The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION JANUARY 2022

LexisNexis

THE BANKING LAW JOURNAL

VOLUME 139 **NUMBER 1** **January 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Matthew T. Burke at ..... (800) 252-9257
Email: ..... matthew.t.burke@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

ISBN: 978-0-7698-7878-2 (print)
ISSN: 0005-5506 (Print)

Cite this publication as:

The Banking Law Journal (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub.4815)

Editor-in-Chief, Editor & Board of Editors

THE BANKING LAW JOURNAL (ISBN 978-0-76987-878-2) (USPS 003-160) is published ten times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, LexisNexis Matthew Bender, 230 Park Ave, 7th Floor, New York, NY 10169.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW, Third Floor, Washington, DC 20005-2207.

Partnering with FinTech Companies: What Banks Need to Know About the Diligence Process

Christopher L. Allen, Robert C. Azarow, Michael A. Mancusi, Charles Yi, and Anthony Raglani*

This article summarizes the key components of recent interagency guidance for community banking organizations on conducting due diligence of financial technology companies when considering prospective relationships with such entities and describes certain lessons to be learned by banking organizations as the agencies continue to refine their supervisory expectations for banks' third-party risk management controls.

The Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation (together, the "Agencies") have published interagency guidance for community banking organizations on conducting due diligence of financial technology ("FinTech") companies when considering prospective relationships with such entities ("Guidance").[1]

The Guidance builds upon a growing body of precedent published by the Agencies and other financial services regulatory agencies regarding supervisory expectations for the third-party risk management controls of supervised institutions.[2]

---

* Christopher L. Allen (christopher.allen@arnoldporter.com) is a partner at Arnold & Porter Kaye Scholer LLP representing bank and nonbank financial industry participants in a broad range of regulatory compliance and investigative matters before federal and state government agencies. Robert C. Azarow (robert.azarow@arnoldporter.com) is a partner at the firm leading the Financial Services Transactions practice. Michael A. Mancusi (michael.mancusi@arnoldporter.com) is a partner at the firm representing domestic and foreign banks, credit unions, and other financial services clients in a wide range of state and federal regulatory, compliance, and enforcement matters. Charles Yi (charles.yi@arnoldporter.com), former General Counsel of the Federal Deposit Insurance Corporation, is a financial services partner at the firm. Anthony Raglani (anthony.raglani@arnoldporter.com) is a senior associate at the firm counseling clients on a variety of financial regulatory matters. David F. Freeman, Jr., Kevin M. Toomey, Howard L. Hyde, and Amber A. Hay, attorneys at the firm, contributed to the preparation of this article.

[1] Conducting Guidance on Financial Technology Companies: A Guide for Community Banks (Aug. 27, 2021), https://www.fdic.gov/news/financial-institution-letters/2021/fil21059.html.

[2] *See, e.g.,* FDIC FIL-44-2008 (Guidance for Managing Third-Party Risk); OCC Bulletin 2013-29 (Third-Party Relationships Risk Management) & FAQs to Supplement OCC Bulletin 2013-29; Federal Reserve SR Letter 13-19 (Guidance on Managing Outsourcing Risk); Federal Reserve Bank Holding Company Supervision Manual §§ 2060, 2124 & 2125 (Outsourcing);

Although tailored to community banks, the Guidance is instructive for all banking organizations in outlining the Agencies' expectations regarding the scope and substance of banks' due diligence of potential FinTech company partners and service providers.

This article summarizes the key components of the Guidance and describes certain lessons to be learned by banking organizations as the Agencies continue to refine their supervisory expectations for banks' third-party risk management controls.

SUMMARY OF THE GUIDANCE

The Guidance sets forth six key topics that banking organizations should consider when conducting due diligence of FinTech companies.

1. Business Experience and Qualifications

A FinTech company's experience, qualifications and strategic objectives and related planning efforts should be sufficient to demonstrate that the company has the ability to fulfill the needs and expectations of bank partners. Banks should consider each FinTech company's record of legal or regulatory actions, customer complaints and management thereof, and service of existing and prior clients in assessing a company's experience and qualifications. Banks should also evaluate a company's strategic plans and management structure and style to assess whether these factors are consistent with the strategic objectives and culture of the bank. To this end, the background, expertise and experience of the executive management team and directors of the FinTech company may serve as indicators of the company's experience and qualifications and its ability to perform relevant business activities and services in a manner consistent with the bank's expectations.

