Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering comparative analysis from top-ranked lawyers

Fintech

USA: Law & Practice

Alex Drylewski, Jeffrey Brill, Heather Cruz, Sven Mickisch and Stuart Levi
Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates

practiceguides.chambers.com

2021

USA

Law and Practice

Contributed by:
Alex Drylewski, Jeffrey Brill, Heather Cruz, Sven Mickisch and Stuart Levi
Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates ***see p.16***

CONTENTS

1. FINTECH MARKET

1.1 Evolution of the Fintech Market

"Fintech" is a broad term that captures a wide range of activities and business models involving the use of technology in the delivery of financial services. Fintech can be used in reference to virtually every subsector of financial services, including the front, middle and back-office functions of banking, non-bank lending, insurance, securities and investment management, derivatives, blockchain, cryptocurrency, compliance and risk management.

COVID-19 Causes Decrease in Venture Investment, but after Several Strong Years

The impact of COVID-19 negatively affected US deal-making activity in 2020, including in the fintech space. The first half of 2020 bore the biggest brunt of the COVID-19 pandemic, which saw a significant decrease in venture investments. But this decline appears dramatic only because of just how robust venture activity had been in the fintech sector over the past few years. Despite a global decrease in investment activity and uncertainty resulting from the impact of the COVID-19 pandemic, total venture investment in fintech in the United States still remained above 2017 levels, even during the worst of the crisis, with USD9.3 billion of total investment in the first half of the year.

Despite significant headwinds arising from COVID-19, the pandemic has not fundamentally changed the factors that have made fintech attractive to many investors and, in fact, has accelerated existing trends towards digitisation and automation. And this was borne out in the second half of 2020, which demonstrated a rebound in activity from the first half of the year. The third quarter witnessed the largest total investment in fintech start-ups in a quarter since mid-2018 and the fourth quarter marked a record high quarterly deal volume, with 435 transactions totalling USD117.4 billion in value, marking a 169% increase in deal volume from Q4 2019, with 216 transactions and USD43.7 billion in deal volume.

Much of this money is being invested in later-stage fintech firms, demonstrating the continued maturation of the US fintech market. However, this activity is not just limited to the unicorns of the fintech world. In a promising sign for a strong fintech pipeline going forward, venture investments in angel or seed rounds in the third quarter of 2020 grew by 20% compared to the second quarter of the year.

Like in 2019, much of this investment activity came from corporate venture investors, reflecting a continuing view among corporations that the fintech space represents an important strategic priority in which to invest their capital.

Pandemic Emphasises Attractions of Fintech

The pandemic is accelerating certain trends that make the fintech space attractive. Since the start of the pandemic, consumer demand for remote/digital banking has accelerated as the utilisation of ATMs, cash and in-person banking has decreased, trends that seem unlikely to reverse. To adapt to the change in consumer preferences, traditional bricks-and-mortar businesses need digital platforms to quickly shift to online retail operations to both retain existing customers and grow their customer base.

Investors are also drawn to fintech firms in part due to the lean operating models and structures: the total cost of operation of a fintech firm may be as much as 70% lower than for a legacy bank with a large branch network. A lower cost profile is attractive for corporates that are always seeking leaner operating models, especially in times of economic uncertainty. Further, innovations in artificial intelligence (AI) and machine learning abound, enhancing fintech firm offerings and adoption. That investments continued to pour into the fntech space during the pandemic is a further testament to the importance corporate investors attribute to growth in the fintech space for the future of finance.

Fintech Funding Rounds Set to Drive M&A Activity

As the US economy emerges from the COVID-19 pandemic, the authors expect to see more funding rounds in 2021 throughout the various stages of a fintech firm's funding cycle, which has the potential to fuel the M&A market for the foreseeable future.

However, while the authors think the more important long-term narrative is the rebound in fintech investment in the second half of the year, the difficulties faced by fintech firms in the first half of the year present important considerations for companies and investors. Pre-pandemic, there were already concerns that some fintech firms may not increase their already high valuation in their next financing round and could be forced to raise funds at a lower implied equity value than in prior rounds (a "down round"). And the impact of COVID-19 highlighted those concerns, causing investors to increasingly approach investments conservatively.

The economic and governance rights of existing investors proved important as the pandemic disrupted business and operation models because existing investors are seeking to avoid economic dilution and maintain their pre-existing governance rights in a down round. The authors believe this will continue to be important as the industry matures, and

as investors have experienced actual down rounds. In last year's version of this chapter, the authors noted – anecdotally – that they were aware of several fintech companies at risk of down rounds during 2019. This proved true in 2020, as valuations for late-stage venture investments decreased by 7.5% compared to 2019 levels.

Fintech sector M&A started 2020 with a bang and quickly cooled as the COVID-19 pandemic took hold. In the first quarter, 300 transactions were announced with USD80.6 billion in deal volume, compared to 309 transactions with USD13.9 billion in deal volume announced in the second quarter. Fintech M&A bounced back in the third quarter, with 265 transactions announced and USD36.7 billion in deal volume, and soared to a record high in the fourth quarter, with 435 transactions and USD117.4 billion in deal volume, accounting for 47% of the total annual deal volume.

A major tailwind to fintech M&A in 2020 was the rise in prevalence of special purpose acquisition vehicles (SPACs) – a publicly listed shell company formed for the purpose of acquiring an existing business. Acquisition by a SPAC is generally less burdensome than effecting an IPO while achieving public listing. Fintech firms were a favoured target of SPACs in 2020: there were nine acquisitions of fintech firms by SPACs in the first three quarters of 2020, compared with two in all of 2019. The authors expect the SPAC trend to continue in 2021 and, as of the time of writing this chapter, a SPAC business combination with SoFi for USD8.65 billion had been announced.

