Chambers
PROFESSIONAL ADVISERS

FinTech

The world's leading advisers
to the FinTech industry

chambers.com

2019

K&L GATES U.S. FINTECH LEGAL OVERVIEW

Robert P. Zinn
Partner

Mr. Zinn serves as co-leader of the firm's FinTech practice, serves as firm-wide practice area leader of the Corporate and Transactional practice, and is a member of the Management Committee. He launched the firm's official FinTech practice in early 2014 and has been involved with iterations of the FinTech industry for several years. Mr. Zinn has led engagements for nearly three decades, on hundreds of transactions, from very small "seed money" financings to multi-billion dollar mergers and acquisitions. Mr. Zinn's client relationships range from start-ups to some of the world's largest corporations, with an emphasis on substantial middle market businesses.

Mr. Zinn is a frequent author on a variety of topics including FinTech and other issues impacting global corporations and startups alike.

Judith Rinearson
Partner

Ms. Rinearson is a noted expert in prepaid and emerging payments systems. She brings more than 25 years of experience in the financial services industry, including 18 years at American Express's General Counsel's Office.

Her practice focuses on developing areas such as prepaid and emerging payment systems, electronic payments, crypto/virtual currencies, reward programs, Automated Clearing House and check processing. She also has experience on the compliance side of the practice, working with clients on state and federal consumer protection laws, anti-money laundering laws, state money transmitter licensing laws and abandoned property laws.

Ms. Rinearson serves on the Advisory Board of the UK's Emerging Payments Association (EPA).

Jennifer L. Crowder
Partner

Ms. Crowder's practice is focused on FinTech, electronic and emerging payments, financial services, and regulatory compliance. She advises clients on the structuring of financial services, technology solutions, and payment products to comply with applicable state and federal regulations.

She has particular experience negotiating and drafting complex technology agreements, commercial agreements, cross-marketing agreements, development and procurement arrangements, and other technology and software related agreements. She also advises clients on compliance with regulations, laws, opinions, and guidance governing financial services, payments, payment technology, PCI DSS, data security, and privacy.

Linda C. Odom
Partner

Ms. Odom is a noted expert in prepaid and emerging payments systems. She concentrates her practice on representing technology companies and technology users in licensing, software development, data processing outsourcing, intellectual property and e-commerce matters and related litigation.

On the corporate side of her practice, she focuses on technology agreements and compliance issues in the banking and payments industries. Since negotiating the technology agreements for the world's second Internet only bank in 1996, she regularly handles technology, service and customer agreements on behalf of a number of financial institutions and advises them on related regulatory issues.

Ms. Odom has handled a myriad of complex national and global agreements for payments companies, banks, retailers, program managers and processors, including the representation of the program manager in one of the largest GPR card programs in the country.

K&L GATES U.S. FINTECH LEGAL OVERVIEW

John ReVeal
Partner

Mr. ReVeal concentrates his practice on bank regulation, consumer financial compliance, and Bank Secrecy Act and anti-money laundering matters.

Mr. ReVeal advises banking institutions and other financial services providers on consumer compliance law and regulation. In addition, he advises bank and non-bank lenders on state interest and usury matters and assists clients in identifying lender licensing requirements and obtaining the necessary licenses. Mr. ReVeal also assists financial institutions in the review and development of Bank Secrecy Act and Anti-Money Laundering programs, and advises financial institutions regarding bank and thrift powers, federal preemption, and exportation of interest rates and charges. His experience includes development and implementation of enterprise-wide compliance management programs; enterprise-wide BSA/AML compliance programs; annual compliance and BSA/AML risk assessments; preparation for compliance examinations; and the development and review of policies and procedures with respect to consumer deposit, prepaid card programs, mortgage lending, credit card lending, retail lending, and other consumer lending.

T. Richard Giovannelli
Partner

Mr. Giovannelli serves as firm-wide practice area leader for the corporate and transactional practice and is a member of the firm's Management Committee and Diversity Committee. He also heads the firm-wide private equity group.

