Fall 2018

COMMUNITY BANKING ADVISOR

VENDOR RISK MANAGEMENT
Time to review your program

SHOULD YOU PARTNER WITH A FINTECH COMPANY?

NONINTEREST INCOME CAN KEEP YOUR BANK ON COURSE

BANK WIRE

MAULDIN & JENKINS

800-277-0080 | www.mjcpa.com

VENDOR RISK MANAGEMENT

Time to review your program

For many years, banks have relied on third-party vendors for a range of services, including core bank processing, IT, accounting, internal audit, appraisals, loan review and servicing, anti–money laundering compliance, collections, sales and marketing, and human resources. Managing the risks associated with outside vendors is key, because such parties are considered an extension of bank personnel.

MINIMIZE EXPOSURE

Outsourcing to a third party doesn't relieve a bank from responsibility and legal liability for compliance or consumer protection issues. And as banks and vendors increasingly rely on evolving technologies to deliver products and services, their exposure to ever-changing cybersecurity risks demands constant vigilance.

Even if you have a solid vendor risk management program in place, you'll need to review it periodically. Banking regulators expect your program to be "risk-based" — that is, the level of oversight and controls should be commensurate with the level of risk an outsourcing activity entails. But here's an important caveat: That risk can change over time. Some vendors, such as appraisal and loan collection companies, have traditionally been viewed as relatively low risk. But in today's increasingly cloud-based world, any vendor with access to your IT network or sensitive nonpublic customer data poses a substantial risk. Last year, for example, Scottrade Bank experienced a data breach that exposed 20,000 customer records when a third-party vendor — a professional services provider — uploaded data to a cloud server that lacked proper security protocols.

ASK QUESTIONS

Here are some questions that will help you review your vendor risk management program:

Have you conducted a risk assessment? Determine whether outsourcing a particular activity is consistent with your strategic plan. Evaluate the benefits and risks of outsourcing that activity as well as the service provider risk. This assessment should be updated periodically.

Generally, examiners expect a bank's vendor management policies to be appropriate in light of the institution's size and complexity. They also expect more rigorous oversight of *critical* activities, such as payments, clearing, settlements, custody, IT or other activities that could have a significant impact on customers — or could cause significant harm to the bank if the vendor fails to perform.

Have you thoroughly vetted your service providers? Review each provider's business background, reputation and strategy, financial performance operations and internal controls. The depth and formality of due diligence depends on the risks associated with the outsourcing relationship and your familiarity with the vendor. If your agreement allows the provider to outsource some or all of its services to subcontractors, be sure that the provider has properly vetted each subcontractor. The same contractual provisions must apply to subcontractors and the provider should be contractually accountable for the subcontractor's services.

Do you rely on one vendor for most outsourced services? Doing so may provide cost savings and simplify the oversight process, but diversification of vendors can significantly reduce your outsourcing risks, particularly if a vendor has an especially long disaster recovery timeframe.

Do your contracts clearly define the parties' rights and responsibilities? In addition to costs, deliverables, service levels, termination, dispute resolution and other terms of the outsourcing relationship, key provisions include compliance with applicable laws, regulations and regulatory guidance; information security; cybersecurity; ability to subcontract services; right to audit; establishment and monitoring of performance standards; confidentiality (in the case of access to sensitive information); ownership of intellectual property; insurance, indemnification, and business continuity; and disaster recovery.

Do providers receive incentive compensation? Review incentives carefully to be sure they don't encourage providers to take excessive risks.

Have you reviewed vendors' disaster recovery and business continuity plans? Be sure that these plans align with your own and are reviewed at least annually, and that vendors have the ability to implement their plans if necessary.

Are you monitoring vendor performance? Monitor vendors to ensure they're delivering the expected quality and quantity of services and to assess their financial strength and security controls. It's particularly important to closely monitor and control external network connections, given the potential cybersecurity risks. The level of oversight required depends on the risks presented by a particular vendor.

