acxell

ADVISOR

Fall 2022

Working with vendors and partners
ARE YOU MANAGING THIRD-PARTY RISK?

HOW TO EXPAND OPTIONS AND IMPROVE YOUR BANK'S BOTTOM LINE

GET READY FOR A NEW CYBERINCIDENT REPORTING RULE

BANK WIRE

acxell

www.acxellrms.com 877.651.1700

Working with vendors and partners

ARE YOU MANAGING THIRD-PARTY RISK?

In today's highly competitive environment, banks increasingly are turning to outside vendors and partners to enhance their products and services, gain access to innovative technologies, benefit from expert advice, increase efficiency and reduce costs. As your bank explores the options, it's important to have processes in place for managing the risks associated with these third-party relationships. Recent guidance indicates that federal banking regulators have high expectations for banks when it comes to third-party risk management.

PROPOSED INTERAGENCY GUIDANCE

In July 2021, the Federal Reserve, Federal Deposit Insurance Corporation (FDIC) and Office of the Comptroller of the Currency (OCC) released proposed interagency guidance on managing risks associated with third-party relationships. One purpose of the proposed guidance is to promote consistent policies among the three agencies. Currently, each agency has its own guidance. The FDIC issued its "Guidance for Managing Third-Party Risk" in 2008, while the Federal Reserve issued its "Guidance on Managing Outsourcing Risk" in 2013. Also in 2013, the OCC followed suit with "Third-Party Relationships: Risk Management Guidance."

> FACTORS TO CONSIDER WHEN NEGOTIATING CONTRACTS WITH THIRD PARTIES INCLUDE THE NATURE AND SCOPE OF THE ARRANGEMENT AND MEASURES USED TO ASSESS PERFORMANCE.

The proposed interagency guidance is generally based on the OCC guidance, which is more detailed and prescriptive than the other agencies' pronouncements on the subject. So, if the proposed guidance is adopted, smaller banks currently subject to the Federal Reserve and FDIC guidance may experience heightened supervisory scrutiny of their third-party risk management programs in the future.

CRITICAL ACTIVITIES

Consistent with existing guidance, the proposed guidance emphasizes that a bank's third-party risk management program should be "commensurate with its size, complexity and risk profile as well as with the level of risk and number of … third-party relationships," and should focus on "critical activities." These are significant bank functions or other activities that:

- Could cause a bank to face 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 provider or bring the outsourced activity in-house.

A significant bank function is "any business line … including associated operations, services, functions and support, that upon failure would result in a material loss of revenue, profit, or franchise value."

RISK MANAGEMENT LIFE CYCLE

According to the proposed guidance, effective risk management for all third-party relationships follows this continuous, six-stage life cycle:

1. Planning,
2. Due diligence and third-party selection,
3. Contract negotiation,

4. Oversight and accountability,

5. Ongoing monitoring, and

6. Termination.

The proposed guidance lists the factors a bank should consider at each stage. For example, in conducting due diligence on a potential vendor or partner, factors to consider include the third party's overall business strategy and goals, as well as its ownership structure and regulatory compliance capabilities, financial condition, resources and prior business experience, and fee structure and incentives. Other factors include, but aren't limited to, the qualifications of its principals and the effectiveness of its own risk management, information security program, and physical security and environmental controls.

Factors to consider when negotiating contracts with third parties include the nature and scope of the arrangement, measures used to assess performance, and responsibility for providing, receiving and retaining information. You also need to take into account the bank's rights to audit and monitor performance, compliance responsibility, confidentiality and integrity of the bank's information, and responsibility for responding to customer complaints, among other factors.

Throughout the life cycle, a bank should follow three principles: 1) oversight and accountability, 2) documentation and reporting, and 3) independent reviews. The proposed guidance outlines regulatory expectations regarding the responsibilities of a bank's board of directors and management to oversee the risk management process, as well as documentation and reporting requirements. It also emphasizes the importance of independent reviews of the risk management process by a bank's internal auditor or an independent third party.