He maintains an extremely active practice advising private equity funds, businesses, management teams and lenders on complex transactions and governance matters. He regularly works with strategic investing groups at leading national banks in structuring, executing, managing, and disposing of strategic equity investments, both as single investors and as part of bank consortiums, in FinTech and other businesses. He frequently speaks at conferences on cutting-edge transactional law topics.

K&L GATES U.S. FINTECH LEGAL OVERVIEW

An Overview of the U.S. FinTech Market

FinTech, the constellation of industries that represent the convergence of financial services and technology, has grown over the last 10 years from something of a novelty into a universally recognized economic factor. FinTech traces its origins to the payments industry — companies offering alternatives to credit cards, such as pre-paid, gift, and loyalty cards. Over time, FinTech companies have continued to develop innovative payments systems but have also embraced many other high-growth areas including online lending; cryptocurrency; roboadvisors and other wealth management platforms; consumer services; regtech; insuretech; real estate and securities brokerage; credit and other data analytics; and fraud detection.

The FinTech Market

FinTech companies range from startups to some of the world's largest corporations and include payment and credit card companies; banks, asset management firms and other financial institutions; and technology and data businesses. They are financed by venture capital, private equity, corporate, and other investors and lenders, and through the public markets. Supporting the FinTech world are financial advisors and investment banks, law firms, compliance organizations, public relations firms, and other service providers with deep industry and regulatory experience. Companies in all industries, including healthcare, insurance, energy, manufacturing, and retail, are adopting new FinTech technologies and exploring how Big Data, AI, and blockchain will enable them to reach new customers, add new services, or reduce overhead and costs. According to McKinsey & Co., FinTech brings greater efficiency through innovative technologies, especially to the capital market infrastructure value chain.

FinTech, by its nature, is global, and no one single geographic location can fairly be called dominant. Any entity seeking to launch or deploy a FinTech product or service in the United States must address the complex legal and regulatory framework that governs U.S. and global financial services. Navigating the FinTech industry requires dexterity in both innovation and regulation.

The following are key areas of legal and regulatory focus within the U.S. for FinTech companies and their advisors looking into 2019 and beyond, each of which are described in more detail below:

- ***Mergers & Acquisitions/Venture Capital Financing.*** With the continuing, substantial growth of the FinTech sector, many incumbent financial services firms and other companies are seeking to buy, rather than build, new financial technology to stay abreast with the pace of change. At the same time, there is a robust market for FinTech investments by venture capital and other investment funds — U.S. and globally — deploying capital to finance disruptive startups, and by larger institutional investors, including operating companies, making investments in these companies and seeking a strategic advantage as well as a financial return.
- ***Federal and state consumer protection laws.*** Consumer, and in some cases business credit, debit and prepaid, products and services are subject to myriad federal and state laws and regulations, including those focused on fair disclosure, fees, and the handling of unauthorized transactions.
- ***State licensing laws.*** Many states require licenses whenever a non-bank entity holds or moves money or other funds under money transmitter, check-cashing, debt collection, credit, and other licensing laws.
- ***Anti-money laundering (AML), Know Your Customer (KYC), and anti-terrorist financing rules and regulations.*** These are mostly federal laws established to fight money laundering and criminal misuse of our financial system, but also include the laws of other countries that affect U.S. businesses, even those that view themselves as primarily domestic and not global in nature.
- ***Privacy and data security laws.*** Federal and state laws designed to protect personal information by regulating the handling, storage, transmission, and use of data as well as responses to security breaches. Increasingly, U.S. FinTech companies must also comply with new foreign directives, such as GDPR.
- ***Federal and state banking laws.*** Banks must pay careful attention to how they may structure and manage not only their own operations, but also their strategic partnerships with non-bank FinTech companies. Even if the entity is not a bank, understanding the banking requirements for third-party relationships is a critical part of any U.S. FinTech entity's business plan.
- ***Blockchain and cryptocurrency.*** Tokenization of information and use of blockchain and other distributed ledger technologies underlie many disruptive FinTech applications, including digital "coins" and other cryptocurrencies, which are subject to an increasingly complex web of legal and regulatory oversight as

U.S. and other regulators grapple with the balance between allowing innovation and protecting consumers, investors, and financial markets.