Do you conduct independent reviews? Banking regulators recommend periodic independent reviews of your risk management processes to help you assess whether they align with the bank's strategy and effectively manage risks posed by third-party relationships. The frequency of these reviews depends on the vendor's risk-level assessment, and they may be conducted by the bank's internal auditor or an independent third party. The results should be reported to the board of directors.

COMMON WEAKNESSES IN VENDOR RISK MANAGEMENT PROGRAMS

According to the Federal Reserve, examiners have observed the following common vendor risk management weaknesses:

- Insufficient oversight by banks' directors,
- Failure to maintain a formal, documented outsourcing policy,
- Vague contract terms — particularly with regard to vendor performance requirements,
- Contract terms that favor the vendor,
- Inadequate disaster recovery tests, particularly with regard to potential cybersecurity events,
- Inadequate review of vendors' information security and cybersecurity procedures,
- Inappropriate risk ratings of critical vendors, and
- Reliance on one vendor for several critical products or services.

BE VIGILANT

If your bank outsources key functions to third parties, it should develop and maintain a comprehensive risk management program for selecting, vetting and overseeing outside vendors. Failure to do so can expose your bank to significant risks, including regulatory noncompliance, cybersecurity breaches, violations of consumer protection laws and lasting damage to your reputation. To protect your institution, a good rule of thumb is to exercise at least the same level of vigilance in managing third-party activities as you do in managing in-house activities. ■

SHOULD YOU PARTNER WITH A FINTECH COMPANY?

When it comes to technology, one thing is sure: Community banks that fail to deliver the digital products and services their customers demand will get left behind. Today's customers, particularly younger ones, want access to banking services on their computers, tablets and phones, and are all too ready to switch banks to obtain the digital experience they desire.

WHERE DOES FINTECH COME IN?

What's less sure is how to get there: Build, buy or partner? Few community banks have the resources to build their own digital services. For many banks, buying the functionality they seek from a vendor is an acceptable option. But an increasing number of banks are partnering with fintech companies to develop more innovative, customized solutions. Some banks are even acquiring fintech companies or investing in fintech "accelerators" — organizations that provide funding and other support services for fintech start-ups.

[FOR MANY BANKS, BUYING THE FUNCTIONALITY THEY SEEK FROM A VENDOR IS AN ACCEPTABLE OPTION.]

One well-known success story involves Boston's $850 million Radius Bank. The bank partnered with fintech and investment firms to create Aspiration Summit Checking, a high-interest online-only checking account named best checking account by *Money* magazine shortly after it was launched in 2015.

IS COLLABORATION THE ANSWER?

Not long ago, banks viewed fintech companies as a threat, but in recent years that attitude has begun to change. In a 2016 study, *Growing Together: Collaboration Between Regional and Community Banks and Fintech*, law firm Manatt, Phelps & Phillips, LLP, and financial intelligence firm Mergermarket reported that the vast majority of responding community banks viewed collaboration with fintech companies as "essential" (43%) or "very important" (43%).

Banks cite several benefits to collaboration, including improving their ability to offer online services — in particular, more convenient and reliable mobile platforms — decreasing technology costs and allowing them to offer lower lending rates. According to the study, fintech companies see working with community banks as an opportunity "to become established in the industry, legitimize their operations in the eyes of skeptical consumers or expand their market share." Some fintech companies, the report goes on, "are also in need of capital and see the bank's liquidity as a potential benefit."

Although the majority of banks (54%) view fintech companies as potential partners, some banks (5%) continue to see them as a threat and a significant number (27%) see them as both potential partners *and* a threat. Nevertheless, the vast majority of banks (88%) believe that, in 10 years, the banking industry will be characterized by "traditional banks partnering with fintech companies in a largely collaborative environment."

But fewer fintech companies (48%) are as optimistic about future collaboration. A significant number of respondents (37%) believe that, in 10 years, the banking industry will be dominated by "a few large banks, with fintech serving all other niches."

