ICLG

The International Comparative Legal Guide to:

Fintech 2017

1st Edition

A practical cross-border insight into Fintech law

A&L Goodbody
Anderson Mōri & Tomotsune
Anjarwalla & Khanna Advocates
BA-HR
Bär & Karrer Ltd.
BonelliErede
Bredin Prat
De Brauw Blackstone Westbroek
ENS Africa
Galicia Abogados, S.C.
Gilbert + Tobin
Gorrissen Federspiel
GVZH Advocates
Haiwen & Partners
Hengeler Mueller Partnerschaft von Rechtsanwälten mbB
Herzog Fox & Neeman
Hiswara Bunjamin & Tandjung (in association with Herbert Smith Freehills LLP)
Kim & Chang
Lee and Li, Attorneys-at-Law
Mannheimer Swartling
Mattos Filho, Veiga Filho, Marrey Jr. e Quiroga Advogados
McMillan LLP
Roschier, Attorneys Ltd.
Shearman & Sterling LLP
Shearn Delamore & Co.
Slaughter and May
SRP-Legal
Trilegal
Udo Udoma & Belo-Osagie
Uría Menéndez
Uría Menéndez – Proença de Carvalho
WKB Wierciński, Kwieciński, Baehr

glg
global legal group

global legal group

Contributing Editors
Rob Sumroy and Ben Kingsley, Slaughter and May

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Paul Mochalski

Editor
Caroline Collingwood

Senior Editors
Suzie Levy, Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
May 2017

ISBN 978-1-911367-49-9
ISSN 2399-9578

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

EDITORIAL

Welcome to the first edition of *The International Comparative Legal Guide to: Fintech*.

This guide provides corporate counsel and international practitioners with a comprehensive worldwide legal analysis of the laws and regulations of fintech.

It is divided into two main sections:

One general chapter. This chapter provides an overview of Artificial Intelligence in Fintech.

Country question and answer chapters. These provide a broad overview of common issues in fintech in 33 jurisdictions.

All chapters are written by leading fintech lawyers and industry specialists and we are extremely grateful for their excellent contributions.

Special thanks are reserved for the contributing editors Rob Sumroy and Ben Kingsley of Slaughter and May for their invaluable assistance.

The *International Comparative Legal Guide* series is also available online at www.iclg.com.

Alan Falach LL.M.
Group Consulting Editor
Global Legal Group
Alan.Falach@glgroup.co.uk

USA

Reena Agrawal Sahni

Shearman & Sterling LLP

Sylvia Favretto

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Innovative financial technology has received enormous interest and regulatory attention in the United States in recent years. Fintech players in the United States come in various forms and sizes and are offering institutional and retail customers an increasing variety of services. While the U.S. fintech landscape and the regulation thereof continue to develop, the increase in new fintech start-ups and investment in the sector show no immediate signs of slowing.

Given the emphasis on technology, the United States has seen many prominent players in fintech, including a significant number of start-ups, emerge out of Silicon Valley, including Square, PayPal, Lending Club and Stripe. The types of fintech businesses that have garnered popularity in the United States provide an array of financial services, such as payments, online lending, robo-advice, and insurance, utilise new technology such as distributed ledger technology (**DLT**) for bitcoin, and are provided across a variety of platforms, including mobile, as well. New fintech providers and platforms continue to emerge, with each endeavouring to provide consumers with increased access to convenient and secure financial interactions.

DLT, in particular, has garnered a significant amount of regulatory attention in the past year, as regulators recognise the immense potential for DLT to transform the world of finance and the implications that DLT may have for market participants. Robo-advising has also been receiving increased attention by consumers and regulators alike, with predictions that the percentage of investment assets being managed by robo-advisors will only continue to increase in the coming years.

Another notable trend in the fintech space over the past couple years is the increase in fintech companies partnering with traditional brick and mortar banks to provide financial services to consumers, providing mutual efficiencies that can serve to further increase consumer inclusion and access to financial technology. Banks' partnerships with, and investments in, fintech firms have allowed banks to participate in new platforms for traditional bank products.

Finally, regulators in the United States are also monitoring growths in the emergence of innovative technology aimed at helping banks achieve effective compliance with regulations, also known as "regtech".