Mergers and Acquisitions and Venture Finance

The digital transformation of the banking and financial services industry has resulted in robust venture capital, private equity, and M&A activity across the sector. According to FT Partners, an investment bank focusing exclusively on FinTech, by Q3 2018 a new record had been set for annual FinTech financing volume, surpassing all prior years.

Incumbent banks and other financial institutions, as well as dominant technology companies, seek to acquire additional capabilities while other buyers and investors look to profit from the disruptive innovation that characterizes the FinTech sector. FinTech deals include venture capital and private equity investments, M&A, strategic corporate alliances, loan transactions, and public offerings. They are often cross-border in nature. Frequently, innovative, growing FinTech companies "dual track" the M&A process by considering another investment round or public offering in order to remain independent. In the same vein, large companies typically engage in a buy-versus-build analysis when considering the acquisition of innovative FinTech companies.

While there can be a perception that FinTech companies are typically small startups scraping together seed or early stage capital to develop and deploy a disruptive technology, the reality is that the growth in size and importance of the FinTech sector has also resulted in large transactions involving major companies. Recent examples include the $14 billion in capital raised by Ant Financial during Q2 2018 and Vantiv's acquisition of WorldPay in Q1 2018 for $12.9 billion.

Whatever the form of transaction, FinTech deals require close coordination between the corporate and transactional teams as well as the regulatory specialists when conducting a due diligence investigation of the company's compliance with the various legal and regulatory requirements described in this article. While most corporate practitioners are aware that an acquisition will require careful examination as to whether the deal will trigger any change of control or other consent or notification requirements, which for some companies may require a 50-state survey of the applicable laws, counsel must also consider such requirements in certain venture capital and other non-control financings. For instance, some states require notification of 25 percent change of ownership (or other thresholds well below a transfer or acquisition of 50 percent of a licensed entity).

Somewhat uniquely, lawyers working on M&A and investment transactions in the FinTech arena are routinely called upon to help evaluate a company's business model as well as its contractual architecture from a legal and regulatory compliance perspective. In light of the maze of these considerations encountered by growing FinTech companies, which can sometimes be ambiguous as to application or materiality, this evaluation usually includes risk assessment as a key component. Experienced legal practitioners counsel against assuming that the levels of risk tolerance are aligned or that compliance has the same priority for companies in the same industry that otherwise appear to be comparable. This can be especially important when conducting due diligence on a resource constrained, growing FinTech company.

Ideally, legal and regulatory compliance should be taken into account when setting up the company and structuring early round financings to ensure that neither the company nor its investors are subjected to unnecessary limitations, regulations, or disclosure requirements. For instance, the Nationwide Multistate Licensing System & Registry (NMLS) and money transmitter licensing (MTL) laws often require disclosure of certain information about direct equity holders, directors, and executive officers of the licensed entity, but may not require the same, if any, information from certain equity holders, directors, or executives of a holding company of that licensee. In such situations, it is often beneficial to structure the licensed entity as an operating company subsidiary below a holding company that will receive the venture capital financing and have the customary investor representatives on its board. Counsel to investors and companies thus should consider such requirements as early as possible, because it is more efficient to implement such structures on the front end rather than undertaking a time-consuming and costly reorganization process later at a more mature stage of the company's life cycle.

Consumer Protection

FinTech companies offering credit, debit, or payment products or services, including prepaid cards and other products, are subject to the possible application of an array of state and federal consumer protection laws, including:

Lender Licensing. Certain banks and savings associations are exempt or excluded from state lender licensing requirements, but most other consumer lenders and many commercial lenders will be subject to local licensing requirements. Licensing requirements often depend on interest rates and the type and amount of loan.

