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

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

www.TheLawReviews.co.uk

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 RECHTSANWAELTE 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
Thomas A Frick

Chapter 1 AUSTRALIA 1
Peter Reeves

Chapter 2 AUSTRIA 15
Stefan Paulmayer

Chapter 3 BELGIUM 28
Pierre E Berger and Marc Van de Looverbosch

Chapter 4 BRAZIL 42
Alexei Bonamin, Marcela Waksman Ejnisman, Carla do Couto Hellu Battilana, Marcus Fonseca, Felipe Borges Lacerda Loiola, Natasha Wiedmann and Victor Cabral Fonseca

Chapter 5 BRITISH VIRGIN ISLANDS 56
Ian Montgomery

Chapter 6 CAYMAN ISLANDS 63
Alan de Saram, Natalie Bell, Aoife Madden, Laura Smalley and Dawn Major

Chapter 7 GERMANY 73
Jens H Kunz

Chapter 8 GUERNSEY 94
Wayne Atkinson

Chapter 9 HONG KONG 103
Yu Pui Hang (Henry Yu)

Chapter 10 ITALY 117
Giuseppe Rumi, Federico Vezzani and Tommaso Faelli

Chapter 11 JAPAN 134
Atsushi Okada, Takane Hori and Takahiro Iijima

Chapter 12 JERSEY 148
Dilmun Leach

Chapter 13 LUXEMBOURG 159
Anne-Marie Nicolas, Álvaro Garrido Mesa and Sandy Brumberg

Chapter 14 MALAYSIA 174
Shanthi Kandiah

Chapter 15 MEXICO 184
Federico de Noriega Olea and Juan Enrique Lizardi Becerra

Chapter 16 NETHERLANDS 194
Martijn Schoonewille, Wendy Pronk, Marije Louisse, Mariska Kool and Pepijn Pinkse

Chapter 17 PORTUGAL 205
Tiago Correia Moreira, Helena Correia Mendonça, Conceição Gamito, José Miguel Carracho and Francisca César Machado

Chapter 18 RUSSIA 220
Roman Buzko

Chapter 19 SAUDI ARABIA 230
Suhaib Adli Hammad

Chapter 20 SINGAPORE 239
Adrian Ang V-Meng and Alexander Yap Wei-Ming

Chapter 21 SOUTH KOREA 247
Jung Min Lee, Joon Young Kim and Samuel Yim

Chapter 22 SPAIN 261
Leticia López-Lapuente and Isabel Aguilar Alonso

Chapter 23 SWITZERLAND 272
Thomas A Frick

Chapter 24 TAIWAN 284
Abe T S Sung and Eddie Hsiung

Chapter 25 TURKEY 295
Cigdem Ayozger Ongun, Filiz Piyal and Deniz Erkan

Chapter 26 UNITED KINGDOM 303
Gareth Malna and Sarah Kenshall

Chapter 27 UNITED STATES 315
Erin Fonte, Scott Kimpel, Carleton Goss, Brenna McGee and Patrick Boot

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 artifical 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

Chapter 26

UNITED KINGDOM

Gareth Malna and Sarah Kenshall[1]

I OVERVIEW

The UK is one of the world's leading centres for 'technology applied to financial services' (the Department for International Trade's definition of fintech),[2] and the market has continued to grow year on year. It benefits from the UK's financial services regulatory regime, which is well established, and the supervision of that regime by the Financial Conduct Authority (FCA), which maintains a reputation as one of the gold standard regulatory bodies worldwide. The trend in the UK over the past decade has been towards ever increasing regulation, and the current climate is no exception. In the past year, legislation has been brought forward to effect the onshoring of EU laws once the current Brexit 'implementation period' ends on 31 December 2020. The FCA has also clarified the rules governing cryptoassets.

There are no dedicated fintech tax incentives in the UK, but there are various features of the UK tax regime that make it attractive for fintech businesses. There are incentives for companies, for example, R&D incentives for both capital and revenue expenditure and the 'patent box' regime.[3,4] Additionally, there are incentives for investors and management, including seed enterprise investment schemes, enterprise investment schemes, venture capital trust reliefs, entrepreneurs' relief, investors' relief and tax-advantaged share option arrangements.

