

THE FINANCIAL  
TECHNOLOGY  
LAW REVIEW

THIRD EDITION

Editor  
Thomas A Frick

THE LAWREVIEWS

THE FINANCIAL  
TECHNOLOGY  
LAW REVIEW

THIRD EDITION

Reproduced with permission from Law Business Research Ltd  
This article was first published in May 2020  
For further information please contact [Nick.Barette@thelawreviews.co.uk](mailto:Nick.Barette@thelawreviews.co.uk)

**Editor**  
Thomas A Frick

THE LAWREVIEWS

PUBLISHER

Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER

Nick Barette

BUSINESS DEVELOPMENT MANAGER

Joel Woods

SENIOR ACCOUNT MANAGERS

Pere Aspinall, Jack Bagnall

ACCOUNT MANAGERS

Olivia Budd, Katie Hodgetts, Reece Whelan

PRODUCT MARKETING EXECUTIVE

Rebecca Mogridge

RESEARCH LEAD

Kieran Hansen

EDITORIAL COORDINATOR

Tommy Lawson

PRODUCTION AND OPERATIONS DIRECTOR

Adam Myers

PRODUCTION EDITOR

Anna Andreoli

SUBEDITOR

Sarah Andreoli

CHIEF EXECUTIVE OFFICER

Nick Brailey

Published in the United Kingdom  
by Law Business Research Ltd, London  
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK  
© 2020 Law Business Research Ltd  
[www.TheLawReviews.co.uk](http://www.TheLawReviews.co.uk)

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at April 2020, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above.

Enquiries concerning editorial content should be directed  
to the Publisher – [tom.barnes@lbresearch.com](mailto:tom.barnes@lbresearch.com)

ISBN 978-1-83862-453-8

Printed in Great Britain by  
Encompass Print Solutions, Derbyshire  
Tel: 0844 2480 112

# ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ALLEN & GLEDHILL LLP

BONELLIEREDE

BURGES SALMON LLP

BUZKO LEGAL

CMS REICH-ROHRWIG HAINZ RECHTSANWALTE GMBH

COLLAS CRILL

DLA PIPER UK LLP

GILBERT + TOBIN

HAMMAD AND AL-MEHDAR

HENRY YU & ASSOCIATES, IN ASSOCIATION WITH L & Y LAW OFFICE

HOGAN LOVELLS

HUNTON ANDREWS KURTH LLP

KIM & CHANG

LEE AND LI, ATTORNEYS-AT-LAW

LOYENS & LOEFF

MORI HAMADA & MATSUMOTO

NIEDERER KRAFT FREY

NOERR LLP

SK CHAMBERS

SRP-LEGAL

TOZZINIFREIRE ADVOGADOS

URÍA MENÉNDEZ

VIEIRA DE ALMEIDA

# CONTENTS

PREFACE.....	vii
<i>Thomas A Frick</i>	
Chapter 1	AUSTRALIA..... 1
<i>Peter Reeves</i>	
Chapter 2	AUSTRIA..... 15
<i>Stefan Paulmayer</i>	
Chapter 3	BELGIUM ..... 28
<i>Pierre E Berger and Marc Van de Looverbosch</i>	
Chapter 4	BRAZIL..... 42
<i>Alexei Bonamin, Marcela Waksman Ejnisman, Carla do Couto Hellu Battilana, Marcus Fonseca, Felipe Borges Lacerda Loiola, Natasha Wiedmann and Victor Cabral Fonseca</i>	
Chapter 5	BRITISH VIRGIN ISLANDS ..... 56
<i>Ian Montgomery</i>	
Chapter 6	CAYMAN ISLANDS ..... 63
<i>Alan de Saram, Natalie Bell, Aoife Madden, Laura Smalley and Dawn Major</i>	
Chapter 7	GERMANY..... 73
<i>Jens H Kunz</i>	
Chapter 8	GUERNSEY ..... 94
<i>Wayne Atkinson</i>	
Chapter 9	HONG KONG ..... 103
<i>Yu Pui Hang (Henry Yu)</i>	
Chapter 10	ITALY ..... 117
<i>Giuseppe Rumi, Federico Vezzani and Tommaso Faelli</i>	

## Contents

---

Chapter 11	JAPAN .....	134
	<i>Atsushi Okada, Takane Hori and Takahiro Iijima</i>	
Chapter 12	JERSEY.....	148
	<i>Dilmun Leach</i>	
Chapter 13	LUXEMBOURG.....	159
	<i>Anne-Marie Nicolas, Álvaro Garrido Mesa and Sandy Brumberg</i>	
Chapter 14	MALAYSIA .....	174
	<i>Shanthi Kandiah</i>	
Chapter 15	MEXICO .....	184
	<i>Federico de Noriega Olea and Juan Enrique Lizardi Becerra</i>	
Chapter 16	NETHERLANDS.....	194
	<i>Martijn Schoonewille, Wendy Pronk, Marije Louisse, Mariska Kool and Pepijn Pinkse</i>	
Chapter 17	PORTUGAL.....	205
	<i>Tiago Correia Moreira, Helena Correia Mendonça, Conceição Gamito, José Miguel Carracho and Francisca César Machado</i>	
Chapter 18	RUSSIA .....	220
	<i>Roman Buzko</i>	
Chapter 19	SAUDI ARABIA.....	230
	<i>Subaib Adli Hammad</i>	
Chapter 20	SINGAPORE.....	239
	<i>Adrian Ang V-Meng and Alexander Yap Wei-Ming</i>	
Chapter 21	SOUTH KOREA .....	247
	<i>Jung Min Lee, Joon Young Kim and Samuel Yim</i>	
Chapter 22	SPAIN.....	261
	<i>Leticia López-Lapuente and Isabel Aguilar Alonso</i>	
Chapter 23	SWITZERLAND .....	272
	<i>Thomas A Frick</i>	

