United States

Paul T Clark, Jeffrey M Berman, Beth H Alter, Casey J Jennings and Nathan S Brownback*

Seward & Kissel LLP

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 | What is the general state of fintech innovation in your jurisdiction?

The United States has been a leader in fintech innovation. Online securities trading, robo-advisers, peer-to-peer (P2P) payment services, platform lenders, mobile banking and other innovations have existed for decades. With many bank and brokerage firm branches closing, either temporarily or permanently, during the pandemic, consumers increased their reliance on online and mobile financial services. The number of trading platforms for digital assets has been increasing, as has the volume of trading. Digital assets have established themselves as an investment class, though the use case for these assets, along with distributed ledger technology, is still evolving.

While the regulatory scheme in the United States is complex, with the jurisdiction of state and federal regulatory agencies frequently overlapping and registration with multiple agencies sometimes required, fintech firms have been able to navigate existing banking and securities regulation without any material changes to the law. State and federal agencies have interpreted existing laws to extend their jurisdiction to protect consumers without stifling innovation. Initiatives to streamline the licensing requirements in certain areas are being considered.

Finally, a substantial amount of venture capital is available to fund fintech start-ups.

Government and regulatory support

2 | Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

Myriad federal and state regulators provide varying degrees of support to financial innovation, taking the form of:

- temporary exemptions from licensing requirements (regulatory sandboxes);
- alternative disclosure requirements;
- formal declarations stating that a given activity complies with existing law; or
- informal discussions and information-sharing arrangements.

Regulatory sandboxes

Arizona, Florida, Nevada, Utah, West Virginia, and Wyoming have all instituted regulatory sandboxes. Financial services providers may apply to the state financial regulator to request exemption from state licensing requirements. Such exemptions are typically limited to a discreet time period. Those admitted to the sandbox must still comply with any applicable consumer protection laws (such as disclosure requirements or interest rate limits) and must agree to share information with the state regulator.

There are no equivalent regulatory sandboxes at the federal level.

Alternative disclosures

The Consumer Financial Protection Bureau (CFPB) has instituted a Trial Disclosure Sandbox in which companies may test for a limited period of time disclosures that financial services providers believe can improve upon existing required disclosures. Companies must share data with the CFPB regarding the effectiveness of the alternative disclosures.

'No-action' determinations

All of the federal financial regulators have instituted formal processes through which financial services providers may provide information regarding their products or services and request a determination from the regulator's staff that such offerings will not be subject to an enforcement action by the regulator for a violation of applicable law. Such 'no-action' relief is not legally binding, but regulators abide by such determinations in practice.

Informal support

The CFPB, Securities and Exchange Commission (SEC), and Commodity Futures Trading Commission (CFTC) have all formally established offices to interact with fintech companies, provide informal guidance and coordinate with non-US regulators. The offices are not, however, endowed with any formal powers to exempt fintechs from existing requirements. The other federal regulators have not established formal offices, but all offer the opportunity for informal discussions with staff members.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

	Agency	Regulated entities
Securities	Securities and Exchange Commission (SEC)	Broker-dealers, investment advisers, securities exchanges
	Financial Industry Regulatory Authority (FINRA)	Broker-dealers
	State securities administrators	Broker-dealers, investment advisers

	Agency	Regulated entities
Banking	Office of the Comptroller of the Currency	National banks
	State banking regulators	State banks
	Federal Deposit Insurance Corporation	State banks, national banks
	Federal Reserve Board	State banks that elect to be a member of the Federal Reserve System, bank holding companies
Money Transmission	State banking regulators	Peer-to-peer (P2P) payment services, issuers of prepaid cards, cryptocurrency exchanges (in some states), others
	Financial Crimes Enforcement Network (FinCEN)	P2P payment services, Issuers of prepaid cards, cryptocurrency exchanges, others
Non-bank Lending	State banking regulators	Non-bank lenders, including non-bank mortgage lenders
	FinCEN	Non-bank mortgage lenders
Consumer protection	Consumer Financial Protection Bureau (CFPB)	Money transmitters, large banks, non-bank lenders, other financial service providers
	Federal Trade Commission (FTC)	Money transmitters, non-bank lenders, other financial service providers

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Activity	Licensing requirement?	Type of regulated entity
Arranging or bringing about deals in investments that are securities	Yes	Broker-dealer
Making arrangements with a view to transactions in investments that are securities	Yes	Broker-dealer
Dealing in investments that are securities as principal or agent	Yes	Broker-dealer
Advising on investments in securities	Yes	Investment adviser
Lending	Yes	Bank, non-bank lender
Factoring	No	N/A
Invoice discounting	No	N/A
Secondary market loan trading	No	N/A
Deposit-taking	Yes	Bank
Foreign exchange trading	No	N/A
Payment services	Yes	Bank, money transmitter

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Consumer lending is regulated at both the federal and state level.

At the federal level, all consumer loans are subject to the Truth in Lending Act (TILA), which requires creditors to provide certain disclosures to consumers regarding the loan, including repayment terms, fees, and interest. TILA imposes additional disclosure requirements on credit cards and mortgage loans secured by a consumer's dwelling. TILA imposes substantive restrictions on mortgage loans.

The Secure and Fair Enforcement for Mortgage Licensing Act (the SAFE Act) mandates a nationwide licensing and registration system for companies that make mortgage loans and for individuals working for such companies.