The UK, like many other jurisdictions, is still addressing some of the transfer pricing and taxable presence problems arising out of fintech businesses. These depend on the value that is placed on a decentralised system, and new types of questions are likely to need to be answered as to what is required for a taxable presence in a country. The starting point for UK tax is to check whether there is a permanent establishment, and typically this will

1 Gareth Malna is an associate and Sarah Kenshall is a director at Burges Salmon LLP.

2 See 'Landscaping UK Fintech' Report 2014, Ernst & Young LLP commissioned by UK Trade and Investment (now the Department for International Trade): https://www.ey.com/Publication/vwLUAssets/Landscaping_UK_Fintech/$FILE/EY-Landscaping-UK-Fintech.pdf.

3 The 'patent box' is simply a calculation, though the way in which the patent is owned and used within a group structure can make the calculation and attribution of relevant amounts easier administratively. It allows the company to benefit for a low tax rate of 10 per cent for profits within the 'box'. The benefit of the regime is no longer available for acquired patents; however, it does cover cases where part of the relevant work was subcontracted. For fintech companies, patents that qualify have become more common. Nevertheless, it is critical to note that because the regime only applies to profits related to patents registered with the UK Intellectual Property Office or the European Patent Office or an European Economic Area State, the benefit of the more flexible regime for software patents in certain jurisdictions (for example, the US and Singapore) is not available.

4 There is no equivalent regime for other forms of intellectual property such as copyrights and trademarks.

involve a physical presence. However, there are also anti-avoidance provisions designed to prevent an avoided permanent establishment or profit fragmentation, and in some cases the arrangements around a fintech business will need to be reviewed to see if there is a risk of triggering these provisions. In some cases, it will be harder to judge how these might apply to a global supply chain compared with a more traditional business.

II REGULATION

i Licensing and marketing

Licensing

The FCA is technology neutral in its considerations on whether a firm is caught by the regulations and, therefore, the source and details of the rules that apply to fintech businesses operating in the UK will depend on the activities being carried on by each business. As a starting point, businesses will have to consider the general prohibition set out in Section 19 of the Financial Services and Markets Act 2000, which provides that it is a crime for any person to carry on regulated activities by way of business in the UK unless that person is authorised or exempt.[5]

The list of regulated activities caught by the general prohibition is set out in the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO) and includes, pertinently, accepting deposits,[6] issuing electronic money, effecting and carrying out contracts of insurance,[7] advising on or arranging deals in investments,[8] dealing in investments as agent or principal, providing credit information services and operating an electronic system in relation to lending.[9] These are known as 'specified activities', and to be regulated activities must relate to certain specified investments also set out in the RAO. Specified investments include electronic money, contracts of insurance, shares, units in collective investment schemes, rights under a pension scheme and credit agreements.[10] It does not matter whether services are offered digitally or in person; an entity carrying on the activities specified in the RAO by way of business in the UK[11] will be carrying on a regulated activity for which it must be authorised or exempt.

Where the activities of a business relate to the provision of payment services then the regime implemented in the Payment Services Regulations 2017 (PSR) will apply to the authorisation, registration and conduct of business obligations of those businesses. These aspects are discussed in more detail in Section IV.

Authorisation and registration applications for carrying on regulated activities under FSMA or specified activities under the PSRs must be made to the FCA and, in some cases, to

5 See Sections 19 and 20 FSMA.

6 Relevant for neo-banks acting with full deposit-taking permissions such as Starling and Monzo who were both granted permission during 2018.

7 Relevant for those platforms offering peer-to-peer insurance.

8 Relevant to digital wealth platforms such as Nutmeg and MoneyFarm.

9 Directly applicable to loan-based crowdfunding platforms such as FundingCircle.

10 See Part III of the RAO.

11 The question of whether an activity is being carried on 'in the United Kingdom' has to be answered in the context of each activity. Entities that arrange deals in investments are said to be carrying on that activity from the place of their establishment, whereas the activity of advising is said to be carried on where the advice is received.

the Prudential Regulation Authority (PRA).[12] Once authorised or registered, either or both of the regulators will continue to regulate the activities of the firm. All firms are regulated by the FCA as regards their conduct of business, but larger trading institutions will also be supervised by the PRA, which focuses on financial concerns that have an ability to negatively impact the broader market and economy.

