# Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

# FinTech

**Australia**
Clayton Utz

chambers.com

2019

# Law and Practice

*Contributed by Clayton Utz*

## Contents

**Clayton Utz** is one of Australia's largest full-service law firms, 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 firm's national FinTech Industry Group draws on internal specialisations across practice areas such as technology, banking and financial services, corporate and regulatory disciplines. Clayton Utz acts for a range of clients in relation to FinTech initiatives, from local and international banks and financial institutions to technology suppliers, large corporate customers and emerging ventures. It provides transactional support and regulatory advice to FinTech clients in relation to capital management, corporate finance, debt and capital markets, derivatives, funds, leveraged finance, project finance, property finance, restructuring and insolvency, securitisation and structured finance. The Corporate Transactions Group's involvement in the FinTech sector encompasses capital-raising, joint ventures, M&A and early capital markets work. It acts for investors and emerging entities, and features a purpose-specific group focused on nurturing Australian start-up ventures. The firm's FinTech expertise spans large-scale IT procurements, outsourcing and transformation projects, software and technology licensing, electronic payment solutions and TMT projects.

## Authors

**Ken Saurajen** is a partner in the firm's Intellectual Property and Technology Law Group, 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 for which there is often little or no precedent. 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 licensing 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 flexible 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.

## 1. FinTech Market

### 1.1 Evolution of the FinTech Market

Over the last 12 months, Australia has continued to consolidate its reputation as a steadily maturing market for innovative commercial applications at the intersection of traditional financial services offerings and new enabling technologies. Innovators and investors generally perceive it as a jurisdiction which offers, in relative terms, a safe and stable regulatory framework, a consumer base that is disposed to quick (albeit discerning) adoption of new technologies and a policy framework that continues to be strongly philosophically supportive of innovation.

The coming 12 months is likely to see continued acceleration of FinTech-related activity across the consumer, business and government sectors in Australia. This will be supported by the following factors:

- a strong cultural disposition among consumers and citizens towards early adoption;
- a financially empowered end-user demographic;
- relatively robust consumer and business risk appetites;
- the continuing evolution of a strong co-working and start-up culture; and
- increased onshore and offshore investor and private equity interest in emerging FinTech ventures.

## 2. FinTech Verticals

### 2.1 Predominant Business Models

Analyst forecasts for the growth of the FinTech sector continue to be optimistic, with some predictions estimating growth of the sector to reach AUD4.2 billion by 2020 (of which AUD1 billion is expected to be entirely accretive to Australia's existing economy). Further, the appetite for new FinTech products and services in Australia is broad and not confined to particular sub-sectors. Recent areas of interest include new payment systems, disintermediated (peer-to-peer) transactions, crowdfunding, initial coin offerings, blockchain and distributed ledgers, smart contracts, robo-advice and rich data-contracting.

Australia's start-up community continues to evolve, supplemented by the increasing involvement of large corporates in FinTech-related ventures. Some established financial institutions have undertaken this by way of organic development activities, insourcing their own expertise to develop proprietary technological solutions, while others participate through strategic, diversified investments in new or emerging businesses.

### 2.2 Regulatory Regime

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.

Broadly, there are no specific types of laws or regulations which seek to apply uniquely to companies which are categorised as 'FinTech' companies as such. Companies which engage in activities 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.

The laws which tend to be most relevant to businesses operating in the FinTech sector are as follows:

- The national Competition and Consumer Act 2010 (Cth) is the principal item of legislation governing trade practices and consumer protection. 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 Competition and Consumer Act 2010 (Cth) 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;
- 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. FinTech businesses engaged in peer-to-peer style 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;
- 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 to constitute 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. FinTech ventures whose activities may involve conducting a financial services business should consider the applicability of AFSL licensing requirements.

As indicated, this legislation is not uniquely targeted to FinTech companies. It will simply apply to any entity which engages in conduct which those laws purport to regulate.

### 2.3 Variations Between the Regulation of FinTech and Legacy Players

Generally, Australian regulatory regimes in relation to FinTech activities do not seek to distinguish between new entrants and legacy participants. However, innovation and new entrants are generally encouraged, consistent with a broader policy narrative that recognises the need for Australia to evolve its historical economic dependency on resources to the intelligent leveraging of ideas.

Both the Australian Federal Government and Treasury have stated their 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 have remained largely unchanged over the last 12 months. These include the following:

- *Regulatory sandboxing* – a key focus area has been 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 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 to not 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 adapt their solutions and delivery to changing consumer preferences quickly and 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. It is also 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. See below **3.1 Requirement for Different Business Models** and **3.2 Legacy Players' Implementation of Solutions Introduced by Robo-advisers**.
- *Crowdfunding* – the Australian Parliament passed into law the Corporations Amendment (Crowd-sourced Funding) Act 2017 (Cth). This Act 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* – another focus area has been 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* – there is an ongoing focus on improved data availability, more intelligent approaches to data sharing and contracting and a maturing appreciation of the economic benefits of the improved use of data. This is supported through 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 set up 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, which led to the development of a new Consumer Data Right.

- *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 is proposing to work with industry to achieve appropriate regulatory reform regarding the treatment of GST in relation to digital currencies.
- *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' – this being the potential impact of FinTech on government procurement. It has also acknowledged the potential for ProcTech to encourage innovation and investment, deliver greater returns from taxpayer contributions and achieve savings that can be applied toward important public services.
- *Payment systems* – the Australian 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* – the importance of cost-effective access to foreign settlement infrastructure has been recognised, particularly in an increasingly global economy that needs to support jurisdiction-agnostic payment solutions, systems and technologies. 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.

### 2.4 Regulatory Sandbox

In February 2017, Australia's chief corporate regulator, ASIC, established a special type of class waiver, designed to allow eligible FinTech businesses 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 the 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.

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.

### 2.5 Jurisdiction of Regulators

Generally, the responsibility for the enforcement and administration of a particular piece of legislation will be conferred by statute on a nominated regulatory body. The limits of that regulator's powers of enforcement are stipulated in the applicable legislation. Theoretically, scopes of enforcement should not directly overlap although there are frequently points of common interest.

