Complying with AML Laws: Challenges for the Fintech Industry

April 5, 2016 By Jodi Avergun and Colleen Kukowski

"*Silicon Valley is coming. There are hundreds of startups with a lot of brains and money working on various alternatives to traditional banking.*"

This warning came not from a pundit or Silicon Valley lobbyist, but from Jamie Dimon, the Chairman and Chief Executive Officer of JPMorgan Chase & Co. New technology in the financial industry is changing how people manage their finances. This merger of financial services with technology, referred to as "fintech," is a booming industry. In 2014 alone, technology-focused venture capital firms invested $12.2 billion in fintech startups, a threefold increase over the previous year. Startups are not the only companies racing to join the industry. Heavyweights in the financial services industry, such as JPMorgan Chase and Goldman Sachs, are also adopting fintech services such as peer-to-peer payments and same-day approval of small business loans.

http://www.crowdfundinsider.com/2016/04/83845-complying-with-aml-laws-challenges-for-the-fintech-industry/

But if Silicon Valley is coming, so is the government. A major challenge to the growing fintech industry comes from government scrutiny and enforcement actions – particularly as they relate to money laundering and the financing of terrorist activity. Since government scrutiny is a likely reality, this article urges fintech companies to be aware of their anti-money laundering obligations and the challenges that they face in designing a robust AML compliance program sufficient to satisfy regulators.

How Does Fintech Work?

Most fintech transactions occur through an application on a smartphone or company website and are completed on an accelerated timetable. Fintech companies' offerings vary, but include the following categories of services:

Mobile Payment Systems and Digital Wallets: Mobile payment and digital wallet apps, such as Venmo, allow users to store, send and receive funds from their account on the app. Users open an account with the app and have the option of linking their credit card or bank account to their Venmo account. Users can then transfer funds from their app account to another app user's account. When one user transfers money to another user's account, the recipient can choose to either store those funds in his/her app account for future payments, or transfer those funds to the linked credit card or bank account.

Peer-to-Peer Money Transfer: Peer-to-peer money transfer companies, such as TransferWise, use peer-to-peer technology to avoid bank fees charged for sending money overseas. If a user wants to transfer money from the U.S. to Europe, for example, the company finds a user who is seeking to transfer money in the opposite direction (Europe to the U.S.), and then makes the transfers from the local euro or dollar accounts, so that no currency crosses a border. Peer-to-peer money transfer systems are the high tech equivalent of the ancient Islamic hawala money transfer system, which transfers money without actually moving it across borders.

Online Marketplace Lending: Companies that offer online marketplace lending use online platforms to lend either directly or indirectly to small businesses and consumers. Companies operating in this industry tend to fall into three categories:

- Balance sheet lenders that originate loans for borrowers (for example, OnDeck);
- Bank-affiliated online lenders that originate loans for borrowers; and
- Peer-to-peer lenders that sell securities to obtain the financing to enable third parties to fund borrowers (for example, Lending Club).

Scrutiny of and Potential Action Against Fintech Companies

The anonymity and speed of fintech services raise the risk that terrorists and criminals will exploit fintech to support their illicit activity. As a result, fintech companies should expect and be prepared for government scrutiny of their compliance with AML laws.

http://www.crowdfundinsider.com/2016/04/83845-complying-with-aml-laws-challenges-for-the-fintech-industry/

For example, when the Paris attacks aroused suspicions that ISIS is using fintech, European Union ministers agreed to strengthen controls on payment methods that can be conducted anonymously. Domestically, it appears that a $28,500 loan from peer-to-peer lender Prosper to the San Bernardino shooter Syed Rizwan Farook may have helped Farook pay for ammunition, pipe bomb components and target practice at local gun ranges. Even if Prosper and its third-party lender, WebBank, committed no wrongdoing, regulators will seek assurance that online lenders and other fintech companies are fully complying with AML laws designed to prevent and detect illicit transaction.

The recent Liberty Reserve prosecutions may also prompt regulators to examine fintech companies' compliance with AML laws. Liberty Reserve was an online payment processor and digital currency system that was closed in 2013. In January 2016, Liberty Reserve's co-founder pleaded guilty to money laundering conspiracy and acknowledged that Liberty Reserve was "susceptible" to being used for criminal activity. The indictment against Liberty Reserve, which is still pending, alleges that "unlike traditional banks or legitimate online payment processors, Liberty Reserve did not require users to validate their identity information, such as by providing official identification documents or a credit card," which made Liberty Reserve Transactions anonymous and untraceable. Consequently, the government alleges, the merchants who accepted Liberty Reserve payments included computer hackers, unregulated gambling businesses, drug dealing websites, and traffickers of stolen credit card data and personal identity information.

AML Regulations That Apply to Fintech Companies

Even though fintech services vary greatly from traditional financial services, many are subject to the same AML regulations as other financial institutions. For example, because digital wallets, mobile payment systems, and peer-to-peer transfer systems are all money service businesses ("MSBs"), they are subject to the Bank Secrecy Act's ("BSA") reporting and compliance requirements. Specifically, MSBs are required to: (1) register with the Treasury Department; (2) develop an effective AML program; (3) file Currency Transaction Reports for transactions that exceed $10,000; and (4) file Suspicious Activity Reports ("SARs") when the company knows, suspects, or has reason to suspect that a transaction may involve money laundering or other illicit activity. Furthermore, Section 326 of the USA PATRIOT Act requires that financial institutions

have customer identification programs in place and maintain related customer due diligence standards, referred to as "know your customer" ("KYC").