At the state level, non-bank companies that make consumer loans are typically required to obtain lender licences. Licensing requirements vary by state and also by the terms of the loans offered to consumers; loans with higher interest rates are more likely to require the lender to obtain a state licence.

Most states also have usury laws that prohibit lenders from charging interest higher than a specified amount. Usury limits vary by state and by type of loan.

Secondary market loan trading

6 | Are there restrictions on trading loans in the secondary market in your jurisdiction?

There are no regulatory restrictions on trading loans in the secondary market in the United States, and trading loans is not subject to direct regulatory authority oversight. Trading or holding some loans may, however, be subject to regulation based on the industry, such as the gaming industry, and the trading of loans in those industries may be subject to governmental or regulatory approvals or other legal and regulatory requirements. Loan market participants such as investment advisers are subject to the Custody Rule under the Investment Advisors Act with respect to loans.

Collective investment schemes

7 | Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

An issuer's compliance with applicable laws, rules and regulations will depend on the nature of the issuer's collective investment scheme. Generally, an issuer may have to register a collective investment scheme involving investments in securities under the Investment Company Act of 1940, as amended (the 1940 Act), unless it qualifies for an exemption. Common exemptions from the 1940 Act registration requirements for private funds include sections 3(c)(1) and 3(c)(7), which exempt issuers that have no more than one hundred beneficial owners and whose beneficial securities are owned by qualified purchasers (as defined under the 1940 Act), respectively.

Any person or entity engaged in the business of providing investment advice concerning securities, including those that provide investment advice to collective investment funds, must consider whether they are required to register with the SEC as a registered investment adviser under the Investment Advisers Act of 1940 (the Advisers Act). State investment adviser registration or other regulatory requirements may apply.

An offering of securities, including shares in an investment company, may need to be registered with the SEC under the Securities Act of 1933. Regulation D under the Securities Act provides issuers an exemption from registration requirements if the offering meets the requirements of Regulation D, including limitations on the number or type of investor.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

In the United States, managers of alternative investment funds that invest in securities are 'investment advisers', and they are regulated by the SEC (under the Investment Advisers Act of 1940) or by state regulators. Managers of commodity pools (ie, funds that invest in commodity interests) are commodity pool operators and commodity trading advisers, which are regulated by the Commodity Futures Trading Commission (CFTC) (under the Commodity Exchange Act).

Managers will need to register as investment advisers, commodity pool operators or commodity trading advisers, as applicable, unless an exception or exemption is available. Unregistered investment advisers, commodity pool operators and commodity trading advisers are still subject to certain requirements, which may include reporting requirements or notice filings, payment of fees or other requirements.

Peer-to-peer and marketplace lending

9 | Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

P2P and marketplace lending is regulated at both the federal and state levels. Consumers obtain both types of loans through a fintech provider that connects borrowers and lenders. Loans are either funded by notes sold to investors or by banks, with the loan then purchased by the fintech provider with funds generated by the sale of notes to investors.

Laws that generally apply to all lenders also apply to P2P or marketplace lenders. For the purposes of both federal and state law, a fintech provider may be treated as the 'true lender' even if a bank originated the loan. Additionally, the funding of these loans by investors implicates the securities laws.

At the federal level, applicable lending laws include TILA, the Equal Credit Opportunity Act, privacy laws and advertising and marketing restrictions under the Federal Trade Commission Act.

At the state level, non-bank fintech providers may require a lender licence, and interest rate restrictions will apply and vary by state. As such, certain P2P lenders may be limited in their activities in certain states. Prosper, for example, is not open to residents of West Virginia and Iowa. Meanwhile, residents of Massachusetts, Mississippi, Nebraska and Nevada are ineligible for Payoff, another prominent peer-to-peer lending platform.

Notes sold to investors to fund P2P or marketplace loans are generally securities for purposes of the Securities Act of 1933 and the Securities Exchange Act of 1934. Securities must either be registered with the SEC or be eligible for an exemption. Restrictions on the sales of such securities may also apply.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

At the federal level, the SEC regulates equity-based crowdfunding in the US, including which investors and issuers can participate and how portal operators should conduct business and adhere to reporting requirements. The SEC's Regulation Crowdfunding enables eligible companies to offer and sell securities through crowdfunding. The rules require all transactions under Regulation Crowdfunding to take place online through an SEC-registered intermediary, either a broker-dealer or a funding portal; permit a company to raise a maximum aggregate amount of US$5 million through crowdfunding offerings in a 12-month period; limit the amount individual non-accredited investors can invest across all crowdfunding offerings in a 12-month period; and require disclosure of information in filings with the SEC and to investors and the intermediary facilitating the offering.

Many states have enacted intrastate crowdfunding laws allowing small and emerging companies in these states to raise capital from local, in-state investors through the issuance of securities.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

Invoice trading in the United States is a fairly unregulated industry. Industry associations, including the Secured Finance Network and the American Factoring Association, encourage members to share best practices and provide training and tools to their members. Certain states have recently adopted certain disclosure requirements applicable to invoice trading. For example, in December 2020, SB 5470B, which regulates invoice trading and other alternative forms of financing, was signed into law in New York. This law, which became effective on 21 June 2021, imposes disclosure requirements analogous to TILA, on providers of commercial financing in a principal amount of US$500,000 or less. The law requires disclosure of key transaction terms and the signature of the financing recipient, which may be in electronic form, on all required disclosures before authorising such recipient to proceed with the financing application. A similar law was passed in California in 2018.

Payment services

12 | Are payment services regulated in your jurisdiction?