## Contents

---

Chapter 24	TAIWAN.....	284
	<i>Abe T S Sung and Eddie Hsiung</i>	
Chapter 25	TURKEY.....	295
	<i>Cigdem Ayozyer Ongun, Filiz Piyal and Deniz Erkan</i>	
Chapter 26	UNITED KINGDOM.....	303
	<i>Gareth Malna and Sarah Kenshall</i>	
Chapter 27	UNITED STATES.....	315
	<i>Erin Fonte, Scott Kimpel, Carleton Goss, Brenna McGee and Patrick Boot</i>	
Appendix 1	ABOUT THE AUTHORS.....	333
Appendix 2	CONTRIBUTORS' CONTACT DETAILS.....	357

# PREFACE

This is already the third edition of *The Financial Technology Law Review*. If anything, concerns about certain aspects of the new developments that blockchain, Big Data and artificial intelligence (AI) trigger in the finance sector have increased since the first edition. In particular, developments such as the announcement of Facebook's Libra project or certain aspects of AI continue to worry regulators. However, the fact that certain high-profile projects receive critical attention should not obscure the fact that fintech has moved to become quite an established part of the financial ecosystem. Both financial market participants and their legal advisers already have considerable experience in implementing fintech projects by now. Not only are a significant number of start-ups presenting new fintech projects, but more and more established market participants such as banks, insurance companies and exchanges are setting up fintech labs and experiments, in part also implementing fintech projects and products.

After the initial hype, the number of active cryptocurrencies imitating Bitcoin and Ethereum have diminished considerably. Other developments continue, in particular, exploring the new ways of organising business that stablecoins and security tokens may offer. The use of Big Data and AI, closely interlinked, is starting to move from exploratory projects to the application stage. After the widespread scepticism that was referred to in the preface to the second edition of this book, market participants are again starting to see the opportunities these new technologies offer, even if not all projects will lead to a disruption of the industry. A new realism and a greater awareness of the opportunities and risks involved seem to have arrived. It may be that the current corona-virus crisis will even encourage this development, as many enterprises are in the process of furthering the digitalisation of their business.

Though the regulators' initial surprise about the sheer dynamism of these projects has ebbed, there are numerous initiatives both on the national and on the international level to provide sandboxes for fintech start-ups and to regulate fintech. Implementation of an effective anti-money laundering system continues to concern not only the regulators, but also banks and other financial market participants. Unless the industry can be certain that participating in the crypto-economy will not lead to increased anti-money laundering risks, established financial players remain cautious. However, even the Bank for International Settlement, after highly critical initial statements, initiated a discussion paper on designing prudential treatment for cryptoassets in December 2019, and the FATF published guidance on virtual assets in June 2019.

The national solutions chosen vary considerably between jurisdictions, not only owing to different regulatory cultures, but also to differences in the treatment under contract and tort law of some of the new issues arising. In the absence of a harmonised international regime, the structured collection of overviews on certain aspects of fintech law and regulation



this book continues to be valuable not only for the international practitioner, but also for anyone looking for inspiration on how to deal with hitherto unaddressed and unthought-of issues under the national law of any country.

The authors of this publication are from the most widely respected law firms in their jurisdictions. They each have a proven record of experience in the field of fintech; they know both the law and how it is applied. We hope that you will find their experience invaluable and enlightening when dealing with the varied issues fintech raises in the legal and regulatory field.

The emphasis of this book is on the law and practice of each of the jurisdictions, but discussion of emerging or unsettled issues has been provided where appropriate. The views expressed are those of the authors and not of their firms, nor of the editor or the publisher. In a fast-changing environment, every effort has been made to provide the latest intelligence on the current status of the law.

**Thomas A Frick**

Niederer Kraft Frey

Zurich

March 2020

# AUSTRALIA

*Peter Reeves*<sup>1</sup>

## I OVERVIEW

The Australian financial services sector has continued to give significant attention to the fintech industry, with a range of regulatory and legislative developments facilitating innovations and new businesses entering the market. Australian regulators and policy-makers have sought to improve their understanding of, and engagement with, fintech businesses by regularly consulting with industry on proposed regulatory changes and entering into international cooperation and information sharing agreements.

Australian regulators have been receptive to supporting the entrance of fintechs, streamlining access and offering informal guidance to enhance regulatory understanding. Both the Australian Securities and Investments Commission (ASIC) and the Australian Transaction Reports and Analysis Centre (AUSTRAC) have established innovation hubs to assist start-ups in navigating the Australian regulatory regime. AUSTRAC's Fintel Alliance also has an innovation hub targeted at combating money laundering and terrorism financing, and improving the fintech sector's relationship with government and regulators.

ASIC has entered into a number of cooperation agreements with overseas regulators that aim to further understand the approach of fintech businesses in other jurisdictions, in an attempt to better align the treatment of these businesses across jurisdictions. These cross-border agreements facilitate the referral and sharing of information on fintech market trends, encourage referrals of fintech companies and share insights from proofs of concepts and innovation competitions. A number of these agreements aim to further understand the approach to regulation of fintech businesses in other jurisdictions in an attempt to better align the treatment of these businesses across jurisdictions. ASIC has committed to supporting financial innovation in the interests of consumers by joining the Global Financial Innovation Network, which launched in January 2019 and currently has 50 member organisations.