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There are currently no U.S. laws or regulations that identify types of business that fintech companies are prohibited from engaging in. However, the business of fintech firms must be in compliance with the general regulatory framework described below in Section 3.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Funding from a wide variety of sources and types is available for new and growing businesses, including angel, seed and later rounds of equity, debt and convertible debt investment. A company can raise money for a variety of purposes – for working capital, to finance an expansion, for marketing purposes, and even as a source of capital to lend (as in the case of a lending marketplace). Funding is available from institutions and corporates, venture capital and hedge funds, private equity, mutual funds, family offices as well as high net worth individuals. The JOBS Act and the regulations promulgated thereunder have provided additional means of raising capital for businesses, including from non-accredited individuals in publicly-sourced crowdfunding transactions. Importantly, the JOBS Act allows new and growing businesses to conduct general solicitations and to access the public markets without the panoply of regulatory burdens typically associated with doing so.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

There may be incentives available from certain local jurisdictions or areas to encourage investment in that region. It is recommended to check with the local governments or chambers of commerce for more information.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The United States uses a disclosure-based system for public securities

offerings, including IPOs, meaning that it is the responsibility of the issuer to disclose all risks and uncertainties regarding the issuer and its business/industry in the IPO prospectus. The U.S. Securities and Exchange Commission (**SEC**) is the chief regulator. There are no specific financial requirements imposed by the SEC, but there may be certain minimum thresholds regarding number of post-IPO shareholders, size of public share float and certain financial measures depending on which trading exchange is chosen for the listing.

Practically speaking, the most important elements for a successful IPO are a business model that is both proven and not easily replicated by potential competitors, a strong management team that can win and keep the trust of their shareholders and sustainable growth momentum that can attract quality investors.

The JOBS Act made it possible for certain companies to conduct "mini IPOs" (capped at $20 million or $50 million per annum, based on whether a company satisfies certain criteria), and allows companies that qualify as "emerging growth companies" to conduct an IPO a bit more easily (including by avoiding certain attestation requirements under Sarbanes Oxley) than would otherwise be possible.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Lending Club, OnDeck, Square and BATS have all achieved IPOs. In addition, China-based fintech company Yirendai also achieved an IPO in the U.S. and China-based China Rapid Finance is expected to list on the New York Stock Exchange in late April 2017. Therefore, the U.S. capital markets can be used to fund non-U.S. businesses as well through both private and public offerings of equity or debt.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Fintech businesses in the United States are not subject to a fintech-specific regulatory framework by any single federal or state regulator. Rather, depending on the activities of the fintech company, that fintech company may be subject to a myriad of federal and state licensing or registration requirements, and, thereby, also subject to laws and regulations at both the federal and state levels.

Many fintech companies find that offering their services in the United States requires licensing and registration with multiple state regulators, subjecting such fintech companies to regulation and supervision by the laws and regulations of each such regulator. The types of licences that may be required at the state level include consumer lending, money transmission, and virtual currency licences. Depending on the number of states and licences that are required to be obtained, a fintech company may then have to contend with on-going compliance with state-level rules and regulations.

On the federal level, the Consumer Financial Protection Bureau (**CFPB**) has jurisdiction over providers of financial services to consumers. Because many fintech businesses are aimed at providing services to consumers, the CFPB has the ability to enforce a range of consumer protection laws (such as consumer lending laws and anti-discrimination laws) that apply to the activities of such companies. The CFPB also has authority to enforce against the use of unfair and deceptive acts and practices generally.

To the extent that the activities of a fintech provider fall within the licensing regimes of other federal regulators, such as the SEC or the Commodity Futures Trading Commission (**CFTC**), such fintech providers will be required to register with such agencies and become subject to enforcement by the same. For example, robo-advisors, being a subset of investment advisers, may be subject to SEC registration requirements for such advisers. Finally, fintech companies may also be required to register with the U.S. Department of Treasury's Financial Crimes Enforcement Network (**FinCEN**) and thus, as described below, comply with the Bank Secrecy Act and other anti-money laundering laws and regulations.