Increasing Focus on Stablecoins as Industry Matures

Traditional forms of investment in blockchain projects continued to advance in 2020 as the industry showed signs of maturing from the "initial coin offering" (ICO) period of 2017 and 2018. Much of the investments continue to be for funding development projects for the underlying blockchain technology, but an increasing number of projects are focused on stablecoins, in which a cryptocurrency is pegged to a fiat currency or other digital assets to stabilise its value or is stabilised through a computer algorithm. Projects to "tokenise" non-digital tangible assets such as real estate and securities are also attracting increased investment by traditional sources of funding, as are projects in the decentralised finance (DeFi) space. In addition, cryptocurrencies such as bitcoin continue to attract attention. It remains to be seen which, if any, of the hundreds of available cryptocurrencies will survive and become true mediums of exchange.

For further discussion of the blockchain and digital asset regulatory environment, see **12. Blockchain**.

2. FINTECH BUSINESS MODELS AND REGULATION IN GENERAL

2.1 Predominant Business Models

Fintech includes a wide range of activities across the traditional subsectors of financial services, including banking, non-bank lending, insurance, securities and investment management, derivatives, blockchain, cryptocurrency, compliance and risk management. The business models employed by fintech companies also vary widely.

For example, in the consumer credit space, many non-bank fintech companies will follow one of two basic business models: obtaining various state-based licences in order to act as principal or acting as a service provider to an unaffiliated bank. Each of these basic business models has advantages and disadvantages, and there are many variations of them. In addition, fintech companies are increasingly pursuing the formation or acquisition of bank charters. Banks are generally exempt from state-based licensing requirements, and they are able to accept Federal Deposit Insurance Corporation (FDIC)-insured deposits, which is an attractive form of funding. However, banks, their parent companies and their affiliates are subject to a comprehensive additional layer of regulation and supervision.

2.2 Regulatory Regime

Like the fintech sector itself, the US legal and regulatory regime governing financial services and fintech is complex and not unified. Numerous governmental and regulatory bodies often have varying, overlapping and sometimes ambiguous jurisdiction over different types of entities and activities.

In many cases, fintech companies are subject to legal and regulatory requirements arising under both federal law and the differing laws of the 50 individual states. These requirements are rapidly evolving, as legislatures, regulators and law enforcement agencies adapt the legacy regulatory framework to address innovative and non-traditional products, services and delivery channels. The need to identify, monitor and comply with this disparate and evolving US regulatory framework can be challenging for many fintech companies.

2.3 Compensation Models

Compensation models vary significantly across fintech, depending on the life-cycle stage of the fintech company, the nature of its activities, and any regulatory requirements or guidance. The regulatory requirements or guidance vary significantly based on the subsector and nature of service

being provided. For example, federal securities laws and state insurance laws have important provisions related to the receipt or sharing of commissions. Banking regulators also have guidance related to sound incentive compensation practices.

2.4 Variations between the Regulation of Fintech and Legacy Players

As a legal matter, the US financial regulatory framework is generally driven by the nature of a company's activities–and not whether the company is styled as a fintech company or a more traditional legacy player. This aspect of the US financial regulatory framework has been a challenge for many fintech companies, the activities of which may not fit neatly into one of the traditional "silos" of US financial regulation (eg, banking, securities, insurance). The culture of rapid innovation, trial-and-error approach and risk appetite that often exist within fintech companies can also be in tension with the more conservative approach taken by financial regulators, who generally expect formal written policies and procedures, testing, and robust compliance and internal control infrastructure to be in place before an initiative is launched.

2.5 Regulatory Sandbox

A number of US regulatory agencies have formed offices or announced initiatives related to fintech.

For example, the Consumer Financial Protection Bureau has adopted several processes by which fintech and other companies can seek no-action relief, compliance assistance, or a sandbox safe harbour for contemplated consumer-oriented financial services. The Securities and Exchange Commission (SEC) has formed a Strategic Hub for Innovation and Financial Technology to encourage responsible innovation in the financial sector, including in evolving areas such as distributed ledger technology and digital assets, automated investment advice, digital marketplace financing, and AI and machine learning. The Office of the Comptroller of the Currency has also formed an Office of Innovation. And California reorganised and renamed its principal financial regulatory agency to become the California Department of Consumer Protection and Innovation with an Office of Financial Technology Innovation.

The substance, maturation and industry utilisation of these various governmental initiatives have varied widely.

2.6 Jurisdiction of Regulators

For any particular fintech company, the relevant US regulatory agencies will depend on the legal characteristics of the company and the nature of its activities. For example, banking organisations are subject to federal regulation by one or more of the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, or the Federal Deposit Insurance Corporation. The issuance and sale of securities, broker-dealers and investment advisers are subject to federal regulation by the SEC and self-regulatory organisations, such as the Financial Industry Regulatory Authority (FINRA). Commodities and certain derivatives activities are subject to federal regulation by the Commodity Futures Trading Commission (CFTC).

Other federal agencies are charged with the enforcement of federal laws related to certain subject areas, such as the Consumer Financial Protection Bureau (consumer protection), the Financial Crimes Enforcement Network (anti-money laundering), the Office of Foreign Assets Control (economic sanctions) and the Committee on Foreign Investment in the United States (foreign investments that may affect national security).

State laws are also highly relevant to fintech companies. These laws vary significantly from state to state. And the policy objectives and priorities of state governments also vary significantly from state to state. Some state financial regulators, such as the New York State Department of Financial Services and the California Department of Financial Protection and Innovation, have been very active in their licensing, supervision and enforcement activities.

2.7 Outsourcing of Regulated Functions

Outsourcing of activities and functions by regulated financial institutions is very common in the United States. Indeed, the business model and legal structure for many fintech companies is predicated on the fintech company acting as a third-party service provider to a regulated financial institution, such as a bank.

The outsourcing model has regulatory implications for both the regulated financial institution and its fintech service provider. For example, services or activities performed by a non-bank company for a US bank are generally subject to examination and enforcement by the federal banking regulators to the same extent as if those outsourced services or activities were performed by the bank itself. Federal banking regulators have also promulgated extensive guidance to banking organisations related to third-party and vendor risk management.

2.8 Gatekeeper Liability

No information is available in this jurisdiction.

