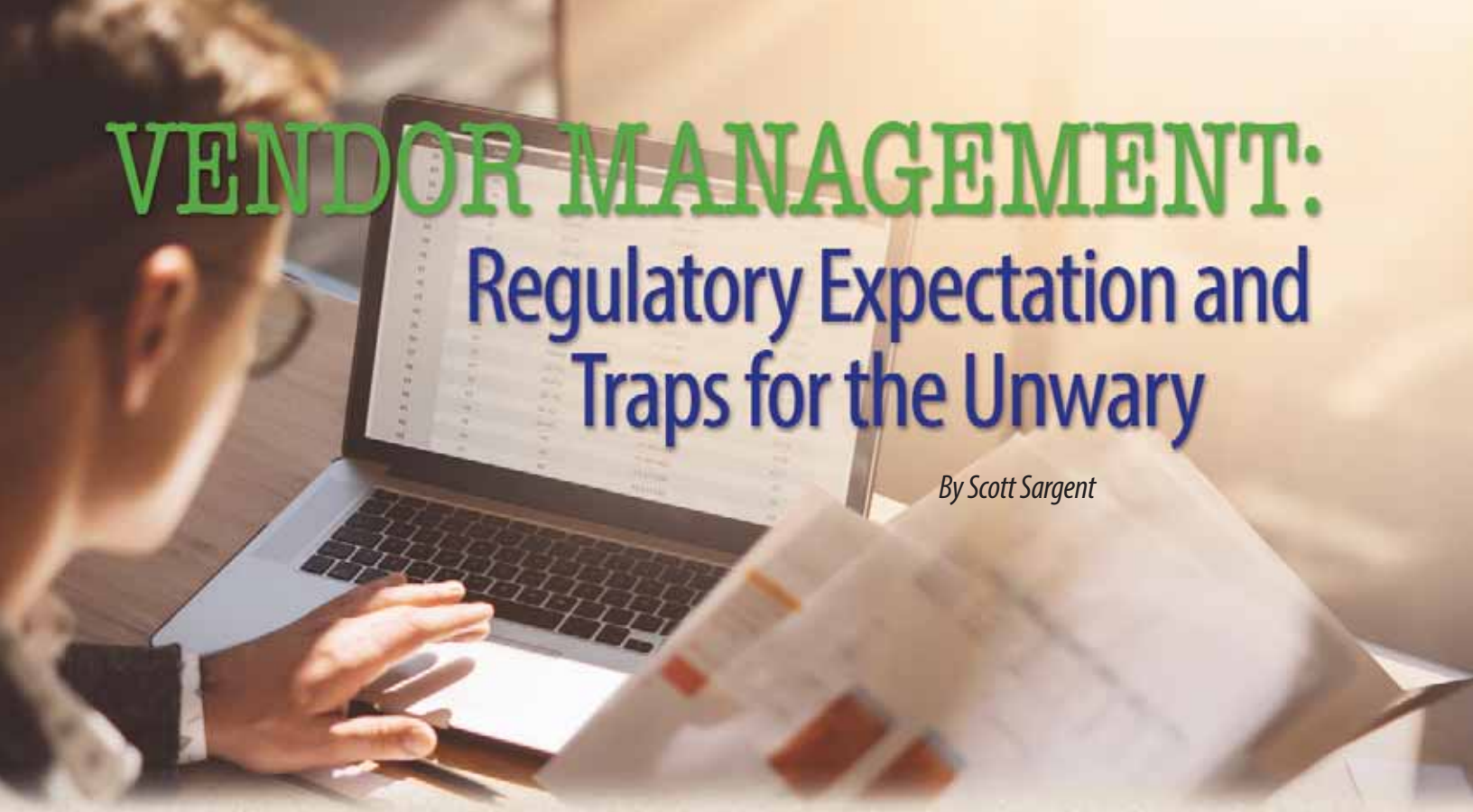

VENDOR MANAGEMENT: Regulatory Expectation and Traps for the Unwary

By Scott Sargent

The directive to banks for effective vendor management has been coming from regulators (the Federal Reserve, OCC, FDIC and CFPB) for several years. They have all issued guidance in this area, and multiple public data breaches caused by third party service providers led them to take a very strict interpretation of their guidance during their examinations. The recent disclosure of a massive data breach at Equifax will likely only reinforce the resolve for effective vendor management, and banks that are not ready will face a difficult examination.

Because the board of directors and senior management are responsible for managing risk posed to an institution through third party service providers, every bank's management team must ensure there is an effective vendor management process.

Risk Assessment

Every vendor management program should start with risk assessment. The bank must first determine whether outsourcing is consistent with its strategic direction, then conduct cost/benefit assessment. Then, some key potential risks from outsourcing functions that should be considered are country risks, reputational risk, operational risk, compliance risk, concentration risk, strategic risk and legal risk.

Due Diligence

Once it is determined the risks of outsourcing are manageable, due diligence on the vendor is the next step. The amount and depth of due diligence required is directly related to the level of risk and complexity of the vendor's service. However, the regulators have identified a number of specific areas to review.

