Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Expectations For Fintech Cos. Providing Services To Banks

By **M. Patricia Oliver, Glenn Morrical and Casey Holzapfel**

Law360, New York (August 4, 2017, 11:23 AM EDT) --

M. Patricia Oliver

Glenn Morrical

Casey Holzapfel

In recent years, there has been an explosion of business models based on using technology solutions to provide or improve services in the financial services industry. At one point, it appeared that many of the financial technology, or "fintech," companies would compete for business of traditional financial institutions. More recently, the trend has been for fintech companies to position themselves to be providers to or partners with traditional institutions.

One of the great challenges for a fintech company supplying a bank or thrift is that the regulators have required increasing levels of oversight by the financial institutions over their providers. The result is that a fintech company will be subjected to a set of standards much higher than may be required of providers in many other industries.

On June 7, 2017, the Office of the Comptroller of the Currency issued a bulletin addressing frequently asked questions regarding the risk management practices that national banks and federal savings associations (collectively, "banks") are expected to put in place with respect to third-party relationships. The FAQs supplement previous guidance issued on the topic by the OCC in Bulletin 2013-29. This article describes the impact that Bulletin 2013-29 and the FAQs can have on fintech companies that intend to provide products or services to banks.

Fintech Services Subject to the FAQs and Bulletin 2013-29

Bulletin 2013-29, issued in October 2013, defines a third-party relationship as a business arrangement between a bank and another entity, by contract or otherwise. This includes activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where the bank has an ongoing relationship or may have responsibility for the associated records. The FAQs acknowledge the trend of banks developing relationships with fintech companies that involve some of these activities, including performing services or delivering products directly to a bank's customer base. The FAQs make clear that if a fintech company performs services or delivers products on behalf of

a bank, the relationship meets the definition of a third-party relationship and the bank must include the fintech company in its third-party risk management process.

The Risk Management Processes

Bulletin 2013-19 describes the lifecycle of an effective third-party risk management process as one that incorporates the following phases:

- Planning;
- Due diligence and third-party selection;
- Contract negotiation;
- Ongoing monitoring; and
- Termination (including developing a contingency plan).

The OCC expects a bank to have risk management processes that are commensurate with the level of risk and complexity of its third-party relationships and the bank's organizational structures. Therefore, the oversight and management of third-party relationships is expected to be more comprehensive and rigorous if "critical activities" are involved. Critical activities include:

- Significant bank functions;
- Significant shared services; and
- Other activities that:
    - could cause a bank to face a significant risk if the third party fails to meet expectations;
    - could have significant customer impacts;
    - require significant investment in resources to implement the third-party relationship and manage the risk; or
    - could have a major impact on bank operations if the bank has to find an alternate third party or if the outsourced activity has to be brought in-house.

On the other hand, for activities that bank management determines to be low-risk, management should follow the bank's board-established policies and procedures for due diligence and ongoing monitoring. The FAQs make clear that services provided by a fintech company are not automatically deemed to be critical activities. Each bank's board and management must perform an assessment of whether its relationship with a fintech company relates to critical activities. Further, this assessment should be updated periodically throughout the relationship, as opposed to being a one-time assessment conducted at the beginning of the relationship.

OCC standards require that contracts with suppliers of critical activities include the right of not only the bank but also the banking regulators to audit the compliance of the company with the terms of the contract. The contracts generally will also include stringent requirements with respect to the safeguards the supplier maintains to protect private information. The contracts can often be burdensome and intrusive on the supplier.

If a bank is unable to obtain all the information it seeks on a critical third-party service provider, particularly from new companies, the FAQs put forth the following steps that bank management is expected to take:

- develop appropriate alternative ways to analyze these critical third-party service providers;
- establish risk-mitigating controls;
- be prepared to address interruptions in delivery (for example, use multiple payment systems, generators for power, and multiple telecommunications lines in and out of critical sites);
- make risk-based decisions that these critical third-party service providers are the best service providers available to the bank despite the fact that the bank cannot acquire all the information it wants;
- retain appropriate documentation of all their efforts to obtain information and related decisions; and
- ensure that contracts meet the bank's needs.

