Conducting Due Diligence on Financial Technology Companies

A Guide for Community Banks

AUGUST 2021

Board of Governors of the Federal Reserve System

Federal Deposit Insurance Corporation

Office of the Comptroller of the Currency

Introduction

Innovation and evolving customer preferences are changing the financial services landscape, including the way financial products and services are delivered. Some banks are exploring ways in which third-party relationships may assist them in responding to the changing landscape. These relationships are particularly relevant in situations in which community banks may benefit from additional expertise. By providing access to new or innovative technologies, companies specializing in financial technologies (or "fintech") can provide community banks with many benefits, such as enhanced products and services, increased efficiency, and reduced costs, all bolstering competitiveness. Like other third-party relationships, arrangements with fintech companies can also introduce risks.[1] Assessing the benefits and risks posed by these relationships is key to a community bank's due diligence process.

This guide is intended to be a resource for community banks when performing due diligence on prospective relationships with fintech companies. Use of this guide is voluntary and it does not anticipate all types of third-party relationships and risks. Therefore, a community bank can tailor how it uses relevant information in the guide, based on its specific circumstances, the risks posed by each third-party relationship, and the related product, service, or activity (herein, activities) offered by the fintech company. While the guide is written from a community bank perspective, the fundamental concepts may be useful for banks of varying size and for other types of third-party relationships. Banks should reference federal banking agencies' relevant guidance.[2]

Due diligence is an important component of an effective third-party risk management process, as highlighted in the federal banking agencies' respective guidance. During due diligence, a community bank collects and analyzes information to determine whether third-party relationships would support its strategic and financial goals and whether the relationship can be implemented in a safe and sound manner, consistent with applicable legal and regulatory requirements. The

---

[1] Engaging a third party does not diminish a bank's responsibility to operate in a safe and sound manner and to comply with applicable legal and regulatory requirements, including federal consumer protection laws and regulations, just as if the bank were to perform the service or activity itself.

[2] For institutions supervised by the Office of the Comptroller of the Currency (OCC), see OCC Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance (October 30, 2013), https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html. For institutions supervised by the Federal Deposit Insurance Corporation (FDIC), see FDIC Financial Institution Letter-44-2008 (June 6, 2008), https://www.fdic.gov/news/financial-institution-letters/2008/fil08044.html. For institutions supervised by the Board of Governors of the Federal Reserve System (Board), see SR letter 13-19 "Guidance on Managing Outsourcing Risk" (December 5, 2013), https://www.federalreserve.gov/supervisionreg/srletters/sr1319.htm.

On July 19, 2021, the Board, FDIC, and OCC (federal banking agencies) published for comment proposed interagency guidance for third-party relationships. See "Proposed Interagency Guidance on Third-Party Relationships: Risk Management," 86 Fed. Reg. 38,182 (July 19, 2021). This guide draws from the federal banking agencies' existing guidance and is consistent with the proposed interagency guidance.

scope and depth of due diligence performed by a community bank will depend on the risk to the bank from the nature and criticality of the prospective activity. Banks may also choose to supplement or augment their due diligence efforts with other resources as appropriate, such as use of industry utilities or consortiums that focus on third-party oversight.

The guide focuses on six key due diligence topics, including relevant considerations, potential sources of information and illustrative examples. There may be other topics, considerations, and sources of information to consider, depending on the unique relationship and the role of the fintech company.

Topics to Consider When Conducting Due Diligence of a Fintech Company

Business Experience and Qualifications

Evaluating a fintech company's business experience, strategic goals, and overall qualifications allows a community bank to consider a fintech company's experience in conducting the activity and its ability to meet the bank's needs.

Business Experience

Relevant Considerations

Operational history provides insight into a fintech company's ability to meet a community bank's needs, including, for example, the ability to adequately provide the activities being considered in a manner that enables a community bank to comply with regulatory requirements and meet customer needs.

Client references and complaints about a fintech company provide useful information when considering, among other things, whether a fintech company has adequate experience and expertise to meet a community bank's needs and resolve issues, including experience with other community banking clients.

Legal or regulatory actions against a fintech company can be indicators of the company's track record in providing activities.

Potential Sources of Information

- Company overview
- Organization charts
- List of client references using the activities being considered
- Volume and types of complaints, including those available from the fintech company, regulatory agencies, and other public sources
- Public records of any legal or regulatory actions and to establish corporate standing, if applicable
- Media reports mentioning the fintech company
- Summary of any past operational failures of the fintech company

Business Strategies and Plans

Relevant Considerations

Discussing a fintech company's strategic plans can provide insight on key decisions it is considering, such as plans to launch new products or pursue new arrangements (such as acquisitions, joint ventures, or joint marketing initiatives). A community bank may subsequently consider whether the fintech company's strategies or any planned initiatives would affect the prospective activity.