WHAT ARE THE CHALLENGES?

Partnering with a fintech company is a complex venture that involves a variety of risks, so thorough due diligence is critical. Bank respondents in the study discussed above said the biggest due diligence challenges in vetting potential fintech partners are:

- Legal/regulatory due diligence (46%),
- Cybersecurity due diligence (32%), and
- Financial analyses (22%).

Be sure to work with experienced legal and financial advisors as you explore your fintech options. ■

NONINTEREST INCOME CAN KEEP YOUR BANK ON COURSE

Banks have to withstand the ups, downs, ins and outs of dozens of variables that may affect their financial status year by year. To help keep the ship afloat, your bank sometimes needs to focus on noninterest income because interest income isn't always enough to maintain a steady and secure bottom line.

WHAT ARE THE SOURCES OF NONINTEREST INCOME?

In addition to deposit account service charges, noninterest income may arise from loan origination and servicing fees, overdraft and NSF charges, and gains on sales of loans and investment securities.

Noninterest income also may be derived from various products and services — including insurance and annuity products, as well as brokerage, trust and financial planning services.

WHAT ABOUT COLLECTIONS?

Community banks have a history of being easy on customers by waiving NSF fees and other penalties when they receive complaints. Although it's important for bank personnel to have the discretion to waive these fees, high waiver rates — some estimates are higher than 50% — can quickly wipe out substantial amounts of revenue.

To keep waivers under control, set a target level for discretionary waivers and train bank personnel to understand the significance of noninterest income, make good decisions regarding fee waivers and handle customer complaints. If you haven't already done

so, try automating the fee initiation process so that nothing falls through the cracks and incorporate waiver targets into your incentive compensation decisions.

Finally, be sure to include fee waiver data in management reports, which will let you monitor results.

HOW CAN YOU STAY AHEAD OF COMPETITORS?

Banks often miss opportunities to charge higher fees because they fail to keep tabs on their competitors. Identify the predominant banks in your market and procure their fee schedules. Comparing competitors' fees to your own may uncover significant pricing opportunities.

That doesn't mean you should increase your fees to match the highest priced banks in your area. But if you find your fee schedule is on the low end of the spectrum, a modest increase can have a substantial impact on your bank's revenue.

If you do increase your fees, monitor your results closely to ensure the strategy produces the desired outcome.

WHAT ABOUT RELATIONSHIP VALUE PRICING?

Relationship value pricing can be a highly effective strategy for enhancing fee revenue. It sets prices based on the overall value of a banking relationship with a customer or group of customers, such as a family or a business and its employees.

In its simplest form, relationship value pricing might involve package deals for products or services. A common example is free checking accounts for customers who maintain a minimum loan balance. A more sophisticated approach is to develop customized pricing based on a valuation of the products and services a specific customer receives.

For relationship value pricing to work, your bank must carefully analyze the costs, benefits and potential profitability of each customer relationship. It's also critical to have systems that monitor the relationship. Banks often lose revenue because they're unaware that the relationship has changed. For example, a bank might continue providing free checking even though the related loan has fallen below the minimum balance or has been paid off.

HAVE YOU CONSIDERED LIFE INSURANCE POLICIES?

Insurance policies on the lives of directors, officers and other key employees can be cost-effective tools for boosting noninterest income. Your bank can buy coverage or use "split-dollar" arrangements to share the costs and benefits of these policies with employees.

Bank-owned life insurance (BOLI) is often used to fund supplemental executive retirement plans, other nonqualified deferred compensation plans and retiree health benefits. BOLI can be a powerful planning tool because a life insurance policy's cash value grows on a tax-deferred basis and, if the policy is held until the insured employee dies, the death benefit is generally tax-free.

A caveat: To enjoy these tax benefits, your bank must comply with strict notice and consent requirements before buying a policy on an employee's life.

WHAT STRATEGIES WORK FOR YOU?