The authorisation process is a lengthy and time-consuming one, and the scope of permissions that firms are required to obtain are not always clear. With that in mind, the FCA launched its regulatory sandbox in June 2016. The sandbox is open to authorised firms, unauthorised firms that require authorisation and technology businesses, and seeks to provide those firms with, among other things, a reduced time-to-market at (potentially) lower cost including by offering a restricted authorisation path, which allows those firms to operate in a limited manner under the close supervision of the FCA.[13] As of May 2019, 29 businesses were accepted into the fifth cohort of the sandbox, including Barclays, British Heart Foundation and Open Banking Implementation Entity. The success of the sandbox grows each year and this year the FCA received an unprecedented 99 applications.

Despite the more informal route that may be open to firms accepted into the sandbox, no special fintech licence or permission regime applies to fintech firms looking to operate in the UK.

Marketing

Subject to certain notable exceptions, firms may generally market themselves freely in the UK as long as any advertisements or marketing materials are accurate, legal, decent, truthful, honest and socially responsible.[14]

Firms may not, however, in the course of business communicate an invitation or inducement to engage in investment activity (a financial promotion) unless the firm is authorised or the content of the communication is approved by an authorised person.[15] Breaches of the restriction on financial promotions carry criminal consequences.

The terms 'invitation' and 'inducement' are typically given their natural meaning and, as such, communications that include a promotional element, (rather than those that seek merely to inform or educate about the mechanics or risks of investment) will be caught by the financial promotion restriction.

A number of exemptions may cause a financial promotion to fall outside of the restriction and, therefore, may freely be made by unauthorised firms within the boundaries of the applicable exemption. Alternatively, unauthorised firms may enter into arrangements under which an authorised entity reviews and approves each promotion at the time it is

12 The PRA supervises around 1,500 banks, building societies, credit unions, insurers and major investment firms.

13 The FCA can also offer through the sandbox: (1) the ability to test products and services in a controlled environment; (2) support in identifying appropriate consumer protection safeguards to build into new products and services; (3) better access to finance; and (4) individual guidance, informal steers, waivers and no enforcement action letters. For further details on the sandbox see https://www.fca.org.uk/firms/regulatory-sandbox.

14 i.e., they must not encourage illegal, unsafe or antisocial behaviour.

15 Section 21 FSMA.

made. This is a structure often implemented in crowdfunding, for example, where a business seeking equity investment through the crowdfunding platform is required to get the platform (which will be authorised) to sign off on the promotion before it is listed on the site.

Authorised firms that make financial promotions in compliance with the financial promotion restriction will also need to bear in mind the additional conduct rules for financial promotions set out in Chapter 4 of the Conduct of Business Sourcebook of the FCA Handbook.

ii Cross-border issues

As identified in the previous section, for a regulated activity to be carried on there must be some link between the activity and the UK. As such, where there is a cross-border element to the services or activities it will be necessary, from a regulatory perspective, to consider where the activity is actually carried on. This will inform the analysis of whether the firm carrying on that activity requires authorisation in the UK under the process described above. Where a business does not carry on any regulated activities in the UK then it will be able to provide those services in the UK, either on a cross-border basis or from a branch office set up in the UK.

As regards those fintechs not based in – but that intend to provide regulated activities in – the UK, it is currently necessary to consider separately those that are based in Europe and those that are based in other continents; though that is likely to change after the end of the Brexit implementation period on 31 December 2020 unless the UK and EU successfully negotiate a free trade agreement.

For those that are based in Europe, the complex web of EU passporting regimes continues to apply, depending on the activities carried on by the fintech business. For example, electronic money institutions may passport under the Second Electronic Money Directive,[16] while fintechs that provide insurance intermediary services may use the regime under the Insurance Distribution Directive.[17] The broadest passporting regimes (i.e., those that cover the most activities relevant to fintechs) are set out in the Markets in Financial Instruments Directive (MiFID II)[18] and Payment Services Directive (PSD2). EEA-based firms should not expect current passporting arrangements to continue after the Brexit implementation period ends. This means that they will need to plan for a range of possible scenarios for the end of the Brexit implementation period, including that the activities they conduct might not be covered by future arrangements agreed between the UK and the EU.

Those firms outside the EU looking to provide similar services in the UK will need to seek separate authorisation in the UK in relation to the regulated activities they intend to carry on.

16 2009/110/EC.

17 (EU) 2016/97.

18 Being the collective noun for both the Directive on markets in financial instruments repealing Directive 2004/39/EC (2014/65/EU) and the Regulation on markets in financial instruments and amending Regulation [EMIR] on OTC derivatives, central counterparties and trade repositories (Regulation 600/2014).