2.9 Significant Enforcement Actions

Financial services companies, including fintech companies, are regularly the target of enforcement action by the US regulatory agencies and law enforcement. These actions can include substantial monetary penalties, requirements to reimburse customers or counterparties, requirements to take remedial action and change business practices, and loss of licence. Particular areas of current enforcement focus include consumer protection, privacy, anti-money laundering and economic sanctions, cryptocurrency and cybersecurity.

2.10 Implications of Additional, Non-financial Services Regulations

The US financial services laws and regulations are regularly changing. In addition, leadership changes at a key agency can also have a significant effect on that agency's supervisory and enforcement priorities. For example, it is expected that the Consumer Financial Protection Bureau under the Biden administration will be far more aggressive in its consumer protection rule-making and enforcement activity.

2.11 Review of Industry Participants by Parties Other Than Regulators

Fintech companies may be subject to review not only by applicable regulators, but also by the regulated financial institutions that they serve, major shareholders and auditors. If a fintech company seeks to raise capital or conduct merger or acquisition activity, it may also be subject to due diligence by its prospective investors, potential acquirers, underwriters or financial advisers. This type of diligence often includes a review of the fintech company's regulatory posture and compliance programme.

2.12 Conjunction of Unregulated and Regulated Products and Services

No information is available in this jurisdiction.

3. ROBO-ADVISERS

3.1 Requirement for Different Business Models

Robo-advisers use algorithms based on a variety of inputs – such as the investor's age, investable assets, investment horizon, risk tolerance and other factors – combined with modern portfolio theory-based investment strategies to provide wealth and investment management services without the human element of, and typically at a lower cost than, a traditional financial adviser.

Traditional financial advisers and robo-advisers provide similar types of services, and therefore both (to the extent that they provide advisory services in the USA) are typically registered as investment advisers with the SEC or one or more state securities authorities. Both must also comply with the securities laws applicable to SEC or state-registered investment advisers. The staff of the SEC's Office of Compliance Inspections and Examinations (OCIE) has provided guidance that, as a statutory fiduciary, when an investment adviser has the responsibility to select broker-dealers and execute client trades, each has an obligation to seek to execute securities transactions for clients in such a manner that the client's total costs or proceeds in each transaction are the most favourable, taking into account the circumstances of the particular transaction.

As a general matter, many robo-advisers tend to focus on exchange-traded fund (ETF) investments, which reflects the increasing preference among the next generation of investors for low-cost, passive, diversified investments. The clients of robo-advisers tend to be younger, cost-conscious, hands-off investors who may initially have less capital available to invest. Because of the increased online presence of this next generation of investors, robo-adviser business models focus more on addressing the needs of their clients primarily through a greater online and social media presence. Many legacy players themselves have built their own robo-advisers, so they are able to offer a comprehensive set of products and services that appeal to a wide variety of investors.

Given the increasing role of electronic advice among providers of wealth and investment management services, OCIE has indicated in its examination priorities for 2021 that one of its areas of focus will continue to be on robo-advisers, in particular with respect to SEC registration eligibility, cybersecurity policies and procedures, marketing practices, and adherence to fiduciary duty, including adequacy of disclosures and effectiveness of compliance programmes.

3.2 Legacy Players' Implementation of Solutions Introduced by Robo-Advisers

No information is available in this jurisdiction.

3.3 Issues Relating to Best Execution of Customer Trades

No information is available in this jurisdiction.

4. ONLINE LENDERS

4.1 Differences in the Business or Regulation of Loans Provided to Different Entities

Many online lenders are organised as non-bank entities. Lending activities by non-banks are governed not only by federal laws, but also significantly by state laws. Non-bank lenders must be mindful of the jurisdictions where their borrowers and applicants are located, as this factor significantly affects the legal and regulatory requirements applicable to the lender.

It is understandably difficult for regulators to keep pace with the rapid changes in online lending technologies. As such, the manner in which regulatory regimes are applied to online, mobile and other innovative delivery channels is evolving and often uncertain. Some states and federal authorities have amended their laws or regulations in this area, but those changes have often been incremental. The principal objective of these changes is the protection of borrowers and other customers. Although some laws apply only to consumer-purpose or residential mortgage lending, some key provisions generally apply to all types of lending, albeit sometimes with different specific parameters. For example, most types of non-bank lending are subject to maximum interest rates established under state law (usury rates), fair lending laws, data security requirements and the federal prohibition on engaging in unfair or deceptive acts or practices (UDAP).

State laws include non-bank licensing requirements that vary significantly from state to state. Even within a single state, the licensing requirements tend to vary based on the type of lending and the type of activity (eg, lending, servicing, brokering, collections). In many states, licensing of non-banks is required only for consumer or real estate-oriented lending activities. However, there are a smaller number of states (including California) that require licensing even for business-oriented, non-real estate lending.

Licensed non-bank lenders are generally subject to supervision, examination and enforcement jurisdiction of the state regulator where they conduct business, which is typically the state banking authority. The regulatory regime for such non-bank lenders differs from that applicable to banks. For example, licensed non-bank lenders are generally not subject to bank-like regulations regarding capital and liquidity, service to the community under the Community Reinvestment Act and deposit insurance assessments.

Many online lenders in the USA that are organised as non-bank entities have partnered with an unaffiliated bank. This bank partnership model seeks to take advantage of certain regulatory advantages (eg, federal pre-emption of state-by-state licensing and usury limits) and operational features (eg, access to traditional card and payment systems) available to banks. The specifics of each bank partnership vary and must navigate risks related to a complicated and fact-sensitive interplay of federal and state laws (eg, "true lender" risk).

4.2 Underwriting Processes

In recent years, online lenders and other industry participants have begun to employ a growing variety of underwriting models. Lenders are implementing advanced algorithms and AI in their underwriting processes to evaluate the credit of consumers, small businesses and other borrowers. These processes rely on a variety of data, such as FICO credit scores, bank transaction data, model-based income, social media, rent history, employment history, phone-number stability, browsing history and behavioural data. Federal and state laws have been slow to keep pace with technological developments used in the underwriting credit models.

