SULLIVAN & CROMWELL LLP

S&C memo

September 3, 2021

Bank Due Diligence on Financial Technology Companies

Federal Reserve, FDIC and OCC Publish Guide for Community Banks

SUMMARY

On August 27, 2021, the three primary federal banking agencies published a guide to conducting due diligence on financial technology companies. The guide is intended to serve as a resource for community banks when evaluating prospective third-party relationships with financial technology ("fintech") companies. Although the guide is directed at community banks, the due diligence steps that banks are encouraged to take also provide guidance to fintech companies on the information that fintechs may be required to provide and the standards that fintechs will be required to meet when working with community and other banks.

NEW GUIDE FROM THE AGENCIES BUILDS ON EXISTING SUPERVISORY GUIDANCE

On August 27, 2021, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency (collectively, the "agencies") issued a new guide, aimed at community banks, expanding upon previous guidance in this area. The guide addresses six common areas where due diligence regarding a potential fintech partner may be appropriate:

- business experience and qualifications;
- financial condition;
- legal and regulatory compliance;
- risk management and controls;
- information security; and
- operational resilience.

Use of the guide is voluntary, but the agencies highlighted that arrangements with fintech companies, like those with other third-party relationships, can introduce risks to the bank. While conducting due diligence, a community bank should collect and analyze various types of information with the ultimate goal of determining whether a proposed relationship with a third-party fintech company would support its strategic and financial goals and could be implemented consistent with safe and sound practices and applicable legal and regulatory requirements.

The agencies stressed that fintech companies may exhibit a range of maturity levels with respect to the highlighted areas of diligence, consistent with a particular company's stage of development and experience. In each situation, however, community banks are encouraged to ensure through due diligence that the company's risk appetite and ability to engage in the proposed activity matches the community bank's own requirements and objectives. The guide provides relevant considerations, potential sources of information and illustrative examples for the six key topics:

1. Business Experience and Qualifications

One key area of interest includes assessment of the fintech's business experience, its strategies and its plans for the future, as well as the qualifications of its directors and company principals. Community banks can draw upon many potential sources of information on operational history and experience. These sources include publicly available company overviews, the volume and nature of past complaints against the company, legal and regulatory actions, and media reports. The fintech company's website and social media accounts can provide insight into both the company's strategy and plans for the future, as well as biographical and professional information on executives and directors. It is important for a fintech to show a community bank that the company's business experience and qualifications will enable it to work with the community bank and provide the services being considered while complying with applicable regulatory requirements and meeting customer needs. The responses to inquiries about a company's strategy and the qualifications of its directors and company principals likewise can provide a community bank with insight into whether the fintech company has sufficient expertise to provide the activity being considered safely and soundly and whether the company's future goals align with the bank's objectives.

2. Financial Condition

The fintech company must also be able to show that its financial condition is sufficiently strong to convince the community bank that the company will be able to remain in business and fulfill its third-party obligations. Both publicly available information—such as annual reports, Securities and Exchange Commission filings and market information—and internal financial reports and projections can provide insight into the financial health and projections of a fintech company. Understanding the company's funding sources and information about the company's competitive environment or client base will help a community bank evaluate the company's viability. Banks should also consider the company's susceptibility to external risks, such as geopolitical events, in this context.

3. Legal and Regulatory Compliance

Assessing a fintech company's legal and regulatory compliance functions can provide insights into the company's familiarity with the community bank's regulatory environment, including privacy, consumer protection, fair lending, anti-money laundering and other matters. It can also provide insight into the company's management and operating environment. In assessing legal issues, potential sources of information include lawsuits and other legal records, and public filings like the company's Form 10-K or Form 10-Q. On the regulatory side, a community bank could propose contract terms that specify the standards for performance of legal and compliance duties. Similarly, community banks may review the fintech's internal policies, procedures, training and internal controls designed to assure compliance with legal and regulatory requirements. Strong insight into and preparation for assuring legal and regulatory compliance could be especially important for fintech companies with limited experience working within the heavily regulated banking world.

4. Risk Management and Controls

Diligence on a fintech's risk management policies, processes and controls can similarly provide insight into the company's ability to conduct the proposed activity in a safe and sound manner and consistent with a community bank's risk appetite. In general, the community bank should seek assurances that the fintech company adequately outlines risk management responsibilities and reporting processes, and also assess whether the company's processes are in line with the bank's own risk appetite, policies and procedures. In addition, information about a fintech company's internal audit work (either in-house or outsourced) can indicate whether the degree to which its risk management and internal controls are effective. Other potential sources of information on risk management and controls include policies and procedures related to the proposed activity, training materials and training schedules, information on risk and compliance staffing and reports to the company's board of directors. As with other areas, the agencies recognize that, particularly in the rapidly evolving fintech sector, a company's audit, risk and compliance functions could vary with the maturity of the company.

5. Information Security

A review of a fintech company's information security program can provide insight into the strength of its processes for handling and protecting sensitive information, which could include community bank customer information. In the context of managing cybersecurity risk, the agencies emphasized the importance of understanding a fintech company's information security framework. Among other relevant considerations, a community bank may need to determine whether existing systems are adequate to perform the proposed activity, or whether additional IT investment would be needed to complete the activity within the appropriate risk framework. Information technology policies, incident management and response policies, and information security and privacy awareness training requirements for staff are pertinent for review. The

agencies recognized that the maturity of information security processes may vary, particularly for fintech companies in early or expansion stages.

6. Operational Resilience

The agencies encourage community banks to assess a fintech company's ability to continue operations through a disruption, including events like technology-based failures, human error, cyber incidents, pandemic outbreaks and natural disasters. Due diligence on operational resilience should consider business continuity planning and incident response, service level agreements and reliance on subcontractors. In evaluating a fintech company's business continuity planning and incident response, a community bank should evaluate a company's plans and ability to continue operations in the event of a disruption by considering such information as disaster recovery and incident response plans, documented system backup processes and insurance documents, among other potential sources. Service level agreements between the bank and the company could set forth the rights and responsibilities of each party in the event of a disruption with regard to expected activities and functions.

IMPLICATIONS

Aside from these six key common areas of concern, the agencies noted there could be other topics, relevant considerations and sources of information to consider depending on the particular relationship involved and the potential role of the fintech company being examined. The guide does not substantively alter existing supervisory guidance issued by the agencies and applicable to banks considering arrangements with fintech companies. It does, however, provide a structured approach to due diligence for community banks and, in particular, for those banks with minimal prior experience partnering with fintechs. Fintech companies seeking to work with this customer base may also find the guidance useful in preparing for discussions with potential bank partners.

* * *

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers, or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.