

THE FINANCIAL
TECHNOLOGY
LAW REVIEW

SECOND EDITION

Editor
Thomas A Frick

THE LAWREVIEWS

THE FINANCIAL
TECHNOLOGY
LAW REVIEW

SECOND EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in May 2019
For further information please contact 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

Gavin Jordan

HEAD OF PRODUCTION

Adam Myers

PRODUCTION EDITOR

Claire Ancell

SUBEDITOR

Gina Mete and Anne Borthwick

CHIEF EXECUTIVE OFFICER

Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK
© 2019 Law Business Research Ltd
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 is accurate as at April 2019, 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

ISBN 978-1-83862-022-6

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

ALLEN & OVERY LLP

BONELLIEREDE

BURGES SALMON LLP

BUZKO & PARTNERS

COLLAS CRILL

DLA PIPER UK LLP

GILBERT + TOBIN

HOGAN LOVELLS

KIM & CHANG

LEE AND LI, ATTORNEYS-AT-LAW

LOYENS & LOEFF

McAFEE

MORI HAMADA & MATSUMOTO

NIEDERER KRAFT FREY

NOERR LLP

SHEARMAN & STERLING

SK CHAMBERS

STADLER VÖLKEL RECHTSANWÄLTE GMBH

TOZZINIFREIRE ADVOGADOS

URÍA MENÉNDEZ

VIEIRA DE ALMEIDA

CONTENTS

PREFACE.....	vii
<i>Thomas A Frick</i>	
Chapter 1	IMPACT OF THE NEW INFOSEC AND EU PRIVACY REQUIREMENTS ON BANKS AND FINANCIAL INSTITUTIONS' USE OF CLOUD COMPUTING.... 1
<i>Roy Kamp and Noémie Weinbaum</i>	
Chapter 2	AUSTRALIA..... 12
<i>Peter Reeves</i>	
Chapter 3	AUSTRIA..... 26
<i>Oliver Völkel and Bryan Hollmann</i>	
Chapter 4	BELGIUM 35
<i>Pierre E Berger, Stéphanie Liebaert and Marc Van de Looverbosch</i>	
Chapter 5	BRAZIL..... 49
<i>Alexei Bonamin, Carla do Couto Hellu Battilana, Ivan Antonio Monteiro Marques, Maria Eugenia Geve de Moraes Lacerda, Thaís Helena Valente Teixeira Lima and Victor Cabral Fonseca</i>	
Chapter 6	BRITISH VIRGIN ISLANDS 59
<i>Stephen Adams</i>	
Chapter 7	CAYMAN ISLANDS 66
<i>Stephen Nelson</i>	
Chapter 8	FRANCE..... 75
<i>Eric Roturier</i>	
Chapter 9	GERMANY..... 85
<i>Jens H Kunz</i>	

Contents

Chapter 10	GUERNSEY	101
	<i>Wayne Atkinson</i>	
Chapter 11	ITALY	110
	<i>Giuseppe Rumi, Federico Vezzani and Tommaso Faelli</i>	
Chapter 12	JAPAN	125
	<i>Asushi Okada, Takane Hori and Takahiro Iijima</i>	
Chapter 13	JERSEY.....	138
	<i>Dilmun Leach</i>	
Chapter 14	KOREA	149
	<i>Jung Min Lee, Joon Young Kim and Samuel Yim</i>	
Chapter 15	LUXEMBOURG.....	163
	<i>Anne-Marie Nicolas, Álvaro Garrido Mesa, Konstantinos Georgiou and Sandy Brumberg</i>	
Chapter 16	MALAYSIA	177
	<i>Shanthy Kandiah</i>	
Chapter 17	MEXICO	188
	<i>Federico de Noriega Olea and Juan Enrique Lizardi Becerra</i>	
Chapter 18	NETHERLANDS.....	198
	<i>Martijn Schoonewille, Wendy Pronk, Marije Louisse, Mariska Kool and Pepijn Pinkse</i>	
Chapter 19	PORTUGAL.....	209
	<i>Tiago Correia Moreira, Helena Correia Mendonça, Conceição Gamito and José Miguel Carracho</i>	
Chapter 20	RUSSIA	220
	<i>Roman Buzko</i>	
Chapter 21	SINGAPORE.....	231
	<i>Adrian Ang V-Meng and Alexander Yap Wei-Ming</i>	
Chapter 22	SPAIN.....	239
	<i>Leticia López-Lapuente and Isabel Aguilar Alonso</i>	