The Office of the Comptroller of the Currency (**OCC**), the primary federal bank regulator for national banks, announced in December 2016 that it will provide a special purpose national bank charter to fintech companies that receive deposits, pay checks or lend money. Fintech companies that choose to apply for and receive this special purpose national bank charter will become subject to the laws, regulations, reporting requirements and ongoing supervision that apply to national banks, and will also be held to the same standards of safety and soundness, fair access, and fair treatment of customers that apply to national banks. The OCC intends that, among other things, this special purpose national charter may help level the playing field between national banks and competing fintech companies, while also protecting consumers and providing greater consumer access to fintech services. The chartering of fintech companies by the OCC has drawn some criticism from state regulators, among others, who argue that the regulation of such companies is better accomplished at the local level by regulators who may have a deeper knowledge of certain fintech industry participants and more tailored regulations.

Regulators with jurisdiction over fintech businesses have not shied away from issuing enforcement actions where fintech businesses are conducting activities in violation of law. In recent years fintech companies have been subject to enforcement actions by regulators, including the CFPB, SEC and CFTC. Enforcement orders have been issued for, among other things, insufficient data security practices, violations of federal securities laws, including anti-fraud laws, failing to obtain requisite licences or registrations, and unfair and deceptive practices.

3.2 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested?

Federal financial regulators have been outspoken regarding the vast potential for financial technology innovation and the simultaneous need to tailor the regulation of the sector to protect consumers and mitigate risk without stifling such potential for industry growth. As the fintech space continues to develop, fintech companies have seen an increasing desire on the part of regulators to gain an understanding of the industry from, and work with, fintech market players. Examples of such efforts include the following:

- The CFPB's "Project Catalyst" initiative aims to increase the CFPB's outreach to and collaboration with fintech companies in connection with the development of fintech policies. As part of this program, the CFPB has implemented a no-action letter policy, whereby fintech providers may request a non-binding no-action letter from CFPB staff stating that the agency, subject to certain caveats and limitations, does not recommend enforcement or supervisory action against the entity in respect of specific regulations that may apply to new fintech products to be offered by the entity.
- The OCC has created an Office of Innovation in order to help provide a regulatory framework that is receptive to responsible

innovation. The Office of Innovation is intended to serve as a central point of contact for requests and information relating to innovation and will also hold office hours to provide increased OCC staff access to fintech market players.

- In September 2016, U.S. House Representative Patrick McHenry (R-NC) introduced a bill, titled the Financial Services Innovation Act, that endeavours to create a broad regulatory "sandbox" regime across various federal financial regulatory agencies and would establish a process whereby fintech companies could petition for regulatory relief from certain specified regulatory requirements in connection with such companies' financial innovation products. The bill would also require certain federal financial regulatory agencies to establish offices tasked with promoting financial innovation, which offices would coordinate with each other on developing fintech regulation while also working to navigate the regulatory framework with those fintech companies whose petitions for relief have been granted.

3.3 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

While there is no regulatory framework that applies specifically to non-U.S. fintech companies, non-U.S. fintech companies must comply with the general licensing and regulatory framework described herein.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Instead of having one national data protection law, a variety of federal laws regulate how fintech businesses collect, use and transmit personal data including: the Gramm-Leach-Bliley Act (**GLBA**); Fair Credit Reporting Act (**FCRA**); Federal Trade Commission Act (**FTC Act**); the Wiretap Act; and the Electronic Communications Privacy Act (**ECPA**). Key federal agencies that have the jurisdiction to enforce these laws include: the OCC; the CFPB; the SEC and the CFTC; and the Federal Trade Commission (**FTC**). A number of states have also passed laws that limit the collection, use and transmission of sensitive information, including social security numbers, drivers' licence information, financial data, health data, and others, and have rules relating to data breach reporting notifications.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

U.S. data privacy laws have generally been accepted to apply to data that is collected by U.S. organisations and stored in the United States and no U.S. law as of yet has any restrictions to international transfers of data (restrictions on data being transferred out of the United States). However, the question of whether the U.S. Department of Justice can use a warrant to seek data that is stored overseas has been litigated in the courts over the past year. In the Microsoft case, the Second Circuit Court of Appeals ruled in July 2016 that Microsoft does not have to provide copies of the data that is stored in Ireland to the Justice Department, whereas in the Google case a U.S. Magistrate Judge in February 2017 ordered Google to hand over the emails stored outside the country in order to comply with an FBI search warrant. Fintech companies should pay close attention to this area of law and monitor developments in regulation and enforcement as there is continuing debate whether certain laws need to be revised to reflect the changes in technology and how companies collect, use and store data.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Various federal agencies and state attorneys generals have brought enforcement actions against companies for failing to comply with data privacy and consumer protection laws. For example, the FTC has brought over 130 spam and spyware cases and more than 40 privacy lawsuits. The California State Attorney General created a "Privacy Task Force" in 2012 and has brought criminal and civil actions against companies and individuals relating to data privacy violations, including failure to post privacy policies and issue timely data breach notifications. In addition, some privacy laws are enforced through class action lawsuits for significant statutory damages and attorneys' fees. Companies can also be sued for violations in data security and privacy practices, such as failure to adequately protect payment card data or for behavioural tracking of consumers without proper privacy notices.