Among other things, these reviews assess the adequacy of a bank's processes for ensuring that third-party relationships align with its business strategy. They also look at how the bank identifies, measures, monitors and controls third-party risk. In addition, the reviews evaluate the bank's understanding of and monitoring of concentration risks and its responses to material breaches, service disruptions or other material issues. Finally, the reviews assess how the bank confirms oversight and accountability for managing third-party relationships.

FINTECH DUE DILIGENCE GUIDANCE FOR COMMUNITY BANKS

Many community banks are partnering with financial technology (fintech) companies to gain access to cutting-edge technologies that can enhance their product and service offerings. To help banks manage the risks associated with these partnerships, the federal banking regulators jointly published "Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks."

The guide focuses on six key due diligence topics that banks should consider when evaluating prospective fintech partnerships:

1. Business experience and qualifications,
2. Financial condition,
3. Legal and regulatory compliance,
4. Risk management and controls,
5. Information security, and
6. Operational resilience.

For each topic, the guide outlines relevant considerations, lists potential sources of information and provides an illustrative example of the due diligence process.

You can find the guide online at fdic.gov/news/press-releases/2021/pr21075a.pdf.

IMPLEMENT BEST PRACTICES

If and when the proposed guidance is adopted, smaller banks with significant third-party relationships will need to implement more rigorous risk management practices. In the meantime, the guidance provides an excellent framework for managing third-party risk and outlines many best practices that banks would be well-advised to consider. ■

HOW TO EXPAND OPTIONS AND IMPROVE YOUR BANK'S BOTTOM LINE

Community banks continue to deal with economic uncertainty as a result of the COVID-19 pandemic and its impact on businesses and organizations. They're also faced with an increasingly rapid pace of technological change affecting many aspects of banking. To help your bank navigate these rough waters, you may want to consider adding some new business lines that can increase your fee income and help stabilize your profits.

TRY SBA LENDING

The U.S. Small Business Administration (SBA) operates several programs designed to help small business owners grow or maintain their businesses. The SBA's two flagship lending programs — 7(a) and 504 — also offer significant benefits for community banks.

Under the 7(a) program, the SBA guarantees a portion (up to 75% or more) of loans to eligible small businesses. These loans, which can reach as high as $5 million, can be used for a variety of business purposes, such as:

- Acquiring or starting a business,
- Purchasing machinery, equipment or supplies,
- Improving land or buildings,
- Financing receivables,
- Augmenting working capital, or
- Refinancing existing debt (under certain conditions).

Benefits to banks that make 7(a) loans include:

Expanded customer base. The program allows banks to serve customers that wouldn't otherwise satisfy conventional underwriting criteria.

Improved risk management. The SBA's guaranty on 7(a) loans mitigates the lender's risk.

Increased lending business. In many cases, the guaranteed portion of a 7(a) loan doesn't count toward a bank's legal lending limit, helping it boost its lending capacity.

Reduced capital requirements. Guaranteed loans have a lower risk weight than unguaranteed loans for regulatory capital purposes, so 7(a) lending can make it easier for a bank to meet capital requirements.

Increased liquidity. Banks are allowed to sell the guaranteed portion of 7(a) loans into the secondary market, providing an alternative source of liquidity.

Under the 504 program, lenders partner with not-for-profit certified development companies (CDCs) to help small businesses expand and modernize by offering favorable financing for real property and major fixed assets. In a typical transaction, the lender and CDC each make a loan to a qualifying small business. The lender's loan usually is secured by a first lien covering 50% of project costs, while the CDC's loan is secured by a second lien covering up to 40% of project costs and backed by a 100% SBA-guaranteed debenture.

The 504 program benefits banks by creating opportunities to serve customers that wouldn't otherwise

satisfy conventional underwriting criteria. In addition, because banks enjoy a 50% loan-to-value (LTV) ratio, the program minimizes collateral risk. And, like 7(a) loans, 504 loans can be sold into the secondary market, providing an alternative liquidity source.