Interest Rates and Fee Limits. State laws limit the interest rates and fees that may be charged for consumer loans and many commercial loans. Banks and savings associations often have preemption options, but other lenders will need to comply with each state's law.

Truth in Lending Act and Regulation Z (TILA). TILA is primarily a disclosure law for consumer loans, but imposes substantive limitations or procedural requirements for certain products and protections from unauthorized use of a consumer *or business purpose* credit card. TILA also regulates the compensation that may be paid to consumer mortgage loan originators.

Equal Credit Opportunity Act and Regulation B (ECOA). Although the ECOA primarily protects consumers and businesses from specified forms of discrimination, the ECOA also requires notices in connection with credit applications and adverse actions taken with respect to applications or existing loans.

Electronic Fund Transfers Act and Regulation E (EFTA). The EFTA applies when electronic fund transfers (EFTs) may be made to or from consumer deposit accounts and certain prepaid card accounts. The account-holding institution is required to provide initial disclosures and periodic statements, and consumers are protected from liability for unauthorized EFTs. In addition, the consumer's written consent is required before EFTs may be made from an account if those EFTs will recur at substantially regular intervals, and no person may require such EFTs as a condition to an extension of credit. Finally, effective April 2019, extensive new requirements will apply to payroll card accounts and most general use prepaid card accounts, with some notable exceptions for certain specialized accounts.

Fair Credit Reporting Act and Regulation V (FCRA). The FCRA imposes numerous requirements and limitations with respect to credit reports and other "consumer reports" on individuals. The FCRA limits the circumstances in which such reports may be obtained, requires adverse action or risk-based pricing notices to consumers when decisions are based on consumer reports, imposes accuracy and dispute resolution requirements on furnishers of information to reporting agencies, and includes rules relating to identity theft, fraud alerts, and active duty alerts.

Real Estate Settlement Procedures Act and Regulation X (RESPA). RESPA applies to loans when secured by liens on residential real property. When RESPA applies, there is an absolute prohibition on the payment or receipt of any compensation or benefit for the referral of "settlement services," which includes virtually every service in the home buying or financing process. RESPA also requires certain disclosures in connection with loan applications and loan closings, and regulates mortgage servicing activities.

Anti-Money Laundering and Related Matters

Despite its name, the Bank Secrecy Act (BSA) applies to many non-bank companies and requires them to maintain and comply with a written AML program. Whether a non-bank FinTech company is subject to the AML program requirement requires careful analysis of the precise nature of its products and services. The following non-bank companies must have a written AML program:

- All "money services businesses," also known as MSBs, including:
  - *Money transmitters* – persons that accept currency, funds, or other value that substitutes for currency from one person and transmits the currency, funds, or value to another location or person by any means.
  - *Virtual currency exchangers and administrators* – FinCEN considers virtual currencies that may be converted to fiat currencies as acting as a substitute for fiat currency, with the result that certain virtual currency participants also are money transmitters. Those persons can include a person engaged as a business in the exchange of virtual currency for real currency or other virtual currency; and a person engaged in issuing a virtual currency and who has the authority to redeem such currency.
  - *Providers of prepaid access* – generally, the participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow participants.

A person will be a provider of prepaid access only if there is a "prepaid program." This generally is an arrangement under which one or more persons acting together provide prepaid access, but excludes, among other things:

- Closed-loop prepaid access to funds not to exceed $2,000 maximum value that can be associated with a prepaid access vehicle; and
- Prepaid access solely to (a) employment benefits, incentives or salaries or (b) funds not to exceed $1,000

maximum value and from which no more than $1,000 maximum value can be loaded, used, or withdrawn on any day through a device or vehicle and does not permit international transfers, transfers between users of prepaid access within a prepaid program, or loading additional funds from non-depository sources.