Payment services and payments services providers are regulated under federal and state law and the rules of private organisations.

Money transmitters, prepaid services providers, money order sellers, and other payment services providers must register with FinCEN and typically must also obtain a licence to operate in each state in which they operate. Each state has separate licensing requirements and there is no multi-state licence.

Electronic payments are subject to the CFPB's Regulation E, which requires certain consumer disclosures and institutes procedures that companies must follow to resolve errors.

The Uniform Commercial Code, as adopted in each state, governs certain non-electronic payment instruments, such as checks.

The rules of the National Automated Clearing House Association govern transfers using the Automated Clearing House network, a method of electronically transferring funds. The rules of the Visa, MasterCard, and Discover card networks govern transfers using those networks.

Open banking

13 | Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

There are no laws or regulations in the United States that require financial institutions to make consumer or product data available to third parties. A consumer may, under US privacy laws, permit financial institutions to share the consumer's data through APIs, but the consumer must provide their specific log-in credentials to permit one financial institution to obtain the consumer's data at another financial institution.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

The SEC defines a 'robo-adviser' as an automated service with respect to investments in securities that takes in investor information to formulate a 'discretionary asset management service . . . through online algorithmic-based programs'. The sponsors of robo-advisers are required to register with the SEC as investment advisers and, as such, are subject to all of the requirements of the Investment Advisers Act of 1940. The SEC has issued guidance on robo-advisers, as well as investor education information on how robo-adviser platforms work.

SEC guidance has emphasised that robo-advisers should be designed to ensure that methods of gathering information and the types of information acquired are sufficient to meet the fiduciary standards of care and loyalty to which registered investment advisers are subject by considering the best ways to disclose risks and tailor advice to investor needs.

Some states have started crafting initiatives to apply fiduciary duties to anyone giving investment advice, even if not classified as an investment adviser under the 1940 Act.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Insurers are solely regulated by individual states rather than at the federal level. Fintech insurance does not yet have an individual regulatory framework and is therefore subject to the same regulatory scheme as conventional insurance sales.

Specifically, insurers are subject to licensing requirements in each state in which they operate. Insurers must meet capital requirements as specified by state statute. These requirements vary by state and type of insurance offered (ie, property insurance, life insurance, etc).

Additionally, the majority of states have adopted some version of the Producer's Licensing Model Act, which requires a licence if a company is attempting to 'sell', 'solicit' or 'negotiate' insurance. Under these licensing acts, 'sell' is understood to include an exchange of money while 'negotiate' includes selling or obtaining insurance on behalf of another purchaser. 'Solicit' includes attempts to sell, which may include quoting insurance rates and offering product recommendations. Most state licensing acts include exceptions where these activities can be conducted without a licence, such as insurance advertisements, which generally do not constitute solicitation.

It remains unclear whether fintech firms providing automated services for customers, such as automated chatbots offering rates, would trigger solicitation or fall under the advertising exception. The National Association of Insurance Commissioners is currently considering the issue.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

The federal Fair Credit Reporting Act (FCRA) governs consumer reports and consumer reporting agencies. A consumer report is any information bearing on the creditworthiness of a consumer and a consumer reporting agency is any entity that sells such a report. The FCRA requires the following:

- a lender must disclose whether a consumer report has been used to deny credit;
- a consumer reporting agency must disclose to a consumer upon request the information on the consumer's report (often, but not always, free of charge);
- a consumer may dispute any incomplete or inaccurate information;
- consumer reporting agencies must correct or delete incomplete, inaccurate or unverifiable information;
- consumer reporting agencies may not report negative information that is more than seven years old or bankruptcies more than 10 years old; and
- consumers must consent if a consumer report is provided to a current or potential employer.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

No. There is no mechanism in the United States for a fintech – or any other entity – that is regulated in a non-US jurisdiction to operate in the United States without the approval of a US regulator if engaged in activities in the United States that subject it to US federal- or state-level regulation. For example, foreign banking organisations may operate branches, agencies, commercial lending companies and representative offices in the United States, but such activities require approval from US state or federal agencies, and are subject to the Federal Reserve Board's Regulation K. Fintech companies that operate as money transmitters or commercial lenders are generally subject to state regulation on money transmission or lending activities made with a jurisdictional nexus to that state (such as, for example, by making loans to residents of the state) regardless of where the fintech company is organised or headquartered.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

Requirements vary from state to state, and a fintech company that engages in regulated activity – deposit-taking, brokerage, investment advice, lending, money transmission, or others – will need to examine state law in each jurisdiction they operate in. In some cases, states will require any business that meets certain minimum contact requirements with the state to establish an agent for service of process. In other cases, whether or not a fintech firm operating in a state has a local presence will affect the licensing or registration process, without necessarily meaning that the state requires a physical local presence. To give one example, the California Department of Financial Protection and Innovation requires licensing for certain commercial lenders, including fintech companies that meet the state's licensing criteria. There is a separate licensing application for California-based lenders than for other lenders.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Federal law prohibits financial institutions from engaging in unfair, abusive or deceptive acts or practices (collectively described as UDAAPs). The prohibitions against UDAAPs are applied by the Federal Trade Commission, the Consumer Financial Protection Bureau and the federal banking regulators to financial institutions within their jurisdiction. False or misleading marketing activities may be deemed UDAAPs.

Financial Industry Regulatory Authority (FINRA) Rule 2210 governs the advertising and marketing practices of broker-dealers. In addition to

prohibiting false or misleading public communications, Rule 2210 also requires broker-dealers in certain cases to submit proposed communications to FINRA for pre-approval.