Lenders (particularly when lending to consumers) should be mindful that the application of many federal and state laws to new and innovative types of underwriting inputs is evolving and uncertain. For example, the use of non-traditional data sources or automated processes could result in an unforeseen or unintentional "disparate impact" on a protected class of borrowers or applicants and create a potential risk under fair lending laws or a risk of UDAP.

4.3 Sources of Funds for Loans

Lenders rely on a variety of funding sources for loans, including deposits, peer-to-peer, lender-raised capital and securitisations.

Non-bank entities are not permitted to accept deposits. Therefore, banks are unique in their ability to accept deposits as a source of funding. Because they are generally insured by the FDIC, deposits are generally viewed as a stable and low-cost source of funding. Banks are subject to extensive supervision, regulation and enforcement from the applicable federal and state banking regulators. Nonetheless, non-bank lenders have been exploring bank charters, such as the Office of the Comptroller of Currency's FinTech Charter and industrial bank charters, which may provide benefits to their specific business models that outweigh the costs associated with being a regulated bank.

As compared to banks, non-bank lenders generally have more limited balance sheet capacity and may rely more on funding from sources such as equity raises, long-term debt,

secured borrowing, securitisations and peer-to-peer funding. Marketplace lenders have historically employed a peer-to-peer funding model, where specific loans are funded mostly by individual investors. Securitisation is also a significant source of funding for non-bank lenders. Securitisation requires an assessment of applicable federal and state securities law, and generally requires extensive disclosure to prospective and existing investors.

4.4 Syndication of Loans

Marketplace lenders generally serve as an intermediary for individuals, institutional investors and others to providing funds for a loan. The processes vary and continually evolve but generally are facilitated by an online platform that connects the potential borrower with investors. These platforms allow the loan funding process – from customer acquisition to underwriting and origination, and through servicing – to be entirely digitised. Borrowers may have reduced borrowing costs, more seamless customer experiences and shorter lead times to closing as a result of electronic delivery channels.

As noted above, lending is regulated by a number of federal and state regulators in the USA and the nature of regulation varies across the bodies, and depends on the type of lender. This regulatory environment was generally developed in the context of traditional lending through physical delivery channels and has not necessarily kept pace with electronic or other innovative delivery channels.

5. PAYMENT PROCESSORS

5.1 Payment Processors' Use of Payment Rails

Payment processors are not required to rely upon existing payment rails, and as consumers and corporations demand faster or "real-time" payments, payment service providers may consider addressing these demands either by building upon the existing model or starting anew. The Clearing House, for example, announced a partnership to enable The Clearing House to provision and manage Mastercard-branded tokens on behalf of banks. Alternatively, some in the fintech space have chosen to build their own payment systems, such as ATCE Holdings's EtudePay Payments System, which is a real-time payments rail delivered on its own settlement platform for processing transactions.

In any case, banks remain key players in the broader payments industry. Therefore, the ability to convince banks to adopt new payment systems is an important consideration when building upon existing models or starting anew. As the industry evolves, both existing and new payment rails are being employed in novel ways to support traditional payment flows, while facilitating up-and-coming payments technology.

5.2 Regulation of Cross-Border Payments and Remittances

A payment processor based in the USA generally will be under the oversight of multiple regulators, including regulators at both the federal and state level. The scope of such oversight depends on the services that the payment processor is providing, as well as the relationships it has with other financial institutions.

Compliance with requirements established by the Office of Foreign Assets Control and the Financial Crimes Enforcement Network (FinCEN) are important considerations regarding cross-border payments. Cross-border payments and remittances also must comport with various industry operating standards. For example, the payment card industry issues requirements applicable to merchants who process, store or transmit credit card information in an effort to ensure a secure transaction environment is maintained. A payment processor may also need to comply with the rules or standards applicable to the various credit card networks, such as the interchange fees that credit card networks may charge merchants. In short, there are numerous rules and standards that a payment processor must be aware of to operate in the USA.

6. FUND ADMINISTRATORS

6.1 Regulation of Fund Administrators

No information is available in this jurisdiction.

6.2 Contractual Terms

No information is available in this jurisdiction.

7. MARKETPLACES, EXCHANGES AND TRADING PLATFORMS

7.1 Permissible Trading Platforms

In the USA, blockchain-based assets, such as digital tokens and cryptocurrencies, are currently characterised as "securities" or, broadly speaking, "something other than securities". Blockchain-based assets that are securities (ie, security tokens) are, to the extent traded on an exchange, required to be traded on an SEC-registered national securities exchange or an alternative trading system (ATS). Conversely, blockchain-based assets such as bitcoin and other

"pure" cryptocurrencies that are not currently characterised as securities are not subject to such a requirement. Therefore, trading platforms are subject to regulation based upon the type of asset that trades on such platform.

Based on recent estimations, there are hundreds of cryptocurrency exchanges and trading platforms around the world (collectively referred to herein as "trading platforms") and new ones seem to launch regularly. The explosion in number of these trading platforms has recently drawn significant attention from US regulators. Although standards vary, as a general matter, many trading platforms will not list any token that could potentially be viewed as a security, but will instead opt to list "utility tokens" or "pure" cryptocurrencies. This allows trading platforms to avoid the regulatory requirements associated with securities.

Trading platforms that advertise themselves to be so-called peer-to-peer trading platforms may fall within the definition of an "exchange" under the federal securities laws (which is broadly defined) and consequently such trading platforms may be subject to a variety of penalties, including monetary fines and orders to cease operations. The rules under the Securities Exchange Act of 1934 (the "Exchange Act") provide for a functional test to determine whether a trading platform is, in fact, operating as an exchange.

7.2 Regulation of Different Asset Classes

No information is available in this jurisdiction.

7.3 Impact of the Emergence of Cryptocurrency Exchanges

See **7.1 Permissible Trading Platforms** for information on cryptocurrency exchanges.