III DIGITAL IDENTITY AND ONBOARDING

There is no official national digital identity in the UK at present. The Government Digital Service has been running GOV.UK Verify as a secure way of accessing government services, but it has largely been considered a failure and it was announced at the end of 2018 that it would be transitioned to the private sector.

Despite that, a number of fintech firms are employing ever more sophisticated digital onboarding services, with the neo-banks in particular now very good at onboarding clients with little more than photographs of passports and a short video. Meanwhile, the market for firms who claim to be able to use cryptographic hashing to create a digital identity for an individual is growing rapidly in the UK. If successful, these services will enable individuals to verify their identity to third parties using only a very small amount of data (e.g., their personal hash, which is a cryptographically generated code combining all elements of that individual's identifying personal data, with a checksum item forming part of the personal hash calcuation, such as the individual's year of birth. In this case the year of birth acts as a way of validating the personal hash and, therefore, the identity of the individual in question).

IV DIGITAL MARKETS, PAYMENT SERVICES AND FUNDING

i Digital markets and funding

The UK has a very strong market in crowdfunding, peer-to-peer (P2P) lending and payment services, all of which sit alongside the UK's world-leading financial services marketplace.

The crowdfunding market in the UK is particularly mature and sophisticated – so much so that in July 2018 the FCA launched a consultation[19] into the market in order to identify whether the existing regulatory framework is still relevant and robust enough to ensure good standards of business are practised by the platforms, particularly where retail investors are involved.

Certain crowdfunding activities require authorisation by the FCA and others do not. All crowdfunding platforms are subject to the FCA's general high-level standards, including the Principles for Businesses and specific Conduct of Business rules, for example in relation to financial promotions. However, there are differences in the detailed regulatory frameworks that apply to investment-based and loan-based (or P2P) crowdfunding platforms.

Investment-based crowdfunding has evolved from more traditional ways of seeking equity-based investments, and the FCA regulates it as such. Therefore, an investment-based platform will usually ask for authorisation from the FCA to carry on activities such as arranging deals in investments (Article 25 RAO), dealing in investments as an agent (Article 21 RAO) and advising on investments (Article 53). Platforms that provide a nominee structure must also apply for a safeguarding and administration of assets permission (Article 40).

Operating a P2P platform was not adequately captured under the existing list of regulated activities, so, in 2014, the FCA introduced the new activity of operating an electronic system in relation to lending (Article 36H RAO), which captures most of what P2P platforms will be carrying on in practice. However, care should be taken if other regulated activities are built into the business model, such as credit broking, debt administration and debt-collecting, each of which require separate permission from the FCA.

19 CP18/20, which closed in October 2018 with a final policy statement due in Q2 2019.

The creation of secondary markets on platforms is not prohibited, but is becoming increasingly unusual with the more established platforms because of the additional regulatory burden of doing so (not least because of the potential financial promotion issues). It is more common for platforms to create venture capital-like fund structures that give investors the ability to exit the fund without having to find other users to buy their units.

ii Payment services

The UK is also a world leader in payment services. Firms will often seek authorisation from the FCA even where they do not intend to serve customers in the UK in order to benefit from the halo effect of being a UK-regulated firm when considering international expansion.

Payment service activities regulated under the PSRs in the UK include, among other things, services relating to the operation of payment accounts (e.g., cash deposits and withdrawals from current accounts and savings accounts), execution of payment transactions (whether covered by a credit line or otherwise), card-issuing and money remittance. PSD2, as implemented by the PSRs, also creates authorisation and registration regimes for payment initiation service providers (PISPs) and account information service providers (AISPs), two activities newly defined in 2017 that capture those businesses looking to utilise open banking standards to provide consumers with information about their finances, or that facilitate payments directly from users' bank accounts without the need to use a payment card.

Firms offering payment services are required to identify at the outset whether they will apply for registration or authorisation under the PSRs. Small payment institutions (SPIs),[20] small electronic money institutions (EMIs)[21] and firms that will only offer account information services can apply to be registered as such, or as a registered account information service provider (RAISP), and a lighter touch registration and conduct regime will apply to those firms. Firms that do not quality as an SPI, small EMI or RAISP but that intend to carry on payment services in the EEA must apply for authorisation and follow more onerous conduct of business requirements. These alternative routes are particularly popular where available.

