Chambers

GLOBAL PRACTICE GUIDES

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

Fintech

USA: Trends & Developments

Erin Illman, Carol Van Cleef, Lee Gilley and Michael Gordon
Bradley Arant Boult Cummings LLP

practiceguides.chambers.com

2021

Trends and Developments

Contributed by:
Erin Illman, Carol Van Cleef, Lee Gilley and Michael Gordon
Bradley Arant Boult Cummings LLP see p.7

Crisis has set the stage for fintech companies in 2021, creating both new opportunities and potentially unprecedented challenges to innovation. While the coronavirus pandemic continues to accelerate the digital transformation of financial services and drive the adoption of new technologies and business models, political turmoil in the United States has heightened racial tensions and sharpened the focus on threats of domestic terrorism complicating daily operations. Astounding data breaches have underscored the fragility of existing infrastructures both in the public and private sectors. At the same time, regulators encourage the deployment of new technologies that offer glimpses of potential solutions.

Our day-to-day lives have been fundamentally altered in many ways, and fintech companies have not been spared. The legal and regulatory environment in which they are trying to innovate continues to evolve, and despite efforts to streamline regulation, the complexities of compliance seem to be compounding. Although no company can ever be fully prepared for every crisis or poised for every opportunity, now is an appropriate time to evaluate whether fintech companies operating in the United States are ready for 2021 and beyond.

Is Fintech Ready for the New Face of Washington, DC?

The start of any new presidency in the United States always generates many questions about the direction of policy and how it will impact different industries. Many aspects of financial services innovation have been relatively unencumbered by significant new regulations in the past four years. But that may be about to change. The polarisation and paralysis of policy-making that dominated United States politics in recent years frustrated many agendas, especially those focused on consumer-related issues. Precariously postured questions related to emerging technologies and the need for quick legislative action to address the COVID-19 pandemic sets the stage for potentially significant new laws that could impact fintech companies.

The election of President Joseph R. Biden, Jr. and the addition of several new senators allow the Democratic Party to start 2021 with control over two of the three branches of the federal government. Although operating with a razor-thin majority, the Democratic-controlled administration can now take substantial steps to shape the legal and regulatory landscape in which fintech companies operate over the next four years. However, while the chances of the party advancing its legislative agenda are better now than they have been in several years, the co-operation of at least some Republicans in Congress (or the occurrence of a major financial crisis) will still be needed to pass major legislative reform like the Dodd–Frank Wall Street Reform and Consumer Protection Act of 2010.

On the legislative front, the top two priorities of President Biden and the Democratic Congressional leadership are reining in the coronavirus pandemic and mitigating its economic impact. Based on experience, pandemic relief legislation may serve as a vehicle for enhancing consumer protections related to debt collection, student lending, loan servicing and credit reporting.

After lacking the power of the majority for several years, the Democratic senators now have the opportunity to accelerate their political agendas in other areas, stepping up their oversight activities and investigative efforts by, among other things, issuing more informational requests and subpoenas to companies. In the current climate, tech companies will likely receive a disproportionately higher number of such requests. Given the implications and associated costs of a Congressional investigation, fintech companies need to manage these processes carefully.

What Will Happen to Rule-Making and Regulatory Guidance Issued over the Past Four Years, and Especially in the Past Few Months?

A new Congress can also reverse administrative rule-making through formal legislative action or through more informal processes that may include hearings, requests for information or other tactics. Like many of his predecessors, President Biden issued an immediate order to suspend for 60 days all pending rule-making to provide his new administration with time to review the regulatory actions of its predecessor. These reviews may be conducted on a centralised basis through the White House or on a more decentralised basis by new leaders of each agency. During this period, agency heads may move to alter, revise or even reverse previously promulgated regulations, some of which may be favourable to fintech companies and some of which are not.

For example, Office of the Comptroller of the Currency (OCC) regulations regarding the true lender doctrine, the valid when made doctrine, and the recently enacted fair access to financial services have drawn negative attention from Democratic lawmakers and could be ripe for revision. Consumer Financial Protection Bureau (CFPB) regulations – including the recently issued debt collection rule, payday lending rule and qualified mortgage rule – have drawn similar scrutiny. While revising or rolling back rules is not something that can be accomplished overnight, there is precedent, including significant precedent from Trump-era regulators, for taking these types of actions.