Each of the Commonwealth Acts referred to above in **2.2 Regulatory Regime** 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:

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

As a general rule, it is open to a regulator to behave either proactively or responsively in relation to the administration and enforcement of relevant legislation. Proactive enforcement might involve a regulator initiating its own investigations or conducting audits into activities which it considers to be of regulatory or prudential concern. A regulator may also publish guidance notes or information circulars, to provide direction to the industry in relation to the enforcement attitude it is likely to adopt in response to certain types of conduct. It may also act responsively by conducting investigations in response to complaints it receives from industry participants regarding alleged instances of specific misconduct.

### 2.6 Outsourcing of Regulated Functions

Appropriately managing the risks, including the compliance risks, associated with the outsourcing of regulated functions has become an important focus area for many corporations, businesses and other entities engaged in technology projects that involve outsourcing or offshoring. The relevant requirement will depend on the industry and the requirements of the legislation that imposes the particular regulatory requirement. From a FinTech perspective, the most relevant requirements tend to be those imposed by APRA in its consolidated prudential standards and practice guides. These include the following:

- *Consolidated Prudential Standard 231 (Outsourcing)* - contains certain requirements for APRA-related institutions who propose to engage in the outsourcing of material business activities. These include requiring the maintenance of appropriate policies, implementing and maintaining sufficient monitoring processes to manage outsourcing, consulting with APRA in relation to offshoring and notifying APRA after outsourcing agreements have been entered into. Importantly, from a transactional perspective, it also sets out specific requirements which outsourcing agreements in relation to material business activities must meet.
- *Information paper* – outsourcing involving cloud computing services which sets out general information regarding how APRA intends to apply the concepts in existing standards and guides in future guidance updates. The Information Paper advocates a proper understanding and management of risks (including approaches to assessment of differing materiality), various risk-management considerations and information about materiality assessments that would inform an obligation to notify APRA of a material outsourcing agreement under Consolidated Prudential Standard 231 (Outsourcing).
- *Consolidated Prudential Standard 234 (Information Security)* – requires an APRA-regulated entity to take measures to improve resiliency against information security incidents by maintaining an appropriate information security capability. Its key focus is to minimise the likelihood that information security incidents will impact the confidentiality, integrity or availability of information assets. It requires APRA-regulated entities to clearly define information security-related roles, maintain an information security capability to enable the entity's continued operation, implement controls to protect its information assets and notify APRA of material information security incidents.

As a headline principle, it is generally not possible for regulated entities to transfer their statutory obligations to third-party suppliers or other persons in a way that abdicates that regulated entity's primary liability for compliance. Of course, regulated entities may subcontract or outsource the performance of various functions, subject to complying with applicable requirements, such as those described above in relation to Consolidated Prudential Standard 231 (Outsourcing). They may also seek to reallocate to the outsourced service provider some of the financial exposure of non-compliance through contractual mechanisms such as indemnities and other similar obligations. However, the regulated entity will still retain its primary statutory obligations under applicable legislation, and to the relevant regulator, to demonstrate compliance and in the event of a breach of regulatory requirements.

### 2.7 Significant Enforcement Actions

The details of specific interactions between individual FinTech industry participants and applicable regulators are typically commercial-in-confidence as between those parties, except to the extent that action taken by a regulator might culminate in formal legal action, fines, penalties or prosecution. Historically, the enforcement practices of ASIC and APRA have had a strong focus on liaison with regulated entities and industry participants and co-operative resolution.

It is possible that this may evolve, given the events of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry in Australia. This recently concluded Royal Commission was a wide-ranging investigation into the conduct of the Australian banking sector. During the course of the investigation the Commission considered various matters relating to the effectiveness of the enforcement activities of key regulators ASIC and APRA and its interim report expressly noted that it was rare for ASIC and APRA to resort to court process to seek public redress for misconduct. The Commission's final report was tabled in the Australian Parliament on 4 February 2019.

On 12 November 2018, APRA announced its 'terms of reference' for a review into its enforcement strategy in conjunction with a statement that it is timely to examine whether its traditional approach on prevention and rectification can be augmented by increased enforcement activities. The review is proposed to comprise a "forward-looking examination of APRA's approach to the use of its enforcement powers to ensure that financial promises made by supervised institutions are met within a stable, efficient and competitive financial system". It will also "assess any legal, practical or structural impediments to APRA taking enforcement action" and include a range of areas, including:

- the considerations in determining when it may be appropriate for APRA to take public enforcement action, including litigation, as a deterrent;
- APRA's process for identifying candidates for enforcement action and its decision-making process on whether to take enforcement action;
- APRA's approach to publicly disclosing enforcement priority areas; and
- whether there is greater need for APRA to co-operate more closely with other regulatory agencies in enforcement-related matters.

Following the review's conclusion and presentation to APRA members, APRA is expected to publicly release its final review and enforcement strategy.

### 2.8 Implications of Additional Regulation

Privacy, anti-money laundering and cybersecurity matters are key considerations for participants in the Australian FinTech industry, whether legacy businesses or new entrants.

**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, such as 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 relating to FinTech ventures). It also addresses the collection, storage, use, disclosure, security and disposal of TFNs and related information, together with the Privacy (Tax File Number) Rule 2015 issued under it.

In addition to the Privacy Act, some sector-specific laws also exist which are relevant to data privacy and dealings with personal information. These can sometimes impact FinTech ventures depending on the scope of activities proposed to be engaged in. These include:

- The Telecommunications Act 1997 (Cth) and Telecommunications (Interception and Access) Act 1979 (Cth), 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); and
- 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 Australian government recently passed new legislation implementing mandatory reporting of data breaches. The Privacy Amendment (Notifiable Data Breaches) Act 2017

(Cth) came 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 are 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), which sets out certain Health Privacy Principles that NSW government agencies must comply with when handling personal health information.

**Anti-Money Laundering**

The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and Anti-Money Laundering and Counter-Terrorism Financing Rules (Cth) implement a principles and risk-based approach to the regulation of illegal transactions. This legislation is administered by the Australian Transaction Reports and Analysis Centre (AUSTRAC), which is the regulatory body responsible for monitoring financial transactions to identify activities such as money laundering, organised crime, fraud and terrorism.

The Act imposes various obligations on reporting entities which provide designated services, such as enrolment and registration with AUSTRAC, obligations to collect and verify 'know your customer' (KYC) information about the identity of a customer, record keeping, establishment and maintenance of an anti-money laundering and counter-terrorism financing programme and ongoing customer due diligence and reporting.

**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 standards and 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). Also relevant is the Consolidated Prudential Standard 234 (Information Security) discussed in **2.6 Outsourcing of Regulated Functions**, above.