7.4 Listing Standards

The SEC does not set listing standards; rather, the various trading platforms set their own standards for listing and continuing to trade securities. Trading platforms that are willing to list securities tokens will often require that the token be linked to a high-quality, differentiated and value-adding product or service; have high-quality code that is as much as possible not susceptible to hacking; and have detailed information regarding technical specifications and legal rights and restrictions.

Given the rapid growth of the blockchain-based assets market and the risks it poses to retail investors who may not understand the difference between these relatively new assets and more traditional assets, OCIE has reiterated in its examination priorities for 2021 that it will continue to identify and examine SEC-registered market participants engaged in this space.

Market integrity, which is often viewed as a fundamental aspect of traditional financial markets, continues to be an area of concern in crypto markets. Given the increasing number of trading platforms worldwide, unlike in traditional financial markets, there is not yet a consistent approach to identity verification of investors (ie, KYC and AML procedures), professional standards, surveillance systems or infrastructure to ensure fairness. In an effort to address some of these issues, at the beginning of 2020, an association of industry participants known as the Blockchain Association launched a "Market Integrity Working Group", which is tasked with the responsibility of ensuring fairness, equity and accountability of cryptocurrency markets.

7.5 Order Handling Rules

No information is available in this jurisdiction.

7.6 Rise of Peer-to-Peer Trading Platforms

See **7.1 Permissible Trading Platforms** for information on peer-to-peer trading platforms.

7.7 Issues Relating to Best Execution of Customer Trades

No information is available in this jurisdiction.

7.8 Rules of Payment for Order Flow

No information is available in this jurisdiction.

7.9 Market Integrity Principles

No information is available in this jurisdiction.

8. HIGH-FREQUENCY AND ALGORITHMIC TRADING

8.1 Creation and Usage Regulations

High-frequency and algorithmic trading strategies (HFT strategies) are increasingly being utilised by proprietary trading shops and hedge funds (trading firms) as an enhancement to implementation of traditional trading strategies. At a high level, HFT strategies involve the application of software-based algorithms to trade in and out of high-volume positions of equities and other financial products at speeds faster than achievable by their human counterparts. HFT strategies vary significantly and can be used for exchange-based and OTC (or off-exchange) trades, as well as trades in currently unregulated markets such as the cryptocurrency markets.

Depending on the role and activities of the particular trading firm utilising HFT strategies, different regulatory regimes may apply to such firm. Hedge funds using HFT strategies are generally treated the same as hedge funds using other strategies and therefore may be regulated as investment advisers and required to register with the SEC or one or more state securities authorities. Such hedge funds must comply with securities laws applicable to SEC or state-registered investment advisers.

8.2 Requirement to Register as Market Makers When Functioning in a Principal Capacity

No information is available in this jurisdiction.

8.3 Regulatory Distinction between Funds and Dealers

Some trading firms employing HFT strategies operate as market makers or dealers, in which case such a firm would be required to register with the SEC as a broker-dealer. Certain broker-dealers rely on Rule 15b9-1 of the Exchange Act, which exempts them from the statutory requirement to become a member of FINRA. As a result of the exemption, FINRA has no jurisdiction over these broker-dealers and is therefore unable to enforce compliance with federal securities laws and rules.

The SEC has proposed amending this exemption, as it prevents FINRA from being able to monitor use of HFT strategies and manipulative behaviour, but as of the end of 2020, the proposed amendment has not been adopted. Despite such trading firms being members of their respective exchanges, the exchanges are not able to regulate OTC activity as typically they only have access to the trade data for trades conducted on their own exchanges.

8.4 Regulation of Programmers and Programming

No information is available in this jurisdiction.

9. FINANCIAL RESEARCH PLATFORMS

9.1 Registration

No information is available in this jurisdiction.

9.2 Regulation of Unverified Information

No information is available in this jurisdiction.

9.3 Conversation Curation

No information is available in this jurisdiction.

10. INSURTECH

10.1 Underwriting Processes

The term “insurtech” covers a wide variety of technological innovations that aim to harness the power of technology to reinvigorate an age-old industry. Disruptors such as Oscar, Root and Lemonade seek to displace the traditional provider-customer relationship for a newer, app-based dynamic. Mature market players, in turn, have embraced innovations to fill a wide range of niches, ranging from policy pricing to fraud detection. Although the fractured regulatory environment insurance companies are subject to may stymie any one-size-fits-all solution, the inexorable march of progress nonetheless continues.

Underwriting processes often vary by product and industry participants. Innovative participants have begun relying on technologies such as big data, AI, wearables and telematics to improve underwriting and provide more accurate conclusions. That said, regulations in a particular jurisdiction may require that rates be filed with, and approved by, the appropriate insurance regulator. Such regulator may also prohibit specific factors from being considered, or may even prescribe the precise factors that must be considered, sometimes at odds with overall technical trends.

As the regulation of insurance in the USA is largely state-based, the regulations may vary significantly. For example, while some states expressly permit credit scores to be considered when rate-setting for property and casualty policies, numerous other states apply strong limitations. Some states expressly permit genetic data to be used in the life and disability space. Others expressly prohibit it. Other regulations, including those related to data privacy and anti-discrimination laws, may also impact the underwriting process. As a result, the process is often a bespoke one by necessity, taking consideration of the variances between jurisdictions. The National Association of Insurance Commissioners, consisting of representatives from each US state, has set up a number of workgroups and task forces to consider regulatory changes in response to technological developments in the industry.

10.2 Treatment of Different Types of Insurance

Industry participants and regulators treat different types of insurance in significantly different ways. For example, they require different licences and different regulations governing the production of such business. This necessarily imposes impediments to any unified national solution. Instead, market participants often need to tailor their products and services to meet not one but 50 different approaches to insurance regulation.

11. REGTECH

11.1 Regulation of Regtech Providers

No information is available in this jurisdiction.

11.2 Contractual Terms to Assure Performance and Accuracy

No information is available in this jurisdiction.