The OCC acknowledges that startup fintech companies may have limited financial information available. Although Bulletin 2013-29 states that banks should consider the financial condition of third parties during the due diligence stage, the FAQs clarify that with respect to fintech companies, banks may consider a company's access to funds, its funding sources, earnings, net cash flow, expected growth, projected borrowing capacity, and other factors that may affect the fintech company's overall financial stability. Banks are also expected to assess changes to the financial condition of fintech companies as part of their ongoing monitoring of the relationship.

Bulletin 2013-19 states that depending on the significance of the third-party relationship, a bank's analysis of a third party's financial condition may be as comprehensive as if the bank were extending credit to the third-party service provider; however, the FAQs clarify that there is no absolute requirement that a third party meet the bank's lending criteria.

Bank Collaboration to Meet OCC Expectations

The FAQs make clear that if multiple banks are using the same service providers to secure or obtain like products or services, the banks may collaborate to meet certain expectations. For example, banks may become members of user groups, which create the opportunity for banks to collaborate with their peers on innovative product ideas, enhancements to existing products or services, and customer service and relationship management issues with service providers. Banks may also have participating third parties complete common security, privacy and business resiliency control assessment questionnaires, which may be shared with multiple banks.

The FAQs specifically mention that information-sharing forums have improved banks' ability to identify cyberattack tactics on banks and third parties with whom they have relationships.

CFPB Guidance

Regulatory guidance on third-party providers is not limited to the OCC. For example, the Consumer Financial Protection Bureau issued a bulletin in 2012 and updated it in 2016 as "Compliance Bulletin and Policy Guidance 2016-02." That bulletin describes a "supervised service provider" not only as a service provider to any institution the CFPB directly supervises, such as banks with $10 billion or more in assets, but also any service provider to a substantial number of small insured depository institutions or small insured credit unions. The bulletin notes that the law grants the CFPB supervisory and enforcement authority over supervised service providers, which includes the authority to examine the operations of service providers onsite, and states that the CFPB will exercise the full extent of its supervision authority over supervised service providers, including its authority to examine for compliance with Title X's

prohibition on unfair, deceptive or abusive acts or practices (UDAAP). Unfortunately, what constitutes a UDAAP is not well-defined, and some institutions have experienced significant consequences from findings of UDAAP involving relatively modest computational errors.

Significant Consequences

The guidance by the financial regulators has caused financial institutions to take tough stances when signing agreements with service providers. The agreements regularly require that the provider agree that it can be examined directly by the bank examiners. Any company that has never undergone an examination by bank examiners is likely to find the experience extremely daunting. Given the vague scope of what constitutes UDAAP, it is even difficult to know what standards will be applied in an examination.

Such agreements also typically require the provider to attest to compliance with banking regulatory standards for the protection of information and give the financial institution the right to audit the provider's compliance with those standards. Agreements may also mandate that the service provider conduct training programs for their personnel on the compliance policies and procedures for the service provider's activities to comply with bank regulatory standards. Agreements generally require that the service provider indemnify the institution for breaches, and an agreement to comply with banking regulatory requirements adds a basis for claims that may be more hazardous than the exposure a company would otherwise have.

Recommendations

Fintech companies intending to provide their products or services to banks should carefully evaluate the way the financial institution regulatory standards will affect the banks' demands on the company and plan accordingly. It will be vital that a fintech supplier to a bank not only is stable and capable of providing services reliably and with tight security but also that the company can demonstrate to the banks and potentially the regulators that this is the case. As noted above, this may require demonstrating future funding sources. One irony in this area is that a fintech company would love to be vital to a financial institution's future, but the more successful the fintech company is in that regard, the more tightly the institution will be required to perform due diligence and impose oversight and audit standards.

M. Patricia Oliver and Glenn E. Morrical are partners, and Casey L. Holzapfel is an associate, at Tucker Ellis LLP in Cleveland.