Fintech firms that are registered investment advisers are subject to the advertising and marketing rule (the Marketing Rule) under the Investment Advisers Act. The Marketing Rule regulates advertisements by the registered investment adviser, including testimonials and endorsements from third parties. In general, the Marketing Rule prohibits marketing materials from including untrue statements of material fact or omit material facts in a way that is misleading. Performance results must be presented in a fair and balanced way.

Additionally, Securities and Exchange Commission Rule 10b-5 prohibits fraud or deceit in connection with the purchase or sale of securities. Rule 10b-5 gives the SEC broad discretion to deem securities marketing activities unlawful.

CHANGE OF CONTROL

Notification and consent

20 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Change in control rules applicable to a regulated fintech entity depends on which regulatory regime applies to that entity. State and federal rules may apply.

At a federal level, for broker-dealers, the applicable self-regulatory organisation, the Financial Industry Regulatory Authority (FINRA), must approve any change of control. For registered investment advisers, the Advisers Act requires that advisory agreements provide for investor consent to a change of control or assignment of an advisory contract.

With respect to state-chartered and national banks, change of control requires filings and approvals under the Bank Holding Company Act, the Change in Bank Control Act and various state laws. The acquisition by a bank holding company of direct or indirect control of more than 5 per cent of the voting shares of a bank requires approval of the Federal Reserve Board, and if any company acquires control of a bank, as the term is defined in the Bank Holding Company Act and regulations thereunder, it becomes a bank holding company subject to the supervision of the Board.

Additionally, the Committee on Foreign Investment in the United States, an interagency group, has the power to review and prevent covered transactions; namely, acquisitions by foreign persons of certain US companies or US real estate that pose or potentially pose national security risks.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

21 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

The Bank Secrecy Act (BSA), initially adopted in 1970, established the basic framework for anti-money laundering (AML) obligations imposed on financial institutions. Among other things, it authorises the United States Department of the Treasury (the Treasury Department) to issue regulations requiring financial institutions and money services businesses to keep records and file reports on financial transactions that may be useful in investigations and the prosecution of money laundering and other financial crimes. Congress has passed other AML laws subsequent to the BSA, including the USA PATRIOT Act, adopted in 2001. The Financial Crimes Enforcement Network (FinCEN), a bureau within the Treasury Department, is the administrator of US AML laws and regulations. The Office of Foreign Assets Control, also a bureau within the Treasury Department, administers US laws governing trade sanctions and terrorist financing.

AML requirements include, inter alia: establishing and following written policies including a customer identification programme, maintaining records of specified transactions, and providing currency transaction reports and suspicious activity reports to FinCEN.

While some fintech firms are not 'covered financial institutions' under the BSA-AML framework, many seek to comply with AML requirements as if they were covered financial institutions. To the extent that the fintech firm partners with a bank, banks may follow their federal regulator's guidance regarding managing third-party risk with respect to vendor relationships by requiring such compliance.

State-registered fintech firms are often subject to state laws requiring AML standards, including, for example, digital asset exchanges that operate with the New York BitLicense.

Guidance

22 Is there regulatory or industry anti-financial crime guidance for fintech companies?

FinCEN regularly issues regulatory guidance on AML and preventing financial crime. Some of these items of guidance relate specifically to fintech firms. For example, a 2019 FinCEN advisory discussed risks resulting from abuse of convertible virtual currencies. It warned that unregistered entities engaged in convertible virtual currency businesses present significant risks of illicit finance even when not deliberately attempting to evade supervision. In particular, FinCEN highlighted darknet marketplaces, unregistered peer-to-peer exchangers, unregistered foreign-located money services businesses, and CVC kiosks as high-risk businesses, and provided examples of law enforcement action by US authorities against each type of convertible virtual currency business.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Loan agreements and security agreements need to be properly authorised by the entity entering into the agreement and executed by an officer or authorised person who has the authority to sign the document on behalf of such entity. Subject to due authorisation, the requirements of the organisational documents of the signing entity and the requirement below, there are no particular requirements in the United States for executing these agreements.

Generally, there will not be any issue with the enforceability of loan agreements and security agreements entered into on a peer-to-peer or marketplace lending platform. Since these agreements will be executed electronically through an online platform, the requirements of applicable statutes relating to electronic signatures (including the Electronic Signatures and Records Act in New York, the Federal ESIGN Act, and the Uniform Electronic Transactions Act(UETA), which has been adopted by 47 states) will apply. An electronic platform that requires a party to affirmatively consent to the documentation and preserves a record of such consent will likely satisfy the requirements of the applicable statute.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

To perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform, a UCC-1 financing statement must be filed in the applicable US jurisdictions naming the assignee as secured party and the assignor as debtor. If the assignment is not perfected by such a filing, the lack of perfection could result in the assignee being treated (1) as an unsecured creditor of the assignor rather than the owner of the assigned loans where the assignor files for bankruptcy in the US or (2) as having a lower priority interest in the loans where the assignor either unethically or accidentally sold the same loans to another party or another party claims to have purchased such loans or be a secured creditor with respect thereto and, in each case, such other party has filed a UCC-1 financing statement evidencing its interest in the loans.

It is possible to assign the loans without informing the borrower; however, until the borrower is notified of such assignment, the borrower would be able to discharge its obligations under the loan by paying the assignor. In such scenario, the assignee would only have recourse against the assignor for such amounts paid by the borrower.