In December 2016, ASIC made certain class orders establishing a fintech licensing exemption and released regulatory guidance detailing its regulatory sandbox for fintech businesses to test certain financial services, financial products and credit activities without holding an Australian financial services licence (AFSL) or Australian credit licence (ACL). There are strict eligibility requirements for both the type of businesses that can enter the regulatory sandbox and the products and services that qualify for the licensing exemption. Once a fintech business accesses the regulatory sandbox, there are restrictions on how many persons can be provided with a financial product or service and caps on the value of the financial products or services that can be provided.

---

<sup>1</sup> Peter Reeves is a partner at Gilbert + Tobin.

Investments in fintechs can, among other structures, be made through Australian incorporated limited partnerships called ‘early-stage venture capital limited partnerships’ and ‘venture capital limited partnerships’. Such investments may receive favourable tax treatment. Depending on the investment vehicle, benefits can include tax exemptions for resident and non-resident investors on revenue and capital gains on a disposal of the investment, plus a 10 per cent non-refundable tax offset available for new capital invested and the carried interest of fund managers being treated on capital account.

A programme known as the R&D Tax Incentive is available for entities incurring eligible expenditure on R&D activities, which includes certain software R&D activities commonly conducted by fintechs. Claimants under the R&D Tax Incentive may be eligible for one of the following incentives:

- a* small businesses (less than A\$20 million aggregated turnover) not controlled by exempt entities: a 43.5 per cent refundable tax offset; and
- b* other businesses (over A\$20 million aggregated turnover or controlled by exempt entities): a 38.5 per cent non-refundable tax offset for eligible expenditure below A\$100 million and 30 per cent for eligible expenditure over A\$100 million.

Significant changes to the R&D Tax Incentive are expected subject to the passing of the Treasury Laws Amendment (Research and Development Tax Incentive) Bill 2019. Among the changes is the introduction of an ‘incremental intensity threshold’ which increases or decreases a business’ non-refundable tax offset based on how much the company spends on R&D. These changes are expected to apply retrospectively to income years commencing on or after 1 July 2019.

## II REGULATION

### i Licensing and marketing

#### *Licensing and marketing*

In Australia, the regulatory framework applicable to fintech companies broadly includes banking regulation, financial services licensing, consumer credit licensing, registration and disclosure requirements, consumer law obligations, data and privacy regulation, payment regulation and anti-money laundering and counter-terrorism financing requirements.

Fintech businesses carrying on a financial services business in Australia must hold an AFSL or be exempt from the requirement to be licensed. The Corporations Act 2001 (Cth) (the Corporations Act), which is administered by ASIC, broadly defines a financial service to include the provision of financial product advice, dealing in financial products (as principal or agent), making a market for financial products, operating registered schemes and providing custodial or depository services. A financial product is a facility through which, or through the acquisition of which, a person makes a financial investment, manages a financial risk or makes a non-cash payment (NCP).

These definitions are broad and will generally capture any deposit taking business, investment or wealth management business, payment service (e.g., NCP), advisory business (including robo-advice), trading platform, crowdfunding platform and other fintech offerings. Certain financial product advice will also require an AFSL, including the provision of automated digital advice so long as it can reasonably be regarded as intending to influence a client to make decisions in relation to financial products or services.

The ACL regime applies to fintechs who engage in consumer credit activities in Australia, for example, providing credit under a credit contract or consumer lease. Any person engaging in consumer credit activities must hold an ACL, or otherwise be exempt from the requirement. Consumer credit activity is regulated by ASIC under the National Consumer Credit Protection Act 2009 (Cth) (the National Credit Act) and associated regulations. In addition to holding an AFSL, fintechs that provide marketplace lending products and related services, such as peer-to-peer lending and crowd-lending platforms, will generally constitute consumer credit activities and trigger the requirement to hold an ACL.

The provision of credit information services in Australia is subject to the Privacy Act 1988 (Cth) (the Privacy Act), which provides that only credit reporting agencies (i.e., corporations carrying on a credit-reporting business) are authorised to collect personal information, collate it in credit information files and disclose it to credit providers. Credit reporting agencies must comply with obligations with regard to use, collection and disclosure of credit information.

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

Most financial services businesses will have obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (the AML/CTF Act) and Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (the AML/CTF Rules). Anti-money laundering and counter-terrorism financing (AML/CTF) laws apply to entities that provide 'designated services' with an Australian connection. Generally, the AML/CTF Act applies to any entity that engages in financial services, remittance or credit (consumer or business) activities in Australia. In 2018, the AML/CTF Act was amended to capture entities that provide digital currency exchange services. Obligations include enrolment (and, in some circumstances, registration) with AUSTRAC, conducting customer due diligence prior to providing any designated services and adopting and maintaining an AML/CTF programme.

Any entity that conducts any 'banking business', such as taking deposits (other than as partial payment for identified goods or services) or making advances of money, or provides a purchased payment facility, must be licensed as an authorised deposit-taking institution (ADI). The Australian Prudential Regulation Authority (APRA) is responsible for the authorisation process and granting of ADI licences (as well as ongoing prudential supervision). In 2018, APRA released the restricted ADI framework, which is designed to assist new businesses wishing to enter the banking industry. Under this regime, entities can conduct a limited range of business activities for two years while they build their capabilities and resources. After such time, they must either transition to a full ADI licence and operate without restriction, or exit the industry. As of January 2020, there is one restricted ADI on APRA's register but several restricted ADIs have transitioned to holding full ADI status since 2018. Being an ADI allows such entities to operate as ADIs without restrictions under the Banking Act 1959 (Cth) (Banking Act).

Cloud computing is permitted for financial services companies. From a risk and compliance perspective, the same requirements, tests and expectations apply to cloud computing as would apply to other areas of a financial services business. ASIC has released

regulatory guidance indicating its expectations for licensees' cloud computing security arrangements as well as frameworks that identify relevant compliance measures that should be put in place.