Contents

Chapter 23	SWITZERLAND.....	250
	<i>Thomas A Frick</i>	
Chapter 24	TAIWAN.....	262
	<i>Abe T S Sung and Eddie Hsiung</i>	
Chapter 25	UNITED KINGDOM.....	271
	<i>Gareth Malna and Sarah Kenshall</i>	
Chapter 26	UNITED STATES.....	283
	<i>Jordan Altman and Reena Agrawal Sahni</i>	
Appendix 1	ABOUT THE AUTHORS.....	293
Appendix 2	CONTRIBUTORS' CONTACT DETAILS.....	311

PREFACE

This is already the second edition of *The Financial Technology Law Review*. Concerns about new developments that blockchain, big data and AI will trigger in the finance sector have not disappeared since the first edition. However, the use of IT in the finance sector is not new and many applications that would be labelled today as fintech are already quite old, at least by today's standards. Financial market participants and their legal advisers already have considerable experience in implementing such changes. As far as improved support products are concerned, the general rules of financial regulations can be applied quite easily to new developments.

Some of the recent developments may already have seen their peak, for example, the great number of cryptocurrencies imitating bitcoin. Others, in particular stablecoins and security tokens, but also robo-advisers and the use of big data, AI and other blockchain applications, may still be at an early stage. They may have the potential to disrupt the industry, at least in some of its sectors. Again, there has been more scepticism, not only in a recent report by the Bank for International Settlements but also in management consultant studies such as 'Blockchain's Occam problem', arguing that blockchain is a technology in search of a problem.

Regulators' surprise about the sheer dynamism of these advances – both the speed of the technical developments and the speed with which such new possibilities were implemented – has ebbed and a number of countries have started to draft (or have already implemented) new laws or changes to their current laws to address fintech issues. This is particularly the case in the area of anti-money laundering rules, a prime concern not only of regulators but also of 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.

The national solutions chosen (and the speed with which regulators are willing to react by providing guidelines to market participants) varies considerably between jurisdictions. This may be a consequence of different regulatory cultures, but in addition, the existing legal systems may pose varying and unplanned obstacles to the some of the new applications. It may, for example, be difficult to transfer rights on the blockchain if the national code prescribes that rights can only be assigned in writing. Therefore, a structured collection of overviews over certain aspects of fintech law and regulation such as the present one continues to be valuable not only for the international practitioner, but also for anyone who looks 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 any of the varied issues fintech raises in the legal and regulatory field.

The emphasis of this collection 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, of the editor or of 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

April 2019

AUSTRALIA

*Peter Reeves*¹

I OVERVIEW

In 2018, the Australian financial services sector 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 sharing of information on fintech market trends, encourage referrals of fintech companies and share insights from proofs of concepts and innovation competitions. ASIC has committed to supporting financial innovation in the interests of consumers by joining the Global Financial Innovation Network (GFIN), which launched in January 2019 and currently has 29 member organisations. GFIN is dedicated to facilitating regulatory collaboration in a cross-border context.

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. In December 2017, ASIC sought industry feedback on the fintech licensing exemption following Treasury consultation on draft legislation designed to enhance the existing exemption.

Investments in fintechs may be made through certain Australian incorporated limited partnerships. Such investments can receive favourable tax treatment. Depending on the

¹ Peter Reeves is a partner at Gilbert + Tobin.

investment vehicle chosen, 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.

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 were announced as part of the Federal Budget on 8 May 2018, such as the introduction of an ‘incremental intensity threshold’ proposed by the Treasury Laws Amendment (Making Sure Multinationals Pay Their Fair Share of Tax in Australia and Other Measures) Bill 2018 (Cth). In February 2019, the Federal government released guidelines to clarify the application of the R&D Tax Incentive.

II REGULATION

i Licensing and marketing

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 investment or wealth management business, payment service, advisory business, 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 particular financial product decisions.

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 to hold an ACL. 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 or be entitled to rely on an exemption.

In addition, 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 (e.g., an exchange). Additionally, 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). These 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 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 on customers prior to providing any designated services and adopting and maintaining an AML/CTF programme.

In 2018, the Australian Prudential Regulation Authority (APRA) released the restricted authorised deposit-taking (ADI) framework, which is designed to assist new businesses wishing to enter the banking industry. Under this regime, entities can seek a restricted ADI licence, allowing them to 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. See Section VI.iv for further detail.

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.

Marketing

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) or through delegated powers.

ii Cross-border issues

Passporting

Carrying on a financial services business in Australia will require a foreign financial service provider (FFSP) to hold an AFSL, unless relief is granted. As at the time of writing, Australia has cooperation (passporting) arrangements with regulators in foreign jurisdictions, which enable FFSPs regulated in those jurisdictions to provide financial services they are authorised to provide in their home jurisdiction to wholesale clients in Australia, without holding an AFSL. Before providing financial services, they must disclose to clients that they are exempt from holding an AFSL and that they are regulated 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.

ASIC has announced that it will be proceeding with a proposal to repeal the passport 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 30 September 2019. This is discussed further in Section VIII.