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

Peer-to-peer or marketplace loan securitisations are subject to the risk retention requirements of section 15G of the Securities Act and Rule 15G thereunder, which require the person who organises a securitisation and sells assets to the issuing entity (ie, the sponsor of the securitisation) to retain 5 per cent of the credit risk associated with the securitisation. There are many factors that determine the sponsor of the securitisation and who is required to retain risk in compliance with section 15G and Rule 15G. The structure of the transaction, the holders of the loans being sold into the issuing entity and related financing structure can all impact the identity of the risk retention holder.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

The Gramm-Leach-Bliley Act (GLBA) governs the privacy and security of data processed and transferred by all financial institutions, including fintechs.

A 'financial institution' is defined, for the purposes of GLBA, as a business that is 'significantly engaged' in 'financial activities' as described in section 4(k) of the Bank Holding Company Act. The list of activities that have been deemed financial in nature is extensive and is likely broad enough to capture a special purpose company used to purchase and securitise peer-to-peer or marketplace loans.

GLBA applies to non-public personal information (NPI) of consumers held by financial institutions. 'Consumers' are individuals who are seeking or have obtained a consumer financial product or service. NPI is personally identifiable financial information that is not publicly available and is comprised of data that can reasonably be linked with a given individual. Aggregated or de-identified data is not NPI and is not subject to the GLBA requirements.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTO-ASSETS

Artificial intelligence

27 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

Both the federal government and the states have enacted legislation regarding artificial intelligence and have applied their own definitions of the term. However, neither federal nor state level regulation of artificial intelligence applies in the financial services industry.

Although no broad system of AI regulation exists in the United States yet, federal and local regulations apply to some of underlying activities that AI is used for. For example, in the financial services industry, sponsors of robo-advisers that use AI to provide investment advice concerning securities to customers are required to register with the Securities and Exchange Commission (SEC) as investment advisers.

Distributed ledger technology

28 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

Distributed ledger or blockchain technology is just that: technology. Use of the technology is not subject to financial regulation except when it is used for financial applications, such as evidencing crypto-assets. Blockchain technology has many current applications, and potentially many more in the future, that have nothing to do with financial regulation. For example, blockchain technology can be used as a recordkeeping mechanism, and has been used to keep records of transfers of property, including art and real estate.

Crypto-assets

29 Are there rules or regulations governing the use of crypto-assets, including digital currencies, digital wallets and e-money?

A key question regarding any crypto-asset is whether it constitutes a security. Traditional instruments such as notes, stocks, bonds and other instruments issued for capital raising purposes, including crypto-assets in those forms, are clearly securities. In the United States, the securities laws can also be applied to new or innovative asset classes that meet the definition of a security under the Supreme Court's 1943 *Howey* test: if there is an investment of money in a common enterprise with the reasonable expectation of profits deriving from the efforts of others, there is an investment contract and therefore a security. In 2019, the SEC published a Framework for 'Investment Contract' Analysis of Digital Assets, which explains how the SEC applies the *Howey* test to digital assets. Issuances of digital assets that are securities are subject to the Securities Act of 1933, and secondary market sales of digital assets that are securities are subject to the Securities Exchange Act of 1934.

Transfers of digital assets that are not securities through digital exchanges are often deemed 'money transmission' under federal and state law, and the digital exchanges must in many cases register with Financial Crimes Enforcement Network (FinCEN) as a money services business, and in many states become licensed as money transmitters.

Although users of virtual currencies are generally not regulated, they are subject to taxation with respect to the virtual currency they own and sell, which is treated as property under IRS Notice 2014-21, Virtual Currency Guidance.

Additionally, since 2018, federal courts have upheld the authority of the Commodity Futures Trading Commission (CFTC) to apply its

anti-fraud authority in the spot market for digital currencies that are commodities, and have found specified virtual currencies to be commodities under the Commodity Exchange Act on a case-by-case basis.

Digital currency exchanges

30 Are there rules or regulations governing the operation of digital currency exchanges or brokerages?

Digital currency exchanges in the United States are required to register as money services businesses with FinCEN and to obtain money transmitter licences in states where their activities constitute money transmission. Certain states, like New York, have established licensing regimes designed to apply to digital currency exchanges or other digital currency businesses, although how well the New York BitLicense works for such businesses is an open question.

Digital currency exchanges are not subject to a comprehensive federal regulatory scheme, though the Chairman of the CFTC recently suggested that Congress should consider passing legislation establishing one, to increase market confidence in US digital currency exchanges.

Digital assets that are securities must be traded on an exchange that is registered as an 'alternative trading systems' (ATSs) with the SEC. The SEC has recently approved new ATSs, including, in May 2021, approving the registration of Figure Technologies as an ATS (and a broker-dealer).

Initial coin offerings

31 Are there rules or regulations governing initial coin offerings (ICOs) or token generation events?

The critical question for how ICOs are regulated is whether the coin or token being offered or generated in the ICO constitutes a security or not. An ICO of coin or token that is a security is subject to the US securities laws that generally apply to the issuing and offering of securities.

Around 2016 and 2017, a wave of initial coin offerings or ICOs took place in which the promoter of the offering highlighted the 'utility' of the coin or token to attempt to distinguish the token from a security. In December 2017, then-SEC Chair Clayton issued a Statement on Cryptocurrencies and Initial Coin Offerings, setting forth the SEC's position that while it is possible for a coin or token to be outside the scope of the US securities laws, most ICOs with which the SEC was familiar at that point were, in fact, offerings of securities. The SEC takes a case-by-case approach to evaluating whether a coin or token issued in an ICO is a security.

