Privacy & Data Security Alert

April 23, 2018
U.S. FinTech Regulatory Landscape for Companies and Investors

By Elizabeth Donaldson, Dowse Bradwell "Brad" Rustin, IV, Craig Nazzaro

The financial technology (“FinTech”) industry has experienced unprecedented and explosive growth in Georgia as investors are taking notice of Atlanta FinTech companies. Federal and state financial regulators have recently released a number of regulations, policies, and initiatives impacting the FinTech market. As new technology emerges and innovation continues to attract investment and generate economic growth, companies and investors should consider that state and federal regulators are paying attention to the development of this market. State and federal regulators are trying to understand how FinTech impacts consumers and which laws may apply, and are communicating to the public on these topics with increasing frequency.

For startups that want to attract investment and remain viable and competitive, compliance should be an essential element of the company’s operations. The financial system has a low tolerance for risk, and spotty compliance today could negatively impact the startup’s potential to attract investment and create red flags for potential acquirers tomorrow. FinTech investors should also closely monitor developments in regulation and enforcement in order to appropriately conduct diligence on the companies in which they have an interest or may choose to invest.
FinTech companies should pay careful attention to rules and regulations issued by the below agencies and assess compliance risks with legal counsel. The range of new regulation introduced in recent years, and the penalties associated with getting it wrong, have created demand for new and innovative ways of managing compliance and reducing risk. Among other issues, FinTech companies should determine whether they must comply with new cybersecurity rules intended for financial services companies. For example, as discussed below, in 2017 the New York State Department of Financial Services adopted cybersecurity regulations intended to apply broadly.

The top agencies to monitor for regulation and rules applicable to Georgia’s FinTech companies:

1. **New York State Office of the Attorney General and New York State Department of Financial Services**

On April 17, 2018, the New York State Office of the Attorney General ("NYOAG") Investor Protection Bureau sent a wide-ranging questionnaire to 13 major virtual currency trading platforms.[1] The questionnaire, entitled "Virtual Markets Integrity initiative Questionnaire," elicits detailed information from these trading platforms in several areas, including ownership and control, basic operations and fees, trading policies and procedures, outages and other suspension of trading, internal controls, and privacy and money laundering. Per NYOAG, the Virtual Markets Integrity Initiative stems from its duty to protect consumers and ensure the fairness and integrity of financial markets. Accordingly, NYOAG is seeking to increase the transparency and accountability of virtual currency trading platforms, and better inform itself and other enforcement agencies, as well as investors and consumers, about them. NYOAG plans to analyze and compare the questionnaire responses it receives, and ultimately, present its findings to the public.

Meanwhile, the New York State Department of Financial Services ("NYDFS") has already implemented regulations that other state regulators are likely to mimic. If a FinTech company operates in New York or has New York customers, these regulations may apply. FinTech companies should consider complying with New York’s standards or at least modeling their practices based on these regulations. As a financial capital, New York State is likely establishing lasting models of regulation.

**Anti-Money Laundering Rules.** NYDFS has issued a final anti-money laundering regulation that requires regulated institutions to maintain programs to monitor and filter transactions for potential Bank Secrecy Act and anti-money laundering ("AML") violations and prevent transactions with sanctioned entities.[2] The final regulation, which impacts money transmitter, check cashing and banking firms operating in New York State, requires regulated institutions annually to submit a board resolution or senior officer compliance finding confirming steps taken to ascertain compliance with the regulation.[3]

**Bitcoin Licensing Rules.** NYDFS rules for businesses that engage in Bitcoin or other virtual currencies apply to both persons located in New York that engage in activities related to virtual currency and persons located outside New York that engage in activities related to virtual currency with persons located in New York. The rules require persons engaged in specified "Virtual Currency Business Activities" to establish and maintain an effective cybersecurity program, including establishing and maintaining written, board-approved compliance policies, among other requirements related to obtaining and maintaining a license.[4]

**Cybersecurity.** In 2017, NYDFS enacted cybersecurity regulations that apply to all entities licensed, required to be licensed, or subject to other registration requirements under New York banking, insurance or financial services laws ("Covered Entities").[5] The cybersecurity regulations are intended to protect customer information and the information technology systems of Covered Entities. The rules require Covered Entities to establish and maintain a cybersecurity program, adopt a cybersecurity policy, designate a chief information security officer, ensure the security of Nonpublic Information held by third parties, conduct annual penetration testing and vulnerability assessments, and train personnel on cybersecurity, among other requirements.
The NYDFS’s cybersecurity regulation for financial service companies further requires that Covered Entities that allow vendors to access certain information engage in appropriate risk assessment, implement written policies and procedures concerning the minimum cybersecurity practices for vendors, conduct due diligence processes of third-party vendors, and periodic assessment of third-party vendors’ cybersecurity practices.