2. Financial Condition

Banks must assess each FinTech company's capacity to provide the activities and services under consideration and remain a viable going concern. This

---

FFIEC Information Technology Examination Handbook (Strengthening the Resilience of Outsourced Technology Services); FFIEC Business Continuity Planning Examination Handbook; FINRA Regulatory Notice 21-29 (Supervisory Obligations of FINRA Member Firms Relating to Outsourcing); FINRA Staff Guidance on Cloud Computing in the Securities Industry. Further, on July 19, 2021, the Agencies proposed new guidance on risk management considerations relating to third-party relationships (including those relating to FinTech companies specifically). *See* Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 Fed. Reg. 38, 182 (Jul. 19, 2021), *available at* https://www.govinfo.gov/content/pkg/FR-2021-07-19/pdf/2021-15308.pdf.

should involve evaluation of financial statements and auditor's opinions, annual reports, public filings required under the federal securities laws, internal financial reports and audits, and information regarding sources of capital and funding strategies. Banks should endeavor to understand the competitive environment in which the company operates, the nature of its client base (including the extent to which the company may rely on a single client or subset of specific clients in order to sustain operations or remain competitive), its exposure to external risks, and its ability to fund ongoing operations and future growth.

A factor that can complicate this aspect of a bank's due diligence is that certain FinTech companies may be in the start-up phase of their development or otherwise less established within the banking industry, and therefore the financial information and performance data available to banks may be limited. In these cases, banks should take care to assess a company's access to and sources of funding, projected borrowing capacity, earnings, net cash flow, and projections for expected growth.

3. Legal and Regulatory Compliance

Banks must evaluate a FinTech company's legal standing and record of compliance to understand whether the company will be able to comply with the legal and regulatory requirements to which the bank is subject when conducting relevant activities. As part of this evaluation, banks should review the company's formation documents, annual and quarterly reports, records of litigation or enforcement actions, and other relevant public information (such as patents, licenses or other records evidencing the company's authority and ability to perform relevant activities).

Banks also should assess the extent to which a FinTech company has worked with other similar banking organizations and the company's development of risk management controls and regulatory compliance processes in areas that are relevant to the activities to be conducted (e.g., consumer protection, data privacy and security, anti-money laundering, fair lending, etc.). Information relating to consumer-facing applications, disclosures, agreements, or marketing materials should be considered in an effort to anticipate potential consumer-related compliance issues.

4. Risk Management and Controls

Banks must evaluate the effectiveness of a FinTech company's risk management policies, processes and controls in order to assess the company's ability to conduct relevant activities in a safe and sound manner and consistent with the bank's risk appetite. Sources of information that banks may wish to consider include the company's policies and procedures relating to the prospective

activities, overall internal control environment and risk management processes, reports of internal audits and other similar compliance reviews, reports of any self-assessments, and information on risk and compliance staffing and resources (including training program materials).

Information on the nature, scope and frequency of control and compliance reviews may be of particular value to banks, as such information may be illustrative of the quality of the FinTech company's risk management and control environment. Additionally, reviewing reports provided to the company's board of directors (or relevant committees thereof) may provide insights into both the company's ability to detect, escalate and remediate control deficiencies or potential regulatory compliance violations and the competence of the personnel responsible for these functions.

Depending upon the nature and scope of the prospective relationship, banks may wish to consider on-site visits in order to more fully evaluate a FinTech company's operations and control environment or engagement of the bank's auditors to assist with due diligence processes.

5. Information Security

Banks must understand the information security framework and controls employed by a FinTech company to manage cybersecurity risk. This aspect of due diligence is of particular importance when a FinTech company may have access to or handle bank customer information or other sensitive or propriety information of the bank in connection with the conduct of relevant activities.

As part of a bank's information security due diligence, the bank should review a company's information security policies and procedures (e.g., data classification, retention and disposal; access management; change management; server/backup management; anti-malware and -phishing; etc.), reports of information security control assessments (e.g., penetration tests or vulnerability assessments or scans), security incident management and response policies and reports of any known incidents and remediation thereof, and information security and privacy awareness training materials.

In certain circumstances, banks may wish to consider information technology investments in, or other support of, FinTech companies with which they seek to partner. This may be necessary, for example, where a FinTech company would be required to support critical aspects of the bank's business or handle significant volumes of transaction activity or bank customer data.

6. Operational Resilience

Banks must evaluate a FinTech company's ability to continue its operations through a variety of disruptions (e.g., technology-based failures or cyberattacks,

natural disasters, pandemics, human errors, etc.). The business continuity and resilience planning of a FinTech company should be commensurate with the nature and criticality of the activities to be performed for or on behalf of the bank. As part of this aspect of due diligence, banks should consider a company's business continuity, disaster recovery and incident response plans, reports of testing of those plans, reports of cybersecurity risk assessments and audits, and copies of insurance policies (or other evidence that the company's financial condition is sufficient to sustain significant losses in the event of operational disruptions or failures).