CONSIDER MUNICIPAL FINANCE

Community banks are increasingly pursuing opportunities to finance capital projects of state agencies, local governments and schools. Although yields on municipal loans tend to be lower than those of other types of loans, they generally enjoy higher credit quality.

They also enable community banks to diversify their business loan portfolios beyond commercial real estate. The added local visibility can attract new customers as well. In addition, they may get Community Reinvestment Act credit if they meet geographic restrictions.

GET INTO INSURANCE PREMIUM FINANCING

As the name suggests, premium financing involves lending money used by the borrower to pay life insurance premiums. The loan is secured by the policy's cash surrender value plus, if necessary, additional collateral (such as publicly traded securities or letters of credit).

Typically, these arrangements involve indexed universal life policies, which offer guaranteed minimum returns. This makes them safe assets that support high LTV ratios — even as high as 100% in some cases.

THINK BIGGER

Simply continuing to conduct business as usual in the face of change is likely a losing strategy in the long run. To stay competitive and financially strong, you'll need to grow and adapt. These are just a few ideas for expanding your bank's offerings. ■

GET READY FOR A NEW CYBERINCIDENT REPORTING RULE

Banks are now required to report significant cyberincidents within 36 hours, under a new rule issued by the Federal Reserve, Federal Deposit Insurance Corporation (FDIC) and Office of the Comptroller of the Currency (OCC) (the "regulators"). The rule became effective April 1, 2022, with compliance required by May 1, 2022.

THE DETAILS

The rule requires banks to report any "computer-security incident" that rises to the level of a "notification incident." A computer-security incident is an "occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores or transmits."

According to regulators, these incidents can result from cyberattacks (for example, destructive malware or malicious software). They also may result from non-malicious causes, such as hardware failures, software failures or human error.

FAQs

Here are the main points to know about the reporting process:

Which incidents should you report? Given the frequency of cyberattacks in the financial services industry, regulators limited banks' reporting obligations under the rule to "notification incidents." These are defined as any "computer-security incident that has

materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade," a bank's 1) ability to carry out banking operations, activities or processes, or deliver products and services to customers, 2) business lines whose failure would result in a material loss of revenue, profit or franchise value, or 3) operations whose failure would pose a threat to U.S. financial stability.

In the preamble to the final rule, the regulators provided a list of events that generally are considered notification incidents, including, but not limited to:

- Large-scale distributed denial-of-service attacks that disrupt customer account access for more than four hours,
- Widespread system outages experienced by a core banking service provider with an undeterminable recovery time,
- Failed system upgrades or changes that cause widespread user outages for customers and bank employees,
- Computer hacking incidents that disable banking operations for an extended period of time,
- Malware that poses an imminent threat to the bank's core business lines or critical operations, and
- Ransom malware attacks that encrypt a core banking system or backup data.

The regulators encourage banks to resolve any doubt about whether they've experienced a notification incident in favor of reporting the incident.

How do you report a notification incident? As soon as you determine that a notification incident has occurred, you should notify your primary regulator as soon as possible, but no later than 36 hours after the determination is made. Notification may be via email, telephone or "other similar methods [the regulators] may prescribe."

What about bank service providers? The rule also imposes reporting obligations on bank service providers subject to the Bank Service Company Act (BSCA). If a service provider determines that it's experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, BSCA-covered services for four or more hours, it must, as soon as possible, notify at least one bank-designated point of contact at each affected bank customer. Armed with this information, a bank can determine whether it's required to report the incident to its regulator. It's important to be aware that this notification requirement doesn't apply to scheduled maintenance, testing or software updates previously communicated to a bank customer.