- Larger dealers in foreign exchange, issuers or sellers of traveler's checks or money orders, and casinos and card clubs.
- Certain dealers in precious metals, precious stones, or jewels.
- Residential mortgage lenders and originators.
- Securities broker-dealers, mutual funds, insurance companies, futures commission merchants and introducing brokers in commodities, operators of credit card systems, and housing government sponsored enterprises.

If an AML program is required, the precise scope of the program depends on the type of business, including the following general requirements:

- A system of internal controls to assure ongoing compliance; independent testing for compliance; a designated AML officer to coordinate and monitor day-to-day compliance; and ongoing training for personnel. In addition, banks and certain others must implement procedures for ongoing customer due diligence that includes, among other things, procedures for identifying the "beneficial owners" of legal entity customers.
- A customer identification program (CIP), which generally requires the company to obtain identifying information about the customer and a taxpayer identification number or the number and country of issuance of another form of government issued identification bearing a photograph or similar safeguard, and then to follow procedures to verify the customer identity.
- Systems to identify suspicious activities indicating possible money laundering, terrorist financing, or other criminal activities.
- Filing of suspicious activity reports when appropriate.
- Filing of currency transaction reports for transactions involving more than $10,000, or the filing of a report when more than $10,000 is received in a trade or business.
- The maintenance of other records relating to specified transactions, including larger extensions of credit, funds transfers, and the issuance or sale of checks, money orders, or similar instruments.
- MSBs also must register with FinCEN as such, except in narrow circumstances for agents of other MSBs.
- Finally, all U.S. persons are required to comply with U.S. sanctions laws administered by the Office of Foreign Assets Control (OFAC), which prohibit or limit transactions with specially designated nationals or certain sanctioned countries or regimes.

Privacy and Data Security Laws

There is perhaps no legal area under more scrutiny in 2018 than data privacy and security. All providers of FinTech products and services will need to establish, implement, and maintain an effective framework and mechanism for ensuring compliance with applicable data privacy and security laws, especially those who handle, store, or process sensitive personal information for consumers.

1. Federal Level

Unlike the European Union (EU), there is no single, comprehensive U.S. federal law that regulates both the collection and use of personal data. Instead, there are various applicable regulations that may apply to a FinTech company.

The Gramm-Leach-Bliley Act (GLBA) regulates all collection, use, and disclosure of personal financial information, and its application is broad. While the GLBA privacy and data security rules apply to all "financial institutions," that term is broadly defined to include most companies that provide financial services and products.

GLBA Title V, Section 501 provides conditions in which financial institutions, irrespective of whether they seek to disclose personal information, must develop precautions to ensure confidentiality and security of all consumer records and information provided, and to provide preventative measures against unauthorized access to or use of such records or information. GLBA Title V, Section 502 requires financial institutions to provide the consumer with a notice of the company's information sharing policies with "clear and conspicuous" disclosures both at the time the customer was originated and annually thereafter. In addition, if the institution would share consumer information beyond certain specific exceptions, the institution must provide the privacy disclosure and adhere to the sharing rules for even non-customer consumers.

The required privacy notice must contain information describing the various categories of information that are

collected, the company's policies concerning disclosing non-public personal information ("NPI") to non-affiliated third-parties, protection of such NPI and the procedure behind disclosure of NPI following the termination of the relationship. In addition to the principles in the GLBA, the FTC has issued a separate rule addressing the requirements of safeguarding all NPI, under the Safeguards Rule 16 CFR Part 314, which provides measures that financial institutions must develop and implement to keep customer information secure.

All FinTech companies must be aware of the various implications of the GLBA and incorporate the requirements in a robust privacy and security program to ensure compliance. Emerging payment products and services will likely handle NPI and may require sharing such information with appropriately contracted third-parties who assist in providing the service. It therefore is essential that FinTech companies fully understand their data privacy and security obligations at the federal level.

