

Client Update

Compliance Issues FinTech Firms (and FinTech Investors) Should Be Focused on in 2016

NEW YORK

Brandon C. Gruner
bcgruner@debevoise.com

Lee A. Schneider
lschneider@debevoise.com

Samuel E. Proctor
seproctor@debevoise.com

Max Shaul
mshaul@debevoise.com

WASHINGTON, D.C.

David A. Luigs
daluigs@debevoise.com

Financial technology (“FinTech”) firms come in all shapes and sizes, and face a wide variety of issues in the course of their operations.¹ Commentators have begun to talk about 2016 as the year of FinTech, but the quantum leaps that many of the firms seek to create have been evolving for many years as the use of technology has grown and spread within financial services. We thought it would be useful to highlight the key compliance issues that FinTech firms should be focused on in 2016, whether they plan to revolutionize the delivery of a financial service, or simply provide better technology solutions to existing industry players. FinTech investors also can use this list to ask questions of the companies they have or will invest in as a way to gauge whether management’s creativity extends to the concerns of key regulators.

ANTI-MONEY LAUNDERING

Financial services regulators focus intensely on anti-money laundering (“AML”) compliance, which will remain a high-risk area for firms throughout the industry given the current political climate. A survey of the landscape yields three themes. First, the scope of the AML regime continues to expand, with new classes of market participants becoming subject to AML rules now that requirements for registered investment advisors have been proposed and are expected to come into force in the next twelve to eighteen months.² Also, New York State’s Department of Financial Services has proposed AML-related rules

¹ FinTech firms generally use software or other technology to offer products and services in or relating to financial services.

² See Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisors, 80 Fed. Reg. 52680 (Sept. 1, 2015).

that, if adopted, will impact money transmitter, check cashing and banking firms operating in the State.³

Second, AML compliance is being broadly interpreted to cover all manner of alleged misconduct. For example, the Financial Industry Regulatory Authority ("FINRA") often views inadequate monitoring protocols to be a violation of AML requirements.

Third, regulators also seek to hold individuals liable for AML failures, bringing a further and more personal dimension to compliance.⁴

It is therefore critical that FinTech firms and investors understand whether and to what extent their businesses are subject to AML laws and regulations. Those firms that provide technology to other market participants should not be surprised if their clients ask about features or capabilities that can assist with such compliance together with representations and warranties around such functionality.⁵

CYBERSECURITY

Cyber and data security issues continue to present compliance challenges for all firms, with media reports of high-profile cyber events now a regular occurrence.⁶ FinTech companies are no exception to this trend. In fact, the intersection between cyber/data security and the FinTech business model means that

³ N.Y. Dept. Fin. Serv., Proposed Superintendent's Regulations Part 504: Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications (Dec. 1, 2015), available at <http://www.dfs.ny.gov/legal/regulations/proposed/rp504t.pdf>.

⁴ See, e.g., FINRA, 2016 Regulation and Exam Priorities Letter (Jan. 5, 2016), available at <http://www.finra.org/industry/2016-regulatory-and-examination-priorities-letter>; see also, the SEC's Office of Compliance Inspections and Examinations, Examination Priorities for 2016 (Jan. 11, 2016), available at www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf.

⁵ The AML rule proposal regarding investment advisers is discussed in: Debevoise & Plimpton LLP, *FinCen Proposes Anti-Money Laundering Rules for Investment Advisers* (Aug. 31, 2015), available at http://www.debevoise.com/~media/files/insights/publications/2015/08/20150831_fincen_proposes_anti_money_laundering_rules_for_investment_advisers.pdf. The rule proposal by NYDFS is discussed in: Debevoise & Plimpton LLP, *NYDFS Proposes New Anti-Money Laundering Requirements, Liability for Compliance Officers* (Dec. 7, 2015), available at http://www.debevoise.com/~media/files/insights/publications/2015/12/20151207_nydfs_proposes_new_anti_money.pdf.

⁶ Kara Scanell & Gina Chon, *Cyber Security: Attack of the health hackers*, FINANCIAL TIMES (Dec. 21, 2015), available at <http://www.ft.com/intl/cms/s/2/f3cbda3e-a027-11e5-8613-08e211ea5317.html#axzz3vjnNV5Ei>.

FinTech firms will likely find themselves increasingly in the cybersecurity “crosshairs” in 2016. In addition to regulators, customers will care deeply about these issues. FinTech companies also should look at their vendors to determine whether they raise any concerns.

FinTech companies and investors should understand the legal, regulatory and functional risks in the cybersecurity realm and consider appropriate responses. Above and beyond the obvious necessity of good systems design and testing, advanced preparation in the form of thoughtful escalation procedures and vendor management should become second nature. Regulators often focus on written policies and procedures, so firms should develop, implement and maintain a playbook to prevent, assess and remediate cybersecurity breaches, including possible external reporting.⁷ Finally, FinTech companies that provide any data hosting services or that will collect, store or maintain any sensitive data on their network should also consider purchasing data breach insurance. Traditional commercial general liability policies often do not cover privacy, data and network security risks.

THIRD-PARTY RELATIONSHIPS

Financial services regulators have increasingly focused on regulation and oversight of third-party outsourcing relationships, also called vendor management. For example, in October 2013, the Office of the Comptroller of the Currency (the “OCC”) issued risk management guidance to national banks and federal savings associations for assessing and managing risks associated with third-party relationships.⁸ Similarly, in December 2013, the Federal Reserve released supervisory guidance on understanding and managing outsourcing risks.⁹ Both sets of guidelines make clear that the financial institution remains liable from a regulatory standpoint for all outsourced functions, require due diligence reviews prior to any such arrangement, and mandate that the regulators be given access to the vendor’s records for purposes of discharging their supervisory obligations. FINRA has taken a similar view for broker-

⁷ See, e.g., Jeremy Feigelson, Lee Schneider & Max Shaul, *SEC Regulation of Cybersecurity Risk and Tech Risk Converges* (Oct. 23, 2015), available at <http://www.law360.com/articles/718238/sec-regulation-of-cybersecurity-and-tech-risk-converges>; Debevoise & Plimpton LLP, *The Cybersecurity Information Sharing Act* (Jan. 6, 2016), available at <http://www.debevoise.com/insights/publications/2016/01/the-cybersecurity-information-sharing-act>.