In March 2016, the CFPB brought its first data security action, exercising its authority under the Dodd-Frank Act to enforce unfair and deceptive acts and practices. Dwolla, an online payment platform company, was ordered to pay a $100,000 penalty to the CFPB's Civil Penalty Fund after finding that Dwolla's data security practices were insufficient and that Dwolla misrepresented the quality of its data security practices to its consumers.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Cybersecurity for financial market participants is among one of the top concerns for U.S. regulators. Federal financial regulators have established various customer data and information technology security rules, examination manuals, handbooks and guidance. Further, the federal banking agencies published for comment in October 2016 an advanced notice of proposed rulemaking on enhanced cyber risk management standards, which, if implemented, will apply to, among others, any fintech companies that obtain a special purpose national bank charter from the OCC. With respect to consumer financial service providers, the CFPB has also issued enforcement actions against such providers, including at least one fintech service provider (as described above), relating to deficient data security practices.

Also notably at the state level, the New York State Department of Financial Services' cybersecurity rules became effective in March 2017, requiring institutions regulated by the state's financial regulator, including money transmitters, to establish and maintain cybersecurity programmes. It is possible that other states will soon follow suit in establishing their own cybersecurity regimes, which regimes could also apply to fintech businesses that obtain licences from such states' financial regulators.

Given the particular concerns that fintech businesses pose to customer's information security and the increasing regulatory emphasis on the subject, it is critical that U.S. fintech companies identify and comply with all applicable laws, regulations and best practices.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

At the federal level, the Bank Secrecy Act (**BSA**) is the primary piece of U.S. anti-money laundering (**AML**) legislation. The BSA requires, among other things, the establishment of a robust anti-money laundering compliance programme and various reporting requirements, including currency transaction reports and suspicious activity reports (the latter of which also now requires the reporting of cybersecurity-related events). The BSA applies to financial institutions, which definition includes "money services businesses". Many fintech businesses conduct activities that require registration with FinCEN as a "money services business", including payment system providers.

Further, "financial institutions" are also required to have in place under the USA PATRIOT Act customer identification programs (**CIP**) that allow such institutions to know and verify the identity of their customers. CIP requirements applicable to certain financial institutions were also recently bolstered by a FinCEN rule requiring further diligence as to beneficial owners in respect of legal entity customers.

Certain states also have in place their own anti-money laundering requirements which may apply to licensed fintech businesses within such states. Additionally, the Treasury Department's Office of Foreign Assets Control administers economic sanctions that prohibit all U.S. persons from transacting with certain persons and countries that may pose a threat to U.S. national security.

It is imperative that fintech companies understand the scope of BSA/AML and sanctions regulations applicable to their businesses, by virtue of registering as a bank, broker-dealer, money services business, or otherwise, and subsequently implement robust anti-money laundering programmes in compliance with such regulations to avoid enforcement by U.S. regulators who have been placing increased emphasis on anti-money laundering concerns.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

With the increase in partnerships between traditional banking institutions and fintech companies, fintech businesses should be mindful of the robust vendor management/third-party outsourcing regulations that banks are required to comply with. The requirements of such regulations could subject fintech partners of banks to rigorous diligence, contract negotiations, indemnification requirements, and the jurisdiction of federal bank regulators.