12. BLOCKCHAIN

12.1 Use of Blockchain in the Financial Services Industry

Blockchain technology, which uses a distributed ledger system and a consensus protocol to verify transactions, has the potential to transform any industry that today relies on a single trusted third party. Nowhere is this more true than across the financial services sector. Over the past several years, numerous firms in the financial services sector have been building out proof of concept platforms that rely on blockchain technology, with some projects already active. This trend is likely to continue and expand.

In most cases, financial services firms are using so-called private, permissioned blockchains when transacting amongst themselves because these ecosystems limit who can join and employing the power of public permissionless blockchains when exploring consumer-facing projects. Potential applications include global payments, clearing and settling, syndicated loans, trade finance, convertible bonds and proxy voting. A number of financial institutions have also filed, and in some cases been granted, US patents on different blockchain applications.

12.2 Local Regulators' Approach to Blockchain

In the USA, regulators are coping with how existing regulations, drafted to apply to centralised ecosystems, apply to decentralised systems where the actors may not be readily identifiable. The concept of blockchain regulation is, of course, anathema to many proponents of the technology who believe that its transparency and decentralisation mean that there is no need for traditional regulation. Set forth below are some key developments in the US regulatory landscape, with the caveat that this is a quickly evolving field.

Federal Legislation

As of the end of 2020, no fewer than 40 bills addressing blockchain technology have been introduced in the US Congress. Several bills, in particular, stand out. The Securities Clarity Act seeks to clarify that an asset (including a digital asset) does not become a security as a result of being sold or transferred pursuant to an investment contract, a noteworthy step towards mitigating the uncertainty around application of the so-called Howey Test (discussed below) to digital tokens. The Digital Commodity Exchange Act proposes to create a single, opt-in federal regulatory scheme for digital asset trading platforms under the exclusive jurisdiction of the CFTC based on the regulatory model for traditional commodity exchanges. Finally, the Stablecoin Tethering and Bank Licensing Enforcement (STABLE) Act seeks to subject prospective issuers of stablecoins to a host of new regulatory obligations.

On 1 January 2021, the US Congress passed, over the President's veto, the Anti-Money Laundering Act of 2020, which expressly expresses the "sense of Congress" that virtual currencies can be used for criminal activity; includes the term "value that substitutes for currency" in key provisions of the Bank Secrecy Act (BSA), thereby codifying FinCEN's existing position that certain virtual currency businesses are subject to the act; and directs the Government Accountability Office to study the role of emerging technologies and payment systems, including virtual currencies, in human trafficking, drug trafficking and money laundering. The focus on virtual currencies in the Anti-Money Laundering Act may signal the US Congress's interest in staying active in this arena in addition to steps taken by regulators. The Anti-Money Laundering Act also strengthens the US government's anti-money laundering capabilities more generally and creates a Bank Secrecy Act whistle-blower programme, both of which may lead to increased cryptocurrency-related enforcement.

In late 2020, FinCEN proposed two new rules that, if implemented, will directly affect virtual currency businesses. In October 2020, FinCEN and the Federal Reserve announced a notice of proposed rule-making to amend the Recordkeeping Rule and Travel Rule regulations under the BSA. The proposed amendments would reduce the applicable threshold for international funds transfers from USD3,000 to USD250 and, consistent with FinCEN's existing guidance, formally extend these rules to cover convertible virtual currencies (CVC) and digital assets with legal tender status (LTDA).

In December 2020, FinCEN issued a proposed rule that would impose new reporting, record-keeping and verification requirements on banks and money services businesses with respect to certain virtual currency transactions. The proposed rule would require banks and money services businesses to file a report with FinCEN for transactions exceeding USD10,000 in value that involve CVC or LTDA held in a wallet not hosted by a financial institution (a so-called unhosted wallet) or a wallet hosted by a financial institution

in specific jurisdictions identified by FinCEN. The proposed rule, if implemented, would also require banks and money services businesses to keep records of a customer's CVC or LTDA transactions and counterparties, including verifying the identity of their customer, if their customer's counterparty uses an unhosted or otherwise covered wallet and the transaction is greater than USD3,000.

State Legislation

Although federal laws are still in their relative infancy, more than 30 states have enacted cryptocurrency or blockchain-related legislation as part of efforts to become hubs for blockchain innovation. Some states – including Arizona, North Dakota, Oklahoma and Washington – have amended laws so that records or contracts secured through blockchain technology are deemed enforceable electronic records. In January 2020, the Illinois Blockchain Technology Act went into effect, which affirms the contractual enforceability of smart contracts and other records for which blockchain technology was used.

Application of Howey Test to Cryptocurrency

In 2019, the SEC released guidance regarding how to determine whether cryptocurrencies constitute securities. The SEC relies on the Howey Test as the current regulatory framework, first articulated in SEC v WJ Howey Co, 328 US 293 (1946). Under the Howey Test, courts analyse whether the instrument or offering in question satisfies all three of the following prongs:

- "an investment of money";
- "in a common enterprise"; and
- "with profits to come solely from the efforts of others".

The SEC first applied the Howey Test to cryptocurrency on 25 July 2018 in its so-called DAO Report, in which the SEC concluded that a particular cryptocurrency called DAO Tokens was a security subject to regulation. Since then, there have been a number of SEC orders and court decisions applying Howey to analyse other digital asset offerings: Unikrn, Release No 10841; Salt Blockchain, Release No 10865; Paragon Coin, Inc, Securities Act Release No 10574 (16 November 2018); CarrierEQ, Inc, D/B/A AirFox, Securities Act Release No 10575; and SEC v Blockvest, LLC et al, No 18-CV-2287-GPC (11 October 2018). In some of these cases, cryptocurrency developers have been required by the SEC to register under the Exchange Act, pay fines and offer rescission to investors. SEC enforcement action in this space picked up considerably in 2019 and 2020, with a number of settlements announced.