On March 22, 2018, the Governor of Arizona signed into law HB 2434 which created the first state “sandbox” program for FinTech companies to test their financial products and services without comprehensive regulatory requirements. Under the RSP, a FinTech company can apply to the Arizona Attorney General to be part of the program by describing the technology to be tested and the associated benefits and risk to consumers. If approved by the Attorney General, companies in the RSP will have 24 months to test their product on a limited number of consumers within certain dollar restrictions. Lenders and money transmitters are still subject to Arizona’s statutory restrictions but will not be required to be licensed within the testing period. The program is the first of its kind within the FinTech legal and regulatory space in its desire to allow entrepreneurs to launch and test products on a small scale without having to incur the costs associated with multistate licensing.

A variety of federal laws apply to FinTech companies, including the Gramm-Leach-Bliley Act ("GLBA"), Fair Credit Reporting Act ("FCRA"), Federal Trade Commission Act ("FTC Act"), and the Wiretap Act and the Electronic Communications Privacy Act. A multitude of state laws analogous to the GLBA and the FTC Act apply as well. These state laws include limitations on the collection, use, and storage of sensitive information, including social security numbers, drivers’ license information, financial data, health data, and other data, as well as data breach reporting and notification laws.

In August 2016, the Federal Trade Commission (the “FTC”) announced plans to review the Safeguards Rule of the GLBA. The Safeguards Rule requires financial institutions to develop, implement, and maintain a comprehensive, written information security program that contains administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. The areas in which the FTC sought comment suggest that the FTC is evaluating a broader definition of financial institutions and security requirements, issues that could have important implications for FinTech companies.

Recent FTC enforcement actions have also indicated a renewed focus on the Safeguards Rule and related privacy rules.

- In February 2018, the FTC announced that it settled charges against Venmo’s peer-to-peer payment service for misleading customers regarding the security and privacy of user financial accounts.[6] As part of the settlement, and consistent with several past GLBA cases, Venmo must obtain third-party assessments of its compliance with GLBA rules every other year for 10 years.
- In November 2017, the FTC announced a large settlement with TaxSlayer, Inc., an online tax preparation service, also for violations of the Safeguards Rule and related privacy rules. The FTC asserted that TaxSlayer failed to implement the necessary safeguards to protect “the security, confidentiality, and integrity” of customer information, which resulted in a data breach between October and December 2015, and failed to provide customers with required privacy notices.[7]

Both the GLBA and the FTC Act require FinTech companies to explain their information-sharing practices to their customers and to safeguard sensitive data. FinTech companies are subject to standards promulgated by FinCEN and the SEC. These regulators focus on AML compliance and other cyber misconduct, and new classes of market participants are potentially becoming subject to the FinCEN’s AML rules now that requirements for registered investment advisors have been proposed.[8]

In September 2017, the SEC established a Cyber Unit within its Enforcement Division to target “cyber-related misconduct,” including:

- Market manipulation schemes involving false information spread through electronic and social media
In its 2018 national examination priorities overview, the SEC’s OCIE explicitly identified cybersecurity and AML as two of its five examination priorities. OCIE’s examination programs, applicable to broker-dealers and investment advisors, among others, will emphasize governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response. In addition, OCIE will review for compliance with applicable AML requirements, including whether examinees are sufficiently adapting their AML programs to address their regulatory obligations.

It is critical that FinTech firms and investors understand whether, and to what extent, their businesses are subject to AML and cyber laws and regulations.

The Office of the Comptroller of the Currency (“OCC”), the regulator of federally chartered national banks and savings associations, has released a white paper providing guidance for financial institutions and companies regarding the development of products and services in the FinTech sector. The OCC’s White Paper opened its formal discussion of whether it will create a specialized charter for FinTech companies. The OCC’s White Paper identifies the principles that the OCC plans to use as it continues to develop its comprehensive framework for understanding and evaluating innovative products, services, and processes.

On April 9, 2018, Comptroller of the Currency Joseph Otting announced that the OCC would release its position on a proposed FinTech charter in the next 60-90 days. FinTech companies that receive a charter would be subject to OCC regulation and standards. Notably, Comptroller Otting stated that if FinTech companies are regulated by the OCC, they would be subject to the same rules and regulations as other banks. State regulators, which currently license FinTech companies, have opposed a FinTech charter on grounds that it would exceed the OCC’s congressional mandate.

