February 2020

# CONDUCTING BUSINESS WITH BANKS

## A GUIDE FOR FINTECHS AND THIRD PARTIES

The FDIC's technology lab, FDiTech, partners with banks, private companies, regulators and others to bring about new technologies that enhance the operations of financial institutions and encourage innovation that meets consumer demand. This Guide is the first in a series of new resources from FDiTech to help fintechs and third parties partner with banks.

Insured banks are examined for safety and soundness, consumer protection, and compliance with laws and regulations. The FDIC is the primary federal banking regulator for more than 3,400 state-chartered banks and conducts regular examinations of these banks every 12 to 18 months. These examinations include an assessment of how a bank manages the risks presented by its relationships with third parties.

*Businesses from outside the banking industry can bring innovation and new insights into the highly regulated business of banking. Understanding the environment in which banks operate will help innovators navigate the regulatory requirements unique to banking.*

## HOW DO BANKS DECIDE WHICH THIRD PARTIES TO USE?

Banks use third parties for many different aspects of their operations. Bank management remains ultimately responsible for identifying and controlling risks and activities conducted by or through their bank, whether these risks and activities arise directly or through an outside party.

Banks establish risk management programs to manage the risks associated with third-party relationships. While each bank is unique, third-party risk management programs generally address four basic elements:

- Assessing the risk associated with the activity being conducted.
- Conducting due diligence in selecting a third party.
- Structuring contracts and reviewing those contracts at appropriate levels at the bank.
- Overseeing and managing the third-party relationship on an ongoing basis.

Banks tailor their third-party risk management program to their specific risk profile and product offerings. However, risk assessment and due diligence considerations generally include the following:


### Compliance with applicable laws and regulations by considering whether:

- The activity to be conducted is permitted by applicable laws and regulations;
- The third party has the appropriate license, charter, or registration to conduct the activity;
- The third party has familiarity with regulated financial institutions, and can demonstrate compliance with applicable laws and regulations; and
- There are complaints, litigation, or regulatory actions against the third party.

### Financial condition of the third party by assessing:

- Available financial information on the third party;
- The impact of the proposed contract on the third party's financial condition;
- Insurance coverage; and
- The third party's current capital, projected earnings, and funding sources to ensure long-term viability. (Sources of future funding may be particularly helpful in the case of a startup third party.)

### Ownership and management structure by reviewing:

- The ownership structure and the qualifications and experience of the third party in implementing and monitoring the proposed activity;
- The third party's organizational structure, business resumption strategy and contingency and management succession plans; and
- The third party's strategies and goals, including service philosophy, quality initiatives, efficiency improvements, and employment policies.

### Special Considerations for Modelers

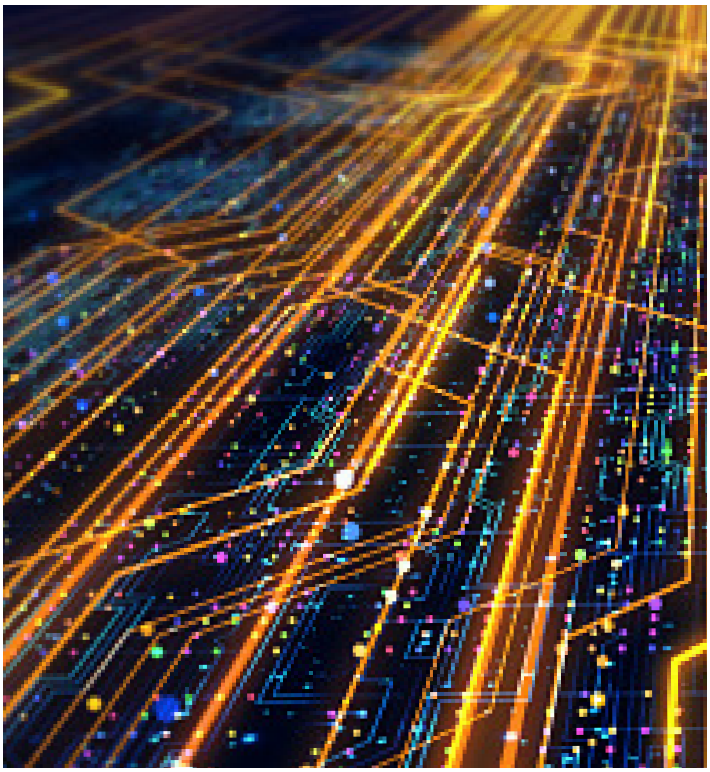
Special attention should be given by third parties providing models to banks or using models in providing products or services. Banks using models, algorithms, or other types of automated decision-making systems may have specific model risk management requirements. A bank's model risk management framework may require:

- Disciplined and knowledgeable development of the model that is well documented and conceptually sound;
- Controls to ensure proper implementation of the model;
- Effective model validation processes; and
- Strong model governance, policies, and controls.