PSD2 and the PSRs also facilitated new open banking standards,[22] requiring banks and building societies to give third parties access to customers' accounts and data where the user consents to it. At the moment, only the UK's nine largest banks and building societies must make customer data available through open banking, but a number of smaller banks and building societies have also opted in to the regime. Relevant third parties that benefit from the open banking regime include PISPs and AISPs, who are able to use customer account data to provide these new breeds of services.

Take-up was initially slow, but in 2019 open banking surpassed 1 million users for the first time. With a greater number of consumers and small businesses authorising their bank accounts to be connected with authorised third parties, responsibility for protection of their data rests with a wider ecosystem of providers. This raises challenges around security, the onward supply of data and the combination of data with other datasets.

20 Firms operating below an average monthly turnover in payment transactions of €3 million.

21 Firms in which total business activities will not exceed an average of €5 million of outstanding e-money immediately before registration.

22 Open banking is one of a series of regulatory remedies mandated by the UK Competition and Markets Authority requiring nine UK banks to implement a common standard API to allow third parties to access customer bank accounts (with customers' explicit consent)

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

Blockchain technology continues to capture the imagination in the UK, and the number of businesses adopting the technology for their own purposes is indicative of longer term trends. To date, key financial industries utilising the technology include the UK insurance and crowdfunding sectors, with asset management following slightly behind.

Of course, blockchain's original use in cryptoassets continues to be relevant, though that market is under a period of significant flux at the time of writing. This is, in part, due to the global development of rules and regulations that has created a period of instability and regulatory uncertainty. While the UK has not implemented any specific cryptoasset laws or regulations, the FCA has carried out work on cryptoassets, both as part of a broader UK Cryptoasset Taskforce and independently. The output of that work is the publication of Policy Statement 19/22, which is intended to help market participants to understand whether the cryptoassets they use are within the regulatory perimeter. In general, cryptocurrencies are not separately regulated by the FCA provided that they are not part of other regulated products or services. Instead, cryptoassets will fall within one of two categories – regulated tokens and unregulated tokens. The latter category does not require regulation and we have not considered those tokens further for these purposes. Regulated tokens can be further broken down into two categories – security tokens and e-money tokens.

Security tokens are tokens that provide rights and obligations akin to specified investments as set out in the RAO, including those that are financial instruments under MiFID II. Consequently, whether a cryptoasset will be treated as a security token will depend on its characteristics such as (1) any contractual rights and obligations the token-holder has by virtue of holding or owning that cryptoasset, (2) any contractual entitlement to profit-share or (3) whether the token is transferrable and tradeable on exchanges.

Separately, the new category of e-money tokens is based on the definition of e-money under the Electronic Money Regulations 2011 (EMR), that is, electronically stored monetary value as represented by a claim on the issuer that is (1) issued on receipt of funds for the purpose of making payment transactions; (2) accepted by a person other than the electronic money issuer; and (3) not excluded by Regulation 3 of the EMR.

Although it is clear that potential anonymity (or, more precisely, pseudonymity) afforded to individuals by cryptoassets means that they may have a role in money laundering and terrorist financing, the applicability of the existing money laundering regulations in the UK is not straightforward. To address that issue, the FCA has taken over supervision of anti-money laundering for cryptoasset businesses under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs), effective from 10 January 2020. The MLRs have been amended to bring cryptoasset exchange providers (including providers of automated teller machines (ATMs), peer-to-peer providers and issuers of new cryptoassets) and custodian wallet providers, within scope of the regulations. Businesses carrying on those activities will need to register with the FCA.

The UK has been reluctant to legislate for the tax treatment of cryptocurrency and crypto-token offerings, and HMRC, the UK tax authority, has focused instead on fitting this within existing tax provisions. However, it was recognised that, in the light of the Final Report from the Cryptoassets Taskforce in October 2018, some clarification was needed, as HMRC's 2014 guidance focused mainly on certain types of cryptocurrency and was very limited in scope. HMRC therefore produced revised guidance, covering the tax treatment of cryptoassets for individuals and where these are used as a form of employee reward (in

December 2018) and the tax treatment of cryptoassets for companies and businesses (in December 2019). Unfortunately, there has so far been no detailed public clarification of HMRC's view on the treatment of ICO and initial token offering issues for the issuing entities, but it is hoped additional guidance will become available in the near future.