These are designed to assist regulated entities in managing their information technology security risk and also elaborate on the steps they should take to protect the data and 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.

## 2.9 Regulation of Social Media and Similar Tools

In keeping with the technology-agnostic policy approach described in **2.3 Variations Between the Regulation of FinTech and Legacy Players** above, there is no specific legislation in Australia which uniquely governs social media and social media applications and tools in a FinTech context. However, an array of existing laws and legal principles (under both common law and statute) may apply to the way in which social media is provided and used, in the same way as such laws and legal principles may apply to other online conduct. These may include defamation law, privacy law, copyright infringement, competition and consumer law (for example, relating to misleading and deceptive conduct), employment law and contract law (such as the consequences of non-compliance with online terms and conditions).

## 2.10 Review of Industry Participants by Parties Other Than Regulators

Beyond formal regulation, the behaviours and activities of FinTech industry participants are disciplined by (as applicable) their own corporate governance requirements, their shareholders and ultimately the expectations of end consumers of their products and services. In certain cases, self-regulatory bodies may be established and appointed to

oversee and administer specific activities (such as Gateway Network Governance Body Ltd, which was established in 2016 to manage the integrity, security and effectiveness of the Australian superannuation transaction network).

### 2.11 Conjunction of Unregulated and Regulated Products and Services

With the current pace of technological evolution, there is a growing conceptual debate in Australia regarding the difference between traditional (regulated) banking functions and pure technology-enablement functions. The essential question is at what point is a vendor or third-party service provider, who provides back-end technological functionality to a regulated entity, effectively beginning to perform functions that should be treated as a regulated activity. The concern is that as disaggregation of functions leads to the fragmentation of service provision, it will become increasingly difficult to unambiguously identify those particular functions which should be subject to regulation.

In late 2018, the Chairman of APRA acknowledged the challenges posed by the intersection of technology and outsourcing, noting that while outsourcing and partnering are not new concepts, they are "increasingly […] occurring for business-critical functions, not just at the periphery of activities", resulting in many critical functions (or at least parts of them) being performed by unregulated entities.

A concentration risk was also acknowledged – that is, "the systemic risk of an ostensibly large and diverse number of entities all dependent on just a few unregulated providers for critical services […] increasing the threat of contagion in the event of a service failure". Such issues will continue to be a focus area for regulators and industry in Australia.

## 3. Robo-advisers

### 3.1 Requirement for Different Business Models

Robo-advice business models feature the substitution of functions traditionally performed by a human financial or wealth adviser with algorithm-based applications. Depending on the levels of functionality supported by the relevant software application, an individual is, theoretically, able to input various personal details and information about his or her risk profile into the relevant application and, based on the operation of the application's underlying algorithms, receive factual, general or personal advice.

In this disintermediated model, the provider of the application receives payment instead of the traditional financial or wealth adviser.

Hybridised robo-advice business models also exist, which combine automatic application functionality (where the user interacts with a front-end application) with back-end human-based recommendations and investment decisions. Notwithstanding some human-level involvement in the advice process, these models still purport to deliver savings on the costs of personal (one-on-one) financial advice.

Some applications also permit investing decisions to be actioned through instructions received through an applications interface.

In terms of payment, the provider of the relevant robo-advice application may receive payment by way of a subscription model, an agreed percentage of the subscriber's account balance or some other agreed fee.

### 3.2 Legacy Players' Implementation of Solutions Introduced by Robo-advisers

The reaction of legacy financial advisers to robo-advice offerings has been mixed. Some existing providers have naturally resisted disintermediation by seeking to enhance their offerings to improve competitiveness and socialise with their consumer bases the aspects of one-on-one personal service which cannot be delivered through competing automation products. One strategic challenge in this regard is that robo-advice offerings, as well as providing a potential for customer churn away from traditional financial advice businesses, also seek to appeal (through ease of use, increased accessibility and lower charges) to that proportion of the market which may not otherwise visit a personal financial adviser. Other existing providers have begun to explore incorporating elements of robo-advice into their current solutions, in a bid to compete through augmented offerings which offer both human and robo-advice elements.

One view is that robo-advice offerings are not directly competitive with legacy businesses because they tend to focus on portfolio management as opposed to specific strategic advice on particular opportunities, and so in fact robo-advice could be complementary to existing offerings.

In Australia, robo-advice solutions are not exempted from the need to comply with a range of legal requirements that would apply to legacy financial advice businesses. Generally, the provision of mere factual advice attracts the lowest regulatory burden, dispensing general advice attracts a higher burden and a solution that delivers personal advice attracts the highest. Problematically, however, while theoretically distinct, in practice the line between the various types of advice is not always clear.

Matters for providers of robo-advice offerings to consider include:

- Australian Financial Services Licence (AFSL) requirements, including both whether the types of advice generated by the applicable algorithm is of a kind that requires an AFSL and also whether persons who refer clients to a

provider of a robo-advice offering are providing a financial service; and
- to the extent the robo-advice solution delivers personal advice, how providers of such a solution will demonstrate compliance with the duty to act in the client's best interests, provide appropriate advice and prioritise the interest of the client over its own (and how the solution will generate and present the statement of advice required to be provided).

Some forms of existing legislation have interesting elements of application in the context of robo-advice. For example, some requirements have arguably been conceived around specific interactions with consumers, such as disclosure at a point in time, as opposed to ongoing provision of information.

Recognising some of the challenges posed by the interaction of new robo-advice offerings with existing regulatory frameworks, in March 2016 ASIC published Consultation Paper 254 (Regulating Digital Financial Product Advice) followed by, in August 2016, Regulatory Guide 255 (Providing Digital Financial Product Advice to Retail Clients).

Regulatory Guide 255 addresses a range of matters relating to the provision, through robo-advice solutions, of general and personal advice to retail clients, such as:

- the scope of AFSL requirements;
- the need for appropriate human and technical resources as a digital advice licensee, and the need for adequate risk management solutions (including in relation to cyber risks and information security);
- the requirement to monitor and test algorithms on which the robo-advice offering is based, as well as the regular sample testing of the advice outputs that the relevant solution produces;
- remediation and reporting steps to be taken, depending on testing outcomes;
- the implementation of systems to identify and filter customers whose requirements fall beyond the advice being offered by the solution or who provide inconsistent answers in relation to their relevant circumstances; and
- the requirement to conduct ongoing reviews of digital advice, the performance of underlying algorithms and rectification of errors detected in algorithms.