Accordingly, banks working with third parties expect to be able to understand the outcome—and the justification for the outcome—for any model used.

### Risk management and controls at the third party by assessing:

- The third party's internal controls, management information systems, systems and data security, privacy protections, and audit coverage;
- The third party's system of ongoing monitoring of risk and risk mitigation strategies;
- The third party's use of models, algorithms, or other types of automated decision-making systems;
- Whether the third party outsources its activities and, if so, how the third party manages other entities and the risks they may present, including cyber risk;
- Whether the third party engages independent entities to periodically test and audit risk mitigation controls; and
- The third party's business continuity and incident response plans.



## WHAT SHOULD I DO IF I WANT TO PROVIDE A SERVICE TO, OR PARTNER WITH, A BANK?

Banks tailor their review of third parties to their specific needs and the type of arrangement they are entering into. There are, however, a few general considerations described below that might help third parties prepare for the due diligence process.

**Understand the framework of laws and regulations that apply to banks.** All FDIC-supervised institutions must comply with safety and soundness standards. The standards cover, among other matters, internal controls and information systems, internal audit, loan documentation and underwriting, and data information security programs. Depending on the proposed activity to be conducted, third parties may also need to be familiar with laws and regulations related to consumer protection, privacy and data security, and the Bank Secrecy Act and federal anti-money laundering laws.

**Maintain a well-managed and financially strong business.** Third parties will be better positioned to do business with banks by demonstrating that management is strong and that the business is able to weather changes or disruptions. Third parties should expect to provide detailed financial and management information to the bank, including forward projections for earnings and equity.

**Be prepared for the questions banks may ask and for potential remediation of concerns.** Third parties should be prepared to provide detailed information about the product, service, system, or activity being offered; the terms on which it will be offered (including user and account agreements); model or service validation records showing product integrity, risk management mitigation, and consumer protection; and a description of governance, including internal controls and quality controls.

The risk assessment and due diligence processes may also result in a bank requiring new policies and procedures from the third party in advance of committing to the engagement. In particular, banks may require contracts to clearly define the degree of confidential treatment of information, including any shared customer information or other bank data, or any required protections of intellectual property and trade secrets. (See below for a list of items bank management may request from a third party as part of its due diligence and contract management process.)

**Demonstrate that the business has appropriate monitoring systems in place.** Once a bank enters into a relationship with a third party, it will monitor the activities to ensure they comport with the bank's business model, risk profile, and strategies, and will typically require the third party to take action to correct any deficiencies. Banks may also subject third parties to audits, cybersecurity/perimeter tests, or periodic on-site reviews, depending on the nature of the relationship. Banks may also require reports to verify compliance with applicable laws and contracts.

Third parties should be prepared to show how they will ensure ongoing compliance with applicable laws and regulations. If the relationship involves a bank's customers, third parties should be prepared to demonstrate how they will ensure compliance with consumer protection laws and regulations, data security and privacy laws and regulations, and how they will track, monitor, remediate, and respond to consumer complaints. Banks may also restrict third parties from using or disclosing the bank's information and require protections for customer personally identifiable information.


The FDIC's **BankFind** tool can help you determine if a bank is FDIC-insured. Check out FDIC.gov/bankfind to learn more.

## ITEMS BANK MANAGEMENT MAY REQUEST FROM A THIRD PARTY

Below is a list of materials and terms bank management may request from a third party as part of its due diligence and contract management process. This list is not intended to be all-inclusive; items will vary depending on the services offered and the institution.

### Background, Initiatives, and Ownership Information

- The third party's mission statement, service philosophy, and quality initiatives;
- State and Articles of Incorporation;
- Business license and tax identification;
- Description and scope of all activities in which the third party is engaged;
- How long the third party has been engaged in the activity under discussion;
- Experience and qualifications of the third party's principals;
- Background and experience with consumer protection laws and regulations;
- Details and history of the third party's website and social media footprint, if applicable; and
- Details on any significant complaints or litigation (past and pending) or regulatory actions against the third party or its owners or principals, if applicable.

### Policies, Procedures, and Infrastructure

- Details on management information systems, including network and data flow diagrams;
- Scope of internal controls, systems and data security, privacy protections, and audit coverage;
- Applicable policies and procedures, including policies (if applicable) on logical account management, data classification and handling, information security, compliance, anti-money laundering, and incident management;
- Audit or independent review engagement package, including résumés of the auditors/ reviewers; underwriting criteria, if relationship involves lending to bank customers;
- Procedures for checking customers against Office of Foreign Assets Control and other related control lists;
- Business resumption strategy and contingency plans;
- Penetration testing and results;
- Quality assurance reports;
- Employment policies, including background check and hiring practices;
- List of subcontractors or other parties used by the third party; and
- Complaint handling and escalation procedures.