To some extent you can foresee, and plan for, your bank's financial progress. But to navigate the choppy waters of profits and losses and make sure you come out ahead, you'll need to supplement interest income with other income streams. ■

BANK WIRE

CRE APPRAISAL THRESHOLD NOW $500,000

The federal banking agencies recently raised the threshold for commercial real estate (CRE) transactions requiring an appraisal from $250,000 to $500,000. The change responds to concerns in the banking industry that the threshold hasn't kept pace with price appreciation in the CRE market. Originally, the agencies proposed raising the threshold, which had been in place for more than 20 years, to $400,000, but ultimately concluded that a $500,000 threshold would materially reduce the regulatory burden on banks without threatening safety and soundness.

Now that you can use evaluations, rather than appraisals, for CRE transactions below the new threshold, it's a good idea to review your evaluation policies and procedures to ensure that they reflect fair market value. ■

FED LAUNCHES NEW CONSUMER COMPLIANCE PUBLICATION

Many banks continue to struggle with the complexities of consumer protection regulations, such as the Truth in Lending Act's Loan Originator Compensation Rule. Recently, the Federal Reserve Board launched a monthly publication that may provide some clarity. The *Consumer Compliance Supervision Bulletin* is designed to keep bankers and others informed about consumer protection developments, provide high-level summaries of relevant supervisory issues, and offer practical steps for banks to consider when managing consumer compliance risks.

The inaugural issue (July 2018) focuses on redlining and other potentially discriminatory procedures, unfair or deceptive acts or practices (UDAP), and regulatory and policy developments. For example, the bulletin explains that, despite the Loan Originator Compensation Rule, fair lending risks can arise when a bank sets discretionary target prices for different loan originators — and the originators with higher target prices tend to serve minority areas. The bulletin offers guidance on managing this risk, such as implementing controls to limit discretion and mapping loans by target price.

You can find the bulletin by visiting federalreserve.gov and typing "consumer" in the search box. ■

LOAN PARTICIPATIONS: HANDLE WITH CARE

Loan participations — that is, loans by two or more lenders to a single borrower — offer several benefits to community banks. For example, they can help you:

- Increase lending activity despite low local demand,
- Serve customers whose credit needs exceed legal lending limits,
- Diversify your portfolio, and
- Enhance liquidity, interest-rate risk management, capital and earnings.

If you're considering this strategy, be sure to work closely with your legal and financial advisors to manage the risks involved. Among other steps, you should conduct your own due diligence on the borrower, even if another institution takes the lead. Also, carefully review the participation agreement, which details each party's rights and responsibilities — particularly who is responsible for collections or payments in the event of a default — and take other steps to manage the risks associated with these transactions. ■

This publication is distributed with the understanding that the author, publisher and distributor are not rendering legal, accounting or other professional advice or opinions on specific facts or matters, and, accordingly, assume no liability whatsoever in connection with its use. ©2018 CBAfa18

MAULDIN & JENKINS

200 GALLERIA PARKWAY, SE | SUITE 1700
ATLANTA, GA 30339
800-277-0080 | www.mjcpa.com

Other offices:
Albany, GA | Birmingham, AL | Bradenton, FL
Chattanooga, TN | Macon, GA

To receive this newsletter electronically,
please send an email to banknewsletter@mjcpa.com

Financial Institution Services

At Mauldin & Jenkins, we have more than 90 years of experience providing audit, tax and advisory services to financial institutions. We understand audit requirements, tax planning strategies, compliance and more. With a dedicated team focused on providing services to financial institutions, we are a recognized and proven leader. Our services include:

- External & Internal Audits
- SOX 404 / FDICIA Internal Control
- Tax Planning & Preparation
- Employee Benefit Plan Audits
- Mergers & Acquisitions
- Compliance & Bank Secrecy Act Reviews
- Loan Reviews
- Risk Management
- Information Technology Reviews

A history of success built one satisfied client at a time!