Marketing financial services may itself constitute a financial service requiring an AFSL. If financial services will be provided to retail clients, a financial services guide must first be provided, setting out prescribed information, including the provider's fee structure, to assist a client to decide whether to obtain financial services from the provider. Retail clients wishing to buy a financial product must receive a disclosure document in the form of a product disclosure statement (PDS), which must contain sufficient information such that the retail client can make an informed decision about their purchase. Broadly, a PDS must contain the risks and benefits of acquiring the financial product, the significant characteristics of the financial product and the fees payable in respect of the financial product.

Fintech businesses are also subject to the Australian Consumer Law, which is administered by the Australian Competition and Consumer Commission (ACCC). Broadly, this includes prohibitions on misleading and deceptive conduct, false or misleading representations, unconscionable conduct and unfair contract terms. While the Australian Consumer Law does not apply to financial products or services, many of these protections are enforced by ASIC, either through mirrored provisions in the Australian Securities and Investments Commission Act 2001 (Cth) (the ASIC Act) or through delegated powers.

## **ii Cross-border issues**

### ***Passporting***

It has been common in Australia for foreign financial services providers (FFSPs) to provide financial services to wholesale clients by relying on ASIC's 'passport' exemption from the requirement to hold an AFSL. Before providing financial services, FFSPs must disclose to clients that they are exempt from holding an AFSL and that they are regulated and authorised to provide those financial services by the laws of a foreign jurisdiction.

FFSPs that are currently provided with passport relief through class orders in Australia include the United Kingdom, the United States Securities and Exchange Commission, Commodity Futures Trading Commission, Federal Reserve and Office of the Comptroller of the Currency-regulated financial services providers, the Singapore Monetary Authority of Singapore, the Hong Kong Securities and Futures Commission, the German BaFin and Luxembourg regulated financial service providers.

However, ASIC has announced that it will be proceeding with a proposal to repeal the passport and limited connection relief outlined above and will implement a new regime that will require FFSPs to apply for a foreign AFSL (i.e., a modified form of an AFSL for FFSPs). Passport relief will cease to be available from 31 March 2020. FFSPs relying on passport relief will have 24 months (until 31 March 2022) to transition to a foreign AFSL or satisfy licensing requirements in some other way. FFSPs relying on limited connection relief will have until 30 September 2020 to transition to a foreign AFSL or satisfy licensing requirements in an other way.

In June 2018, the Australian government passed the Corporations Amendment (Asia Region Funds Passport) Act 2018 (Cth), which incorporates the Asia Region Funds Passport (Passport) into the Corporations Act. The Passport is a region-wide initiative to facilitate the offer of interests in certain collective investment schemes established in Passport member economies to investors in other Passport member economies. It aims to provide Australian fund managers with greater access to economies in the Asia-Pacific by reducing

existing regulatory hurdles. Australia, Japan, Korea, New Zealand and Thailand are all signatories to the Passport's Memorandum of Cooperation. Following its official launch on 1 February 2019, the Passport now has the first application for registration as a passport fund under review with the New Zealand Financial Markets Authority. Japan, Thailand and Australia are also available to receive registration applications from local prospective funds and entry applications from foreign Passport funds.

The Australian Treasury has also completed three tranches of consultation in relation to the Corporate Collective Investment Vehicle scheme (CCIV). The CCIV will be a new type of investment vehicle that aims to expand the range of collective investment schemes offered in Australia and will enhance the competitiveness of funds by improving access to overseas markets. The CCIV regime is intended to complement the Passport, which will allow Australian fund managers to pursue overseas investment opportunities through a company structure. The CCIV will be implemented through the Treasury Laws Amendment (Collective Investment Vehicle) Bill 2017 and an additional Bill to enact amendments to other legislation, including the Corporations Act.

Although there are concerns that the reforms will add extra complexity to existing corporate, partnership and tax laws, the enactment of the Passport and the CCIV has the potential to open significant financing opportunities for fintech businesses.

### ***Australian presence***

Foreign companies, including fintechs, wishing to access Australian customers must overcome a number of regulatory hurdles. These include registering with ASIC in order to carry on a business in Australia which is generally satisfied by either establishing a local presence (i.e., registering a branch office) or incorporating an Australian subsidiary. Generally, the greater the level of system, repetition or continuity associated with an entity's business activities in Australia, the greater the likelihood registration will be required.

### ***Marketing foreign financial services***

Generally, an offshore provider can address requests for information, pitch and issue products to an Australian customer if the customer makes the first approach (i.e., there has been no conduct designed to induce the investor, or that could have been taken to have that effect) and the service is provided from outside Australia.

If the unsolicited approach relates to credit activities that are regulated under the National Credit Act, the provider is required to hold an ACL irrespective of the unsolicited approach.

### ***Foreign exchange and currency-control restrictions***

Australia does not have foreign exchange or currency-control restrictions on the flow of currency into or out of the country. However, there are cash-reporting obligations to AUSTRAC. To control tax evasion, money laundering and organised crime, AUSTRAC must receive reports of transfers of A\$10,000 or more (or the foreign currency equivalent) and reports of suspicious transactions from reporting entities such as banks, building societies and credit unions. Unless an exemption applies, reporting entities must also submit an AML/CTF compliance report to AUSTRAC, which collects information about the appropriateness of a reporting entity's money laundering and terrorism financing risk assessments and of its AML/CTF compliance programme.