In early 2016, the Consumer Financial Protection Bureau (“CFPB”) finalized its Innovation Policy, as a part of the CFPB’s Project Catalyst initiative. The Innovation Policy establishes a new process for financial institutions and companies to apply for No-Action Letters regarding the application of consumer regulations to new products that offer the potential for significant consumer-friendly innovation. Through this new process, the CFPB intends to permit financial institutions and companies to clarify regulatory uncertainty during the FinTech product development process. Note, however, that the process is limited in scope and the CFPB will only issue No-Action Letters for unreleased financial products or services, and not for “well-established products or purely hypothetical products.” The process to obtain a No-Action Letter requires that a requestor provide a substantial amount information to the CFPB both initially and throughout the covered period. In September of 2017, the CFPB issued the first No-Action Letter to FinTech company Upstart, to permit them to utilize alternative data in assessing the creditworthiness of prospective borrowers.

In addition, the CFPB released its Final Rule on prepaid financial products, including traditional prepaid cards, mobile wallets, person-to-person payment products, and other electronic accounts with the ability to store funds. The new rule, effective October 1, 2017, applies specific federal consumer protections to broad swaths of the prepaid market for the first time. The rule is intended to provide consumers with additional federal protections under the Electronic Fund Transfer Act analogous to the protections checking account consumers receive. The CFPB has also indicated that it will focus on oversight of third-party vendors.
The CFPB has also penalized companies for misrepresentations regarding data security practices, such as when it subjected the Iowa-based payment processing startup, Dwolla, Inc., to a consent order and hefty fine.[19]

Conclusion

The legal and regulatory landscape continues to evolve for FinTech companies. Those companies that identify legal and regulatory risks during the initial product development phase, and incorporate compliance into their operations from the outset, could create additional value. Ultimately, such compliance is in the long-term strategic interest of the company. For investors, understanding risk in these areas and knowing the questions to ask could be a valuable source of market intelligence.

If addressed correctly, regulatory compliance tends to bring with it legitimacy that can be a market differentiator that elevates FinTech companies above competitors and goes a long way towards more sustainable growth. Get it wrong, however, and a FinTech company can face difficulty raising funding, criminal, civil, and regulatory sanctions, and damage to the value of the business and reputation of the brand. The challenge for FinTech companies remains staying on the right side of legislation and regulators in the highly scrutinized industry of financial services.

FinTech companies should be forward-looking when it comes to compliance and bake in these strategies to help make their company attractive to investors:

- Budget for compliance as a cost of doing business.
- Seek adequate investor funding to address the requirements imposed or anticipated in a rapidly-changing regulatory landscape.
- Establish processes to effectively implement the necessary regulatory changes within the required deadlines.
- Evaluate whether to employ a vendor to manage the company’s data security and to secure sensitive data.
- Engage experienced outside counsel under the attorney-client privilege, along with information security experts, to conduct a comprehensive legal and security risk assessment to evaluate current compliance against current and anticipated regulations.
- Establish an internal working group and work with qualified outside counsel and security consultants to create and develop a comprehensive audit plan for the cybersecurity programs, policies, and procedures that may be required under current and anticipated regulations.
- Review existing third party vendor contracts with counsel and work to develop and then negotiate a contractual addendum that will comply with current and anticipated regulations’ requirements, including cybersecurity requirements.
- Develop with counsel a tailored privacy policy describing how consumer data is collected and used and for what purposes, and publish its privacy policy on any consumer-facing website or mobile application.

For more information, contact:

David Katz at david.katz@nelsonmullins.com or 404.322.6122
Carlos Encinas at carlos.encinas@nelsonmullins.com or 404.322.6908
Elizabeth DeVos at liz.devos@nelsonmullins.com or 864.373.2248
Brad Rustin at brad.rustin@nelsonmullins.com or 864.373.2320
Craig Nazzaro at craig.nazzaro@nelsonmullins.com or 404.322.6969


View on Website

These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship. Internet subscribers and online readers should not act upon this information without seeking professional counsel.

GET IN TOUCH

Elizabeth Donaldson
Associate
T 864.373.2248
liz.donaldson@nelsonmullins.com

Dowse Bradwell "Brad" Rustin, IV
Partner
T 864.373.2320
brad.rustin@nelsonmullins.com