2. State Level

In addition, many state laws also govern the collection and use of personal data. For example, the California Financial Information Privacy Act (CFIPA) imposes information-sharing consent requirements that go beyond the GLBA opt-out requirements when sharing certain information with nonaffiliated third parties. In June 2018, California passed the Consumer Privacy Act of 2018 (CCPA), which will take effect on January 1, 2020. The CCPA governs a broader range of information than the CFIPA, allows consumers to request information from businesses about the sources from which the business collects information, and allows consumers to opt-out of the sale of their personal information. The CFIPA could lead to similar legislation in other states.

In addition, 48 states and the District of Columbia have enacted laws that require notification of security breaches concerning the disclosure or dissemination of personal information. California has been extremely active in enacting and amending various laws to combat the growing cyber-threats and innovation in technology. The California Security Breach notification law (California Civil Code § 1798.82) was the first of its kind and required any person or business in possession of personal information to disclose any breach of the system consisting of such information. Since the wider enactment of such laws, it has become apparent that initial preventative measures were required and as such more stringent laws have been passed in various states. As a result, it is essential that emerging payment providers fully understand their data privacy and security obligations at the state level.

3. International

FinTech companies that are positioned to provide their products and services to a global consumer base, or may otherwise collect data from such consumers, must be aware of potentially applicable rules governing their global data privacy and security obligations, such as the recent European Union General Data Protection Regulations ("GDPR").

State Money Transmitter Licensing Laws

Forty-nine states (excluding only Montana) and the District of Columbia have MTL requirements for entities that conduct money transmission and/or payment activities in that state. Although many states have adopted a version of the Uniform Money Services Act (the UMSA), there remains a significant degree of variation in the specific statutes adopted by each state. Thus, careful state-by-state analysis is required, both as to whether the company's activities will in fact trigger these MTL requirements and as to the application and registration process within each state once such requirements apply.

Covered Activities and Exemptions

MTL requirements generally apply to businesses that receive and hold consumer funds with the promise of making funds available later or sending funds elsewhere, or issue or sell "payment instruments" that include "stored value." As noted below, only 27 states have made a clear determination as to whether these requirements apply to cryptocurrencies.

Companies with lines of business that fall within this scope should determine if an exemption to the licensing requirements could apply. The UMSA provides an exemption to licensing for, among others: (i) federal, state, and local governmental entities and contractors providing electronic funds transfer of governmental benefits solely on behalf of certain governmental entities; (ii) banks and bank holding companies; (iii) certain companies otherwise registered or regulated under other federal securities, commodities, or similar laws such as commodities brokers, settlement agencies for boards of trade, registered clearing agencies, broker-dealers; and (iv) operators of payment systems solely between otherwise exempt entities.

Some states, however, exempt relatively few persons when compared with the UMSA scope. For example, Connecticut exempts only banks, the U.S. Postal Service, and a person whose activity is limited to the electronic funds transfer of governmental benefits on behalf of the United States, or a state or a subdivision thereof. Conn. Gen. Stat. Ann. § 36a-609. Other states may have an exemption for an agent of a payee, a payroll processor, or a trust company.

Application Process and Requirements

While the state statutes and regulations generally describe the registration process, regulators have broad discretion in choosing how to implement their states' requirements. Unfortunately, this leads to great variance, as each state's application process can be relatively straightforward and simple or lengthy and more involved. On one hand, some states simply require an applicant to submit an application (and an application fee), and, absent any unique characteristics or foreign ownership, the applicant can receive a decision and a license two to three weeks thereafter. Other states, perhaps most notably California, have additional steps in their licensing process and an in-person pre-filing meeting with the Department of Business Oversight is highly recommended. [http://www.dbo.ca.gov/Licensees/money_transmitters]

Even though each state has its own respective registration requirements, many states use the NMLS, as the electronic, web-based portal, allowing an MTL applicant to upload its records, business plans, or other documentation to be viewed by all participating states. The NMLS was originally designed as a national platform for state registration of mortgage loan originators, but has been expanded to allow MTL registration in these states. This provides some efficiency for MTL applicants, and also allows for improved coordination and information sharing among regulators in NMLS-participating states.