### **III DIGITAL IDENTITY AND ONBOARDING**

There is no generally recognised digital identity in Australia. However, following a request for information from the industry on its alpha design phase, the Australian federal government's Digital Transformation Agency (DTA) is currently in the beta stage of developing a centralised digital identity platform. The national overarching digital identity technology called 'GovPass' is divided into four components; the Trusted Digital Identity Framework (TDIF), the exchange gateway, the digital identity services and the services providers. The TDIF governs the platform Govpass and allows people to choose their identity provider and access a range of government services, with an opportunity for future integration with the private sector.

Currently, the GovPass digital identity has only been used for a limited number of government services. However, this is set to change in March 2020 with the Australian government's identity provider, 'myGovID', set to replace AUSKey, a secure login that identifies individuals using participating government services on behalf of a business.

There is also another digital identity service in use in Australia called 'Digital iD', which was launched in mid-2017 by Australia Post. The smartphone-based platform is being used by Australia Post and certain early adopter organisations. The DTA has partnered with Australia Post to work towards the incorporation of Australia Post's Digital iD as one of the identity providers under the broader GovPass project.

Financial services providers are able to carry out fully digitised onboarding of clients, subject to know your customer (KYC) and AML/CTF obligations being complied with. Under the AML/CTF Rules, electronic verification of client information and data may be undertaken with or without hard-copy documentation. Financial services providers may use safe harbour documentation-based or electronic-based procedures to verify individuals where the reporting entity determines that the relationship with the customer is of medium or lower money laundering or terrorism risk.

Entities required to report to AUSTRAC who want to use electronic verification must verify the client's name and residential address using reliable and independent electronic data from at least two separate data sources and either the client's date of birth or residential address, or the client's transaction history for at least the past three years. Financial services providers must also receive express and informed client consent to use electronic verification. Reporting entities are required to retain information about verification requests and assessments for the life of the client relationship and for seven years from the date of the request after ceasing to provide the designated services to a client.

### **IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING**

#### **i Digital marketplaces and cryptoassets**

At the time of writing, there are no special rules in Australia that have been implemented to specifically regulate digital markets or cryptoassets. Generally, cryptoassets are regulated under existing regulatory frameworks. If a digital marketplace deals in cryptoassets that are financial products, then the platform is operating a market and a range of Australian laws apply, including the requirement to hold an Australian market licence and an AFSL. See Section II for further detail.

## **ii Collective investment schemes**

Collective investment schemes in Australia are generally referred to as managed investment schemes, which can be contract-based schemes, unincorporated vehicles (typically structured as unit trusts or unincorporated limited partnerships) or bodies corporate (which are incorporated and typically structured as companies or incorporated limited partnerships).

Depending on the structure, a platform or scheme operated by a fintech company may fall within the scope of the Australian collective investment scheme regulations. They may also be subject to AFSL, ACL, consumer law and financial services laws relating to consumer protection under the ASIC Act.

## **iii Crowdfunding**

In September 2017, a regulatory framework was introduced for crowd-sourced equity funding (CSF) by public companies from retail investors. The CSF regime enables companies to raise funds from large pools of investors by utilising a licensed CSF platform instead of listing on a stock exchange. While the regime reduces the regulatory barriers to investing in small and start-up businesses, the framework also created certain licensing and disclosure obligations for CSF intermediaries (i.e., persons listing CSF offers for public companies). ASIC has released Regulatory Guides 261 and 262 to assist companies seeking to raise funds through CSF and intermediaries seeking to provide CSF services, respectively.

The government passed the Corporations Amendment (Crowd-sourced Funding for Proprietary Companies) Bill 2017 (Cth), extending the CSF regime to proprietary companies. While there are a range of reporting requirements imposed on proprietary companies engaging in crowdfunding, there are also a number of concessions made with respect to restrictions that would otherwise apply to their fundraising activities.

Notably, the government has previously indicated its intention to consult on the extension of the existing CSF regime to debt funding. Although debt financing is less common than equity raising for fintech businesses in Australia, businesses can approach institutions, suppliers and finance companies in relation to debt finance.

## **iv Marketplace lending**

Providers of marketplace lending products, including those peer-to-peer lending services, are generally structured such that they need to hold an AFSL and comply with the relevant requirements outlined in the Corporations Act including appropriate disclosure and resourcing requirements.

Where the loans are consumer loans (e.g., loans to individuals for domestic, personal or household purposes), the provider will also need to hold an ACL and comply with requirements in the National Credit Act and the National Credit Code. Similarly, all loans (including loans for a business purpose that are not regulated under the National Credit Act) are subject to consumer protections provisions in the ASIC Act, including prohibitions on misleading or deceptive representations. Peer-to-peer lenders are sometimes structured as managed investment schemes, which must be registered with ASIC if the investment is offered to retail investors.

There are generally no restrictions on secondary markets for trading loans; however, such activities may trigger licensing obligations for the provider of the market, market maker and market participants.



**v Payment services**

Payment services may be regulated as financial services because this concept captures services relating to deposit-taking facilities made available by an ADI in the course of carrying on a banking business or a facility through which a person makes a NCP.

If an entity facilitates an NCP, the service provider must hold an AFSL or be exempt from the requirement to do so. ASIC has outlined a number of exceptions including general exemptions in relation to specific NCP products such as gift vouchers and loyalty schemes.

As discussed in Section II, any entity that conducts banking business must also be licensed as an ADI.

**vi Data sharing**

In Australia there is no requirement to make client data accessible to third parties; however, this is often necessary for lenders and credit reporting agencies who must comply with obligations with regard to use, collection and disclosure of credit information (see Section II).

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

In Australia significant changes are proposed in relation to how customer data is shared with third parties across every sector of the Australian economy. In 2018, the Notifiable Data Breaches (NDB) scheme was introduced requiring entities regulated under the Privacy Act to notify any affected individuals and the Office of the Australian Information Commissioner in the event of a data breach (i.e., the unauthorised access to or disclosure of information) that is likely to result in serious harm to those individuals. The NDB scheme applies to agencies and organisations that the Privacy Act requires to take steps to secure certain categories of personal information.