Likewise, new agency heads can be proactive and alter the course of proposed regulations, although there is no certainty of such an outcome, and the results may be influenced by many events. For example, operating under the auspices of the United States Department of the Treasury, the Financial Crimes Enforcement Network (FinCEN) issued a "midnight" proposal at the beginning of the two-week holiday period encompassing Christmas and New Year's Day. As proposed, the new regulation would impose new and significantly burdensome reporting and record-keeping obligations on banks and money services businesses offering virtual currency services. Asking 24 specific questions requiring detailed answers, and truncating the public comment period to an unusually short 15 days, FinCEN effectively interrupted the holiday break of many company employees, many of whom were working from home in the middle of a pandemic. The result was the submission of almost 8,000, mostly angry comments within the final two weeks of the Trump administration. For many early-stage cryptocurrency businesses, the cost of implementing the proposal, if ever finalised, could put them out of business.

How Will Potential Shifts in the Priorities of United States Regulators Affect a Fintech Company?

As a corollary to the last question, new leadership at the regulatory agencies will often also result in a reordering of regulatory priorities. Indeed, if legislative prospects are somewhat dimmed by an evenly split Congress, pressure may increase on the regulatory agencies to take bold action to protect consumers and investors and address other more traditional Democratic priorities. Regulators such as the CFPB are likely to focus on issues that impact special populations such as students, older Americans, and military members.

For companies offering cryptocurrency services or using blockchain or distributed ledger technologies (DLT), shifts in regulatory priorities at several agencies could determine the course of these companies and technologies for the next several years. For example, in the last six months of the Trump administration, the crypto-friendly acting Office of the Comptroller of the Currency (OCC) took several actions to significantly accelerate national bank adoption of blockchain technology and the use of cryptocurrencies. The OCC's decision to conditionally allow a virtual currency business operating under a state trust charter to convert to a national bank trust charter six days before the end of the Trump administration was not without controversy. The new Comptroller will play a key role in determining the speed of expanded use of blockchain technology and stablecoins in national banks and integration of cryptocurrency businesses with the banking industry.

The new chairpersons of the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) similarly play significant roles in determining the agenda of their respective agencies. They determine the direction of pending regulatory initiatives on crypto-assets and what legislative proposals on the subject to support. They also play a key role in determining the agency's enforcement policy, including whether to continue with pending cases and other matters under investigation, and when to initiate new investigations.

Historically, United States regulators have been less likely to provide regulatory flexibility and encourage innovation through tools such as no-action letters, compliance sandboxes, trial disclosure programmes and other similar mechanisms. While Trump-era regulators began to increase regulatory flexibility for fintech companies, significant Democratic lawmakers have been sceptical of those actions. Indeed, Congresswoman Waters, the chairwoman of the House Committee on Financial Services, as well as other Democratic leaders have been highly critical of these efforts.

Nonetheless, it is unlikely we will see a significant rollback of the initiatives taken during the past four years by the federal agencies, including FinCEN, and some state regulators to interact with fintech companies both formally and informally. The regulators have aggressively encouraged dialogue with fintech companies to help the agencies understand better fintech developments. Recognising how the technology may cut across agency jurisdictions, the head of the SEC Innovations unit has even offered, as appropriate, to help invite other regulators into meeting with her offices.

Does the Company Fully Understand Its Data Privacy Obligations and the Implications of a Compliance Failure?

The nature and scope of a company's privacy obligations continued to expand during 2020, both in the United States

and internationally, and that expansion is likely to continue in 2021. Just a few short years ago, personal information included specific pieces of sensitive personal information that directly identified an individual, such as their social security number or credit card number. Historically, privacy laws, particularly in the United States, focused on preventing identity theft or misuse of sensitive personal information. That is no longer the case. The definition of personal information has vastly expanded, and certain laws now define sensitive personal information to include any information that can "identify, relate to, describe, be associated with, or be reasonably capable of being associated" with an individual. Moreover, an influx of privacy-related litigation will continue to shape and shift the legal requirements that fintech companies must consider when innovating and implementing services that involve the collection, use, sharing or retention of personal information. While the ambit of privacy law continues to expand, fintech companies are increasingly collecting and processing significant amounts of personal information, often on behalf of other financial institutions. In this environment, fintech companies must apply resources to ensure they are complying with both privacy laws and the contractual obligations imposed by their partners.