The guide also affirms ASIC's technology-neutral approach to regulation generally, and confirms that the obligations applying to traditional financial product advice and digital advice are equivalent.

### 3.3 Issues Relating to Best Execution of Customer Trades

The ASIC Market Integrity Rules (Securities Markets) 2017 require that when handling an order for a client, a market participant must take reasonable steps to obtain the best outcome for that client. This is generally referred to as the 'best execution' obligation. For a retail client, the best outcome means the best total consideration, and for a wholesale client it may also include other factors such as price, cost, speed, likelihood or execution of any other relevant outcome. Subject to certain requirements being met, the market participant must also take reasonable steps to satisfy the client's instructions.

In May 2018, ASIC also published Regulatory Guide 265 (Guidance on ASIC Market Integrity Rules for Participants of Securities Markets), which provides additional guidance on how market participants are expected to comply with best execution requirements. This elaborates on the requirements for market participants to maintain adequate policies and procedures to assist them in complying with their best execution obligation (and detail on what those policies and procedures should address), disclose certain information to clients, regularly review and monitor the effectiveness of execution arrangements and have the ability to demonstrate compliance.

The use of automated processes are not prohibited or deemed to be incapable of satisfying best execution obligations. For example, the regulatory guide acknowledges that market participants may use smart order routing, or "tools to connect to multiple order books to scan the various markets to determine which one delivers the best outcome on the basis of predetermined parameters and to transmit orders to the selected order books and other matching mechanisms". However, to the extent market participants choose to utilise automated functions, it is their obligation to ensure that those processes remain compatible with its best execution policies and procedures and ensure its ability to comply with the applicable rules. The regulatory guide emphasises that "this applies irrespective of whether the […] automated processes have been developed by the market participant or provided by a third party".

Chapter 5 of the ASIC Market Integrity Rules (Securities Markets) 2017 requires that a trading participant which uses its system for automated order processing ensures that the system has in place certain features, such as:

- organisational and technical resources, including appropriate automated filters and parameters to enable trading messages to be submitted into a trading platform without interfering with the efficiency and integrity of the relevant market;
- trading management arrangements to enable the determination of origin of orders and trading messages;
- security arrangements to monitor for and prevent unauthorised access to a gateway, an open interface device or a connected computer;

- automated controls that enable immediate suspension, limitation or prohibition of automated order processing at certain levels; and
- controls that enable immediate suspension and cancellation of trading messages and orders.

Before using their system for automated order processing, a trading participant must also review its procedures and systems, provide a written certification to ASIC and receive a confirmation of compliance from ASIC.

## 4. Online Lenders

### 4.1 Differences in the Business or Regulation of Loans Provided to Different Entities

Activities relating to the provision of consumer credit are highly regulated in Australia. The National Consumer Credit Protection Act 2009 (Cth) implements the National Credit Code and also requires all providers of consumer credit to obtain an appropriate licence from ASIC, the national regulator for consumer credit.

Credit licensees are required to comply with a range of requirements such as:

- general conduct obligations requiring them to perform credit activities honestly and fairly, manage conflicts of interest and undertake basic steps such as maintaining organisational competence, undertaking training, having adequate financial resources, maintaining appropriate dispute resolution procedures and having adequate compensation and insurance arrangements;
- responsible lending obligations involving, principally, not entering into a credit contract with a consumer that may be unsuitable for it – this will require the making of reasonable inquiries regarding a consumer's financial situation and appropriate assessments; and
- the submission of annual compliance certificates.

### 4.2 Underwriting Processes

From a financial assurance perspective, the National Consumer Credit Protection Act 2009 (Cth) safeguards the interests of consumers by requiring credit licensees to have adequate financial resources and adequate compensation arrangements for compensating customers for loss or damage suffered because of breaches of that Act by the credit licensee or its representatives.

With respect to the requirement to have adequate financial resources, ASIC Regulatory Guide 207 (Credit Licensing – Financial Requirements) expressly states that the credit licensee is responsible for deciding how to comply with financial resource requirements. However, it sets out ASIC's minimum expectations for demonstrating this, including:

- having sufficient resources to meet debts as and when they become due and payable;
- planning and monitoring cash flows; and
- keeping written records to demonstrate regular monitoring of financial resources.

ASIC Regulatory Guide 210 (Compensation and Insurance Arrangements for Credit Licensees) notes that a credit licensee must have adequate arrangements in place for compensating consumers, and that the primary way of complying with this obligation is to have appropriate professional indemnity insurance in place (although it is also noted that ASIC may approve alternative arrangements). Regulation 12 of the National Consumer Code Credit Protection Regulations 2010 (Cth) requires the holding of professional indemnity insurance that is adequate having regard to:

- the credit licensee's membership of external dispute resolution schemes, taking into account the maximum liability that realistically has potential to arise in connection with one or all claims; and
- relevant considerations relating to its credit activities, such as business volume, number and kind of clients, kind of business and number of representatives.

### 4.3 Sources of Funds for Loans

Loans may be established in Australia through a broad range of funding sources. From a FinTech perspective, the legal and regulatory issues relating to peer-to-peer, or 'marketplace', lending, have received particular attention in Australia.

ASIC has acknowledged that a range of business models may be used to deliver peer-to-peer or marketplace lending products, such as managed investment schemes, the issue of derivatives or securities or the operation of a financial market. A marketplace-lending scenario may involve matching retail or wholesale investors seeking to earn a return from investing with consumers or businesses seeking borrowings, often through a website, online platform or smartphone application. This could involve a single investor being matched to fund a loan pool or, alternatively, multiple investors funding one loan.

ASIC has noted that marketplace lending involves a number of risks, including:

- a failure to adequately manage conflicts of interest of the marketplace operator;
- fraud and cybersecurity; and
- a lack of sufficient understanding of investors and borrowers about the marketplace-lending product.

As such, it is important for providers of peer-to-peer or marketplace lending solutions to ensure that participants are fully informed regarding the loan product and that investors are given all information necessary to make an informed invest-

ment decision. Providers of such products will generally be characterised as providing a financial service and will need to obtain an Australian Financial Services Licence (AFSL) under the Corporations Act 2001 (Cth). To the extent it is participating in loans to consumers, the investor will also need to obtain a credit licence under the National Consumer Credit Protection Act 2009 (Cth) as described in **4.1 Differences in the Business or Regulation of Loans Provided to Different Entities**.