First, ensure that the vendor's business strategy, such as its plans for mergers and divestitures, aligns with the bank and that the vendor has the appropriate licenses and the necessary internal controls and programs, including appropriate risk management, to provide the services in compliance with applicable laws and regulations.

Next, review the vendor's financial statements and records and be sure to thoroughly examine the vendor's market share, resources, business model and prior results. While considering financial information, be sure the proposed fees cannot create inappropriate risks such as high upfront fees or fees that could incentivize inappropriate behavior.

(Continued on page 26)

Vendor Management: Regulatory Expectation and Traps for the Unwary

Continued from page 24

The bank should then turn its attention to the vendor's employees. There should be a review of the vendor's programs to train employees on policies and procedures and the banks should verify that the vendor conducts background checks on its management and employees as well as subcontractors who have access to critical systems or confidential information.

Of course, any due diligence requires that the bank have a clear understanding of the vendor's technology systems, processes, maintenance and compatibility with regard to the services they will provide. As part of this evaluation, the bank may need to assess the vendor's information security and physical security programs and policies which may require site visits to the vendor's facilities and/or a review of internal and/or external audit reports depending on the criticality and sensitivity of the services to be provided. When looking at a vendor's systems, the bank should also evaluate the vendor's ability to deal with service disruptions and determine how those disruptions and recovery times and places will impact its operations.

One topic the regulators have been very concerned about recently is subcontractors. Before engaging any third party vendor, the bank should thoroughly assess any use of and reliance on subcontractors. The vendor's ability to manage and monitor the subcontractors is very important and the bank must ensure that, when critical or sensitive services are involved, they have access to the subcontractors audit information and may require ability to directly audit the subcontractor as well.

Finally, the bank will need to determine if the vendor has a sufficient process to identify, report, escalate and resolve incidents, including data security incidents, employee related incidents, operational disruptions or failures, compliance related and/or legal claims. Further, the bank will need to assess the vendor's insurance coverage to insure that appropriate types and levels of coverage exist to cover any potential incidents.

Documentation

Once the due diligence is done and a vendor is selected, attention must turn to the contract. The regulators have identified key provisions that should be considered in each service agreement. Basic, traditional terms should be included:

- description of the services to be provided along with service levels, metrics, deliverables or benchmarks;
- fees and payments; confidentiality requirements;
- obligations to follow applicable law;
- intellectual property rights;
- data retention;
- choice of law; and,
- dispute resolution and termination.

However, the regulators have become very specific about what they expect from some of these clauses and even added some additional topics for consideration.

For instance, with data retention, the contract should require the vendor to provide and retain timely, accurate, and comprehensive information that allows the bank to monitor performance. However, the regulators further recommended the prompt notification of financial difficulty, catastrophic events and significant incidents such as information breaches, data loss, service or system interruptions, compliance lapses, enforcement actions or other regulatory actions; personnel changes, or implementing new or revised policies, processes and information technology; and/or notification to the bank of significant strategic business changes, such as mergers, acquisitions, joint ventures, divestitures or other business activities that could affect the activities involved.

From the risk perspective, the regulators are being very specific that any indemnities and limitations of liability

(Continued on page 28)

Continued from page 26

should reflect the risk inherent in the relationship. A formula based on fees paid should not be readily accepted unless that reflects the true risk to the bank.

The contract should also address disaster recovery plans and the results of periodic testing; insurance coverages and proof of coverage; customer complaints; and subcontracting restrictions and notifications. Last but not least, the contract should stipulate that the performance by the vendor is subject to regulatory oversight, including access to all work papers, drafts and other materials.

Ongoing Monitoring

Once a contract is signed, banks need to establish procedures to monitor the activities of the vendor on an ongoing basis particularly when critical information or functions are involved. Banks also should ensure that their ongoing monitoring adapts accordingly as both the level and types of risks change over the lifetime of third-party relationships.

The monitoring requirements the regulators published require banks to continue updating the due diligence required on the front end with the additional obligations to monitor: (1) contract reporting requirements, (2) any key personnel changes, (3) any third party agreements that may pose a conflict of interest or introduce risk to the bank, (4) confidentiality obligations, and (5) consumer complaints.

Vendor management is essential to a safe and sound financial institution. A program should be established with appropriate reporting structures so that the senior management and board members have the information necessary to control and monitor risks to the bank. Finally, when appropriate, the bank should engage independent parties to review or audit a vendor's performance, processes, procedures, facilities or whatever is necessary to allow a bank to assess the ongoing risk.

Scott Sargent, of counsel in Baker Donelson's Birmingham office, advises community, regional and international banks on regulatory compliance and risk management. As part of his banking practice and work with Financial Technology companies, Sargent helps his clients implement regulations and best practices concerning data security, privacy and protecting confidential information generally and customer information specifically. He can be reached at ssargent@bakerdonelson.com.