Inquiring about a fintech company's strategies and management style may help a community bank assess whether a fintech company's culture, values, and business style fit those of the community bank.

Potential Sources of Information

- Mission statement, service philosophy, and quality initiatives
- Geographic footprint information (such as locations of offices and operations)
- Overview of strategic plans and/or expansion strategies
- Patents and licenses
- Summary of key personnel and subcontractors (if utilized)
- Employment policies, including background check and hiring practices
- Fintech company website and social media sites

Qualifications and Backgrounds of Directors and Company Principals

Relevant Considerations

Understanding the background and expertise of a fintech company's directors and executive leadership may provide a community bank useful information on the fintech company's board and management knowledge and experience related to the activity sought by the community bank.

A community bank may also consider whether the company has sufficient management and staff with appropriate expertise to handle the prospective activity.

Potential Sources of Information

- Ownership information
- Biographical and professional information on board of directors' and executive directors' backgrounds, often available on company websites and in public records
- Resource plans (including succession plans)

Illustrative Example

A fintech company, its directors, or its management may have varying levels of expertise conducting activities similar to what a community bank is seeking. A fintech company's historical experience also may not include engaging in relationships with community banks. As part of due diligence, a community bank might therefore consider how a fintech company's particular experiences could affect the success of the proposed activity and overall relationship.

Understanding a fintech company's qualifications and strategic direction will help a community bank assess the fintech company's ability to meet the community bank's expectations and support a community bank's objectives. When evaluating the potential relationship, a community bank may consider a fintech company's willingness and ability to align the proposed activity with the community bank's needs, its plans to adapt activities for the community bank's regulatory environment, and whether there is a need to address any integration challenges with community bank systems and operations.

Financial Condition

Evaluating a fintech company's financial condition helps a community bank to assess the company's ability to remain in business and fulfill any obligations created by the relationship.

Financial Analysis and Funding

Relevant Considerations

Financial reports provide useful information when evaluating a fintech company's capacity to provide the activity under consideration, remain a going concern, and fulfill any of its obligations, including its obligations to the community bank.

Understanding funding sources provides useful information in assessing a fintech company's financial condition. A fintech company may be able to fund operations and growth through cash flow and profitability or it may rely on other sources, such as loans, capital injections, venture capital, or planned public offerings.

Potential Sources of Information

- Financial statements and auditors' opinions as available
- Annual reports
- U.S. Securities-related filings, often available from the Securities and Exchange Commission
- Internal financial reports and projections
- List of funding sources

Market Information

Relevant Considerations

Information about a fintech company's competitive environment may provide additional insight on the company's viability.

Information on a fintech company's client base provides insight into any reliance a fintech company may have on a few significant clients. A few critical clients may provide key sources of operating cash flow and support growth but may also demand much of a fintech company's resources. Loss of a critical client may negatively affect revenue and hinder a fintech company's ability to fulfill its obligations with a community bank.

A community bank may consider a fintech company's susceptibility to external risks, such as geopolitical events that may affect the company's financial condition.

Potential Sources of Information

- Publicly available market information on competitors
- Information on client base

Illustrative Example

Some fintech companies, such as those in an early or expansion stage, have yet to achieve profitability or may not possess financial stability comparable to more established companies. Some newer fintech companies may also be unable to provide several years of financial reporting, which may impact a community bank's ability to apply its traditional financial analysis processes.

When audited financial statements are not available, a community bank might seek other financial information to gain confidence that a fintech company can continue to operate, provide the activity satisfactorily, and fulfill its obligations. For example, a community bank may consider a fintech company's access to funds, its funding sources, earnings, net cash flow, expected growth, projected borrowing capacity, and other factors that may affect a fintech company's overall financial performance.

Legal and Regulatory Compliance

Evaluating a fintech company's legal standing, its knowledge about legal and regulatory requirements applicable to the proposed activity, and its experience working within the legal and regulatory framework enables a community bank to verify a fintech company's ability to comply with applicable laws and regulations.

Legal

Relevant Considerations

Organizational documents and business licenses, charters, and registrations provide information on where a fintech company is domiciled and authorized to operate (for example, domestically or internationally) and legally permissible activities under governing laws and regulations.