Additionally, it is important to reiterate that depending on the nature of the activities conducted by a fintech business, such business could be subject to the various laws and regulations specific to such activities at both the state and federal level, including, lending laws, securities laws, data protection laws and certain consumer protection laws.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

With the exception of immigration law (see question 5.3 below), there are few formal legal requirements or impediments to hiring or dismissing employees in the United States, which generally is an "at will" employment jurisdiction. That being said, employment actions (including employers' decisions regarding hiring, firing, promotions and compensation) with the purpose or effect of discriminating on the basis of sex, age, race, national origin or other categories protected by local law may give rise to government enforcement actions or private litigation. In addition, under federal and, in some cases, state and local law, advance notice (or pay in lieu of notice) may be required in the event of "plant shutdowns" or "mass layoffs".

5.2 What, if any, mandatory employment benefits must be provided to staff?

Generally, none, although mandatory payroll taxes are used to contribute to certain government-provided benefits. Benefits are a matter of agreement between employees and employers, but businesses customarily provide some kind of retirement and medical benefits as well as paid vacations. Once benefits are provided to any employees, there may be legal restrictions on excluding other employees from coverage. The Family Medical Leave Act mandates up to 12 weeks of unpaid, job protected leave per year, for the birth or care of a newborn child, as well as for medical leave for the employee and the care of family members. In addition, the Fair Labor Standards Act and its state and local analogues require that "non-exempt" employees be paid one and a half times their normal rate of pay for hours worked beyond 40 in a workweek. "Exempt" employees are salaried employees receiving compensation above a specified level and performing supervisory or managerial duties. Note that the most important threshold issues in determining whether the above and other legal requirements apply to a "staff" member is whether the individual is an employee or an independent contractor. Many technology companies have been subject to enforcement actions or litigation where they have attempted to categorise service providers as independent contractors but the government or service providers assert employment status, thereby entitling them to certain legal protections, including overtime pay.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

All employers must verify the eligibility of prospective employees to work in the United States through completion of an I-9 form and presentation of documentation confirming identity and employment authorisation. Technology companies have availed themselves of the H-1B visa programme to bring scientists, programmers and other specialised educated employees from outside the jurisdiction to the United States. This programme, which issues 85,000 temporary visas per year to permit the hiring of highly-skilled workers where there is a shortage of qualified workers in the country, as of this writing is subject to heightened scrutiny and potential modification by the Trump administration, which has vowed to combat "fraud and abuse" of the programme and ensure that it is not utilised by employers to replace qualified domestic with less highly paid foreigners.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

In the United States, inventions can be protected by patents. By statute, a process (or method), a machine, manufacture, or composition of

matter are all considered eligible for patenting. The patent-eligibility of methods is important to fintech companies whose inventions often involve methods practiced using computer technology. While patent protection of methods appears quite broad, recent court decisions have narrowed it considerably. In *Alice Corporation Pty. Ltd. V. CLS Bank International*, the Supreme Court held that certain claims in a patent were ineligible for patenting because they were drawn to an abstract idea. Abstract ideas are not patentable in the United States. Furthermore, claiming the use of a generic computer implementation failed to transform the abstract idea into patent-eligible subject matter. Fintech companies should be aware that applications that simply require an otherwise abstract method to be performed on a computer will not be considered patent-eligible subject matter.

Software code and certain aspects of computer programs (like text presented on a screen) are copyrightable works in the United States. Copyrighting software offers protection from rivals copying a firm's software.

Finally, fintech companies can protect their inventions and innovations, particularly the source code in computer programs, through trade secret law. Unlike patents and copyrights, trade secrets do not expire. Since trade secrets are primarily protected by state law, there is a patchwork of different laws protecting trade secrets across the United States. However, in 2016, the Defend Trade Secrets Act created a federal cause of action for trade secret misappropriation. Fintech companies should be aware that trade secrets must be continuously guarded by them from public disclosure and do not protect against independent development by another party.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Ownership rights in a patent or trade secret originate with the inventor(s). Ownership rights in a copyright originate with the author(s) of the copyrighted work, unless the copyrighted work is a work made for hire, in which case the entity that commissioned the work is considered its author by the United States Copyright Office (**USCO**).

