in material form. The copyright work must also be original, in the sense of being attributable to an author and not reproduced or copied from another source.

In the context of computer programs which are protected as a copyright work, the owner of the copyright will usually be the individual who creates the program or develops the relevant underlying code itself, as opposed to (if different) the person who conceptualised the functional purpose of the relevant software. As such, it is important for FinTech ventures who are commissioning third-party contractors to perform software development work to ensure that such work is commissioned on terms that assign the copyright in the developed software back to the entity which is intended to own it. Where the creator of the computer program is an employee and develops the computer program in the course of their employment duties however, the copyright in that computer program will vest in that person's employer.

Owners of copyright under the Copyright Act 1968 (Cth) are granted various exclusive statutory rights in relation to the relevant work, including to reproduce it in material form, publish it, communicate it to the public and make an adaptation of it. In practical terms, these exclusive rights would encompass the right for a FinTech venture to commercially license a computer program owned by it to a commercial licensee. The duration of copyright protection for published works, such as a computer program, is generally 70 years from the death of the copyright owner.

Patents

A patent is a statutory right which may be granted in respect of an invention that meets particular criteria. The granting of a patent in Australia provides the registered patent owner with a legally enforceable right to exclusively exploit its invention in Australia for the applicable patent term. As noted by IP Australia, the national administrator of Australia's patent rights system, a patentable invention may be "a device or machine, a substance, a process or computer hardware and software, and even some business methods."

The Australian patent system supports two types of patent grants. The traditional patent is a standard patent, which offers up to 20 years protection and exclusive control over an invention (and up to 25 years in respect of pharmaceuticals). There is also the option to apply for an innovation patent, which is a comparatively faster and less expensive form of protection with less stringent requirements for patentability in certain respects and a shorter time to grant. However, the period of protection is limited to a shorter eight-year period. Many FinTech ventures with inventions they consider to be patentable are showing a high level of interest in innovation patents, given the fast-moving nature of technological development in Australia, the less onerous fees and the shorter timescales to grant.

To be eligible for patentability, an invention must meet certain criteria under the Patents Act 1990 (Cth). Specifically:

- An invention should be an actual manner of manufacture. Ideas, proposals and theories themselves are not patentable. This also applies to many business method patents that may be implemented by way of a computer, which is the focus of various FinTech start-ups. In Commissioner of Patents v RPL Central Pty Ltd [2015] FCAFC 177, the Full Federal Court of Australia confirmed that for a business method implemented in or by a computer process to be

patentable, a separate result beyond the typical working of a computer must be achieved;
- The invention should be novel, with reference to the prior art base. That is, it should not have been publicly disclosed anywhere in the world (not just in Australia) in any form. As such, FinTech ventures should be careful to ensure that their disclosure, early publicising or demonstration of their inventions does not jeopardise prospects of patentability. It is also important that the invention not have been previously secretly used;
- For a standard patent, the invention should demonstrate some inventive step. This will be interpreted in a common sense way, but broadly it should not be an obvious step to a person with experience and skills in the relevant field;
- For an innovation patent, thereshould be some innovative step reflecting a difference between the invention and the then current technological knowledge base which makes a substantial contribution to how the invention works; and
- The invention should do what is intended of it.

Trade Marks
Most FinTech businesses in Australia will develop a name, brand or logo and seek to use that in connection with its activities, to begin to build goodwill in its products and services. This practice can give rise to trade mark rights.

A trade mark is a mark that is used to indicate the trade origin of goods or services. Australia recognises both common law trade marks and registered, statutory trade marks under the Trade Marks Act 1995 (Cth).

A common law trade mark is a name, logo or other mark that is used in relation to goods or services to an extent that distinguishes it from the goods and services of other persons or entities. Common law trade marks arise naturally, without any process of registration or application, and infringement may give rise to rights such as the right to take action for the passing off or for misleading and deceptive trade practices.

Alternatively, a business can choose to apply for registration of its trade mark under the Trade Marks Act 1995 (Cth) and obtain a statutory trade mark for use in particular classes of goods and services. Once an application is granted, the owner of a registered trade mark has the exclusive right to use that trade mark for the goods and services in the classes for which that trade mark has been registered. This prevents third parties from using a mark which is substantially identical or deceptively similar to the registered mark.

As noted by Australia's national administrator of trade marks, IP Australia, trade marks are not confined to logos. The Trade Marks Act 1995 (Cth) defines a sign as "the following or any combination of … any letter, word, name, signature, numeral, device, brand, heading, label, ticket, aspect of packaging, shape, colour, sound or scent."

