LJN LAW JOURNAL NEWSLETTERS

Cybersecurity LAW & STRATEGY®

An ALM Publication

August 2017

Third-Party Cybersecurity Strategies Critical to Preparedness

This article examines the guidelines published by Board of Governors of the Federal Reserve System on managing outsourcing risk, along with the Office of the Comptroller of the Currency (OCC) 2013 OCC Bulletin 2013-29 and the supplemental Jan. 24, 2017, examination procedures, which are designed to help bank examiners tailor the examinations of national banks and federal savings associations determine the scope of the third-party risk management examination.

By David F. Katz, Richard D. Smith, Elizabeth K. Hinson, Jason Mark Anderman and Sarah Statz

Understanding third-party service provider relationships and the security risks they present to any organization is an essential element of cybersecurity planning. Bad actors continue to exploit the risks presented by third-party service providers that maintain access to corporate-owned information systems. Over the last several years, companies have found themselves the victim of costly and high profile data breaches occurring as a result of a third-party service provider's security failures. *See, e.g., In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154 (D. Minn. 2014); *In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at 1 (N.D. Ga. May 18, 2016).

In an era of ubiquitous data collection, reliance on these third parties for virtually all aspects of the business' technical operations has become standard operating procedure for many companies. At times, this reliance makes sense, as the provider may be better positioned to reduce risk in providing this service. To that end, the client must ensure it has the oversight capability to ensure the provider is successfully managing risk.

Identifying third-party service provider relationships and evaluating the risks they present requires careful planning and organization on the part of the business. Strong information governance and security controls for the evaluation of third-party service providers are required to manage risk effectively and, with increasing frequency, to comply with the legal expectations. Strong contractual protections with third-party service providers are also essential. For organizations that desire to formalize such processes, there are useful resources and guidance available to achieve these objectives.

This article examines the guidelines published by Board of Governors of the Federal Reserve System on managing outsourcing risk, along with the Office of the Comptroller of the Currency (**OCC**) 2013 OCC Bulletin 2013-29 and the supplemental Jan. 24, 2017, examination procedures, which are designed to help bank examiners tailor the examinations of national banks and federal savings associations determine the scope of the third-party risk management examination.

This article also considers the March 2017 regulations promulgated by the New York Department of Financial Services. *See,* N.Y. Comp. Codes R. & Regs. tit. 23, §500.00. The regulations and guidance provide an instructive framework for understanding third-party risk. Additionally, this article provides an overview of this framework and analyzes key considerations in adopting a third-party vendor management program. While this regulatory framework appears on its face to focus on service providers, there are benefits to using the framework to risk assess a wider range of third-party relationships, including partnerships where one company works with another to jointly offer a product to a customer.

Central Premise

Even organizations that do not operate in financial services would benefit from reviewing the guidance and regulations to develop an overall framework for handling the risk associated with third-party service providers. First, the guidance is

David F. Katz and **Elizabeth K. Hinson** are attorneys in the Privacy and Information Security Practice at Nelson Mullins (Atlanta). **Richard D. Smith** is managing partner of the firm's New York office. **Jason Mark Anderman** is vice president and senior counsel in the American Express General Counsel's Organization for vendor management, information security and real estate legal functions. **Sarah Statz** is vice president and senior counsel in the American Express General Counsel's Organization for information security. The authors gratefully acknowledge the assistance of Nelson Mullins summer associate, **Daniel Lockaby**, in the preparation of this article.

useful in navigating the complex third-party risk environment. Second, the framework guides entities on how to develop a viable risk management and contract negotiation strategy. Third, the framework shows how to mitigate data security risk. The framework can also be valuable to third-party service providers. For providers to remain viable in the market and continue to service customers that must comply with these legal expectations, a review of the regulatory requirements and legal guidance is valuable to identify the baseline requirements in order to compete effectively in any given market.

FRB SR 13-19: Guidelines Published by the Federal Reserve

The Board of Governors of the Federal Reserve System issued Guidance on Managing Outsourcing Risk to assist financial institutions in understanding and managing the risks associated with outsourcing a bank activity to a third-party service provider. Although this guidance from the Federal Reserve is specifically directed to financial institutions, it can easily be adapted to apply more broadly to other industries (as an aside, this guidance was intended to supplement the existing guidance contained in the Federal Financial Institutions Examination Counsel's (**FFIEC**) Outsourcing and Technology Services Booklet; the FFIEC is a larger agglomeration of regulators).

The guidance broadly characterizes six types of risks to financial institutions emanating from the use of third-party service providers. Among the six are: compliance risks; concentration risks (when reliance is placed upon too few limited providers); and reputational risks (where the provider performs poorly or whose failure leads to reputation damage on the part of the financial institution). The remaining three risks are: country-specific risks (when a financial institution has international operations); operational risks (when exposure can occur as a result of inadequate or failed internal processes); and legal risks (where exposures to lawsuits and fines could result to the financial institution). The legal risk stands out as unique here; an active third-party management program directly tackles the other risks and, in doing so, reduces legal risk of litigation and other challenges with third parties.