2020 was a watershed year for privacy in the United States. On 1 January 2020, the United States' first comprehensive privacy law, the California Consumer Privacy Act (CCPA), took effect. On 4 November 2020, California passed the California Privacy Rights Act (CPRA), which significantly expands the CCPA. Although the CPRA's additional requirements do not go into full effect until 2023, the changes are extensive, and fintech companies should start working now to ensure compliance. Fintech companies that utilise automated processing and decision-making technologies need to pay particular attention to the CPRA, as it creates new rights that allow consumers to opt out of the use of automated decision-making technology, including "profiling", in connection with decisions related to a consumer's work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. The CPRA creates a new California privacy agency tasked with creating regulations that allow consumers to request meaningful information about the logic involved in the decision-making processes and a description of the likely outcome based on that process.

Even smaller fintech companies, which may not meet the scope and applicability standards of the CCPA or CPRA, should carefully consider strategic compliance as part of their investment, market, and mergers and acquisition strategies. Smaller fintech companies, particularly those who serve as servicer providers for regulated financial services companies, must carefully consider whether their clients are obligated to comply and whether their clients will push compliance obligations down to their service providers. Regulators have increasingly required financial services companies to impose certain compliance obligations, such as CCPA and CPRA compliance, on their service providers, and this trend will likely continue in 2021.

The expansion of privacy requirements has served as a catalyst for a growing group of fintech companies that have been able to assist partner companies in meeting privacy-related obligations. This compliance-oriented group of fintech companies likely will continue to expand in 2021.

Finally, fintech companies that service a global client base, particularly clients that are active in the European Union (EU), must continue to ensure and monitor compliance with the General Data Protection Regulation. In some cases, the establishment of a subsidiary or affiliate in the EU may help facilitate compliance.

Is the Company Making Appropriate Investments in Cybersecurity, and Is It Prepared to Respond to a Data Breach?

2020 showed no signs of a slowdown in cyber-attacks. In fact, there was an uptick in attacks, with criminals debuting a multi-phased evolution of ransomware with data exfiltration. The increase in quantity and quality of cyber-attacks makes cybersecurity one of the most important issues for fintech companies to consider.

Fintech companies are likely to see even more pressure from their business partners and regulators to the extent they are regulated on cybersecurity as well. In December 2020, the OCC, Federal Reserve Board and Federal Deposit Insurance Corporation jointly proposed a new rule, similar to a New York rule, that would require supervised banking organisations to provide notification of significant cybersecurity incidents to their primary federal regulator within 36 hours. Noteworthy for fintech companies, under the proposed rule, service providers would be required to notify at least two individuals at the financial services organisation immediately after the fintech company experiences a computer security incident that it believes in good faith could disrupt, degrade or impair services provided for four or more hours. While current law focuses on incidents that compromise sensitive customer data, this proposed law would substantially alter the reporting requirements to include incidents that have the potential to disrupt operations, even for a few hours.

Fintech innovations can be ground-breaking and vital to the financial services ecosystem. However, those technologies

will be viewed by others through the lens of privacy and cybersecurity. While the use of data aggregation and analytics can be an invaluable asset for financial institutions and their customers alike, the collection, use, storage and protection of that data must be assessed to mitigate the risks of violating privacy or exposing the company (and its business partners) to criminal cyber-attacks that could result in regulatory consequences, litigation, reputational damage and loss of business.

Is the Company Appropriately Licensed or Authorised to Conduct Business?

Whether a fintech company is considering the initial launch of its business or looking to add new products, bring on new vendors, work with new partners, expand into new states, or open up new channels, the company should first ask whether engaging in the proposed activity or offering a proposed service requires any kind of specialised licence or charter under either federal or state law.

Whether the activity involves lending, money transmission brokering of securities or other financial services, the second question is where it needs to be licensed or chartered. If the company is serving customers in multiple states, is a licence required in each state or at the federal level? The follow-up questions are typically how long it takes to get such licences and how much it will cost.