Special circumstances that may impact the nature and scope of a bank's review of a FinTech company's operational resilience include cases where a company operates, in whole or in part, outside of the United States and/or transmits data, potentially including bank or bank customer data, to offshore data centers, as well as instances in which a company outsources portions of its activities to subcontractors. Under these circumstances, banks may wish to obtain a greater amount of information regarding a company's continuity and resiliency planning and financial resources, and/or seek contractual commitments from the company to offset any heightened operational risk.

LESSONS TO BE LEARNED BY BANKING ORGANIZATIONS

The publication of the Guidance underscores the importance from the Agencies' perspective of banks' implementation of and adherence to robust third-party risk management controls and practices when considering relationships with FinTech companies. The Guidance makes clear that banks must develop a thorough assessment of a company's ability to meet the needs of the bank, adapt to and operate within the legal and regulatory framework applicable to the bank, manage integration challenges and sustain operations in the face of business disruptions, and demonstrate that its information technology infrastructure and data security and privacy practices are commensurate with the scope and complexity of the company's activities and cybersecurity risk exposure.

As appropriate based on the nature of the proposed relationship with a FinTech company and the findings of a bank's due diligence review, banks may wish to tailor the terms and conditions of their contracts with a company to address specific matters including legal and regulatory compliance (e.g., by obtaining commitments from the company to adhere to the legal and regulatory requirements applicable to the bank and granting the bank access to the company's records and the right to audit the company periodically), termination rights and/or pricing adjustments (e.g., in the event that a company fails to meet specific technical or operational requirements or

performance standards), integration and transition management (i.e., with respect to the onboarding of the company and, if necessary, the transition to a new service provider), and performance expectations and metrics.[3]

Additionally, as noted above, many FinTech companies may be in the start-up phase of their development and have limited financial and performance data to evaluate. In these cases, banks may wish to develop plans for ongoing monitoring of the company's performance and specific contingency plans in the event that the company experiences a significant business disruption or encounters financial difficulties.

A significant complicating factor to a successful due diligence process is the speed with which many FinTech companies seek to onboard their clients, including banks and other supervised entities. This is often driven by competitive pressures on the FinTech companies to report new business relationships in the marketplace, the need to show success in the face of ongoing capital needs and thereby help assure continued access to capital, and a culture in which the speed of new technology advancements drives the need to monetize those advancements with new business relationships before the prevailing technology changes again. As a result, significant pressure often exists to compress the due diligence process into a short amount of time and financial institutions have experienced significant resistance to the type and extent of diligence that the Agencies are requiring. Both the FinTech companies and the supervised financial institutions will need to adapt to the needs of the other to assure a thorough yet timely diligence process.

Further, as banks' relationships with FinTech companies expand and evolve, it is more likely that the services provided by such companies will involve critical bank activities. These can include activities relating to critical bank functions (e.g., payments, clearing, settlements, custody, information technology, etc.) or those that could cause the bank or its customers significant harm if the service provider fails to meet expectations or require significant investments in resources to manage risk and remediate any deficiencies or operational failures. Banks' executive management teams should have clear policies and procedures for identifying critical bank activities and evaluating and onboarding any service provider, including FinTech companies, that may provide or be involved in such activities as part of a relationship with the bank.

---

[3] The Agencies have published various forms of guidance on recommended contract terms for banks' engagements with FinTech companies or providers of information technology services. *See*, *e.g.,* FDIC FIL-19-2019, Technology Service Provider Contracts (Apr. 2, 2019); FFIEC, Outsourcing Technology Booklet; FDIC FIL-44-2008, Guidance for Managing Third-Party Risk (June 6, 2008).

As the FinTech industry grows and FinTech companies and the services that they provide become more prominent, the legal, regulatory and supervisory framework governing such companies, their activities and their relationships with banks and other financial institutions can be expected to continue to take shape. As this occurs, banks should be vigilant in monitoring developments and maintaining a dialogue with their supervisors to ensure that any plans to engage with a FinTech company, particularly as part of an expansion of the bank's activities or a deviation from core banking activities, are consistent with evolving legal and regulatory standards. Additionally, banks should periodically re-evaluate their risk tolerances and make any necessary adjustments or enhancements to their third-party risk management policies and practices in order to continue to meet the Agencies' expectations for the evaluation, selection and management of third-party relationships with FinTech companies.