### 4.4 Syndication of Loans

As set out above in **4.3 Sources of Funds for Loans**, a marketplace-lending scenario implemented through a website, platform or other application could match multiple investors to fund a single loan, depending on the lending and borrowing parameters specified by the participants and the configuration of the matching application. Regulation is as specified in the aforementioned sub-section.

## 5. Payment Processors

### 5.1 Payment Processors' Use of Payment Rails

Typically, payment processors and payment gateways in Australia operate within the established interchange ecosystem as opposed to creating a new payment network infrastructure. They do this by providing a means by which transaction information is communicated between the merchant, the issuing bank (the bank that hosts the account of the customer) and the acquiring bank (the bank that acquires the transaction for the relevant merchant). Effectively, in very simple terms, such entities provide customers and merchants with access to the existing payment interchange network to enable them to conduct and conclude transactions.

In relation to 'card present' transactions, being transactions involving the presentation of a physical card by a customer to a merchant, the service provided by a payment processor usually includes the provision of a physical point of sale interface (such as a card-processing terminal) to a merchant, which authenticates a customer's card in the course of a transaction initiated by that cardholder. The terminal will relay the proposed transaction details to the bank that has issued the card for that transaction to be approved or declined. If it is approved, the payment processor relays that information to the acquiring bank to enable the transaction to be completed.

For 'card not present' transactions (such as where a transaction request is initiated through an application or over the internet), the additional role of a payment gateway is important. In the absence of a physical terminal to perform the authentication function, the payment gateway will perform the functions that would otherwise have been performed by the terminal. This includes authentication, relaying of encrypted information and secure transmission of transaction details to the payment processor.

## 6. Fund Administrators

### 6.1 Regulation of Fund Administrators

There are various types of legislation that may be relevant to the administration and management of investment funds in Australia, including the Corporations Act 2001 (Cth) and the Superannuation Industry (Supervision) Act 1993 (Cth). Relevantly, ASIC requires the providers of certain financial services to obtain an Australian Financial Services Licence and comply with consequent obligations in relation to conduct, reporting and disclosure. Some of the obligations which may apply relate to:

- requirements to register collective investment vehicles with ASIC;
- dealing honestly and fairly in the conduct of its business;
- complying with investor disclosure requirements and certain safeguards with respect to the management of client trust monies;
- taking steps in relation to anti-money laundering; and
- reporting of breaches to ASIC.

In July 2018, a range of new comprehensive regulatory guides were published by ASIC providing guidance to the funds industry. These address matters such as establishing and registering a fund, compliance and oversight, funds management and custodial services, constitutions, discretionary powers and foreign passports.

### 6.2 Contractual Terms

In addition to the regulatory requirements that might be attracted by activities relating to the administration and management of investment funds (see **6.1 Regulation of Fund Administrators**), it is open to commercial counterparties to augment statutory duties (such as the requirement to deal honestly and fairly) with contractual requirements relating to quality, timeliness, due care and skill and other business requirements.

### 6.3 Fund Administrators as 'Gatekeepers'

As set out above in **6.1 Regulation of Fund Administrators**, administrators and managers of investment funds may be required to comply with obligations of a financial services licensee including monitoring and reporting on compliance and reporting relevant breaches to ASIC. To the extent their activities also attract anti-money laundering regulations, the relevant entity may also have obligations to report suspicious matters to AUSTRAC under the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017 (Cth).

## 7. Exchanges and Trading Platforms

### 7.1 Permissible Trading Platforms

In addition to their core brokerage services (whether in relation to shares, currency or some other commodity), many brokers will offer their clients access to enhanced functionality in the nature of electronic trading platforms. These are essentially software-based applications which enable self-service execution of trades, account-monitoring capabilities and other related characteristics. The commercial terms on which such access is offered may vary and there may be a variety of features offered by different providers, with different subscription models. Generally, the technical requirements for such platforms are not statutorily prescribed or governed by regulation. However, the operator of the relevant platform will still need to comply with applicable laws relating to its core or underlying activities.

If a trading platform involves the use of a system for automated order-processing, the trading participant using that system will need to comply with certain requirements in relation to that system as set out in Chapter 5 of the ASIC Market Integrity Rules (Securities Markets) 2017 (Cth). See above, **3.3 Issues Relating to Best Execution of Customer Trades** in relation to those requirements.

### 7.2 Impact of the Emergence of Cryptocurrency Exchanges

In response to the issues posed by the emergence of digital currency exchange-providers, the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017 (Cth) was passed to extend the scope of Australia's existing anti-money laundering legislation to capture such activities. See **12.7 Virtual Currencies**, below.

### 7.3 Listing Standards

Companies that wish to have their securities quoted on Australia's primary securities exchange, the Australian Stock Exchange (ASX), must apply to be listed on the official list of the ASX, be admitted onto that list and agree to comply with the ASX Listing Rules. Those rules address matters such as continuous and periodic disclosure, securities, changes in capital, new share issues, trading halts and suspensions.

The ASX Listing Rules are enforceable against that company pursuant to the Corporations Act 2001 (Cth). A breach or failure to comply with the ASX Listing Rules may result in the relevant company being removed from the ASX list or its securities being suspended from quotation.

### 7.4 Order-handling Rules

See above **3.3 Issues Relating to Best Execution of Customer Trades** in relation to the obligation provided for in the ASIC Market Integrity Rules (Securities Markets) 2017 (Cth). In addition to that obligation, those market integrity rules provide for other obligations in relation to client order priority, such as the requirement for market participants to deal fairly and in due turn with clients' orders and the requirement to allocate market transactions fairly.

### 7.5 Rise of Peer-to-Peer Trading Platforms

Most trading platforms in Australia are based on the development of products and services relating to the trading of shares on Australia's primary securities exchange, the ASX, as opposed to via a separate peer-to-peer ecosystem. In relation to digital currency exchanges, these may be required to register and enrol with AUSTRAC as described in **12.7 Virtual Currencies**, below.

### 7.6 Issues Relating to Best Execution of Customer Trades

See above, **3.3 Issues Relating to Best Execution of Customer Trades**.

## 8. High-frequency and Algorithmic Trading

### 8.1 Creation and Usage Regulations

High-frequency trading is a practice that relies on high-capacity computer processing to process a large volume of transactions in a short space of time, powered by algorithms which automate rapid market analysis and order execution.