SEC Enforcement Actions

The SEC has continued its trend of pursuing high-profile enforcement actions against prominent digital asset developers for alleged unregistered offers and sales of securities. See, eg, SEC v Kik, 19-cv-5244(AKH)(S.D.N.Y.); SEC v Telegram, 19-cv-9349(PKC)(S.D.N.Y.); and SEC v Ripple, 20-cv-10832(AT)(S.D.N.Y.). In the Telegram matter, the SEC obtained a preliminary injunction enjoining the defendant from distributing its cryptocurrency token, called Grams, to purchasers. The action was subsequently settled. In the Kik matter, the SEC secured summary judgment on the ground that Kik's offering of digital tokens, called Kin, violated the federal securities laws. Most recently, in December 2020, the SEC instituted an action against Ripple Labs and two of its executives, alleging violations of Sections 5(a) and 5(c) of the Securities Act of 1933 and claims for aiding and abetting such violations. The complaint alleges that the defendants offered and sold a digital asset, called XRP, without a valid registration statement.

Finally, in October 2020, the SEC filed an action against computer programmer and entrepreneur John David McAfee for allegedly leveraging his fame to make more than USD23.1 million in undisclosed compensation by recommending at least seven ICOs to his thousands of Twitter followers. The SEC accused Mr McAfee of violating Sections 17(a) and 17(b) of the Securities Act of 1933 and Section 10(b) of the Securities Exchange Act of 1934. The complaint also named Mr McAfee's bodyguard, Jimmy Gale Watson, Jr, who allegedly negotiated the deals with the ICO issuers, helped Mr McAfee monetise the proceeds of his promotions and directed his then wife to tweet fake interest in an ICO that Mr McAfee was promoting at the behest of the offeror.

The SEC has also focused on trading platforms, seeking to have them register as exchanges and imposing fines (Zachary Coburn, Securities Act Release No 84553 (8 November 2018)).

Beyond enforcement, the SEC has also encouraged developers to engage in voluntary discussions with staff regarding their projects and compliance issues. To that end, the SEC established FinHub in October 2018, which is specifically designed to provide guidance to developers in this space. In December 2020, the SEC announced that FinHub would become a standalone office, with its new director reporting directly to the SEC chairperson.

CFTC Interpretations and Enforcement

For its part, the CFTC has taken the position that cryptocurrencies that are not securities are commodities. This position has been supported by multiple federal court decisions. For

example, in CFTC v McDonnell, 287 F Supp. 3d 213 (EDNY 2018), a federal district court in New York held that the CFTC can regulate cryptocurrencies as a commodity because they are "'goods exchanged in a market for a uniform quality and value" and they also "fall well within the common definition of 'commodity' as well as the [Commodity Exchange Act's] definition of 'commodities.'" Similarly, in CFTC v My Big Coin Pay, 334 F Supp 3d 492 (D Mass. 2018), a federal district court in Massachusetts held that cryptocurrencies are subject to CFTC regulation as a commodity class because futures trading exists on bitcoin, a subset of that class.

If a blockchain asset such as a cryptocurrency is a commodity, the CFTC has enforcement authority to police fraud and manipulation in spot markets for the asset. If there are derivatives contracts on blockchain assets (ie, futures, swaps and options), the CFTC will have full regulatory authority over those contracts. For example, futures contracts on bitcoin currently offered on some futures exchanges are subject to the full regime of futures regulation under the Commodity Exchange Act.

Thus far, the CFTC has focused its enforcement authority on protecting retail customers engaged in unregulated spot transactions in cryptocurrencies. However, the CFTC will face more complex questions with respect to the scope of its authority over blockchain as innovators begin exploring the use of smart contracts to facilitate decentralised trading in derivatives. To prepare for these types of questions, the CFTC upgraded its financial technology research wing in October 2019. Known as LabCFTC, the wing is dedicated to promoting the development of new financial technologies in order to ensure that innovators can easily access and understand the CFTC's regulatory framework and the agency's approach to oversight.

In 2019, the CFTC moved ahead with approving and allowing more digital asset/virtual currency products. For example, the CFTC approved the applications of two entities to register as a designated contract market and a derivatives clearing organisation, respectively, to offer or clear virtual currency derivatives products.

The CFTC approved LedgerX's DCM application in June 2019 to offer bitcoin spot and physically settled derivatives contracts, including options and futures, to retail clients of any size. LedgerX had previously been registered as a derivatives clearing organization (DCO) in July 2017 to clear fully collateralised digital currency swaps. The CFTC also approved Eris Clearing's DCO application in July 2019 to clear fully collateralised virtual currency futures.

In October 2019, CFTC Chairman Tarbert publicly stated that ether, like bitcoin, is a commodity that falls under the CFTC's jurisdiction. Previously, in December 2018, the CFTC had sought public comments on the Ethereum network and the cryptocurrency ether to better inform the commission's understanding.

On 21 October 2020, the CFTC Division of Swap Dealer and Intermediary Oversight (DSIO) published an advisory (the "Advisory") for futures commission merchants (FCMs) regarding the segregation of virtual currency in customer accounts. The Advisory was published in response to requests from market participants for DSIO to explain how the customer protection provisions of the CEA and the CFTC regulations apply to virtual currencies deposited by futures customers or cleared swaps customers with FCMs to margin futures, options on futures and cleared swaps.

On 24 March 2020, the CFTC adopted an interpretation of the term "actual delivery" with respect to retail virtual currency transactions (the "2020 Guidance"). Under the 2020 Guidance, transactions in cryptocurrencies with retail customers conducted with margin, leverage or other financing must be traded on a CFTC-licensed futures exchange, unless the cryptocurrency is free of any liens, other interests or legal rights of the offeror or seller, and the purchaser has full control of the virtual currency within 28 days of the transaction. Trading platforms, custodians and other market participants considering entering into cryptocurrency transactions on margin or with financing should ensure they are familiar with the 2020 Guidance to avoid running afoul of the Commodity Exchange Act.