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. The Passport officially launched on 1 February 2019; however, as at the time of writing, Australia is the only participating economy to have passed laws to enable the Passport to operate.

In addition to the Passport, the Corporate Collective Investment Vehicle scheme (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. Public consultation on the third tranche of legislation closed on 26 October 2018 and two draft Bills implementing the CCIV regime were released for public consultation on 17 January 2019.

Australian presence

Foreign companies wishing to carry on business in Australia, including in fintech, must either establish a local presence (i.e., register with ASIC and create a branch) or incorporate 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. Generally, a company obtaining an AFSL will be carrying on a business in Australia and will trigger the requirement.

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 digital identity technology called 'GovPass' is intended to be used with government services with an opportunity for future integration with the private sector. A core component of the GovPass digital identity platform is the identity exchange. The identity exchange uses a double blind and acts as an intermediary between the government service and the identity provider. It ensures that personal information cannot be shared and ensures that the relying party receives an identity assurance that has been verified, without revealing the source of the assertion. In October 2018, the Australian government launched the first pilot of the GovPass digital identity platform, which enables Australians to opt in through a mobile application to apply for a tax file number.

At this stage in the testing of the platform, the extent to which a GovPass digital identity may be used for transactions beyond government services is unknown. The national identity system will be available to Australian residents who can produce their official identity documents, and is predicted to launch in mid-2019.

There is another digital identity service in use in Australia called 'Digital iD', which 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, working 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, conditional on 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 used in absence or together with 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, FUNDING AND PAYMENT SERVICES

i 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 Australian Securities and Investments Commission Act 2001 (Cth) (the ASIC Act).

ii 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.

In October 2018, the government passed the Corporations Amendment (Crowd-sourced Funding for Proprietary Companies) Bill 2017 (Cth), officially 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.

iii 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 generally 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 market for trading such loans or financings; however, such activities may trigger licensing obligations for the provider of the market, market maker and market participants.

iv Payment services

Payment services may be regulated as financial services, because this 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.

Any entity that conducts banking business, such as taking deposits (other than as part-payment for identified goods or services) or making advances of money, or provides a purchased payment facility, must be licensed as an ADI. APRA is responsible for the authorisation process and granting of ADI licences (as well as ongoing prudential supervision). Recently, APRA released the Restricted ADI framework, which is discussed in Section VIII.

v 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).

Currently, the Australian Privacy Principles (APP) dictate when APP entities may use or disclose personal information. They may do so where an individual could expect for the data to be shared or when an exception applies.

In Australia there has been significant change 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 scheme was introduced; this scheme mandates that entities regulated under the Privacy Act are required to notify any affected individuals and the Office of the Australian Information Commissioner in the event of a data breach (i.e., unauthorised access to or disclosure of information) that is likely to result in serious harm to those individuals.

Additionally, the Australian government announced that it 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. The Open Banking regime is slated to commence in February 2020.

V CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS

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 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 licences.

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 has long-arm jurisdiction and that the prohibition on misleading and deceptive conduct will 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. 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 relevant disclosure obligations. Additionally, cryptocurrencies are subject to the general consumer protection provisions, whereby providers must not make false or misleading representations or engage in 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. These amendments are 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 will be 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 will also be required to keep certain records relating to customer identification and transactions for up to seven years. The offence for operating a registrable digital currency exchange service without registering with AUSTRAC will carry 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 (such as bitcoin) as neither money nor a foreign currency. Under Australian income tax laws, gains made on the disposal of cryptocurrencies (including where cryptocurrencies are used as the payment for services or goods) contribute to the taxable income of a taxpayer. The ATO's views on the income tax implications of transactions involving cryptocurrencies is in a state of flux owing to the rapid evolution of both cryptocurrency technology and its uses.

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.

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 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.

iv 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 1959 (Cth). 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 term 'neobank' is largely a fluid construct, but generally, these entities will use an internet or mobile platform to interact with customers and offer a different user experience from a traditional bank. For example, the ability to make mobile deposits, person-to-person payments using email addresses or phone numbers, real-time digital notifications of receipts, no monthly fees, no automated teller machines fees and intuitive budgeting tools are typical characteristics of a neobank.

The Australian banking sector is highly regulated, with stringent licensing and reporting requirements. Consequently, neobanks face significant regulatory challenges entering the market. Under Australia's current regulatory framework, APRA prohibits ADIs, with less than A\$50 million in capital, from using the word 'bank'. In 2018, APRA released the Restricted ADI framework, which is designed to assist new businesses to enter the banking industry. Under this regime, entities can seek a Restricted ADI licence, allowing them to 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 or exit the industry.

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.