Cryptoassets may currently be marketed to UK residents from other jurisdictions, but the UK financial promotion regime will apply and market participants will need to ensure that any financial promotion of products and services, whether regulated or unregulated, is carried on in a way that is clear, fair and not misleading. Firms must make clear in their promotions which activities are, and are not, regulated, especially when marketing their FCA-authorised status, so care will need to be taken in this regard.

VI OTHER NEW BUSINESS MODELS

The UK is awash with new business models. Of the new models available, 2019 was the year in which open banking really started to take off, with a rise in the number of AISPs becoming operational. Other popular business models include robo-advisers (including fully automated investment processes), e-wallets, crowdfunding, information aggregators and trust-based platform arrangements. Third-party financial comparison sites are commonplace, with insurance the largest category in both the consumer and business sectors. These sites are subject to the usual credit broking and insurance-related regulation (among others), and the same data protection and competition rules as any other business.

Self-executing, or 'smart' contracts are permitted, and the usual legal framework for contracts applies to them. That means there are a few legal questions still unanswered, especially around liability and agency. When it comes to making corrections, the court is the default option, unless an alternative was agreed in the contract.

Finally, use of big data is also on the rise as a tool to aggregate, analyse and increase the value of vast datasets. For example, the UK's implementation of open banking promises a world of build-your-own services and jealously guarded white-labelling agreements. To facilitate data transfers we are seeing trust-based arrangements with clear accountabilities and risk allocation for all participants, careful governance and security governing access, including third-party supply chain players.

VII INTELLECTUAL PROPERTY AND DATA PROTECTION

i Intellectual property

There are no intellectual property protections that are peculiar to fintech. However, in common with all evolving technologies, some fintech technologies do test the limits of the existing legal framework, this having not been written with these new technologies in mind. The most notable challenges come from blockchain technologies and technologies delivering artificial intelligence and machine learning applications.

The most important intellectual property rights for artificial intelligence are confidentiality, copyright and patent rights. The laws of confidence pose no unusual issues

for artificial intelligence. However, from a wider financial services policy perspective, it would be preferable for innovators to disclose AI innovations rather than opt to keep these as trade secrets,[23] so other protections come to the fore.

Copyright raises some issues in respect of ownership of the output of artificial intelligence, but otherwise copyright protection of source code remains as applicable to artificial intelligence software systems as it does for more traditional software systems.

It is in the realms of patent that the interesting issues around protection arise. In the UK, and under the European Patent Convention, in order to be granted a patent, the invention must be new, inventive, and capable of industrial application and not specifically excluded from protection as a patent. Mathematical methods are excluded, as are computer programs, which are, of course, at the heart of artificial intelligence development.

This is not to say artificial intelligence and machine learning algorithms cannot form part of a computer-implemented invention where they can be shown to have a 'technical effect'; they are just not patentable in and of themselves. Where they form part of platforms and applications that solve specific technical problems, then the success of a patent application improves significantly. In summary, a combination of copyright and patent protection should provide a good basis for protecting investment in artificial intelligence and machine learning in the UK.

Artificial intelligence is, of course, inextricably linked with the data it consumes and the financial services industry generates vast amounts of data. The data itself comes with a set of intellectual property protections – mostly confidentiality, sometimes copyright and, potentially, the sui generis database right.[24] For example, look-up tables (databases accessed by software routines) are potentially protected by copyright in the structure of the database and by the sui generis database right protecting the extraction and reutilisation of the data contained in the database (provided the owner can show substantial investment in obtaining the data).

The database right is a powerful right, and while the protection ostensibly lasts for 15 years, each time substantial investment is expended in obtaining, verifying or presenting the contents of the database, a new database is likely deemed created and thus a rolling protection obtained.[25] There has been some debate as to whether aggregations of data, for example, sensor or machine-generated data, can fulfil the 'substantial investment in obtaining' requirement of the database right. The debate continues as to where the threshold of effort lies. Irrespective of whether or not the contents of a database are protected by confidentiality or database rights, both can provide limitless protection. Because big data is becoming such an integral part of any business dealings, the UK competition authorities are sure to consider moves to counteract potentially monopolistic effects of vast datasets being controlled by relatively few market players.

Turning to blockchain technologies, similar issues are encountered: patent protection for spreadsheets is not available, and there will need to be some actual technical effect, similar

23 European Patent Office, Patenting Artificial Intelligence 30 May 2018.

24 EU Directive 96/9/EC on the legal protection of databases (the Database Directive) implemented in the UK by the Copyright and Rights in Databases Regulations 1997 (SI 1997/3032) (the Database Regulations).