Reviewing the nature of the proposed relationship, including roles and responsibilities of each party involved, may also help a community bank identify legal considerations.

Assessing any outstanding legal or regulatory issues may provide insight into a fintech company's management, its operating environment, and its ability to provide certain activities.

Potential Sources of Information

- Charters, articles of incorporation, certificates of good standing, and licenses, such as those recorded with the relevant state
- Other relevant public information, such as records related to patents and intellectual property
- Lawsuits, settlements, remediation, enforcement actions, fines, and consumer complaints
- Form 10-K filing
- Form 10-Q filing

Regulatory Compliance

Relevant Considerations

Reviewing a fintech company's risk and compliance processes helps a community bank to assess the fintech company's ability to support the community bank's legal and regulatory requirements, including privacy, consumer protection, fair lending, anti-money-laundering, and other matters.

A fintech company's experience working with other community banks may provide insight

Potential Sources of Information

- Policies, procedures, training, and internal controls pertaining to compliance with legal and regulatory requirements
- Proposed contract terms that specify performance of legal and compliance duties
- Information regarding customer-facing delivery channels or applications (for example, mail, online, and telephone)

Regulatory Compliance—continued

Relevant Considerations

into the fintech company's familiarity with the community bank's regulatory environment.

Reviewing information surrounding any consumer-facing applications, delivery channels, disclosures, and marketing materials for community bank customers can assist a community bank to anticipate and address potential consumer compliance issues.

Considering industry ratings (for example, Better Business Bureau) and the nature of any complaints against a fintech company may provide insight into potential customer-service and compliance issues or other consumer protection matters.

Potential Sources of Information

- Proposed marketing materials and regulatory disclosures with product details such as fees, interest rates, or other terms
- Methods used to monitor, remediate, and respond to customer complaints
- Customer complaint records involving the fintech company

Illustrative Example

Some fintech companies may have limited experience working within the legal and regulatory framework in which a community bank operates.

To protect its interests, community banks may consider including contract terms requiring

- compliance with relevant legal and regulatory requirements, including federal consumer protection laws and regulations, as applicable;
- authorization for a community bank and the bank's primary supervisory agency to access a fintech company's records; or
- authorization for a community bank to monitor and periodically review or audit a fintech company for compliance with the agreed-upon terms.

Other approaches might include

- instituting approval mechanisms (for example, community bank signs off on any changes to marketing materials related to the activity), or
- periodically reviewing customer complaints, if available, related to the activity.

Risk Management and Controls

Evaluating the effectiveness of a fintech company's risk management policies, processes, and controls helps a community bank to assess the company's ability to conduct the activity in a safe and sound manner, consistent with the community bank's risk appetite and in compliance with relevant legal and regulatory requirements.

Risk Management and Control Processes

Relevant Considerations

Reviewing a fintech company's policies and procedures governing the applicable activity provides insight into how the fintech company outlines risk management responsibilities and reporting processes, and how the fintech company's employees are responsible for complying with policies and procedures. A community bank may also use this information to assess whether a fintech company's processes are in line with its own risk appetite, policies, and procedures.

Information about the nature, scope, and frequency of control reviews, especially those related to the prospective activity, provides a community bank with insight into the quality of the fintech company's risk management and control environment. A community bank may also want to consider the relative independence and qualifications of those involved in testing.

A fintech company may employ an audit function (either in-house or outsourced). In these cases, evaluating the scope and results of relevant audit work may help a community bank determine how a fintech company ensures that its risk management and internal control processes are effective.

Potential Sources of Information

- Policies, procedures, and other documentation related to the prospective activity
- Policies and procedures related to the fintech company's internal control environment and overall risk management processes
- Information on risk and compliance staffing
- Recent results of control reviews and audit reports related to the prospective activity
- Issue management policies, procedures, and reports
- Schedule of planned control reviews and audits
- Self-assessments
- Training materials and training schedule
- Inventory of key risk, performance, and control indicators
- Sample key risk, performance, and control indicator reports

Risk Management and Control Processes—continued

Relevant Considerations

The findings, conclusions, and any related action plans from recent control reviews and audits provide insight into the effectiveness of a fintech company's program and the appropriateness and timeliness of any related action plans.

Evaluating a fintech company's reporting helps a community bank to consider how the fintech company monitors key risk, performance, and control indicators; how those indicators relate to the community bank's desired service-level agreements; and how the fintech company's reporting processes identify and escalate risk issues and control testing results. A community bank may also consider how it would incorporate such reporting into the bank's own issue management processes.