HAVE A PLAN

To comply with the new rule, all banks may want to consider whether any service provider contracts require revision. They also should develop policies and procedures for monitoring computer-security incidents, determining whether they're notification incidents and reporting them to the appropriate regulator. ■

BANK WIRE

OCC DISCUSSES BANKING RISKS

In the latest installment of its *Semiannual Risk Perspective*, the Office of the Comptroller of the Currency (OCC) examines key issues facing the federal banking system and the effects of the COVID-19 pandemic on the banking industry. Regarding the pandemic, the agency says that banks "are showing resilience in the current environment with satisfactory credit quality and strong earnings, but weak loan demand and low net interest margins … continue to weigh on performance."

The report also notes that "operational risk is elevated as banks respond to an evolving and increasingly complex operating environment and cyber risks" and that "regulatory changes and policy initiatives that continue to challenge risk management" are driving heightened compliance risk. Also discussed is an OCC initiative to act on climate change risks. ■

IRS FINALIZES LIBOR TRANSITION REGULATIONS

As banks make the transition away from using the London Interbank Offered Rate (LIBOR) as a reference interest rate for loans and other financial instruments, the IRS has finalized its guidance on the tax consequences. Under the final regulations, modification of a debt instrument to replace LIBOR or another discontinued interbank offered rate (IBOR) with a new reference rate won't result in a taxable exchange, provided certain requirements are met. Briefly, a "covered modification," which doesn't trigger tax consequences, is one that:

- Replaces an operative rate that refers to a discontinued IBOR with a qualified rate (as defined by the regulations),
- Adds a qualified rate as a fallback to an operative rate that refers to a discontinued IBOR, or
- Replaces a fallback rate that refers to a discontinued IBOR with a qualified rate. ■

LOOK OUT FOR RANSOMWARE ATTACKS

Recently, in light of an increase in the frequency and severity of ransomware attacks, the Financial Crimes Enforcement Network (FinCEN) replaced its October 1, 2020, ransomware advisory with *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, issued on November 8, 2021. The advisory reminds banks of their obligation to detect, prevent and report suspicious transactions associated with ransomware attacks and lists a dozen potential red flags of ransomware-related illicit activity.

Many of these red flags involve convertible virtual currency (CVC), the preferred payment method of ransomware perpetrators. For example, one red flag is a customer with no or a limited history of CVC transactions that sends a large CVC transaction. Another red flag is a customer that uses a foreign-located CVC exchanger in a high-risk jurisdiction known to have inadequate anti-money laundering/counter financing of terrorism (AML/CFT) regulations. ■

acxell ("acxell") has been meeting the specific risk management needs of community banks of all sizes since 1991. As a high quality and affordable alternative to other firms, acxell provides internal audit, regulatory compliance, BSA/AML, information technology, SOX/FDICIA and enterprise risk management review services and software. acxell is exclusively dedicated to the banking industry, providing clients with dedicated, focused and hand-held services reflective of a wide range of skills, experience and industry expertise. As a Firm, we have also been proactive in assisting our clients with the designing, implementation and testing of the internal control environment to assist management with the attestation requirement under the Sarbanes-Oxley Act.

acxell's uniqueness is characterized by its experienced staff and partners. Their hands-on involvement on each engagement provides our clients with a wide range of skills, experience and industry expertise. We employ the use of Subject Matter Experts — designated individuals performing audits in their specific field of expertise. The use of such professionals provides a unique value-added approach that is both efficient and productive.

We believe that a significant aspect of our services is our degree of involvement and responsibility to assist management by making suggestions for improvement, keeping them informed of professional developments and by acting as an independent counsel and sounding board on general business matters and new ideas.

We pride ourselves in our ability to provide effective and practical solutions that are commensurate with our clients' needs by emphasizing high-quality personalized service and attention. Our services are truly customized.

For **Solutions** *to your risk management needs, please contact our service coordinators at (877) 651-1700, or log-on to www.acxellrms.com to learn more.*

www.acxellrms.com

Headquarters:
646 US Highway 18
East Brunswick, NJ 08816

Offices:
New York, NY
Philadelphia, PA
Chicago, IL
Miami, FL