LJN LAW JOURNAL NEWSLETTERS

Business Crimes Bulletin ®

An ALM Publication

Volume 23, Number 9 • May 2016

FinTech: The Emerging Financial Crime Compliance Minefield

By Daniel R. Alonso and Timothy C. Stone

More than ever, the intersection of technology and financial crime compliance (FCC) for financial institutions is dynamic terrain. At the same time, technology continues to improve, and sometimes disrupt the way in which consumers and businesses participate in the financial services industry. The proliferation of so-called "FinTech" — particularly by startups outside the financial sector — raises a host of thorny FCC issues for regulators and financial institutions required to comply with the Bank Secrecy Act (BSA) and its anti-money laundering (AML) mandates. These include how to define the financial crime risks at play; if, how, and to what extent a new technology or service falls within the scope of existing regulations; and, for banks and other institutions that partner with FinTech startups, ensuring compliance with rules on third-party risk.

THE PROLIFERATION OF SO-CALLED "FINTECH" — PARTICULARLY BY STARTUPS OUTSIDE THE FINANCIAL SECTOR — RAISES A HOST OF THORNY FCC ISSUES FOR REGULATORS AND FINANCIAL INSTITUTIONS REQUIRED TO COMPLY WITH THE BANK SECRECY ACT (BSA) AND ITS ANTI-MONEY LAUNDERING (AML) MANDATES.

Background

In one sense, FinTech is nothing new. In the 1960s, mainframe computers and ATMs were early precedents, marking the analog-to-digital evolution of financial services. But these days, we more commonly associate FinTech with the rapid and pervasive wave of innovations in financial services over the last decade that, by and large, has tracked advances in computing and mobile technology. In retail banking, for instance, consumers already take for granted some recent forms of FinTech — mobile check depositing comes to

Daniel R. Alonso, a member of this newsletter's Board of Editors and a former federal and state prosecutor, is Managing Director and General Counsel of Exiger, which specializes in financial crime compliance. **Timothy C. Stone**, an Associate Director at Exiger, is a former Assistant District Attorney in Manhattan.

mind — as indispensable parts of the banking experience. Other emerging FinTech areas range from public funding sources ("crowdfunding") and streamlined electronic payment processes ("e-payments") to consumer-driven lending ("person-to-person lending") and artificial-intelligence-based financial advisory services ("robo-advisers"). One need only glance at Forbes' "Fintech 50," published for the first time in December 2015, to appreciate the breadth and, at times, groundbreaking potential of these new technologies.

Regulatory Risk

With such potential, of course, comes the FCC and regulatory risk. At their core, most FinTechs allow money to change hands faster and more efficiently, whether via electronic payments, new methods of lending or investing, or even entirely new "virtual" currencies. These technologies carry great potential for abuse not only by money launderers, but also by sanctions evaders and terrorist financers. Illustrating the point is the tragic mass shooting in San Bernardino, CA, on Dec. 2, 2015. As revealed by investigators, the shooters used a pretext to obtain an almost $30,000 loan from a "marketplace lender," a FinTech that combines investment capital with data-driven online platforms for lending money to consumers and small businesses. The shooters reportedly used the loan funds to help pay for ammunition, pipe bomb components, and target pactice at local gun ranges. In other words, they financed an act of terrorism with money that, but for a new FinTech-based lending tool, might not have been available.

Compounding the problem is that FinTech innovators often come from outside the traditional banking and financial world, and may fail to grasp the implications — both direct and indirect — of financial crime risk. Some FinTech business models, such as mobile payment services, fall squarely within the BSA's scope, and those companies must address FCC issues head-on. But all FinTechs, even those not expressly bound by the BSA, have to be concerned about financial crime exposure, as banks may demur from doing business with customers that pose too great a financial crime risk. FinTech pioneers can thus face a real predicament, having frequently begun as startups with only a handful of employees, devoid of compliance history and culture. Indeed, such firms may question why their business should be subject to FCC-centric scrutiny better aimed at banks, or they may simply be unaware of, or confused by, which rules govern them.

And some FinTechs, operating on shoestring budgets, may be disinclined to spend the money to get answers to such questions, much less to build a compliance-driven infrastructure from the ground up. Indeed, part of the appeal of FinTech is that such firms are nimble, focusing on growth and maximizing profits.

What's more, FinTech-specific compliance challenges can be as nuanced and manifold as financial innovation itself. Take, for example, the implications of "blockchain" technology — the underpinnings of the virtual currency Bitcoin — for the future of global banking. Itself a form of FinTech, "virtual" or "digital" currencies are not backed by any central bank or

government, and do not have legal tender status in any jurisdiction. Bitcoin was the first major virtual currency, and the blockchain is Bitcoin's revolutionary engine: network nodes verify any transaction using the currency and record them on the blockchain — a virtual public register or "distributed ledger."