Unfortunately, answering these questions typically requires a state-by-state analysis and/or possibly a deep dive into federal law. A company is not required to ask regulators or incur legal fees to determine whether it needs to be licensed. However, if it needs to have a licence in any particular state to engage in the business of transferring money or value that substitutes for money, and does not have such licence(s), it could find itself facing federal and state criminal charges, being assessed for monetary penalties, having assets seized and forfeited, and even being jailed. Other types of unauthorised conduct of business – such as lending – may be subject to penalty as well.

If a licensee is being acquired or there is some other type of change in control, it is likely most regulators will require some type of prior notice or approval of the transaction. The failure to obtain such approval could result in criminal charges in some states.

Is the Fintech Company Compliant with All Applicable Laws and Prepared to Be Scrutinised for Such Compliance?

Another question that needs to be answered is whether the company is prepared to comply with all applicable laws. After struggling with the threshold question of whether their business activities are subject to a state licensing scheme, the companies often find themselves confronting the operational challenges of fully complying with multiple state compliance regimes that include safety and financial soundness, consumer protection, anti-money laundering compliance and data security regulations. Depending on the regulatory regime, the company may be subject to examination by one or more state regulator(s).

Tracking relevant laws and maintaining a multi-state compliance programme is always a challenge. As the coronavirus pandemic took hold in the United States, this task became even more complicated as virtually every state regulatory authority began issuing regulations, as well as formal and informal guidance on a wide range of regulatory compliance issues. This flood of information exacerbated the difficulties in tracking and complying with varied, and sometimes conflicting, legal requirements issued by a variety of states.

Those companies subject to examination should be prepared to answer questions in their 2021 state exams on whether they effectively implemented the state's coronavirus-related guidance. State-licensed fintech companies should carefully assess how well they addressed state regulatory guidance, particularly guidance with a direct consumer impact, and remediate any issues so that they are prepared to explain their coronavirus response.

Fuelled by competition with a host of federal regulators wrestling over who is best positioned to license and regulate various types of fintech companies, state regulators continue their efforts to improve co-ordination of their examination, licensing and enforcement efforts. This co-ordination helps reduce the regulatory burden associated with maintaining multiple state licences, but it also increases the likelihood of a multi-state regulatory enforcement action should a problem arise. Over the past ten years or more, the number of multi-state actions has grown significantly, including a series of significant settlements with state-licensed mortgage lenders. Companies that failed to appropriately address the consumer impact of the coronavirus may find themselves vulnerable to such actions in this new regulatory regime.

Is the Company Prepared to Be Examined by a Regulator?

Fintech companies are potentially subject to several types of regulatory examinations even if they do not have a primary federal or state regulator. A fintech company may be subject to an examination by the Internal Revenue Service for compliance with the federal Bank Secrecy Act – even if

it is not registered with FinCEN as a money services business. Likewise, it could be subject to an examination by the CFPB without regard to how it is regulated. In both cases, the need to be prepared for these examinations in advance is critical as the regulators expect compliance from the first day the business started interacting with customers. In addition, fintech companies that provide services to banks may be subject to examination by bank regulators.

The combination of new agency heads at the federal level, an increased focus consumer protection, and the never-ending efforts of criminals to exploit new technology and crisis will likely result in even more robust regulatory examinations in the coming years. While each regulator has their own scope of authority and approach to exams, fintech companies should always apply some basic rules for successfully navigating a regulatory exam. First, virtually every agency that conducts regulatory exams publishes a fairly detailed examination handbook. This handbook is generally the regulator's exam playbook, so it is critical that exam-focused personnel be familiar with relevant materials and ensure that any critical information is distributed throughout the company. Second, fintech companies must be prepared to provide thoughtful information in a timely manner. Regulators generally expect companies to provide significant amounts of initial documentation within 15-30 days of being notified of the examination and to provide prompt responses to follow-up questions. Timely responses are critical, but all relevant stakeholders (ie, the business unit, legal and compliance) should be permitted adequate time to review the submissions.

Companies should take time (i) to prepare appropriately for the personal interaction with the examiner and be prepared to tell their compliance story, (ii) actively review the examination results with the examiner, and (iii) consult with counsel before signing off on a final report. For example, the final IRS BSA exam report is submitted to FinCEN automatically upon completion. Upon review, FinCEN may use the report to initiate enforcement actions.