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

The Privacy Act regulates the handling of personal information by Federal government agencies and private sector organisations with an aggregate group revenue of at least A\$3 million. The Privacy Act includes 13 APPs, which create obligations on the collection, use, disclosure, retention and destruction of personal information.

In 2018, the Australian Government announced that 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. These sharing arrangements are intended to facilitate easier swapping of service providers, enhancement of customer experience based on personal and aggregated data, and more personalised offerings.

Additionally, the European Union (EU) General Data Protection Regulation has extremely broad extraterritorial reach and may significantly impact the data handling practices of Australian businesses offering goods and services in the EU.

VIII YEAR IN REVIEW

i Royal Commission

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. The Royal Commission's findings of misconduct have resulted in a marked decrease in consumer trust in both the traditional financial services industry generally and the institutional ability to prioritise customer needs, with 42 per cent of customers acknowledging that trust in banks had deteriorated significantly over the past year.

Traditional financial services providers were not the only targets of the Royal Commission with corporate regulators generating criticism 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. In keeping with its broader strategic change to strengthen its governance and culture, ASIC plans to implement all recommendations from the Royal Commission that were directed at ASIC and require no legislative change. Significantly for businesses, the Treasury Laws Amendment (Strengthening Corporate and Financial Sector Penalties) Act 2018 (Cth) has commenced and provides ASIC with additional penalty provisions to provide greater deterrence value. ASIC has also stated that it will establish a separate Office of Enforcement within ASIC in 2019 to centralise decision-making processes when determining whether to commence enforcement action.

ii Asia Region Funds Passport regime

See Section II.ii for details of the Asia Region Funds 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) has recently received Royal Assent. 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 Tiered marketing licensing regime

In May 2018, ASIC introduced a two-tiered licensing regime for financial markets and updated corresponding regulatory guidance. Specifically, the guidance reflects the risk-based assessment that will take an internationally consistent approach to the administration of the market licensing regime. Under the market licence regime, market venues can be designated as either Tier 1 or Tier 2 licensees, depending on their nature, size, complexity and the risk they pose to the financial system, investor confidence and trust.

Generally, Tier 1 market venues are, or are expected to become, significant to the Australian economy or the efficiency and integrity of (and confidence in) the financial system. Tier 2 licences will be able to facilitate a variety of market venues, including specialised and emerging market venues, and will have reduced licence obligations to accommodate new and specialised market platforms.

The tiered market licence regime is expected to impact, among others, market operators and operators of market-like venues (i.e., those that facilitate financial product trading on the basis of being exempt from the Corporations Act requirement), as well as platforms seeking to offer secondary trading.

v Passport relief

In late 2018, ASIC announced that from 30 September 2019 it will no longer allow FFSPs to rely on 'passport' class order relief or on 'limited connection' relief from the requirement to hold an AFSL in order to provide financial services in Australia to wholesale clients. Instead, ASIC will be proceeding with its proposal to implement a new regime that will require FFSPs to apply for a foreign AFSL. FFSPs currently relying on passport relief will have 12 months to transition to a foreign AFSL or satisfy licensing requirements in some other way. ASIC plans to release, in the first half of 2019, a draft Regulatory Guide and draft instruments relating to the foreign AFSL regime.

vi Restricted ADI

An entity that conducts any banking business, such as taking deposits (other than as part-payment for identified goods or services) or making advances of money, must be licensed as an ADI. In 2018, APRA released the Restricted ADI framework, which allows new businesses entering the banking industry to conduct a limited range of banking activities for two years while they build their capabilities and resources. See Section VI.iv. for further detail.

IX OUTLOOK AND CONCLUSIONS

There has been a variety of regulatory and legislative developments in the fintech industry, with 2019 bringing further developments that are likely to have an ongoing impact on 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 incoming Asia Region Funds Passport regime and the commencement of open banking, fintech is likely to have greater opportunities for growth as the sector moves from speculation to development to implementation.

While the government continues to promote fintech investment and innovation, consumer protection remains a central focus point for 2019. Following the findings of the Royal Commission's Final Report, there is likely to be a greater focus on service over sales

across the financial services sector and corporate regulators will look to financial service providers to comply with the law in a way that is consistent with broader and developing community expectations. We expect to see more rigorous engagement with ASIC and APRA during licence application processes, and for non-compliance to be dealt with in a way that is prompt and firm.

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 consumer demand for bespoke offerings and tailored customer services, while established institutions face the challenge of redesigning their existing commercial 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 2019* ranks Peter in Band 1 for fintech.

GILBERT + TOBIN

Lever 35, Tower Two
International Towers Sydney
200 Barangaroo Avenue
Barangaroo NSW 2000
Australia
Tel: +61 2 9263 4000
Fax: +61 2 9263 4111
preeves@gtlaw.com.au
www.gtlaw.com.au

Law
Business
Research

ISBN 978-1-83862-022-6