While trade marks are strictly not required to be registered, a registered trade mark owner enjoys additional benefits, such as easier enforcement against infringements; a true property right that may be dealt with as a licensable or transferable asset offering a statutory defence to any other claim of infringement; and being on the public record as a useful notice and deterrent to any persons considering the use of similar marks.

6.2 Trade Secret Regime
There is no dedicated regime in Australia that governs trade secrets. However, trade secrets, as a subset of confidential information, are the subject of a duty of confidence under the principles of equity and may be subject to terms of a contract. The parties to a contract may also define any information as confidential and attach contractual duties of confidence to that information.

In determining whether information is confidential for the purposes of establishing an equitable duty of confidence, a party will be required to demonstrate a number of factors including that the information possesses the quality of confidence; that the information was imparted in circumstances importing a duty of confidence (although the obtaining of information by reprehensible or surreptitious means or by third parties who know that the information is confidential may also be covered); and that unauthorised use of the information will cause detriment to the party seeking to enforce the duty.

In circumstances in which a party receives confidential information, equity will operate to restrain any improper use, disclosure or handling of such information by a receiving party. The disclosing party may also be entitled to seek equitable remedies for misappropriation, which may include an account of profits or injunctive relief. The disclosing party may also have a claim for contract damages, if a person to whom it has disclosed confidential information pursuant to the terms of an agreement misappropriates that information in breach of those terms.

Employees are under a separate duty not to use confidential information gained in the course of their employment to the detriment of their employer. This duty of loyalty may be breached where the employee engages in unfair or wrongful acts. An example would be a circumstance in which an employee purposely memorises customer lists so that he or she can subsequently establish a competing business. However, in the absence of special contractual terms, an employee is not generally restrained from utilising 'know-how' or information naturally learnt during the course of employment to further his or her career.

6.3 Copyrights, Patents, Trade Marks
See **6.1 Intellectual Property Protection Regime**.

6.4 Protection of Intellectual Property or Trade Secrets
The key forms of protection available to FinTech companies in Australia are addressed under **6.1 Intellectual Property Protection Regime** and **6.2 Trade Secret Regime**. Parties may also enter into bespoke contractual arrangements with private counterparties under which they agree to other commercial arrangements in relation to the protection, exploitation, commercialisation or licensing of their intellectual property rights, know-how or other valuable information or materials.

6.5 Joint Development of Intellectual Property
The treatment of jointly developed intellectual property differs depending on the type of intellectual property involved, especially with respect to the issue of the level of consent required between co-owners for future dealings with intellectual property that is jointly owned. Joint ownership may arise by mutual agreement (by contract) or as a natural result of the joint contribution of multiple parties to a particular item in which intellectual property subsists.

The position with respect to jointly owned copyright and statutory trade marks is relatively similar. Under both the (Cth) and Trade Marks Act 1995 (Cth), the consent of joint owners to future exploitation is required. This is an important feature of joint ownership which should be noted by FinTech start-ups which are considering what kind of intellectual property ownership model is appropriate in the context of multiple stakeholder contributions. While joint ownership can intuitively sound like a fair approach to such situations, it can result in a lack of flexibility with respect to future dealings with the relevant intellectual property.

The position with respect to patents differs in that under the Patents Act 1990 (Cth) a joint owner can exploit rights in a patent without the consent of the other co-owner(s) (and retain the profits from that exploitation, without accounting for those profits to other joint owners). However, it cannot assign its co-interest nor grant licences to its rights without the express consent of other joint owner(s).

Of course, joint owners may contractually agree to arrangements different to the statutory default positions. For instance, they may contractually agree to provide each other with consents in relation to particular future dealings, which would introduce greater prospective flexibility (and certainty) in relation to how a particular party might maximise the value from jointly owned intellectual property rights, address how other joint owners might share in the economic benefits of such exploitation and provide for whether a jointly owned interest may be on-licensed or assigned.

6.6 Intellectual Property Litigation
Given the relatively high rates of technology adoption in Australia, it is unsurprising that intellectual property disputes are a notable source of litigation. As a general observation, Australia features a sophisticated business environment with a high consciousness of the value of intellectual property rights and the importance of respecting a party's rights and obligations regarding protectable intellectual property. Such litigation may take the form of enforcing rights against alleged infringers or defending claims received from third parties. Various types of relief are available, including injunctions and damages. Most intellectual property-related litigation is initiated in the Federal Court of Australia (given the federal nature of certain intellectual property legislation, such as the Copyright Act 1968 (Cth), the Patents Act 1990 (Cth) and the Trade Marks Act 1995 (Cth)). However, the Supreme Courts of individual states also enjoy some jurisdiction with respect to intellectual property matters.