To the extent blockchain assets held by a fund are considered securities, the Investment Advisers Act of 1940, as amended, applies and to the extent such assets are considered commodities, the Commodity Exchange Act applies. The investment advisers of such funds that invest in blockchain assets that are considered securities are typically registered with the SEC or one or more state securities authorities and must comply with the securities laws applicable to SEC or state-registered investment advisers. In this firm's experience, such funds are exclusively structured as "Section 3(c)(1)" or "Section 3(c)(7)" private funds. A trading platform on which blockchain assets that are securities are traded is required to be an SEC-registered national securities exchange or an ATS.

DOJ Enforcement

The US Department of Justice has also signalled increased scrutiny of cryptocurrency. On 8 October 2020, the DOJ issued its Cryptocurrency Enforcement Framework, the

first comprehensive statement of its approach to investigating and prosecuting cryptocurrency-related crimes. The framework evinces concern about "business models and activities" in the cryptocurrency space that "may facilitate criminal activity", particularly peer-to-peer exchanges and anonymity-enhanced cryptocurrencies. Notable DOJ enforcement activity in this area in 2020 included DOJ and CFTC actions against BitMEX, a cryptocurrency exchange and derivatives trading platform, for Bank Secrecy Act and CFTC registration violations; and a DOJ criminal prosecution and parallel FinCEN civil enforcement action against Larry Dean Harmon, the founder and operator of two alleged convertible virtual currency "mixers" or "tumblers". "Mixing" and "tumbling" are techniques that combine potentially identifiable digital coins with other coins to make it difficult to trace the source, owner or recipient of the first set of coins.

12.3 Classification of Blockchain Assets

See **12.2 Local Regulators' Approach to Blockchain** for information on classification of blockchain assets.

12.4 Regulation of "Issuers" of Blockchain Assets

See **12.2 Local Regulators' Approach to Blockchain** for information on issuers of blockchain assets.

12.5 Regulation of Blockchain Asset Trading Platforms

See **12.2 Local Regulators' Approach to Blockchain** for information on blockchain asset trading platforms.

12.6 Regulation of Funds

No information is available in this jurisdiction.

12.7 Virtual Currencies

See **12.2 Local Regulators' Approach to Blockchain** for information on virtual currencies.

12.8 Impact of Regulation on "DeFi" Platforms

Blockchain technology has the potential to revolutionise how personal information is stored and processed. However, the benefits of blockchain technology will need to be reconciled with California's new privacy law, the California Consumer Privacy Act (CCPA), that went into effect in January 2020. Further guidance might be required on whether one can exercise a right of deletion on a blockchain-based system. US companies building out blockchain applications in the fintech space will need to take privacy laws such as the CCPA into account and monitor this area of the law closely.

13. OPEN BANKING

13.1 Regulation of Open Banking

Open banking, an emerging space within fintech, can be thought of as a system whereby financial institutions' data can be shared with third parties, such as data aggregators and app providers, through application programming interfaces. Open banking may be a gateway to providing more services to customers and is generally considered a more secure method for sharing financial account and transaction data than so-called screen scraping, but it also introduces its own concerns.

13.2 Concerns Raised by Open Banking

Relative to Europe and certain Asian countries, the USA lags behind in its development of laws and regulations around open banking. Some have viewed the fragmented nature of financial regulation in the USA as an impediment to the development of a comprehensive regulatory scheme. Some argue that the lack of an industry standard or regulatory framework in the USA for open banking is an obstacle to the development of its full potential.

As with many emerging areas, there is a debate as to whether the private sector or the public sector should lead the pathway forward. While the US Treasury and others have advocated for a private sector-led solution to open banking, others have raised concern that a solution determined by financial services companies – rather than consumers – may adversely impact the types of services that fintech data aggregators and consumer application providers may be able to develop.

When entering into open banking relationships with financial institutions, data aggregators, app developers and others, it will be important to consider a multitude of data-related issues, including consumer protections, protections for data privacy and security, data ownership, allocation of liability in the event of breach and responsibilities for responding to any breach.

Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates advises financial institutions and their investors and counterparties around the world on their most complex, high-profile matters, providing the guidance they need to compete in today's business environment. The financial technology industry presents businesses and private equity, venture capital and other investors with extraordinary opportunities as well as challenging legal and regulatory issues. Skadden has helped clients to navigate this complex environment since the industry's inception. The FinTech practice draws on the firm's global platform and market-leading corporate finance, financial regulation and enforcement, intellectual property and technology, privacy and cybersecurity, and M&A capabilities, making it uniquely qualified to offer clients exceptional depth of experience and full-service capabilities.

Skadden would like to thank financial institutions regulation and enforcement partners Brian Christiansen and Eytan Fisch, and counsel Collin Janus; M&A and financial institutions partner Jon Hlafter; derivatives of counsel Jonathan Marcus; investment management associate Prem Amarnani; financial institutions of counsel Patrick Lewis; financial institutions associates Tim Gaffney and Han Lee; and M&A associate Marcel Rosner for their invaluable contribution to this chapter.

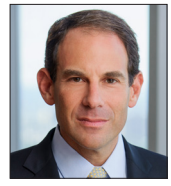
AUTHORS

Alex Drylewski is a partner at the firm. He represents companies and individuals in complex commercial litigation, government investigations, trials and appeals involving emerging technologies, including blockchain platforms and digital assets.

Jeffrey Brill is a partner in Skadden's Mergers & Acquisitions group. He specialises in corporate and commercial transactions for financial institutions and fintech companies. He co-coordinates Skadden's fintech practice.

Heather Cruz is a partner at the firm. She specialises in investment management. Heather is a member of the Private Investment Funds Committee of the Association of the Bar of the City of New York.

Sven Mickisch is co-head of Skadden's Financial Institution Group. He specialises in mergers and acquisitions in the financial services space. He co-coordinates Skadden's fintech practice.



Stuart Levi is co-head of Skadden's Intellectual Property and Technology Group. His key practice areas are blockchains, smart contracts and digital assets; intellectual property and technology; outsourcing; cybersecurity; and privacy.

Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates

One Manhattan West
Skadden Arps
New York
NY 10001

Tel: +1 212 735 3288
Fax: +1 212 735 2000
Email: info@skadden.com
Web: www.skadden.com