DATA PROTECTION AND CYBERSECURITY

Data protection

32 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The Gramm-Leach-Bliley Act (GLBA) governs the privacy and security of data processed and transferred by all financial institutions, including fintechs. GLBA applies to non-public personal information (NPI) of consumers held by financial institutions. 'Consumers' are individuals who are seeking or have obtained a consumer financial product or service. NPI is personally identifiable financial information that is not publicly available and is comprised of data that can reasonably be linked with a given individual. Aggregated or de-identified data is not NPI and is not subject to the GLBA requirements.

Generally, under GLBA:

- a financial institution may not share NPI with non-affiliated third parties without first providing a consumer with notice and an opportunity to opt-out of the sharing;
- a financial institution must provide initial and annual notices to customers describing their privacy policies, including the type of data processed and shared, with whom the financial institution shares NPI, and the financial institution's data security policies; and
- a financial institution must protect the security and confidentiality of NPI.

There are no additional specific restrictions on consumer data transfers from the US to another country. Consumer data may generally only be transferred from the EU to a US third party if the US third party agrees to the Standard Contractual Clauses adopted by the European Commission.

Some states, such as California, have adopted privacy laws that govern the use of data of those states' residents. However, those state laws typically exempt data that is subject to GLBA.

Cybersecurity

33 What cybersecurity regulations or standards apply to fintech businesses?

GLBA is the primary federal law governing the security of data collected and processed by all financial institutions, including fintechs. GLBA requires financial institutions to develop a written information security plan (WISP) and:

- designate one or more employees to coordinate the WISP;
- identify and assess the risks to NPI and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards programme, and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, including contractual requirements to maintain safeguards, and oversee their handling of NPI; and
- evaluate and adjust the programme as needed.

Some states have adopted laws governing data security, which generally apply to businesses, including fintechs, with consumers in those states. Massachusetts has adopted the most stringent law, which includes all of the data security requirements of GLBA listed above, while further imposing specific data security protocols, including encryption of all consumer data at rest or in transit.

Additionally, numerous states have adopted data breach notification laws, which require companies (including fintechs) with consumer data that has been subject to unauthorised access to notify affected individuals and, in some cases, notify the relevant state regulator or chief law enforcement officer.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

34 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Legal requirements and regulatory guidance relating to outsourcing of a material aspect of a financial services business depend on the type of financial services business, but in general, federal and state regulators place limits and impose requirements when certain functions are outsourced. These requirements generally provide that the outsourcing of functions to third parties requires oversight of those third parties, and that the financial services firm continues to be responsible for its own compliance with applicable laws.

The federal banking agencies have issued guidance relating to mitigating risks arising from the use of third-party vendors generally.

For example, the Federal Reserve Board (FRB) has published SR 13-19, Guidance on Managing Outsourcing Risk, which provides methods for financial institutions to evaluate their contracts with third-party service providers and to mitigate risks related to using such services. Collectively, through the Federal Financial Institutions Examination Council (FFIEC), the federal banking agencies have also issued guidance on outsourcing technology services and on banks' supervision and management of relationships with technology services providers (TSPs). Such TSPs are often fintech firms providing technology services in coordination with the bank.

With respect to broker-dealers, the Financial Industry Regulatory Authority's NASD Notice to Members 05-48 provides that outsourcing to a third party any function that would require that third party to register as a broker-dealer means that the third party will be treated as an associated person of the broker-dealer, and that broker-dealers are not relieved of responsibility for compliance with legal requirements relating to outsourced services.

Cloud computing

35 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

The use of cloud computing by financial services firms raises issues relating to data privacy and data protection, because a cloud computing environment entails a third-party servicer creating information systems for and hosting consumer data on off-site servers.

Federal financial services agencies have published guidance on cloud computing in the financial sector including the FRB's SR 13-19 and the FFIEC Statement on Security in a Cloud Computing Environment (2020) (the FFIEC Statement). SR 13-19 and the FFIEC Statement apply to state-chartered and national banks.

The use of cloud computing by financial institutions also raises issues relating to business continuity. A disruption in service or cyber-attack on a cloud-based, third-party network could cause serious problems for a financial institution and its customers. Financial institutions are required to create and maintain business continuity plans and protections for their IT systems. Banks, broker-dealers, and investment advisers are all subject to regulations requiring business continuity plans from their respective federal regulators.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

36 Which intellectual property rights are available to protect software, and how do you obtain those rights?

There are three primary types of intellectual property rights available to protect software: copyright, trade secret and patent.

Copyright

Copyright protects software code in certain circumstances but does not protect the underlying idea or functional expression of software. To be protectible under the copyright laws, the code must constitute an original work of authorship fixed in a tangible form of expression. Software code is fixed for purposes of copyright protection when it is in a medium that allows it to be perceived either directly or with the aid of a machine or device.

Copyright protection exists from the moment software code is fixed in a tangible form of expression. It is not necessary to register a copyright in order to obtain copyright protection. Copyright registration does have several benefits, however, including creation of a public record; the right to sue for infringement; the availability of statutory damages; and other benefits. Registering the copyright in software code requires a completed application form, as well as a filing fee and nonreturnable deposit submitted to the Copyright Office.

Trade secret

Software may be protected as a trade secret provided that the software is kept secret and that the secrecy gives the owner of the software a competitive advantage. Registration is not required to obtain trade secret protection.