Australia's corporate regulator ASIC has conducted various consultations, taskforces and other activities to investigate and consider the impact of such activities on Australia's financial markets. In 2013, following the work of ASIC's internal taskforces assessing the impact of 'dark liquidity' and high-frequency trading on market quality and integrity, ASIC determined that public concerns regarding high-frequency trading had, to some degree, been overstated and that the overall Australian corporate regulatory framework was sufficiently resilient without the need for wholesale structural changes. Notwithstanding this, following its 2012 reviews, ASIC amended its Market Integrity Rules to:

- help manage conflicts of interest and provide for the ability for wholesale clients to request that participants disclose when they have traded with their clients as principal; and
- provide greater transparency in relation to transaction data and the operations of certain 'crossing systems'.

ASIC conducted further reviews of high-frequency trading in 2015 which confirmed the adequacy and effectiveness of the existing regulatory framework. In 2018, it undertook a further review, which identified that while high-frequency traders continue to maintain a large presence, their contribution to overall turnover had slightly declined and that investment in faster technologies is not necessarily translating to additional competitive advantage.

### 8.2 Exchange-like Platform Participants
See **8.1 Creation and Usage Regulations**, above.

### 8.3 Requirement to Register as Market Makers When Functioning in a Principal Capacity
As described in **8.1 Creation and Usage Regulations** above, following its reviews of high-frequency trading activities in 2012, ASIC adjusted its Market Integrity Rules to enable wholesale clients to request that participants disclose when they have traded in a principal capacity. This change was designed to assist in the management of conflicts of interest.

### 8.4 Issues Relating to the Best Execution of Trades
See above, **3.3 Issues Relating to Best Execution of Customer Trades**.

### 8.5 Regulatory Distinction Between Funds and Dealers
Not applicable in Australia – see **8.1 Creation and Usage Regulations**.

### 8.6 Rules of Payment for Order Flow
Not applicable – see **8.1 Creation and Usage Regulations** above. For a discussion in relation to regulatory requirement for best execution of trades, see above **3.3 Issues Relating to Best Execution of Customer Trades** in relation to ASIC Market Integrity Rules (Securities Markets) 2017.

## 9. Financial Research Platforms

### 9.1 Registration
Companies and business that provide pure information or research services in the FinTech industry are not specifically or uniquely registered or required to register in Australia, provided their products and services are restricted to the assembly of factual and historical information and do not venture into activities that would require an Australian Financial Services Licence to be obtained, such as the provision of general or personal financial advice.

One exception may be in relation to certain types or categories of information where the statutory agency responsible for the maintenance of an authoritative register requires information brokers in that industry to be authorised before it will permit those brokers to access and disseminate information from that statutory register (for example, NSW Land Registry Services which maintains real property and titling information in the State of New South Wales and administers an application process for persons to become an authorised information broker in respect of the information in the register it maintains).

### 9.2 Regulation of Unverified Information
Financial research companies will generally seek to manage the risks associated with the supply of their products and services by drawing their information from sufficiently authoritative sources and applying appropriate due care and skill to their research and verification activities. Contractually, they will also seek to supply their products and services on terms and conditions which limit their liability to the extent commercially reasonable and which provide that, while reasonable care and skill has been applied to the development of products, absolute currency and accuracy may not be able to be completely assured.

Individuals who purposely disseminate false, misleading, fraudulent or damaging information may potentially be exposed to other statutory, criminal or tortious actions.

### 9.3 Conversation Curation
Online forums or platforms which permit public discussion regarding financial or investment opportunities will naturally entail some degree of risk associated with the activities enabled through those forums or platforms. This includes the potential for use of the forum to disseminate false or incorrect information, divulge information in breach of privacy or confidentiality obligations owed to third parties or to seek to manipulate market perception of value with respect to particular stocks or securities.

Various options are available to platform operators to mitigate this risk, including:

- ensuring that the terms and conditions applicable to participation in the platform are very clear as to the basis on which information may be posted or exchanged and the risks associated with the reliance on that information;
- devoting reasonable resources to moderating instances of clearly unacceptable comments and behaviour;
- maintaining an easily accessible, online complaint lodgement mechanism to facilitate the reporting of incidences of unacceptable conduct by other users; and
- applying and enforcing acceptable user policies and conditions of participation, such as excluding users who breach those policies and conditions.

### 9.4 Platform Providers as 'Gatekeepers'
There is a strategic question as to the extent to which operators of such online forums or platforms should allow users to come to rely on that operator's policing or moderation of platform conduct. One view is that an active moderation role also attracts some risk, as it may increase users' reliance on and expectation as to the diligent administration of those activities. There is also a risk associated with the need to make quick substantive judgments as to which comments should be allowed to be or remain published and which comments should be restricted or removed. However, good practice suggests that platform moderators should – as described in **9.2 Regulation of Unverified Information** – always be very clear with users regarding the risks associated with the platform and the 'best efforts' nature of its modera-

tion activities and ensure that it conscientiously responds to any complaints or requests for particular instances of unacceptable conduct to be moderated or redressed.

## 10. InsurTech

### 10.1 Underwriting Processes

Insurance underwriting agencies are generally considered to be operators of financial services businesses, requiring them to obtain, and operate under, an Australian Financial Service Licence. In addition to complying with applicable licence conditions, the specific processes they may adopt for the purposes of performing underwriting activities are influenced by commercial requirements and the needs of the insurers for whom they perform underwriting activities. Their processes will also need to be sufficiently robust for insurers to be confident that applicable risks have been assessed and sized appropriately.

From an InsurTech perspective, a close relationship is being discovered between big data and the technology-driven tools and applications that may be used to improve, streamline and enhance risk-assessment and quantification. Potential solutions range from applications that deliver back-end functionality, such as the use of artificial intelligence and algorithms to inform pricing for premiums, to front-end capability, such as portals or interfaces that connect consumers to, and assist them in comparing, the offerings of different insurance providers.

### 10.2 Treatment of Different Types of Insurance

The market for the provision of insurance-related products and services in Australia is highly regulated through statutory instruments such as the Insurance Act 1973 (Cth), the Insurance Contracts Act 1984 (Cth), the Life Insurance Act 1995 (Cth) and the Corporations Act 2001 (Cth), with each of APRA and ASIC responsible for administering various statutes which impact insurance-related activities. For example:

- with respect to general insurance, a person cannot carry on an insurance business in Australia unless they are authorised, by APRA, to do so as an authorised general insurer under the Insurance Act 1973 (Cth) – once authorised, that person must carry on its business in accordance with the requirements of the legislation and comply with other prudential standards prescribed by APRA;
- under the Life Insurance Act 1995 (Cth), only a registered life insurance business may issue a life insurance policy – similarly, APRA is responsible for assessing applications, granting registration and setting standards with which registered businesses must comply; and
- a separate system of registration applies to private health insurers under the Private Health Insurance Act 2007 (Cth) – such businesses must apply to the Private Health Insurance Administration Council, which regulates registration and related activities.

