Credit Union Times
Trusted News for Credit Union Leaders
An ALM Publication
JUNE 14, 2017 | CUTIMES.COM

GUEST OPINION

Comply Now: Six Regulatory Considerations for CUs and Fintechs

Xavier Oustalniol
Partner
StoneTurn
xoustalniol@stoneturn.com

Jamal Ahmad
Managing Director
StoneTurn
jahmad@stoneturn.com

Fintech, the emerging financial technology services sector, has experienced explosive growth in recent years as new products continue to launch across various sectors, including cyber currencies, consumer finance, banking, insurance and investment advisory services. Non-bank lending and digital payment processing (including online payment processing, mobile wallet payment and online peer-to-peer money transferring), two areas of fintech most closely associated with "traditional banking," account for much of this growth.

As these new technologies and companies continue to launch in tandem with a growing credit union industry, opportunities for fintechs and credit unions to collaborate are also on the rise. However, along with this growth of the non-bank lending space comes growing regulatory scrutiny. For instance, the FDIC has noted its concerns about the risks it associates with marketplace lending, including third-party compliance, transactional risks, servicing and liquidity. The CFPB has also begun accepting consumer complaints regarding online marketplace lenders making consumer loans.

Oftentimes, given the limited resources of a "start-up" or emerging organization, ethics and compliance programs are considered only after unknown risks are taken and regulatory issues arise. The programs put in place are often underfunded, understaffed and mostly insufficient to withstand regulatory scrutiny. Therefore, for those looking to seize opportunities for continued growth in the non-bank lending space, these six regulatory considerations should be prioritized:

1. Know the Rules

Develop an enterprise-wide view of regulatory compliance to facilitate a holistic understanding of the applicable laws and agency rules, and then tailor the compliance program to satisfy those rules and optimize compliance costs.

No area is more important for U.S. financial institutions than compliance with Bank Secrecy Act/Anti-Money Laundering, and Office of Foreign Assets Controls and terrorist financing rules and regulations. While BSA/AML compliance is broadly interpreted to cover alleged misconduct, and fintech companies may generally be subject to the same BSA/AML regulations as traditional financial institutions, some offered products and services may be considered exceptions. For example, peer-to-peer lenders are not responsible for BSA/AML compliance on loans – only the originating banks are responsible. Similarly, payment processors need to be aware of and comply with the requirements of federal consumer protection laws, as well as the guidelines of the various states in which they operate.

The Office of the Comptroller of the Currency has proposed special purpose national charters for payment processors and lenders. If successful, this would create a national regulatory framework instead of the current disparate state programs.

2. Know Your Risks

Conduct periodic and robust assessments to identify risks arising from applicable regulations, new product offerings and customer bases. Key risks may include: The potential financial impact of regulatory enforcement, reputational risks as a result of public actions, and operational risks associated with potential cease and desist orders. Risk and performance indicators developed using both quantitative and qualitative data should be captured, consistently measured and reported.

The risk tolerance for an established fintech firm may differ from that of a start-up. Thus, it is important to understand the level of risk your organization will accept relative to its stage of development and identify the necessary resources to mitigate them. Once identified, risks should be weighed against established

controls, while deficiencies and weaknesses around key entity and business level processes should be mapped to defined laws, regulations and industry standards for periodic testing.

Understanding the rules and knowing the risks may involve ensuring there are knowledgeable personnel in the company, sufficient internal processes to be credible in establishing appropriate preventative and detective controls, and including the right professionals to advise management and the board.

3. Use Technology

Companies should define the scope and frequency for monitoring and testing of transactions and consider the relevant factors (e.g., results of the company's due diligence and risk assessments). Use of a technology-based monitoring system to review transactional data in real time and flag problematic transactions indicative of violations of laws or regulations eliminates the need for a fully-staffed compliance department to manually monitor and review transactions. Additionally, establish a workflow to allow flagged transactions to be researched thoroughly with documented results. The challenge is to isolate true problems and not expend resources chasing false positives.

4. Geography Matters

As fintech companies expand, they will need to tailor their compliance programs to applicable U.S. and foreign laws. For instance, depending on the country in which it operates, a payment services provider may find itself subject to a multitude of varying regulations.

Non-bank lenders face similar concerns. For example, the China Banking Regulatory Commission recently announced it will require peer-to-peer lending platforms to use commercial banks as third-party fund custodians and Shanghai's financial authority is proposing new rules that will require these lenders to disclose more financial data. The U.K.'s Financial Conduct Authority requires online lending platforms to provide, among other things, a detailed explanation of the risks to potential investors.

5. Third-Party Risk Management

Any fintech risk management initiative would be incomplete without proper consideration given to third-party risk management, including customer relationships, vendor risk management, and the potential for related BSA/AML, OFAC and terrorist financing issues. Many fintechs also have partnerships with financial institutions that require them to abide by rigorous third-party programs.

Accordingly, and similar to traditional banks, both payment processors and non-bank lenders must develop robust Know Your Customer and Enhanced Due Diligence protocols to understand their customers and vendors, and assess the extent of the risk associated with those third parties. Due diligence procedures should be sufficiently documented and negative findings, if any, pursued.

6. Protect Your House

As fintech companies obtain greater amounts of information about customers and other third parties and store it online, protection of data becomes a primary compliance concern. Many countries, such as the U.S., U.K. and Canada, have rules designed to protect consumer data and some regulators have started to require companies to establish cybersecurity policies. It is crucial to understand the legal, regulatory and functional risks associated with cybersecurity and consider appropriate responses.

As regulators increase the spotlight, fintech companies must rise to the challenge and ensure that their compliance programs can withstand regulatory scrutiny. This enhanced effort early in the company's life cycle may separate it from the competition, permitting management to focus on the core mission of the enterprise. ■