Patent

Patent protection may be available for software-implemented inventions or business methods in certain circumstances. Patent rights are obtained through registration.

IP developed by employees and contractors

37 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Generally, the copyright in a work belongs to the person who created the work. However, when employees have created a work within the scope of their regular employment duties the employer is considered the author and copyright owner of the work unless the parties have agreed otherwise in writing.

In the case of works developed by a contractor or consultant, the hiring party will be considered the author and the copyright owner of the work if: (1) the parties expressly agree in a signed written instrument that the work is a 'work made for hire', and (2) the work was specially ordered or commissioned for use as one of nine categories of works set out in the copyright code. In the absence of these criteria, the contractor or consultant is considered the author and copyright owner. Alternatively, contractors and consultants may agree in writing to assign their rights to the hiring party.

Joint ownership

38 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Joint owners each have an independent right to use, distribute, copy and grant non-exclusive licences to any work of which they are a joint owner. In the case of copyrights, joint owners have a duty to account to their fellow joint owners for any profits made. A joint owner, however, can only transfer their own rights, not those of another joint owner, and cannot grant an exclusive licence to any third party without the approval of their fellow joint owners. Joint owners are free to change any of these rights by way of written agreement.

Joint owners of a trademark have unlimited rights to use the mark just as if ownership were vested in a single person or entity. However, joint ownership of trademarks is generally discouraged since a trademark is supposed to identify and distinguish a single source of products and services. The law is unsettled as to the extent to which a joint owner of a trademark may assign their entire interest without the approval of their fellow joint owners.

Trade secrets

39 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Companies protect their trade secrets by requiring employees, consultants, service providers and business counterparties to enter into

non-disclosure agreements preventing the unauthorised use or disclosure of confidential and proprietary information and trade secrets. Employees and consultants also will be required to enter into intellectual property assignment agreements to ensure that the company is the owner of any works created by the individual in connection with their services to the company. Companies will also implement internal controls at their physical work site as well as on their computer networks and company-owned hardware to limit access, use, copying and removal of sensitive materials. Federal and state statutes may provide a private right of action for theft of trade secrets.

During court proceedings, trade secrets may be protected by seeking to limit the scope of discovery, by entering into confidentiality agreements with opposing parties, or by seeking court orders to permit the filing of sensitive materials under seal or to close the courtroom to the public for portions of the legal proceedings. Local rules and statutes will define the parameters a court will consider when deciding whether to seal documents or close the courtroom to the public. Generally, however, a court will balance the public's common-law right of access to judicial proceedings against the trade secret owner's right to maintain the secrecy of its proprietary information in determining whether to grant a litigant's motion to seal court filings or close the courtroom.

Branding

40 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Obtaining a federal trademark registration is one of the best ways to protect branding. A trademark is a word, phrase, symbol, design or other indicia of ownership, or any combination thereof, used to identify and distinguish the source of a product or service. The owner of a trademark can prevent third parties from using the same or a confusingly similar mark to sell the same or related products or services as those of the owner.

In the US, trademark rights are generally acquired through use of the mark in commerce. However, ownership of a federal trademark registration confers significant advantages over relying on unregistered rights. Among others, these advantages include the following:

- a presumption that the registrant has the exclusive right to use its mark throughout the entire United States;
- presumptions that the registrant owns the mark and that it is valid;
- the registration entitles the owner to file actions concerning the mark in federal court; and
- the registration entitles the owner to enhanced damages if successful in an infringement action.

Registration is obtained by filing an application with the US Patent and Trademark Office.

To avoid infringing existing brands, a trademark search should be conducted prior to adopting a mark or filing an application to see if any identical or confusingly similar brands already exist.

Remedies for infringement of IP

41 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

The remedies available for IP infringement are injunctions, monetary damages – both actual damages and statutory damages – attorney's fees and seizure of the infringing goods. There may also be criminal sanctions for certain violations.

The remedies available for IP infringement are injunctions, seizure of the infringing goods, monetary damages – both actual damages and statutory damages – and attorney's fees. There may also be criminal sanctions for certain violations.

Courts may grant an injunction if a copyright or patent owner establishes that:

- the plaintiff suffered irreparable harm;
- the plaintiff's purported injury outweighs the damage an injunction would inflict on the defendant; and
- an injunction is not counter to public interest.

Once a plaintiff establishes infringement, an injunction can be either temporary or permanent; courts generally grant permanent injunctions where there is evidence of past infringement and a strong likelihood of future infringements. Additionally, during an infringement proceeding, courts may take into custody any copies or records of the infringing goods as deemed reasonable and can order the destruction or disposition of such goods as part of its final judgment.

A copyright owner is entitled to recover the actual damages suffered as a result of the defendant's infringement plus the defendant's profits attributable to the infringement. Plaintiffs may also elect to seek statutory damages. Copyright owners may seek between US$750 and US$30,000 before a final judgment, as determined by the court. Alternatively, if the copyright owner successfully establishes willful infringement, the court may award up to US$150,000 at its discretion. If the infringement was not willfully committed, the court in its discretion may reduce the statutory damages to as little as US$200. Courts may also award reasonable attorney's fees to the prevailing party. If the court determines the infringement was willful, criminal punishments including fines and prison sentences up to 10 years may be ordered.