The transparency and security of the distributed ledger can obviate the need for financial intermediaries, such as banks, to facilitate and verify that a transaction is genuine. In the correspondent banking realm, such technology can potentially be used for currency clearing and settlements — potential that is quickly becoming reality. As of February, J.P. Morgan has reportedly been testing blockchain on U.S. dollar transfers between London and Tokyo, and may expand testing to real trades as soon as the third quarter of 2016. The impending use of distributed ledger technology for cross-border asset transfers invites new compliance challenges, such as how best to adapt and integrate current transaction-monitoring systems and other compliance tools.

Considering these and other factors, it is no surprise that FinTech has been attracting attention from regulators, with money laundering and related concerns a key focus. On the one hand, some FinTechs fit within established regulatory paradigms such as the BSA. This includes mobile payment services, which are generally "money transmitters" under the BSA's regulatory framework, and must therefore abide by the currency reporting and AML compliance program requirements for "money services businesses." Other areas of financial innovation, though, have triggered targeted responses from regulators, including the issuance of new rules.

Virtual Currencies

Consider virtual currencies like Bitcoin. At the federal level, in 2013, the Financial Crimes Enforcement Network (FinCEN) issued guidance defining certain types of virtual currency purveyors — "administrators" and "exchangers" — as money services businesses, and thus within the scope of the BSA. This set the groundwork for FinCEN's first enforcement action against a virtual currency company for BSA violations, with FinCEN sanctioning the firm in May 2015 for, among other things, failing to implement and maintain an adequate AML program. (Notably, the Chief of IRS Criminal Investigation, Richard Weber, warned at the time that unregulated virtual currency "opens the door for criminals to anonymously conduct illegal activities online," "creating a Wild West environment where following the law is a choice rather than a requirement.")

New York State has charted its own regulatory course for virtual currencies. In August 2015, the state banking regulator established a "BitLicense": a full suite of regulatory requirements for those engaging in the commercial exchange of virtual currency from, or through, New York. Subject to certain exceptions, licensees must pay a several-thousand-dollar fee and comply with a host of rules that include AML and KYC program requirements (*e.g.*, maintaining customer identification and verification documents, as well as records linking clients to their respective accounts and balances). Across the Atlantic, in

March 2015, the UK (HM Treasury) signaled in response to its earlier public call for information regarding virtual currencies that it intends to apply its current AML framework to virtual currency exchanges.

On the Horizon

Both at home and abroad, additional regulatory activity concerning FinTech is on the horizon for 2016 and beyond. In February, the G20's Financial Stability Board announced its forthcoming consideration of rules to address the destabilizing effects of FinTech — seemingly the first time that global-level regulators have focused specifically on the matter. Although no silver bullet will ever exist for handling all the potential compliance issues at stake, firms using FinTech can take some commonsense steps to prepare themselves from an FCC risk perspective.

Banks and financial institutions should heed the standards of the Financial Action Task Force (FATF): before using new or developing technologies, conduct a risk assessment to identify and assess the money-laundering or terrorist-financing risks, and fashion appropriate measures to manage and mitigate those risks. If partnering with FinTech firms, this should ordinarily involve rigorous due diligence, including developing compliance intelligence by proactively engaging with the company. FinTech startups faced with the financial sector's daunting regulatory and FCC environment should consider seeking expert advice or aligning with businesses that already have in place mature compliance infrastructures.

In New York, nascent FinTech companies can take advantage of legal clinics that seek to attract startups by offering assistance with regulatory and compliance matters, such as the Brooklyn Law Incubator, the Cardozo Law Tech Startup Clinic, and the Fordham Law Center on Law and Information Policy (which are collaborating with the New York State Attorney General and the New York City Corporation Counsel). Consumer-protection-focused regulators also have programs meant to help companies navigate the financial sector, thereby benefiting consumers through fostering innovation. This includes in the United States (the Consumer Financial Protection Bureau's "Project Catalyst") and the United Kingdom (the Financial Conduct Authority's "Project Innovate").

Conclusion

What is clear is that because FinTech poses unique FCC and regulatory risks, both FinTech companies and those that use FinTech, must be prepared. Startups pride themselves on being nimble, but they are obligated to understand the financial crime implications of their technology and the regulatory environment in which they operate. Banks and financial institutions, to the extent they are engineering their own forms of FinTech or partnering with startups, need to tread responsibly in embracing financial innovation. The regulators will undoubtedly be watching, and learning.

—❖—