## 11. RegTech

### 11.1 Regulation of RegTech Providers

Third-party technology providers of RegTech services who are not themselves naturally regulated may or may not become regulated depending on the particular activity they are performing on behalf of another entity.

In one scenario, certain legislation may impose a primary obligation on a particular regulated entity. As described in **2.6 Outsourcing of Regulated Functions**, regulated entities cannot then generally transfer their statutory obligations to third-party suppliers or other persons in a way that abdicates that regulated entity's primary compliance liability. However, they may sub-contract the performance of certain functions, subject to complying with applicable prudential or other regulatory requirements, such as those in Consolidated Prudential Standard 231 (Outsourcing). The RegTech provider may then be subject to contractual obligations owed to the regulated entity, but does not itself become a regulated entity or answerable to the relevant regulator.

In other circumstances, the applicable legislation will apply to any entity within the jurisdiction engaging in acts or providing types of services which that legislation purports to regulate – for example, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth). This may require the RegTech provider to comply directly with applicable regulatory requirements, which can sometimes include registration and licensing.

### 11.2 Contractual Terms to Assure Performance and Accuracy

The provisions of sub-contracts between regulated entities in the financial services sector and their technology providers will be dictated by both regulatory and commercial requirements. For instance, Consolidated Prudential Standard 231 (Outsourcing) mandates the inclusion of certain provisions in agreements governing the outsourcing of material business activities by a regulated entity. These require that such an outsourcing agreement must address scope, commencement and end dates, review provisions, pricing and fee structure, service levels, the form in which data is to be kept and provisions relating to ownership and control of data, reporting requirements, audit and monitoring procedures, business continuity, confidentiality, privacy and security, breach and termination provisions, dispute resolution arrangements, liability and indemnity, insurance and offshoring. There are also particular requirements that need to be included with respect to sub-contracting and audit.

Other contractual provisions will be informed by commercial drivers and the regulated entity's risk appetite, such as indemnities in respect of breach and non-compliance. The regulated entity may also seek to impose contractual obligations on a technology provider which, while not strictly mandatory, are desirable to facilitate that regulated entity's own compliance obligations as between it and a regulator (such as information provision and reporting obligations).

### 11.3 RegTech Providers as 'Gatekeepers'

Generally, there is no common law duty on a RegTech provider to report suspicious activities. However, as described in **11.1 Regulation of RegTech Providers**, the obligations of RegTech providers may alternatively be imposed by legislation, to the extent they engage in activities that fall within the ambit of that legislation, or in contract requirements with regulated entities who choose to sub-contract the performance of those regulated functions to the RegTech provider. To the extent that either statute or contract imposes obligations in the nature of suspicious matter reporting on a RegTech provider, then it will need to comply with them.

## 12. Blockchain

### 12.1 Use of Blockchain in the Financial Services Industry

Blockchain caused a high degree of initial excitement in the Australian FinTech community, founded in the expectation that distributed ledger technology had the potential to revolutionise a broad range of financial services-related business models and industries. Since that initial reaction, discussion with respect to potential blockchain applications has evolved into a more measured discussion which, usefully, seeks to differentiate between:

- those more far-fetched or speculative applications of blockchain technology;
- applications which could be implemented using some form of distributed ledger technology, but for which the business case necessitating the use of that technology for those purposes is not proven or obvious; and
- those applications in respect of which the use of blockchain would be uniquely disruptive, in a way which could not conceivably be achieved by alternative technologies or solutions in a cost-effective manner.

Particular areas of interest have included cybersecurity solutions for financial services transactions, the use of smart contracts and automated settlements.

### 12.2 Local Regulators' Approach to Blockchain

To date, in keeping with Australia's technology-neutral approach to regulation of new innovations, no specific legislation has been passed targeting or uniquely regulating blockchain applications, assets or providers. As such, until such time as policy observations identify a need for reform and design and implement the appropriate legislation, the question as to how the Australian legal landscape impacts new blockchain assets or solutions will be answered through an overlay of existing laws and regulations against the characteristics of that new asset or solution.

For example, it is possible that the undertaking of functions or activities that utilise blockchain technology may require an Australian Financial Services Licence to be obtained. In this regard, ASIC has released an assessment tool to assist businesses in evaluating services based on distributed ledger technology and also published information regarding other licensing obligations that may be relevant to such activities. Similarly, the scope of activities may attract obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), depending on the nature and characteristics of the solution and the manner in which it is provided.

Notable industry developments include:

- the publication by Standards Australia in March 2017 of a Roadmap for Blockchain Standards, which supported the development of a collective Australian viewpoint on matters relevant to the development of international blockchain standards;
- the Australian National Blockchain project, involving a consortium established in 2018 by the Commonwealth Scientific and Industrial Research Organisation (CSIRO) and other industry participants, focused on the piloting of a cross-industry, digital platform to enable collaboration between Australian businesses using blockchain-based smart contracts; and
- the Australian Stock Exchange undertaking a project to move to distributed ledger technology for post-trade equity market clearing and settlement functions, projected to go live in 2021.

### 12.3 Classification of Blockchain Assets

This is not applicable as Australia has not adopted asset-based forms of regulation for blockchain or distributed ledger technologies. See above **12.2 Local Regulators' Approach to Blockchain**.

### 12.4 Regulation of 'Issuers' of Blockchain Assets

See **12.2 Local Regulators' Approach to Blockchain**.

### 12.5 Regulation of Blockchain Asset-trading Platforms

See **12.2 Local Regulators' Approach to Blockchain**.

### 12.6 Regulation of Invested Funds

There is no specific legislation in Australia prohibiting, or uniquely regulating, private investments in ventures that sell products or services that incorporate distributed ledger tech-

nologies. However, it is possible for assets based on blockchain technology to be designed, packaged or marketed in a way that attracts the application of existing regulation. For example, initial coin offerings, depending on how they are structured and designed, might attract regulation under Australian corporations legislation as a financial product, a managed investment scheme or an offer of shares or derivatives. Their characterisation under existing laws will also be influenced by the rights that the designers of those products purport to attach to them.