COMPETITION

Sector-specific issues

42 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

Fintech merger activity has drawn considerable attention from the antitrust division of the Department of Justice over the past year. A speech by then-assistant attorney general Michael Murray in October 2020 described a 'muscular role for antitrust' in fintech as well as banking and financial services generally. The antitrust division has followed through. In 2021, Visa announced the cancellation of its planned acquisition of Plaid, Inc and cited antitrust objections from the DOJ. (Plaid provides a technology platform that allows apps to connect to customer bank accounts.)

In January 2021, the antitrust division reorganised a new unit focused on antitrust enforcement in the financial services sector, the Financial Services, Fintech, and Banking Section. Antitrust scrutiny of the fintech industry is likely to increase going forward.

TAX

Incentives

43 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

The federal government does not provide specific incentives to fintech companies. General R&D tax credits are available for a variety of investments including fintech development.

Certain states have programmes designed to support start-ups (and small businesses) generally but none are specifically geared to the fintech sector, including funding, tax credits, incubator space and partnerships with other businesses, direct government financing, direct

and indirect private investment incentives, R&D credits, Small Business Innovation Research and Small Business Technology Transfer Grant Program-related incentives, and sales or use tax and property tax exemptions.

Increased tax burden

44 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

The United States federal income tax (USFIT) law that generally took effect in 2018 reduced the USFIT rate from 35 per cent to 21 per cent. The current presidential administration has sought to raise these rates.

For technology companies, an incentive rate of 13.125 per cent may apply to intangible-based business income of a US corporation that is earned from sources outside of the United States. This incentive rate, coupled with a new penalty tax meant to discourage investment in the technology sector outside of the United States, was introduced as part of the 2018 law with the intent of increasing technology investments in the United States. The incentive rate is scheduled to become less generous beginning after 31 December 2025, and the penalty tax is scheduled to become more severe at the same time.

The G7 nations have recently agreed to a global minimum 15 per cent tax. These changes will mostly affect the largest multinationals but could have implications on fintech companies as they reach global scale.

IMMIGRATION

Sector-specific schemes

45 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

The US Department of State overseas a 'first preference' list with respect to immigration into the United States pursuant to employment-related visas. None of the top preferences are specifically related to employees of fintechs as a class. However, there may be many officers and employees of fintech firms who can meet one or more of the preference criteria. The preference levels most likely to be applicable to officers or employees of fintech firms are as follows:

- First preference: 'Persons with extraordinary ability' in, among other areas, sciences or business; outstanding professors and researchers, and multinational managers or executives of a non-US affiliate of a US employer.
- Second preference: Professionals holding an advanced degree and 'persons with exceptional ability' in, among other areas, sciences or business.
- Third preference: Workers whose jobs require a minimum of two years of training or work experience, or professionals with a baccalaureate degree or its equivalent.

Other immigration categories may apply, depending on the circumstances of a given potential immigrant, including a category for immigrant investors.

SEWARD & KISSEL LLP

Paul T Clark
clark@sewkis.com

Jeffrey M Berman
bermanj@sewkis.com

Beth H Alter
alter@sewkis.com

Casey J Jennings
jennings@sewkis.com

Nathan S Brownback
brownback@sewkis.com

901 K Street NW
Washington, DC 20001
United States
Tel: + 1 202 737 8833
Fax: +1 212 480 8421

One Battery Park Plaza
New York, NY 10004
United States
Tel: +1 212 574 1200
Fax: +1 212 480 8421

www.sewkis.com

UPDATE AND TRENDS

Current developments

46 Are there any other current developments or emerging trends to note?

Both the new administration and the ongoing effects of the coronavirus pandemic have impacted, and will continue to impact, the fintech industry.

On 20 January 2021, Joseph Biden was sworn in as the new President of the United States, replacing Donald Trump. A new President has the authority to appoint various officials to regulatory agencies and change the direction of the agencies. It is possible that Biden appointees to the Office of the Comptroller of the Currency (OCC), the Consumer Financial Protection Bureau and the Securities and Exchange Commission, among other agencies, will change the approach of these agencies to fintech, including digital assets. The OCC may withdraw its support for a fintech banking charter and be less vocal in its advocacy of digital assets. The Federal Deposit Insurance Corporation may be more reluctant to approve insurance applications for certain banking charters that fintech companies prefer to utilise.

As the United States sheds the restrictions imposed during the pandemic, banks may choose to close, or choose not to re-open, branches because consumers have been willing to utilise mobile banking services. A cautionary note: personal loans originated by major fintech lending platforms significantly decreased during the pandemic, while origination increased at traditional banking organisations. Customers may be signalling their preference for personal service over ease of access.

Coronavirus

47 What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programmes, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

Coronavirus relief legislation was one of the top, if not the top, priorities of Congress in 2020 and 2021. Three pieces of major legislation – the 2020 CARES Act, the 2020 Omnibus Appropriations Act and the 2021 American Rescue Plan Act – either included or centred on coronavirus relief for individuals, states and other local governments, as well as businesses. A number of coronavirus relief programmes targeted small businesses in particular. While none of these laws applied exclusively to fintech firms, any fintech firm that met the criteria in the legislation was eligible. For example, the 2020 CARES Act's Paycheck Protection Program was designed to provide loans for small businesses to maintain payroll costs. The Emergency Injury Disaster Loan Assistance programme allowed businesses to take out loans for business operating expenses, and also allocated portions of available funds toward small businesses.

* *The authors acknowledge and appreciate the contributions of Jack Yoskowitz, Daniel Bresler, Daphne Coelho-Adam, Julia Spivack, Jessica Cohn, Joseph Nardello, and Warren Samlin.*