Because money transmission involves holding money on behalf of or intended for others, many states require specific information about the applicant and its owners, such as fingerprinting and background checks of the principal owners, directors, and/or executives.

Subject to certain exceptions, MTL licenses generally are not transferable or assignable and most states require licensees to apply for approval if they are undergoing a change of control (generally a change of more than 25 percent in ownership). These provisions require careful examination during sale and certain financing activities of licensed entities and their controlling owners.

Ongoing Operational Requirements

Because consumers entrust money transmitters with funds they owe to third parties, regulators impose certain financial requirements upon MTL applicants, including net worth minimums, evidence of a surety bond, and the mandatory financial reporting. As regulators do employ some discretion, they often reserve

the right to impose stricter net worth, surety bond, or financial statement requirements at will should they have concerns given the information provided. Some states also have "permissible investment" limitations on the funds held for money transmission.

Many startup and smaller FinTech payment companies who find the capital or net worth requirements too challenging or expensive may be able to avoid registration by contracting for secure payment services with an MTL licensee as an "authorized delegate" of a licensee. These agreements require careful attention to ensure compliance with applicable state laws.

Penalties and Fines

Failure to obtain or maintain a license can lead to a wide range of penalties depending upon the state and the nature of the infraction. Violations can lead to severe and costly penalties, as many states consider offenses to be ongoing concerns and levy fines on a per-transaction and/or per-day basis. For example, a regulator could levy a fine of $1,000 per day and per offense, such that the penalty compounds until resolution.

Blockchain and Cryptocurrency

The FinTech world is abuzz with controversies and media reports about the impact of virtual, digital, and/or cryptocurrencies such as Bitcoin, LiteCoin, and Ethereum and their underlying technology, the blockchain. While cryptocurrencies are still making headlines and are an important aspect of FinTech, many believe that the underlying technology of the distributed ledger, or blockchain, is more likely to have a lasting impact on global financial services.

At present, however, the most regulatory scrutiny has been focused on cryptocurrencies, which are essentially digital coins or tokens registered on a blockchain technology platform. Regulators are concerned that consumers are being misled or even defrauded by those selling cryptocurrencies, or that such products are being misused by criminal forces. Therefore, initial focus has been on

licensing, securities law, and anti-money laundering compliance.

With the proliferation of these cryptocurrencies, many consumers now hold some form of digital coin, token, or other cryptocurrency. FinTech companies are rushing in to allow such consumers to use those assets to make payments in the same way that they would otherwise use traditional payment methods such as credit, debit, and prepaid cards. So far, 27 states have addressed whether and how their money transmitter law applies to these and other uses of virtual currency. Some of these states have done this through legislative regulatory amendments, whereas others have provided regulatory guidance explaining how existing state law applies to virtual currencies. Others have announced that they do not regulate cryptocurrencies since they are not legal tender. Most states that regulate cryptocurrencies require issuers, exchanges, or platforms holding, trading, or transferring cryptocurrencies to obtain money transmitter licenses.

As for anti-money laundering laws, FinCEN issued guidance in 2013 regarding the "Application of FinCEN's Regulation to Persons Administering, Exchanging or Using Virtual Currencies" ("Guidance"). The purpose of the Guidance was to "clarify the applicability of the regulations implementing the Bank Secrecy Act (BSA) to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies," which the Guidance refers to as "users," "administrators," and "exchangers."

Both the SEC and the CFTC have consistently announced concerns and have recently taken significant enforcement actions relating to a lack of registration of, and allegedly rampant securities fraud related to, "initial coin offerings," which has led many issuers to instead pursue a "security token offering" where the coins or tokens are issued in compliance with Regulation D or similar securities law requirements. In addition, these agencies, as well as the New York and other state attorneys general, have also taken numerous other enforcement actions against issuers, investors, traders, custodians, and other participants in cryptocurrency and related markets. The regulatory landscape for cryptocurrencies or other tokens is changing quickly and care must be taken to monitor changing developments in both regulatory and enforcement positions.