The Australian government will be implementing the national consumer data right (CDR) framework, which will give customers a right to share their data with accredited services providers (including banks, comparison services, fintechs or third parties). The CDR framework will first be applied to the banking sector under the Open Banking regime by which consumers can exercise greater access and control over their banking data. In September 2019, 10 companies were selected to participate in a trial, with the Open Banking regime slated to formally commence in July 2020.

The European Union (EU) General Data Protection Regulation also has a broad extraterritorial reach and may significantly impact the data handling practices of data for Australian businesses providing goods and services in the EU.

**V CRYPTOCURRENCIES, INITIAL COIN OFFERINGS (ICO) AND SECURITY TOKENS**

**i Blockchain**

There are currently no specific regulations dealing with blockchain technology in Australia. However, in March 2017, ASIC released guidance outlining its approach to the regulatory issues that may arise through the implementation of blockchain technology and distributed ledger technology (DLT) solutions in fintech businesses more generally. ASIC reaffirmed their ‘technology neutral’ stance in applying the financial services regime and the notion that businesses considering operating market infrastructure or providing financial or consumer credit services using DLT will still be subject to the compliance requirements that currently exist under the applicable regulation.

## **ii Cryptocurrencies**

In May 2018, ASIC updated its guidance on initial coin offerings (ICOs) to include clarification on the corporate and consumer law consequences that may arise in an ICO context, including the prohibition on misleading and deceptive conduct. While tokens may be offered to Australian residents from abroad, token offerors should note that the Australian Consumer Law on misleading and deceptive conduct will still apply.

ASIC's regulatory guidance informs businesses of their approach to the legal status of coins or tokens offered through ICOs in Australia. The legal status of such coins is dependent on how the ICO is structured and the rights attached to the coins. Depending on the circumstances, ICOs may be considered to be managed investment schemes, an offer of securities, an offer of derivatives or fall into a category of more generally defined financial products all of which are sometimes referred to as an STO or security token offering. In these instances, entities offering such coins will need to comply with financial services regulatory requirements under the Corporations Act. An entity that facilitates payments by cryptocurrencies may also be required to hold an AFSL. If an ICO constitutes an offer of financial products, this will impact the marketing of the ICO and its disclosure obligations. Cryptocurrencies are also subject to the general consumer protection provisions, prohibiting false or misleading representations and unconscionable conduct.

Under the AML/CTF Act, the Australian government has brought cryptocurrencies and tokens within the scope of Australia's anti-money laundering regime. The regime is focused on the point of intersection between cryptocurrencies and the regulated financial sector, namely digital currency exchanges, and came into force on 3 April 2018. Digital currency exchange providers are required to register with AUSTRAC in order to operate. Registered exchanges are required to implement KYC processes to adequately verify the identity of their customers, with ongoing obligations to monitor and report suspicious and large transactions. Exchanges are required to keep certain records relating to customer identification and transactions for up to seven years. Operating a registrable digital currency exchange service without registering with AUSTRAC is an offence carrying a penalty of up to two years' imprisonment or a fine of up to A\$105,000, or both.

For income tax purposes, the Australian Taxation Office (ATO) currently views cryptocurrencies as neither money nor a foreign currency. Instead, each cryptocurrency is treated as a separate capital gains tax (CGT) asset. This means that gains made on the disposal of a cryptocurrency may be subject to income tax. In some instances where a cryptocurrency is held as an investment for at least 12 months, taxpayers may be entitled to a CGT discount to reduce the capital gain made on the disposal of the cryptocurrency. Also, certain capital gains or losses may be disregarded where there is a disposal of a cryptocurrency that is a personal use asset (i.e., an asset kept or used mainly to purchase items for personal use or consumption). The ATO's views on the income tax implications of transactions involving cryptocurrencies is in a state of flux due to the rapid evolution of both cryptocurrency technology and its application.

Effective from 1 July 2017, the Australian government amended the goods and services tax (GST) Act to the effect that the sale, including ICOs, or purchase of cryptocurrencies (namely those fulfilling the requirements for 'digital currencies' in the GST Act, such as Bitcoin, Ethereum, Litecoin, Dash, Monero, ZCash, Ripple and YbCoin) is not subject to GST. Instead, these sales and purchases will be input taxed such that no GST will be payable but entities registered for GST may be restricted from claiming input tax credits on the costs associated with the sale or purchase of cryptocurrencies. No GST will be payable

if the cryptocurrency is acquired by a non-resident for its overseas business because this will be a GST-free supply. The GST treatment is different still for businesses that receive cryptocurrency in return for their goods and services – in these circumstances, they will be subject to the normal GST rules. In other words, where taxable supplies of goods and services are made by businesses for which cryptocurrency is received as payment, GST will be imposed at the usual rate of 10 per cent on the taxable supply. This is because cryptocurrency is treated as a method of payment and the GST consequences of using it as payment are the same as the GST consequences of using money as payment.

### **iii Security tokens**

As discussed in Section II, if a token falls within the definition of a financial product, the Australian laws relating to financial products will apply. Regardless of whether a token constitutes a financial product, ICOs and security token offerings will be subject to Australian consumer law restrictions and AML/CTF reporting requirements. There have been significant technological developments and sandbox experiments digitising security interests in a blockchain environment, but no corresponding legal reform to facilitate issuing or transferring legal title to such products on-chain. The numerous small-scale Australian and offshore blockchain-based bond issuances to date only mirror off-chain transactions on an on-chain ledger and do not provide for dealings in legal title or an on-chain payment rail that are impediments to widespread adoption.