25 The organisation that originates the contents of the database does not get the benefit of the protection as they do not need to expend time finding, checking and verifying the contents (since they originated the contents). Clearly, the key is investment in collection rather than creation of the content.

to software-enabled inventions. Copyright is the most common form of protection for blockchain, both proprietary and open-source. The basic building blocks of many blockchain technologies are open-source software codes, but those building on top of the originating technologies may want to protect their inventions through more commercial protections, such as more restrictive copyright and patent licensing.

ii Data protection

In the same way as for intellectual property, financial services technologies also test the existing legal framework around data protection, despite the General Data Protection Regulation (GDPR) being of very recent provenance.

The UK Information Commissioner's technology priorities for 2019 include cybersecurity, artificial intelligence, big data and machine learning and online tracking technologies, all of which are highly pertinent to technologies within the financial services sector.

Big data analytics again poses difficulties for data protection law. Difficulties include running large numbers of algorithms against vast datasets to find correlations; the opacity of the processing; the tendency to collect 'all the data'; the repurposing of data and the use of new types of data; not to mention the hurdles of distinguishing between data controllers and data processors. Clearly all of these activities have implications for data protection.[26]

The Information Commissioner's Office is reaching out to partners as part of its Technology Strategy to better understand these technologies, and is seeking to establish a regulatory sandbox, drawing on the successful sandbox process that the FCA has developed. The sandbox is expected to enable organisations to develop innovative digital products and services, while engaging with the regulator, who will provide advice on mitigating risks and data protection by design.[27]

New blockchain technology also poses data protection challenges. There has been significant debate as to whether or not the hashed information contained on the blockchain could be considered personal information and, if it is, how the GDPR can be reconciled with the benefits of the blockchain being an immutable source of the truth without the need for trusted intermediaries. This question has yet to be resolved.

In addition to the GDPR, PSD2 includes a number of specific rules concerning the processing of personal data. For example, PSD2 provides for 'explicit consent' raising the question of whether this constrained the use of the various other bases for processing set out in the GDPR. The European Data Protection Board has clarified that it did not. 'Explicit consent' referred to in PSD2 is a contractual consent that is an additional requirement of a contractual nature. Payment services are always provided on a contractual basis between payment service user and payment service. There still needed to be a requisite basis for processing the data under the GDPR, for example, processing necessary for the performance of a contract to which the data subject is party.

26 ICO Big Data, artificial intelligence, machine learning and data protection report 2017.

27 ICO Technology Strategy 2018–2021.

VIII YEAR IN REVIEW

The year 2019 saw the publication of 'Liability for Artificial Intelligence and Other Emerging Digital Technologies', an expert report from the European Commission. Its findings are particularly pertinent to fintech, which has been an early adopter of AI and robo-advisers.

In particular, the report noted that a resolution to the question of who (in principle) is liable for the output of an AI tool is becoming increasingly urgent as powerful AI systems are being created. In the UK, these are likely to take the form of contract and tort-based claims specific to the facts of each case. While such claims may be complicated, the year ahead is likely to see the development of ways that the complexity might be addressed. For example, in the case of robo-advisers competing in the independent financial adviser/fund manager market, potential issues can arise in establishing a breach of duty of care given potential 'black box' problems. These issues might be addressed by focusing on the inputs and the outputs of the AI, for example, whether the investments match the instructions given. The report also concluded that, in the case of AI, it is not necessary to create a further category of legal personality, as the harm it causes should be attributable to existing legal persons or bodies.

Last year saw record investment in the UK fintech sector, with London attracting the biggest number of international investors, overtaking New York for fintech investment deals, which is underpinned by supportive regulation and an early adopting customer base.

The end of 2019 saw the signature of the UK–EU Withdrawal Agreement. Under the agreement, from 31 January 2020, the UK is no longer a member of the EU. Nevertheless, the parties agreed an implementation period where the UK continues to be subject to EU rules and remains a member of the EU Single Market and customs union. This allows the parties to continue their current relationship while a future trading relationship is negotiated. The implementation period is due to end on 31 December 2020, whether or not a trading relationship has been agreed.

IX OUTLOOK AND CONCLUSIONS

Much of the focus in the coming months will be on the outcome of the future trading relationship between the UK and the EU and how it affects the market based on the deal (or lack of it) reached with the remaining EU Member States.