### 12.7 Virtual Currencies

Similarly to assets comprised of blockchain technologies, the legal status of a virtual currency product will depend on its specific characteristics and the rights attaching to it. In Australia, much of the focus surrounding the need for regulation of crypto-currencies has focused on anti-money laundering and taxation impacts.

With respect to anti-money laundering, Australia introduced new laws in 2018 requiring digital currency exchange-providers with operations in Australia (being businesses that exchange traditional currency for digital currency, or vice versa) to register and enrol with AUSTRAC, adopt and maintain an anti-money laundering and counter-terrorism financial programme, comply with suspicious matter reporting requirements and satisfy various record-keeping obligations. This was implemented through the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017 (Cth), which extended the scope of Australia's existing anti-money laundering legislation.

With respect to taxation, one of the key FinTech priorities historically identified by the Australian government is working with industry to achieve appropriate regulatory reform in relation to the treatment of Goods and Services Tax (GST) in relation to digital currencies, noting the potential for effective double taxation on consumers who use digital currencies to purchase goods or services.

The Australian Taxation Office (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. Rather, it has equated transacting with bitcoins to a barter arrangement and issued several rulings relating to income tax, fringe benefits tax and GST. Notably, however, the ATO has indicated that, in the context of general crypto-currency transacting, it will treat the disposal of bitcoin and other crypto-currencies as the disposal of an asset for the purposes of Capital Gains Tax (CGT).

### 12.8 Impact of Privacy Regulation on Blockchain

As described above in **2.8 Implications of Additional Regulation**, the Privacy Act 1988 (Cth) regulates the collection, use and handling of information that is considered personal information. There has been some discussion in Australia regarding whether certain of these requirements are inconsistent with the characteristic of blockchain technology that involves the creation of an indelible, immutable record of a transaction series (to the extent that personal information becomes part of that record). Specifically, consideration is being given to how a permanent and transparent record can be said to be consistent with:

- Australian Privacy Principle 6, relating to not using or disclosing personal information for a purpose other than that for which it was collected;
- Australian Privacy Principle 11, which requires the destruction or de-identification of personal information when it is no longer needed for the purposes for which it was collected; and
- Australian Privacy Principle 13, regarding the correction of inaccurate, out-of-date or incomplete information.

The answers to these questions are still evolving. However, industry focus to date has been largely on exploring possible technical solutions. These include exploring the use of cryptographic principles such as zero-knowledge proofs (to limit the extent to which personal information or meta-data relating to that personal information needs to form part of a blockchain's indelible record) and investigating whether the consensus-validation functions of a blockchain can be limited to certain authorised participants only, as opposed to necessarily being seen by all network participants.

## 13. Open Banking

### 13.1 Regulation of Open Banking

The imminent implementation of open banking in Australia will represent the country's first sector-specific adoption of a national Consumer Data Right first announced by the Federal Government in 2017. It is part of a broader policy implementation journey that gathered momentum following the findings of an inquiry conducted by the Australian Productivity Commission in relation to data availability and use in Australia.

On 8 May 2017, the Productivity Commission of the Australian Government issued its final report in relation to the availability and use of public and private sector data in Australia. Its terms of reference included considering the costs and benefits of making public and private data sets more available, assessing options for the collection, sharing and release of data and identifying ways in which consumers might benefit from access to data (including data relating to themselves) while preserving individual privacy and levels of control. That report made various findings, among them being that improved data access and use had the potential to transform everyday life, drive efficiency, create productivity gains and allow better decision making. It also proposed that marginal changes to existing legislation would not suffice,

but that reforms were required to transform a risk-avoidance system into one based on transparency and confidence which treated data as an asset as opposed to a threat.

In keeping with this, it advocated a new comprehensive right for consumers to have active use of their own data, including the right to have a copy of their data provided to a third party nominated by the consumer.

In response, later that year the Australian Government announced the development of the Consumer Data Right (CDR). The CDR will be implemented, economy-wide, on a phased sector-by-sector basis, initially in the banking sector and followed by energy and telecommunications.

In conjunction, the Australian Government commissioned an Open Banking Review to determine the most appropriate manner in which to implement the CDR in the banking sector. That review delivered a broad range of recommendations relating to the framework for regulation, the types of banking data involved, security and safeguards, the recommended technical manner of data transfer (that is, through application programming interfaces) and implementation issues.

From a regulatory perspective, open banking is proposed to be implemented through amendments to the Competition and Consumer Act 2010 (Cth), with primary regulation by the Australian Competition and Consumer Commission and a supporting role performed by the Office of the Australian Information Commissioner in relation to privacy matters.

While initially anticipated to commence on 1 July 2019, the Australian Government has recently announced the deferral of the commencement of the public open banking scheme to 1 February 2020. In the interim, a pilot scheme will operate involving Australia's major banks, consumers and other FinTech industry participants.

### 13.2 Concerns Raised by Open Banking

The Open Banking Review expressly acknowledged the need for safeguards to inspire confidence among consumers, particularly in relation to dealings with their data, noting that "[c]ustomer confidence is critical to the success of open banking" and acknowledging a particular concern in relation to online privacy and the need for "high regard to data security to ensure that customers' privacy and confidentiality are maintained". The review also acknowledged industry submissions identifying the importance of customer control, including in relation to what data is shared, with whom, for what purpose and for how long. Interestingly, the review also highlighted the potential for open banking to reduce risks in certain circumstances – for example, by establishing a common secure technical standard for the sharing of data as opposed to current, more ad hoc, processes such as 'screen-scraping'.

The review's recommendations to address privacy and security concerns included:

- making open banking data recipients subject to the requirements of the Privacy Act 1988 (Cth);
- modifications to certain Australian Privacy Principles to deliver improved protections, including those relating to collection of solicited personal information, dealings with unsolicited personal information, notification of collection, use or disclosure, direct marketing and cross-border disclosure;
- ensuring that customer consents, including with respect to sharing of data with a third party, are explicit, fully informed and able to be constrained according to the customer's instructions; and
- ensuring that, to be accredited for participating in open banking, participants comply with designated security standards set by the relevant standards body.

**Clayton Utz**

Level 15
1 Bligh Street
Sydney, NSW 2000
Australia

CLAYTON UTZ

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