Information on a fintech company's staffing and expertise, including for risk and compliance, provide a means to assess the overall adequacy of the fintech company's risk and control processes for the proposed activity.

Information on a fintech company's training program also assists in considering how the fintech company ensures that its staff remains knowledgeable about regulatory requirements, risks, technology, and other factors that may affect the quality of the activities provided to a community bank.

Potential Sources of Information

- Project plans associated with any plannedchanges to systems or reporting capabilities
- Sample reports to the fintech company's board of directors

Illustrative Example

A fintech company's audit, risk, and compliance functions will vary with the maturity of the company and the nature and complexity of activities offered. As a result, a fintech company may not have supporting information that responds in full to a community bank's typical due diligence questionnaires. In other cases, a fintech company may be hesitant to provide certain information that is considered proprietary or a trade secret (for example, their development methodology or model components). In these situations, a community bank might take other steps to identify and manage risks in the third-party relationship and gain confidence that the fintech company can provide the activity satisfactorily.

For example, a community bank might consider on-site visits to help evaluate a fintech company's operations and control environment, or a community bank's auditors (or another independent party) may evaluate a fintech company's operations as part of due diligence.

Other approaches might include

- accepting due diligence limitations, with any necessary approvals and/or exception reporting, compared to the community bank's normal processes, commensurate with the criticality of the arrangement and in line with the bank's risk appetite and applicable third-party risk management procedures;
- incorporating contract provisions that establish the right to audit, conduct on-site visits, monitor performance, and require remediation when issues are identified;
- establishing a community bank's right to terminate a third-party relationship, based on a fintech company's failure to meet specified technical and operational requirements or performance standards. Contract provisions may also provide for a smooth transition to another party (for example, ownership of records and data by the community bank and reasonable termination fees); or
- outlining risk and performance expectations and related metrics within the contract to address a community bank's requirements.

Information Security

Evaluating a fintech company's information security measures allows a community bank to assess the adequacy and integrity of a fintech company's processes for handling and protecting sensitive information, including community bank customer information, depending on the third-party relationship and activity proposed.

Information Security Program

Relevant Considerations

It is important to understand any security framework that a fintech company employs to manage cybersecurity risk.

A fintech company's information security control assessments (for example, penetration testing, vulnerability assessments, etc.) highlights the fintech company's approach to identifying, mitigating, or correcting vulnerabilities in its security posture.

A fintech company's information security policies can provide insight into the company's ability to perform the proposed activity in a safe and sound manner and how or whether the fintech company trains and tests employees and subcontractors (for example, phishing or vishing exercises).

Assessing a fintech company's policies and practices related to privacy and information security is important in understanding the relevant controls in place to support a community bank's ongoing ability to comply with safeguarding requirements and its privacy and information security requirements.

Understanding a fintech company's security incident response and notification procedures may assist a community bank in determining any challenges to comply with its own incident response requirements.

Potential Sources of Information

- Completed information security controls assessments
- Incident management and response policies
- Incident reports with associated post-mortem and remediation activities
- Information security policies (for example, access management, data center security, backup management, change management, and anti-malware policies)
- Information security and privacy awareness training requirements for staff
- Policies addressing relevant safeguarding and privacy laws and regulations

Information Systems

Relevant Considerations

Understanding a fintech company's operations infrastructure and the security measures for managing operational risk may help a community bank evaluate whether those measures are appropriate for the prospective activity.

A community bank may evaluate whether the proposed activity can be performed using existing systems, or if additional IT investment would be needed at the community bank or at the fintech company to successfully perform the activity. For example, a community bank may evaluate whether the fintech company's systems can support the bank's business, customers, and transaction volumes (current and projected).

A fintech company's procedures for deploying new hardware or software, and its policy toward patching and using unsupported (end-of-life) hardware or software, will provide a community bank with information on the prospective third party's potential security and business impacts to the community bank.

Potential Sources of Information

- Information technology policies (for example, data protection including data classification, retention, and disposal)
- Overview of the fintech company's technology and processes supporting the prospective activity
- Completed controls or standards assessments

Illustrative Example

Fintech companies' information security processes may vary, particularly for fintech companies in an early or expansion stage. Community banks may evaluate whether a fintech company's information security processes are appropriate and commensurate with the risk of the proposed activity. Depending on the activity provided, community banks may also seek to understand a fintech company's oversight of its subcontractors, including data and information security risks and controls.