⁸ OCC, Risk Management Guidance (Oct. 30, 2013), available at <http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html>.

⁹ Fed. Res. Sys., SR 13-19: Guidance on Managing Outsourcing Risk (Dec. 5, 2013), available at <http://www.federalreserve.gov/bankinforeg/srletters/sr1319.htm>.

dealers.¹⁰ Moreover, the CFPB has also indicated that it will focus on oversight of third-party vendors.¹¹ Thus, FinTech firms that act as service providers to financial institutions, or that are otherwise working with financial institutions, should be cognizant of the increased regulatory focus on third-party vendor management and should be prepared to have financial institutions (i) conduct due diligence, (ii) negotiate contractual provisions concerning breach notification, compliance with privacy regulations, audit rights, and indemnification, and (iii) limit access to specified parts of a financial institution's network.

CONSUMER AND INVESTOR PROTECTION REGULATIONS

Laws and regulations governing the provision of financial services and products to consumers/retail investors are part of the FinTech competitive landscape. Depending on the nature of the particular product or service, companies may need to understand:

- An array of laws and regulations enforced by the Consumer Financial Protection Bureau ("CFPB"), including the Truth in Lending Act, Truth in Savings Act, and the prohibition on unfair, deceptive and abusive practices ("UDAAP"). The CFPB, a new federal government agency created in the wake of the financial crisis, is tasked with protecting consumers in the financial sector. It has very broad jurisdiction (including over banks, credit card issuers, payday lenders, check cashers, debt collectors and other financial companies assisting consumers with cash or loans).¹²
- Securities laws and regulations that apply to FinTech companies operating in the retail securities space such as the Investment Advisers Act of 1940 (the "Advisers Act"), which may require companies offering investment advisory services to register as investment advisors with the Securities and Exchange Commission ("SEC"). This includes advisors to certain types of investment funds, such as those utilizing hedge or private equity strategies. Companies

¹⁰ See also FINRA, Regulatory Notice 05-48: Members' Responsibility When Outsourcing Activities to Third-Party Service Providers (Jul. 2005), available at <https://www.finra.org/sites/default/files/NoticeDocument/p014735.pdf>.

¹¹ See CFPB, Bulletin Regarding Service Providers (Apr. 12, 2012), available at http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf.

¹² See, e.g., Debevoise & Plimpton LLP, The CFPB Eyes Mobile Financial Services (Dec. 17, 2016), available at <http://www.debevoise.com/insights/publications/2015/12/the-cfpb-eyes-mobile-financial-services>.

offering brokerage services might have to register with the SEC and FINRA as a broker-dealer.

- Aspects of securities laws that govern securities offerings, whether public, private, or crowdfunded, for those FinTech companies seeking to raise capital from individual investors.¹³
- Laws and regulations relating to duties of care that might apply to certain FinTech firms, particularly to those offering trust and asset management services. For example, the Employee Retirement Income Security Act of 1974 (“ERISA”) imposes fiduciary duties on persons exercising discretionary authority or control with respect to the management of ERISA plan assets. In April 2015, the U.S. Department of Labor (the “DOL”), which is the agency primarily responsible for promulgating regulations under ERISA, proposed a number of ERISA-related regulatory changes, including an extensive overhaul of the definition of “investment advice” for purposes of determining who is a fiduciary of employee benefit plans under ERISA.¹⁴ The DOL’s revised definition would treat as a fiduciary virtually anyone making an investment-related recommendation to an ERISA plan or an IRA, or to an ERISA plan participant or an IRA beneficiary, when receiving any compensation in connection therewith.¹⁵

THE OUTLOOK FOR 2016

Each new year brings a sense of excitement. We hope that 2016 continues the trend of FinTech innovations that make our financial lives easier. The firms that bring us these advances also should recognize that as they become more successful, regulators will increasingly turn their attention to FinTech. The regulatory regimes discussed above may provide the lens through which regulators will seek to understand the FinTech industry. Even firms that “only” provide their technologies to others will feel the pressure from vendor management requirements.

¹³ See, e.g., Debevoise & Plimpton LLP, *The SEC Hands Out a Halloween Treat to Crowdfunding Supporters* (Nov. 17, 2016), available at http://www.debevoise.com/~media/files/insights/publications/2015/11/20151117_the_sec_hands_out_a_halloween_treat_to_crowdfunding_supporters.pdf.

¹⁴ See Definition of the Term “Fiduciary”; Conflict of Interest Rule – Retirement Investment Advice, 80 Fed. Reg. 21928 (Apr. 20, 2015).

¹⁵ For a further discussion of the DOL’s proposal, see Debevoise & Plimpton LLP, *DOL Catches Many in Expanded Fiduciary Net; Is Proposed Exemption an Escape Hatch or a Trap Door?* (Apr. 21, 2015), available at <http://www.debevoise.com/insights/publications/2015/04/dol-catches-many-in-expanded-fiduciary-net>.

As regulators become more sophisticated about new trends and technologies, they will ask better questions. We encourage FinTech companies to stay abreast of directly applicable regulations, and in addition, to develop a familiarity with those regulations relevant to their customers and clients.

* * *

Please do not hesitate to contact us with any questions.