6.7 Open Source Code
In Australia, there are no specific laws or regulations in Australia that govern the use or incorporation of open source software into proprietary software or otherwise. A FinTech venture proposing to incorporate open source code into its proprietary software or use open source software as part of its general business operations will be required to comply with applicable obligations of the relevant open source licences. Like any other company, FinTech companies that rely heavily on open source code or build it into their proprietary platforms or systems should be mindful of any viral terms that may be imposed by the applicable open source licence and how this may impact the strategic value of their proprietary solutions.

Generally, market participants and end customers who use a particular service or licence a vendor solution will not know whether the software underlying that service or solution incorporates any open source code, unless this is disclosed by the licensor or if it obtains rights to conduct a technical audit of the applicable source code (which is relatively uncommon). However, it is not unusual for Australian agreements related to the purchase of software or related services to include obligations on suppliers to ensure that open source code is not included in the relevant software or solution.

7. Tax Matters

7.1 Special Tax Issues, Benefits or Detriments
Notable regulatory reforms and proposals in Australia from a tax perspective relating to FinTech activities have focused on venture capital tax concessions for FinTech investment, encouraging eligible FinTech businesses to explore existing research and development tax incentives, and evaluate more

closely how digital currencies should be treated from a tax perspective.

More specifically:

- With effect from 1 July 2016, the Tax Laws Amendment (Tax Incentives for Innovation) Act 2016 (Cth) came into effect, implementing for investors a 10% carry-forward tax offset on investments made through an early-stage venture capital limited partnership. Those amendments also increased the maximum fund size for such partnerships (both new and existing) to AUD200 million. In May 2016, the Australian government sought submissions on how to ensure investors in FinTech start-ups are eligible for these tax concessions (including for banking and insurance activities). Promoting access for FinTech companies in this regard remains a policy focus area.
- The Australian government's Research and Development Tax Incentive provides eligible entities which have an aggregated turnover of less than AUD20 million with a refundable tax offset, and all other eligible entities with a non-refundable tax offset. This is intended to boost competitiveness and improve productivity across the Australian economy. FinTech ventures who qualify may access the incentive, although it is important to note that the incentive is based on specific types of activities and specialist advice should be obtained if there is doubt as to the eligibility of research and development-related claims.
- In relation to virtual currencies, the ATO has stated its view that bitcoin (for example) is neither money nor a foreign currency, and the supply of bitcoin is not a financial supply for GST purposes (although bitcoin will treated as an asset for CGT purposes). Rather, it has equated transacting with bitcoins to a barter arrangement and issued several rulings relating to income tax, fringe benefits tax and GST.

As noted in **1.6 Approach to FinTech Innovation**, one of the FinTech priorities identified by the Australian government is working with industry to achieve appropriate regulatory reform in relation to the treatment of GST in relation to digital currencies, noting the potential for effective double taxation on consumers who use digital currencies to purchase goods or services.

8. Issues Specific to the Specified Activities

8.1 Additional Legal Issues

A notable area of recent attention in Australia has been innovation in payment systems, specifically the current development by Australia's central bank of a world-leading payments infrastructure to deliver enhanced improved payment processes for Australian consumers, businesses and government entities.

The RBA is undertaking the development of a new payments infrastructure that will enable real-time, 24/7, data-rich and more easily addressed payments. This project is called the New Payments Platform (NPP).

The NPP arose in response to the RBA's conclusions arising from a two-year strategic review of innovation in the Australian payments system, which identified that collaborative innovation between Australian financial institutions in the payments sector could be improved. That review encompassed extensive consultation with a range of payments system stakeholders.

The NPP is being funded by 12 financial institutions including large Australian banks, the RBA, other banks (including foreign banks) and a number of payment service provider entities. It was projected to go live in late 2017.

Clayton Utz
Level 15
1 Bligh Street
Sydney 2000
New South Wales
Australia

CLAYTON UTZ

Tel: +61 2 9353 4000
Fax: +61 2 8220 6700
Email: ksaurajen@claytonutz.com
Web: http://www.claytonutz.com/