## **VI OTHER NEW BUSINESS MODELS**

### **i Smart contracts**

Self-executing contracts or ‘smart contracts’ are permitted in Australia under the Electronic Transactions Act 1999 (Cth) (ETA) and the equivalent Australian state and territory legislation. The ETA provides a legal framework to enable electronic commerce to operate in the same way as paper-based transactions. Under the ETA, self-executing transactions are permitted in Australia, provided they meet all traditional elements of a legal contract: intention to create legally binding obligations, offer and acceptance, certainty and consideration.

Any attempt at an analysis of correction mechanisms, such as arbitration and mediation, in regard to this type of contract is challenging because there is little case law on smart contracts in Australia. Self-executing contracts may alter traditional dispute resolution in Australia based on the possibility of self-executing dispute resolution through online dispute resolution platforms.

### **ii Automated investments**

Generally, fully automated investments are permitted in Australia on the condition that the automated service provider holds an AFSL, or is an authorised representative of a holder of an AFSL, with the requisite managed discretionary account (MDA) authorisation. Automated services providers and their retail clients are required to enter into individual MDA contracts to engage in this process. An MDA contract allows trades to be completed on a client’s behalf and includes the ability to automatically adjust the asset allocation of a client’s portfolio, without prior reference to the client for each individual transaction. Automated investment service providers must also comply with certain conduct and disclosure obligations applicable to providing the automated financial product service.

### **iii Artificial intelligence**

At the time of writing, in Australia there are no special laws applicable to the use of artificial intelligence and machine learning. However, other general data protections including the Privacy Act and the NDB regime will apply. See Section IV(vi) for more detail.

### **iv Third-party websites**

Third-party comparison websites that allow consumers to compare quotes on financial products must ensure they are providing accurate information and not misleading consumers, and may need to be licensed or be an authorised representative of an AFSL holder. ASIC has released guidance for operators of comparison websites, noting that generally operators should clearly disclose the basis of awards or ratings, disclose any links to the providers of products being compared including a warning if not all providers are being compared, clearly disclose advertisements and, where necessary, include a warning that the financial products compared do not compare all features that may be relevant for the consumer.

The ACCC, as Australia's competition and consumer law regulator, also has jurisdiction over comparison websites. The ACCC is primarily concerned with the way in which comparison websites drive competition and help consumers make informed decisions. Comparable to ASIC, the ACCC sets out guidance on how third-party comparison websites can facilitate honest comparisons of financial products and services, disclose commercial relationships between comparisons and financial product providers, and provide full disclosure of the financial products and providers that are being compared.

### **v Other new business models**

In January 2019, the first Restricted ADI licensee was granted a full ADI licence allowing it to operate as an ADI without restrictions under the Banking Act. The licensee is a 'neobank', which is a wholly digital bank that intends to provide full banking services to customers via a solely mobile-based platform. The Restricted ADI licence which launched in 2018, is designed to assist new businesses to enter the banking industry and overcome the significant regulatory challenges faced when entering the market. There has been an increase in the number of digital-only banks and consumer support for the same, with two new neobanks launched in Australia and another neobank with an approved banking licence that is yet to be launched to the public.

There has also been a steady increase in the establishment of NCP platforms and solutions aimed at maximising cost and time efficiencies and improving customer experience. The New Payments Platform (NPP) was launched in Australia in February 2018 as the result of industry-wide collaboration between Australia's largest banks and financial institutions as well as Australia's central bank, the Reserve Bank of Australia. Over time, the NPP is expected to replace a significant portion of direct payments between consumers' bank accounts, particularly those that are time-critical or benefit from additional data capabilities.

Australia has also seen a proliferation in the use of blockchain technology and a growth of interest in the use of DLT by established businesses. Fintech businesses are gradually moving beyond the concept stage to formalising actual use cases in areas of managing supply chains, trading derivatives, managing and issuing assets, making cross-border payments and digital currency exchanges. The Australian Securities Exchange (ASX) is continuing with its plan to replace its core clearing and settlement process with a blockchain-based system. The ASX is currently in its consultation and development phase and has set a target go-live date of April 2021.

There have also been a number of private sector projects that have used blockchain to deliver services to consumers. Three of Australia's four major banks have partnered with IBM and Scentre Group to establish an eight-week trial managing bank guarantees for retail property leases on blockchain, reducing the issuance period for a bank guarantee from up to a month to approximately the same day.

## **VII INTELLECTUAL PROPERTY AND DATA PROTECTION**

The most appropriate forms of intellectual property (IP) protection in Australia for fintech business models and related software are patent and copyright.

Patent protection is available for certain types of innovations and inventions in Australia. A standard patent provides long-term protection and control over an invention, lasting for up to 20 years from the filing date. The requirements for a standard patent include the invention being new, involving an inventive step and being able to be made or used in an industry. An innovation patent is targeted at inventions that take an innovative step and have short market lives, lasting up to eight years.

Business schemes and plans are not patentable, nor are abstract business models that happen to involve a new type of corporate structuring to bring about a certain result. However, there are some business methods that are patentable. In order to be patentable, the business method must directly involve a physical device that is used to bring about a useful product. If the method involves the application of technology, the technological aspect must be substantial and a useful product. Related software may only receive patent protection if it meets the requirement for a manner of manufacture, and is an industrially applicable solution to a technological problem.

Fintech businesses may attain copyright protection for the literacy work in source code, executable code and data sets of new software. This usually protects the exact code that causes a computer to bring about a certain result; however, whether this can be extended to the look and feel of the software is debatable.