For a fintech company that provides transaction processing or that accesses customer data, for example, community banks may request information about how the fintech company restricts access to its systems and data, identifies and corrects vulnerabilities, and updates and replaces hardware or software. The bank may also consider risks and related controls pertaining to its customers' data, in the event of the fintech company's security failure. Also, contractual terms that authorize a community bank to access fintech company records can better enable the bank to validate compliance with the laws and regulations related to information security and customer privacy.

Operational Resilience

A community bank may evaluate a fintech company's ability to continue operations through a disruption.[3] Depending on the activity, a community bank may look to the fintech company's processes to identify, respond to, and protect itself and customers from threats and potential failures, as well as recover and learn from disruptive events. It is important that third-party continuity and resilience planning be commensurate with the nature and criticality of activities performed for the bank.

Business Continuity Planning and Incident Response

Relevant Considerations

Evaluating a fintech company's business continuity plan, incident response plan, disaster recovery plan and related testing can help a community bank determine the fintech company's ability to continue operations in the event of a disruption.

Evaluating a fintech company's recovery objectives, such as any established recovery time objectives and recovery point objectives, helps to ascertain whether the company's tolerances for downtime and data loss align with a community bank's expectations.

How a fintech company considers changing operational resilience processes to account for changing conditions, threats, or incidents, as well as how the company handles threat detection (both in-house and outsourced) may provide a community bank with additional information on incident preparation.

Discussions with a fintech company, as well as online research, could provide insights into how the company responded to any actual cyber events or operational outages and any impact they had on other clients or customers.

Potential Sources of Information

- Business continuity plans
- Disaster recovery plans
- Incident response plan
- Documented system backup processes
- Business continuity, disaster recovery, and incident response test results
- Cybersecurity reports and audits
- Insurance documents

[3] Disruptive events could include technology-based failures, human error, cyber incidents, pandemic outbreaks, and natural disasters.

Business Continuity Planning and Incident Response—continued

Relevant Considerations

Understanding where a fintech company's data centers are or will reside, domestically or internationally, helps a community bank to consider which laws or regulations would apply to the community bank's business and customer data.

A community bank may consider whether a fintech company has appropriate insurance policies (for example, hazard insurance or cyber insurance) and whether the fintech company has the financial ability to make the community bank whole in the event of loss.

Service Level Agreements

Relevant Considerations

Service level agreements between a community bank and a fintech company set forth the rights and responsibilities of each party with regard to expected activities and functions. A community bank may consider the reasonableness of the proposed service level agreement and incorporate performance standards to ensure key obligations are met, including activity uptime.

A community bank may also consider whether to define default triggers and recourse in the event that a fintech company fails to meet performance standards.

Potential Sources of Information

- Proposed service level agreements
- Evidence of status meeting existing service level agreements

Reliance on Subcontractors

Relevant Considerations

A fintech company's monitoring of its subcontractors (if used) may offer insight into the company's own operational resilience. For example, a community bank may inquire as to whether the fintech company depends on a small number of subcontractors for operations, what activities they provide, and how the fintech company will address a subcontractors' inability to perform.

A community bank may assess a fintech company's processes for conducting background checks on subcontractors, particularly if subcontractors have access to critical systems related to the proposed activity.

Potential Sources of Information

- The fintech company's policies on outsourcing and its use of subcontractors
- Independent reports or certifications regarding subcontractors
- List of third parties used by the fintech company

Illustrative Example

As with previous due diligence scenarios, fintech companies may exhibit a range of resiliency and continuity processes, depending on the activities offered. Community banks may evaluate whether a fintech company's planning and related processes are commensurate with the nature and criticality of activities performed for the bank.

For example, community banks may evaluate a fintech company's ability to meet the community bank's recovery expectations and identify any subcontractors the fintech company relies upon for recovery operations. A fintech company may have recovery time objectives for the proposed activity that exceed the desired recovery time objectives of a community bank. If a fintech company can meet the community bank's desired recovery time objectives, the bank may consider including related contractual terms, such as a contract stipulation that the community bank can participate in business continuity testing exercises and that provides appropriate recourse if the recovery time objective is missed in the event of an actual service disruption.

A community bank may also consider appropriate contingency plans, such as the availability of substitutable service providers, in case the fintech company experiences a business interruption, fails, or declares bankruptcy and is unable to perform the agreed-upon activities. In addition to potential contractual clauses and requirements, a community bank's management may also consider how it might wind down or transfer the activity in the event the fintech company fails to recover in a timely manner.