Chapman and Cutler LLP

To the Point!

February 3, 2016 Legal, Operations and Strategy Briefs for Financial Institutions

FDIC Emphasizes Corporate Leadership to Address the Key Risk Management Issues Raised by Cybersecurity and Marketplace Lending

On February 1, 2016, the FDIC issued Financial Institution Letter 9-2016 announcing the publication of its Supervisory Insights issue for Winter 2015. In addition to the regular Regulatory and Supervisory Roundup that summarizes recently released regulations and supervisory guidance, this edition of Supervisory Insights includes articles on two hot topics for financial institutions and regulators alike: cybersecurity and marketplace lending. The two articles were prepared by the fraud and financial crimes and risk management staff of the FDIC, respectively. In each article, the FDIC emphasizes that the challenges and opportunities banks face must be addressed at an organizational level with the leadership and involvement of the board of directors.

The FDIC's Winter 2015 edition of Supervisory Insights can be found at the following link: https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin15/SI_Winter2015.pdf

A Framework for Cybersecurity

The FDIC continues to identify cybersecurity as a critical issue facing financial institutions and outlines how banks can enhance their information security programs to more effectively mitigate and manage emerging cybersecurity risks. The requirement to establish an information security program has been imposed on financial institutions since 1999 pursuant to the enactment of the Gramm-Leach-Bliley Act. The FDIC explains that a cybersecurity framework should be implemented as part of a bank's information security program and should be updated regularly to appropriately address emerging risks. Four components are recognized as critical to designing an effective cybersecurity framework: corporate governance, threat intelligence, security awareness training, and patch-management programs.

Corporate governance is the basis for developing a cybersecurity framework. It is crucial that a bank's board of directors and executive management institute a corporate culture prioritizing cybersecurity, which should be implemented through enterprise-wide initiatives rather than focusing solely on those employees with technology-related roles.

Banks are also required to monitor and maintain sufficient awareness of cybersecurity threats and vulnerability, *i.e.,* threat intelligence, in order to react and respond appropriately. The FDIC lists several resources banks can use to enhance their threat intelligence, including the U.S. Computer Emergency Readiness Team, which is part of the Department of Homeland Security and offers educational materials and alerts concerning cyber threats to subscribers.

The FDIC also highlights the risk posed by a single bank employee who unintentionally opens a malicious email attachment or visits a malicious website, which risk can be mitigated by conducting organization-wide security awareness training. Training should be role-specific for each group of employees, keeping in mind that certain types of

employees may be more likely to be targeted in cybersecurity attacks (*e.g.,* executives, comptrollers, and cashiers). The FDIC also encourages banks to offer training to other parties with access to the bank's systems, including customers and vendors.

Effective patch-management programs are also deemed critical in preventing security breaches. Banks are required to implement adequate policies and procedures to prioritize, inventory, monitor, and replace or apply patches to systems as required to mitigate risk of cyber threats, with periodic audits to validate the effectiveness of the program.

The FDIC identifies multiple resources provided by regulators that offer guidance to banks in establishing a cybersecurity framework. In conclusion, the FDIC reiterates its mandate to bank boards and senior management to create an organization-wide cybersecurity culture and provide their full support to identify and mitigate cyber risks. Banks should take care to document how their leadership has created and fostered such an environment.

Marketplace Lending

In this FDIC article, "marketplace lending" is defined broadly as "any practice of pairing borrowers and lenders through the use of an online platform without a traditional bank intermediary." The FDIC provides a high-level overview of bank involvement with marketplace lenders, including the potential relationship structures and related risks, and highlights the importance of a pragmatic business strategy when banks enter into such relationships. Banks can serve as investors to marketplace lenders or work with marketplace lenders through third-party arrangements. The FDIC identifies two models of marketplace lending—loans made directly by the marketplace lender (the *"Direct Funding Model"*) and loans made by a third-party bank (the *"Bank Partnership Model"*).

The FDIC points out that marketplace lending depends in large part on the willingness of investors to take on the credit risk of (often unsecured) borrowers, and investors may not have a full picture of the potential risks due to the newness of the industry and the fact that interest rates have been low and steady. Other risks identified by the FDIC include third-party risk, compliance risk, transaction risk, and liquidity risk. The FDIC cites its 2008 publication, Guidance for Managing Third-Party Risk, and its 2015 guidance, Advisory on Effective Risk Management Practices for Purchased Loans and Purchased Loan Participations, both of which emphasize the importance of conducting due diligence prior to engaging with a third party such as a marketplace lender and of structuring contract terms in a manner that protects the bank, including permitting audits of the marketplace lender and the ability to validate compliance with applicable law and regulations.

The overall supervisory perspective provided by the FDIC is that a bank's relationship with a marketplace lender, however structured, should be consistent with the bank's overall business strategy. It is up to each institution to conduct an appropriate due diligence review and risk assessment in order to determine whether the risks presented by a marketplace lender relationship align with the bank's business strategy. Banks that decide to work with marketplace lenders must manage these relationships like other third-party vendor relationships and investments, including appropriate risk management, monitoring, and oversight.

The FDIC concludes by explaining that it reviews how banks manage relationships with marketplace lenders as part of their overall program for managing third-party relationships, and the results of this review are considered in the FDIC's supervisory evaluation of bank management. As a result, it is important for bank boards of directors and management to be involved in the review and approval of any proposed or current relationships with marketplace lenders to ensure they are consistent with the institution's risk tolerance and that appropriate monitoring and oversight occur for the duration of any such relationship.

While the FDIC supervises and examines banks involved in the marketplace lending industry, this is one of the first public pronouncements from a banking regulator on this topic. It appears that the FDIC is treating marketplace lending similar to other bank products and services, which is positive news for those institutions that are currently or may in the future consider engaging with a marketplace lender under the Bank Partnership Model.

Chapman and Cutler LLP

Attorneys at Law · Focused on Finance®

To the Point! is a summary of items of interest and current issues for financial institutions with primary focus on regulatory, consumer, and corporate issues. Chapman maintains a dedicated practice group with the experience to counsel on these issues and other enterprise risk management matters facing financial institutions. If you would like to discuss any of the items contained in these briefings or other legal, regulatory, or compliance issues facing your institution, please contact one of the members of our Bank Regulatory Group:

Marc Franson • 312.845.2988
Heather Hansche • 312.845.3714
John Martin • 312.845.3474
Scott Fryzel • 312.845.3784
Dianne Rist • 312.845.3404
Lindsay Henry • 312.845.3869