### Financial Information and Marketing Materials

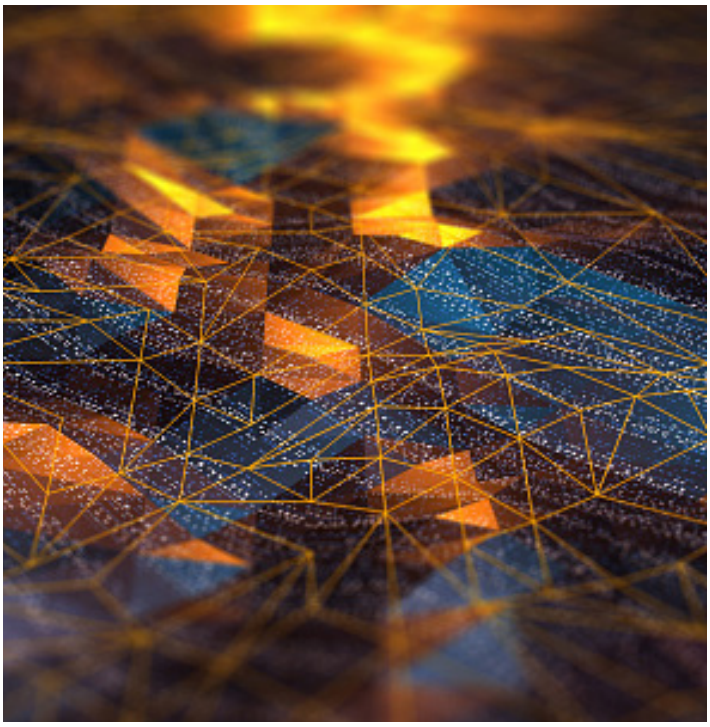
- Filings with the U.S. Securities and Exchange Commission;
- Insurance coverage;
- Three to five years of audited financial statements, annual reports, and other available financial information;
- Marketing materials involving the bank's name and products; and
- Details on any fees, interest rates, or other terms for products or services offered through the bank.

### Terms an FDIC-Supervised Bank May Request in a Business Contract

- Terms that require the third party to comply with applicable consumer protection laws, regulations, and regulatory guidance;
- Authorization for the bank and the appropriate regulatory agency to access third-party records related to evaluating compliance with applicable laws and regulations;
- Authorization for the bank to monitor and periodically review the third party for compliance with the agreement;
- Prohibitions from using or disclosing the bank's information outside of the terms of the agreement;
- Protection of consumers' personally identifiable information;
- Access rights for the bank to audit the third party; and
- Proper destruction of customer information in the event of contract termination.

### Items a Bank May Review or Require on an Ongoing or Periodic Basis

- Annual review of the third party's licensing or registrations;
- Annual review of the third party's financial statements, financial obligations, annual reports, and owners' and principals' financial condition;
- Annual review of the third party's insurance coverage;
- Audit reports or other reports of the third party;
- Regular review of internal controls and security environment, which may include on-site quality assurance reviews;
- Review of the third party's business resumption contingency planning and testing; and
- Review of any customer complaints involving the products and services provided by the third party.



## ADDITIONAL FDIC RESOURCES

The following information may be useful to third parties who conduct business with banks. This is not intended as an all-inclusive list.

- Interagency Guidelines Establishing Standards for Safety and Soundness (Part 364 of the FDIC Rules and Regulations)
- Policy Statement on Discrimination in Lending
- Bank Secrecy Act and Related Rules and Regulations and Other Supervisory Resources
- Supervisory Guidance on Model Risk Management (FIL-22-2017, June 7, 2017)
- Interagency Guidance Regarding Unfair or Deceptive Credit Practices (FIL-44-2014, August 22, 2014)
- Social Media: Consumer Compliance Risk Management Guidance (FIL-56-2013, December 11, 2013)
- Third-Party Risk: Guidance for Managing Third-Party Risk (FIL-44-2008, June 6, 2008)
- Unfair or Deceptive Acts or Practices under Section 5 of the Federal Trade Commission Act (FIL-26-2004, March 11, 2004)

## OTHER RESOURCES

- Board of Governors of the Federal Reserve System
- Office of the Comptroller of the Currency
- U.S. Department of the Treasury: Office of Foreign Assets Control

---

This Guide provides information for people and companies that wish to do business with insured banks supervised by the Federal Deposit Insurance Corporation. It does not contain requirements or supervisory guidance and does not require action by banks or those with whom they do business.