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

Under the Copyright Act 1968 (Cth), creators of copyright works such as literacy works (including software) also retain moral rights in the work (for example, the right to be named as author). Moral rights cannot be assigned but creators can consent to actions that would otherwise amount to an infringement.

### **i Client data**

See Section IV(vi) for further detail on client data and data sharing.

## VIII YEAR IN REVIEW

In 2018, the Australian government launched the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (the Royal Commission), which revealed findings of industry-wide misconduct and systemic problems in the operation and processes of Australian organisations and regulators. On 4 February 2019, the Royal Commission made available its Final Report, containing 76 recommendations calling for reforms across banking, superannuation, financial advice and rural lending industries.

Its findings have brought into focus the culture and governance of financial services providers and prompted industry change to prioritise the interests of consumers (and not providers) in the provision of financial services and to address the marked decreased in consumer trust, with 42 per cent of customers acknowledging that trust in banks had deteriorated significantly over the past year. Corporate regulators were also criticised during the Royal Commission for their enforcement practices regarding inaction against corporate misconduct and breaches of the law. Both the Interim Report and Final Report of the Royal Commission commented on the lack of action in response to industry misconduct, noting that conduct was often unpunished or met with penalties that were insufficiently strict. With respect to the two regulators, ASIC rarely took providers to court, and APRA never went to court at all. Given this criticism, it is likely that these regulators will increase their enforcement action in the future and be firmer and more proactive in their responses to misconduct or breaches, rather than reaching negotiated outcomes.

Following the conclusion of the Royal Commission, there has been increased investment in regulatory technology (regtech) and supervisory technology (suptech) by financial services businesses. In 2019, ASIC received government funding for four regtech initiatives to promote Australia as a world leader in developing and adopting regtech solutions to risk management and compliance problems relating to financial services. One initiative included the proof-of-concept chatbox, which is designed to assist businesses in navigating the credit and financial services licensing regulatory framework.

### **i Digital wallets**

The use of digital wallets in Australia has continued to grow. The Council of Financial Regulators (comprising Australia's major financial regulators) made recommendations to the Australian government for a new framework for stored-value facilities to be overseen by APRA. Stored-value facilities include digital wallets that are increasingly being used as a means of payment and store significant value for a reasonable period of time. The new framework is intended not only to be fit for purpose for the new current financial system but also be able to accommodate future developments and technological advances, such as proposals for global stablecoin ecosystems.

### **ii Asia Region Funds Passport regime**

See Section II(ii) for details of the Passport regime.

### **iii Design and distribution obligations and product intervention powers**

The Treasury Laws Amendment (Design and Distribution Obligations and Product Intervention Powers) Act 2019 (Cth) (the DDOPIP Act) introduces design and distribution obligations in relation to financial products as well as a product intervention power for

ASIC to prevent or respond to significant consumer detriment. The DDOPIP Act, with the exception of Schedule 1, came into effect on 6 April 2019. Schedule 1, which introduces the design and distribution obligations, will commence on 5 April 2021.

#### **iv Smart contracts**

Initially, smart contracts were predominantly used in the cryptocurrency sector in relation to ICOs to automatically mint and distribute tokens. However, in the past 18 months there has been an increase in the institutional adoption of smart contracts to digitise readily automatable processes. This has primarily occurred in the financial services sector with multiparty arrangements such as issuing bank guarantees or debt instruments through smart contracts. The most prominent example of this in Australia is ASX's proposed replacement of its clearing and settlement system with DLT (see Section VI(v)). Although there is yet to be a widely adopted framework for this, there has been a number of initiatives that aim to develop a framework for the standardisation and regulation of smart contracts such as the Australia's national science agency, CSIRO's Data61.

## **IX OUTLOOK AND CONCLUSIONS**

There has been a variety of regulatory and legislative developments in the fintech industry, and 2020 will likely see changes impacting consumers and businesses. With the outcomes of the Royal Commission and landmark announcements such as ASIC's decision not to extend licensing relief for FFSPs, the Passport regime and the commencement of Open Banking, fintech is likely to see continued opportunities for growth as the sector moves from speculation to development to implementation.

While the government has a broad commitment to encouraging growth and productivity within the technology and financial services industry, in recent times market regulators have become more focused on consumer education and issued warnings on the risk of trading and investing in new innovations, such as cryptocurrencies. Similarly, following the findings of the Royal Commission, we expect to see more rigorous engagement with ASIC and APRA in the licensing process and a firmer and more proactive approach to enforcement.

Fintechs and start-ups, which historically have emerged to provide consumer focused solutions (powered by technological capabilities) to traditional financial services, can shape new business models to meet increasing demand for bespoke offerings and tailored services, while established institutions continue to face the challenge of redesigning their existing technology platform, strategies and capabilities.

# ABOUT THE AUTHORS

## **PETER REEVES**

*Gilbert + Tobin*

Peter Reeves is a partner in Gilbert + Tobin's corporate advisory group and is an expert and market-leading practitioner in financial services regulation and funds management. He leads the financial services and fintech practices at G+T. Peter advises domestic and offshore corporates, financial institutions, funds, managers and other market participants in relation to establishing, structuring and operating financial services sector businesses in Australia. He also advises across a range of issues relevant to the fintech and digital sectors, including platform structuring and establishment, payment solutions, blockchain solutions and global cryptoasset strategies. *Chambers 2020* ranks Peter in Band 1 for fintech.

## **GILBERT + TOBIN**

Level 35, Tower Two  
International Towers Sydney  
200 Barangaroo Avenue, Barangaroo  
Sydney, NSW 2000  
Australia  
Tel: +61 2 9263 4000  
Fax: +61 2 9263 4111  
[www.gtlaw.com.au](http://www.gtlaw.com.au)



an LBR business

ISBN 978-1-83862-453-8