These regulations are robust. An AML compliance program must be in writing and must provide: (1) a system of internal controls to ensure ongoing compliance (which includes verifying customer identification); (2) independent testing for compliance; (3) an individual designated as responsible for coordinating and monitoring day-to-day compliance; and (4) training for appropriate personnel. Fintech MSBs must also make and retain records for any fund transmissions amounting to $3,000 or more.

AML Challenges for the Fintech Industry

To comply with the law – and to ensure that their services are not exploited by bad actors – companies offering fintech services must know how to comply with AML regulations, as well as how to avoid common pitfalls in fintech compliance programs. Detailed below are just a few of the challenges that fintech companies face in complying with AML regulations:

- **Fintech companies need to have operational AML programs as soon as their business opens.** Fintech companies are required to have robust AML programs that are fully operational when they begin offering financial services. However, because many fintech companies start small and grow over time, there may be a gap between when a company first offers financial services and when its compliance program is fully running. As a result, financial transactions may go unmonitored, and companies may unwittingly operate without complying with all regulations, and thus may be vulnerable to prosecution or enforcement action.

For example, in May 2015, the Financial Crimes Enforcement Network (FinCEN) assessed a $700,000 civil money penalty against Ripple Labs, a digital currency operator, for its failure to register as an MSB and its failure to implement and maintain an adequate AML program. Although Ripple Labs began selling digital currency in August 2013, it did not fully implement its AML compliance program until nearly a year after it began its sales. During that year, Ripple Labs engaged in a series of transactions for which it failed to generate the required SARs.

- **Rapidly growing fintech companies need to ensure that their compliance program grows in scale with their business.** Once a fintech company has established an AML compliance program, the AML compliance program may not keep pace with the company's business. For example, an effective AML program requires conducting KYC due diligence. A fintech startup may conduct adequate KYCs on the company's initial customer base; however, the KYC process may be overwhelmed as the company grows and attracts larger volumes of customers from diverse backgrounds and locations. Similar problems may arise in generating SARs and satisfying other reporting requirements

as transactions taking place across an app increase rapidly over a year.

As Bruce Wallace, chief digital officer of Silicon Valley Bank Financial Group, recently observed:

"*Banks have hundreds, sometimes thousands, of employees committed to compliance functions. Just think for a moment of a startup with five or six employees, mostly engineers, who now have to navigate the landscape of a highly complex regulatory environment. In many cases, it's not as simple as 'if your fintech company does X' then you simply put this specific program in place. They have to spend a lot of cycles figuring out what they need to be in compliance with and then build and institutionalize their program.*"

- **Anonymous payments should not be permitted for any transaction, regardless of amount.** Financial institutions are required to verify a customer's identity. Given that anonymous payments were the focal point of the Liberty Reserve prosecutions, and attracted the scrutiny of European regulators after the Paris attacks, fintech companies should be wary of allowing users to process any payments without verifying their identities – regardless of transaction limits. Some fintech companies currently allow users to complete low-valued transactions (for example, $299.99 or less) without requiring the users to verify their identities. Fintech companies need to consider the possibility of conducting KYC procedures on all users, no matter how small the amount of the transaction. For example, the 2004 Madrid bombers used the sales of Moroccan hashish to support their terrorist attacks. Similar payments for drugs, so long as they fall under the $300 transaction limit, can still occur anonymously on some mobile payment and digital wallet systems. When multiple small payments are layered or aggregated, terrorists (or other criminals) have the means to finance low-cost attacks such as those in Paris and San Bernardino. Undoubtedly alert to this threat, regulators are not likely to hesitate to take action against fintech companies that allow the threat to persist.

- **Peer-to-peer lending companies need to implement fully operational AML programs whether they are subject to the BSA regulations or not.** The recent scrutiny of Prosper's loan to San Bernardino shooter Syed Rizwan Farook confirms the importance of peer-to-peer lending companies having full AML programs in place. Because the banks that originate their loans bear full responsibility for complying with the BSA's AML requirements, peer-to-peer lending companies may not have the same incentives to ensure that they are adequately detecting, reporting and preventing money laundering or terrorist financing. Nevertheless, peer-to-peer lenders cannot take a *laissez-faire* approach to putting adequate KYCs in place. Although a peer-to-peer lender may not be liable for failing to comply with the BSA, it can still suffer reputational damage if a loan made to a customer is implicated in a terrorist or criminal scheme.

Conclusion

As the fintech industry transforms traditional banking practices, it falls under enhanced government scrutiny. Without a thorough AML compliance program in place, fintech companies risk damage to their reputation and the loss of investor and customer confidence in their business. In order to continue growing without the risk of not complying with AML laws, fintech companies – and the financial institutions that partner with them – must know the AML requirements that apply to their business, identify potential weaknesses within their AML compliance programs, and implement gold standard AML compliance programs.

Jodi L. Avergun is a partner at **Cadwalader, Wickersham & Taft LLP** in Washington. Her practice focuses on representing financial institutions, corporations and individuals in criminal and regulatory matters involving, among other things, the FCPA, securities enforcement, anti-money laundering, health care, and general white collar matters. Prior to joining Cadwalader, Jodi spent 17 years as a federal prosecutor with the United States Attorney's Office for the Eastern District of New York and with the Criminal Division of the Department of Justice.

Colleen D. Kukowski focuses her practice on white collar criminal defense and compliance issues. She advises clients in a variety of criminal and regulatory matters, concentrating primarily on international corruption and internal corporate investigations. Prior to joining Cadwalader, Colleen served as an intelligence analyst in the Federal Bureau of Investigation's Counterterrorism Division, where she supported top priority terrorism investigations and worked extensively with Foreign Intelligence Surveillance Act (FISA) surveillance.

http://www.crowdfundinsider.com/2016/04/83845-complying-with-aml-laws-challenges-for-the-fintech-industry/