When the implementation period has expired, whether firms will continue to be able to make use of existing passporting regimes will depend on the terms of the agreement over the future relationship between the UK and the EU.

The payments sector is the most likely to be affected by Brexit, given the strength and size of the UK's banking sector relative to other jurisdictions. Indeed, as firms begin to make the most of the new markets created by PSD2, it was the UK that stood to gain most from those. However, a question now remains as to how much of that opportunity will be lost, despite the fact that, the rules will be transposed into the UK statute book so as to continue to be effective at least in the short term.

It will also be worth keeping one eye on the asset management industry in 2020. As wealth-tech providers including technologically advanced asset management solutions proliferate, the retail asset management industry looks set to face a regulatory shake-up by the FCA and Bank of England following issues with Neil Woodford's investment funds and liquidity structuring. That could create the perfect environment for the wealth-tech firms to gain significant market share in the event that the FCA and Bank of England do recommend a repositioning of the market.

The UK is the third most connected country in the world, and maintenance of dataflows between the UK and the EU will be a priority in the forthcoming negotiations. The UK is keen to obtain an 'adequacy' decision as part of the future trading relationship – otherwise it will become a third country from the perspective of EU dataflows, and companies will have to put in place more cumbersome compliance mechanisms to govern these, such as binding corporate rules, EU standard contractual clauses or other approved arrangements.

From an IP perspective, the European Patent Convention is not directly linked to the European Union, so European patents should not be affected by Brexit. By contrast, Community Trade Marks are linked to membership of the European Union. Thus, once the transition period ends, Community Trade Marks will technically cease to have effect in the UK. However, the UK government has indicated that even if there are no deals with the EU they will permit Community Trade Mark registrations that are in force at the time of exit from the EU to be extended in to the UK so that pre-existing trade mark rights will not be lost. As for the sui generis database right, the government's Regulatory Policy Committee states that the UK government's preferred option is to maintain the status quo after Brexit so far as possible for UK database creators and consumers.[28]

Blockchain will continue to present challenges around applicable law, as it involves computers located across the globe. In cross-border decentralised blockchains, individual transactions will need to analysed on a case-by-case basis.

28 Intellectual Property (Amendment) (EU Exit) Regulations 2018 and various impact assessments published by the Regulatory Policy Committee (RPC).

Appendix 1

ABOUT THE AUTHORS

GARETH MALNA

Burges Salmon LLP

Gareth is an associate in Burges Salmon's funds and financial regulation team, and specialises in financial services regulation. He coordinates the financial services regulatory aspects of the firm's fintech practice, with a primary focus on payment services, crowdfunding, blockchain solutions and the implementation of RegTech solutions at regulator level.

Gareth also has expertise in the establishment, structuring, operation and winding up of UK regulated fund structures, such as OEICs, authorised unit trusts and authorised contractual schemes.

He is also the lead contact on the financial services regulatory aspects of the fintech sector and has been heavily involved with a number of policy initiatives in this sector with the FCA, Bank of England and Treasury, including a digital regulatory reporting pilot project.

His fintech clients include payment institutions and acquirers, neobanks, crowdfunding platforms and investment funds that offer tokenisation. He also advises authorised fund managers including host ACDs, investment managers and other regulated product providers.

He is the co-author of the UK chapter in The International Comparative Guide to Public Investment Funds 2018 (ICLG, 2018).

SARAH KENSHALL

Burges Salmon LLP

Sarah leads Burges Salmon's cross-departmental fintech practice and is a director in the firm's technology and communications team. She has been involved in advising on evolving technologies for over 15 years, including work on high-profile transformational project procurements, structuring business models for commercialising new technologies, advising on commercial delivery and providing practical risk analysis and guidance.

Sarah's team supports fintech companies with their establishment, expansion, commercial contracts, fundraising and M&A, and sponsored the 2018/2019 Tech Nation's new fintech growth programme and the Go: Tech Awards (AI category) 2019. Sarah is a member of Tech UK.

BURGES SALMON LLP

One Glass Wharf
Bristol BS2 0ZX
United Kingdom
Tel: +44 117 939 2000
gareth.malna@burges-salmon.com
sarah.kenshall@burges-salmon.com
www.burges-salmon.com

an LBR business

ISBN 978-1-83862-453-8