Companies with innovative or unfamiliar business models or new technologies should be prepared to explain the business model and how the company addresses compliance challenges. This is a challenge for cryptocurrency businesses, where regulatory and examination staffs often lack the breadth and depth of expertise in the technology as it is evolving so quickly.

Conclusion

Fintech continues to evolve at warp speed. The legal and regulatory environment may not evolve at the same speed or in the same direction as the technology. The challenges that legal and regulatory compliance present to the business need not be a negative factor; in many cases, this compliance can provide substantial benefits. Regardless, if the fintech entrepreneur applies the same talent and energy that make the business successful to addressing the legal and regulatory challenges, creative and compliant solutions will emerge, often from the technology itself.

Bradley Arant Boult Cummings LLP is a full-service law firm with a reputation for skilled legal work, exceptional client service and results-oriented strategic advice. With more than 500 attorneys, the firm serves as a vital partner to domestic and foreign clients ranging from market leaders to emerging companies across a variety of industries. The cross-disciplinary fintech team assists clients in achieving their business objectives in a heavily regulated environment. It understands the nuances of applicable laws and regulations that affect clients' businesses. It helps maximise client growth through mergers, acquisitions and other transactions, and assists clients in launching new products and services. The firm advises on federal and state lending and payments laws, including money transmitter licensing, anti-money laundering and sanctions compliance, cybersecurity, data protection, consumer protection requirements and risk management. The team includes former bank regulators, in-house counsel, information technology executives and prosecutors, recognised experts in emerging and alternative payments systems, and certified anti-money laundering specialists.

AUTHORS

Erin Illman is co-chair of Bradley's privacy and cybersecurity practice and leader of the firm's fintech team, who is an experienced thought leader in fintech, privacy, data security and the integration of technology into business practices. She works closely with clients in the growing fintech space in the areas of payment technology, digital banking and lending, personal finance and robo-advising, investing and venture capital, cryptocurrency, blockchain, and electronic products and services. In addition to providing proactive privacy and information security compliance and legal advice, Erin manages privacy-related enforcement actions and litigation. Her practice includes representing companies in reactive incident response situations, including insider cybersecurity threats, electronic and physical theft of trade secrets, and investigation, analysis and notification efforts with respect to security incidents and breaches.

Lee Gilley represents financial institutions – including banks, mortgage companies, debt collectors, small-dollar lenders and payments providers – in regulatory matters related to compliance with numerous state laws and regulations. He focuses his practice on providing proactive advice to companies regarding their compliance obligations and on assisting companies as they interact with regulators through examinations, investigations and the rule-making process. Through his practice, Lee has assisted clients in engaging with the state financial regulators, state attorneys general, the Consumer Financial Protection Bureau, the Office of the Comptroller of the Currency and the Federal Reserve Board.

Carol Van Cleef is an internationally recognised authority and pioneer in legal issues involving cryptocurrencies and blockchain technology. Carol leads the firm's virtual currencies and blockchain work to help clients navigate the complex, dynamic and rapidly evolving issues in these areas. With a focus on regulatory, compliance and enforcement matters, Carol has built a global reputation as a leading attorney, counsellor and problem solver working with fintech companies, blockchain developers, virtual currency exchanges and wallets, payment processors, prepaid access programmes, virtual gaming companies and other business ventures. Her clients also include banks, securities firms, insurance companies and money services businesses. Carol is also a certified anti-money laundering specialist.

Michael Gordon is an accomplished consumer finance lawyer with more than 20 years of experience as a law firm partner, senior federal regulator and fintech general counsel. His practice includes consumer finance and fintech, banking and bank partnerships, consumer and commercial credit, payments, regulatory strategy, risk management and corporate governance. Michael has advised banks, lenders (mortgage, student, auto, credit card, personal and small business), loan servicers, debt buyers, credit bureaus, online lenders, fintech investors and fintech firms. He served in senior roles in the Consumer Financial Protection Bureau and the US Treasury Department.

Contributed by: *Erin Illman, Carol Van Cleef, Lee Gilley and Michael Gordon,* ***Bradley Arant Boult Cummings LLP***

Bradley Arant Boult Cummings LLP

One Federal Place
1819 Fifth Avenue North
Birmingham
AL 35203

Tel: 205 521 8000
Fax: 205 521 8800
Email: eillman@bradley.com
Web: www.bradley.com