Each fintech company should take steps to make sure that it owns the IP generated by or for its business. For example, it should insert a clause into all contracts with employees and contractors that requires the other party to assign all rights to the company in any inventions or works made during the engagement or employment. This clause may add that the parties agree all copyrightable works made by the employee/subcontractor during the term of engagement are works made for hire with the authorship attributed to the company. Furthermore, these contracts should also contain confidentiality obligations that obligate the other party to maintain the confidentiality of all proprietary information generated by them during the engagement or employment.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

In the United States, IP rights are granted locally on the national or state level. The United States Patent and Trademark Office (**USPTO**) grants patents and registers trademarks. Copyrights are granted by the USCO. State agencies also register trademarks used within their borders. Copyrights and trademarks do not need to be registered as the owner's rights commence from the creation of the work and the use of the mark, respectively. There is no registry for trade secrets. Instead, rights in trade secrets derive from the owner taking reasonable measures to keep proprietary information which gives its business an advantage secret.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

The primary means of exploiting IP in the United States is through selling goods and services that incorporate the IP and enforcing them against a competitor that uses the IP without permission in its own goods or services.

IP has also become an important tool for raising money. IP portfolios can be sold like any other asset. Fintech companies can use their IP as collateral in loans and gain better terms from the lenders. Also, more complex approaches to patent monetisation are becoming more common. Fintech companies with long track records of generating revenue from their IP assets may securitise them, thereby securing a large, up-front injection of capital in exchange for making payments in the future. The terms of these deals are negotiable, providing flexibility in deal structure. Finally, fintech companies can attempt to monetise their IP by licensing it to others for a royalty or suing infringers for damages.

Acknowledgment

The authors would like to acknowledge Jordan J. Altman, a partner in Shearman & Sterling's Intellectual Property Transactions Group, John J. Cannon, a partner in Shearman & Sterling's Compensation, Governance & ERISA Group, David O'Steen, an associate in Shearman & Sterling's Intellectual Property Transactions Group, Alan Seem, a partner in Shearman & Sterling's Capital Markets Group, Jeewon Kim Serrato, a counsel in Shearman & Sterling's Privacy & Data Protection Group, and Chuck Thompson of Blockchain Consulting LLC, for their assistance in preparing this chapter.

Reena Agrawal Sahni
Shearman & Sterling LLP
599 Lexington Avenue, New York,
New York 10022
USA

Tel: *+1 212 848 7324*
Email: *reena.sahni@shearman.com*
URL: *www.shearman.com*

Reena Sahni is a partner in the global Financial Institutions Advisory & Financial Regulatory Group. She has extensive experience advising on bank regulation, bank insolvency, recovery and resolution planning and bank capital markets transactions, including Dodd-Frank implementation for U.S. and non-U.S. banks and other financial institutions. Ms. Sahni was shortlisted for the 2016 Euromoney Americas Women in Business Law Awards – Best in Financial Regulation. She was recognised as a "Rising Star" by *IFLR 1000* in 2016. Ms. Sahni also advises on corporate governance, OFAC and AML compliance, internal investigations and regulatory enforcement actions.

Sylvia Favretto
Shearman & Sterling LLP
401 9th Street NW
Washington D.C. 20004
USA

Tel: *+1 202 508 8176*
Email: *sylvia.favretto@gmail.com*
URL: *www.shearman.com*

Sylvia Favretto is Counsel in the Financial Institutions Advisory & Financial Regulatory Group of Shearman & Sterling. Her practice consists of providing guidance to domestic and foreign banks on U.S. financial regulatory reform and the U.S. federal banking laws, including providing advice to financial institutions with respect to Dodd-Frank implementation and compliance. Ms. Favretto has worked with various international bank and non-bank financial institutions in connection with their operations in the United States, Bank Holding Company Act compliance, and investment opportunities. Ms. Favretto was recently named a "Rising Star" in the Banking and Financial Services sector by *IFLR 1000* in 2016.

SHEARMAN & STERLING LLP

Shearman & Sterling LLP distinguishes itself by harnessing the intellectual strength and deep experience of its lawyers across its extensive global footprint. The firm is organised as a single, integrated partnership that collaborates to deliver its best to clients. With approximately 850 lawyers in many of the commercial centres around the world, we operate seamlessly across practise groups and offices and provide consistently superior results. Our lawyers come from some 80 countries, speak more than 60 languages and practise US, English, EU, French, German, Italian, Hong Kong, OHADA and Saudi law. We also practice Dubai International Financial Centre law and Abu Dhabi Global Market law. With a deep understanding of our clients' needs, we develop creative ways to address their problems and are ideally situated to counsel them in this challenging 21st century global economy.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com