The guidance also provides a detailed overview of the key elements necessary for the creation of a service provider risk-management program. Additionally, this guidance emphasizes the responsibility of boards of directors and members of senior management to manage and understand third-party risk. There are three core elements here. First, a customer must evaluate the operations and internal controls of third-party providers via an initial due diligence and selection phase. Second, a customer must negotiate for certain valuable contract provisions to minimize the risk. Third, the customer must engage in ongoing oversight over the provider to ensure that known risks are effectively contained and new risks are properly managed.

In the due diligence and selection phase, the guidance provides specific criteria for the evaluation of third-party service providers. Depending on the characteristics of the service, some or all criteria may be necessary for review, and include: internal controls; facilities management (such as access and the sharing of facilities); staff training; system security; privacy protections (for the financial institution's confidential information); maintenance and retention of records; business resumption and contingency planning; services support and delivery; employee background checks; and adherence to applicable laws and regulations.

In the contractual and negotiation phase, the guidance focuses on the key terms and provisions that should be part of any contract for service with an outsourced third-party service provider. In particular, the agreement should establish the proper scope by defining the rights and responsibilities of the parties. For example, there should be clear provisions on support and maintenance obligations, customer service criteria, timeframes, compliance with applicable laws, the ability to subcontract services and insurance requirements, audit rights, access to audit reports, performance standards, and the confidentiality and security of information. Other topics include data ownership and licensing, hardware, software, and intellectual property; these can be the most sensitive to negotiate because the parties are deeply dependent on each other for the creation and output of information generated as a result of the relationship between the parties.

Lastly, the guidance emphasizes typically expected clauses such as indemnification, dispute resolution, limitation of liability, insurance, consumer complaint resolution, and termination. Especially in riskier relationships, the guidance emphasizes that a customer should develop a termination clause that is harmonized with the termination plan. The goal is to know ahead of time all available options to migrate properly away from a problematic third-party service provider, including switching to a competitor, performing the service in-house or retiring the service due to lack of future need.

2013 OCC Bulletin 2013-29 and Supplemental Jan. 24, 2017 Examination Procedures

While the Federal Reserve guidance is helpful to consider the risks of implementing and contracting third-party agreements, the OCC bulletin encourages companies to consider the "strategic risk" of entering such relationships. For instance, the bulletin recommends that companies consider whether the service provider agreement is compatible with the company's strategic goals, whether the service provider's performance can be adequately monitored, whether the return on investment justifies contracting with outside parties, and alternatively whether the same functions could be performed in-house for less cost and risk. Looking to its own goals and weighing the benefits of third-party involvement under the OCC procedures, a company may decide that

it can efficiently forego third-party risks entirely.

The primary value of the supplemental examination procedures lies in the roadmap such procedures provide. First, the supplemental examination procedures enable a customer to determine the quantity of risk and the quality of risk (*i.e.*, low, moderate or high). In order to determine the quantity of risk, the customer would evaluate the full inventory of its third-party relationships, enabling the customer to identify concentrations of services among third parties, foreign-based relationships, subcontractor usage, third parties' ability to comply with legal expectations, and all intellectual property right transfers (among other issues).

Second, these procedures enable the evaluation of the quality of risks while also assessing whether customer risk management is strong, satisfactory, insufficient or weak. Engagement at the highest level of the organization, including the board of directors, is emphasized for adopting effective policies that are appropriate to the size, nature and scope of risk. These procedures also outline detailed guidance for planning when entering into a third-party service provider relationship, including detailed issues lists for the diligence, selection and contract negotiation phases as well as ongoing monitoring. Finally, the procedures include examination criteria for reviews to determine whether third-party relationships can be safely supervised (with board of director level involvement).

The New York DFS Cybersecurity Regulations

Effective as of March of 2017, the New York Department of Financial Services' (DFS) cybersecurity regulations apply to all entities licensed, required to be licensed, or subject to other registration requirements under New York banking, insurance or financial services laws. *See*, N.Y. Comp. Codes R. & Regs. tit. 23, §500. This legislation is broad in its application to entities spanning across multiple economic sectors. Given its broad applicability, unregulated companies may consider these rules in developing their own approach to managing risk inherent in the engagement of third-party service providers. Other states may adopt similar standards.

In addition to a number of other requirements, the New York rules require that a covered entity implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers. *See, Id.,* §500.11. The statute defines information systems broadly to mean "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems." *Id.,* §500.01(e). Under the rule, a third-party service provider is "an unaffiliated third-party company that provides services to the covered entity and maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the covered entity." *Id.,* §500.01(n). Nonpublic information is defined broadly under the rule to include both personally identifying information and nonpublic sensitive company information.

While the rule mandates the implementation of written policies and procedures, such policies and procedures must be based on a risk assessment of the covered entity. Additionally, the company must specifically address their efforts to identify and risk assess each third-party service provider. *See, Id.,* §500.11(a)(1). The company must establish and document the minimum cybersecurity practice requirements, which must be met by third-party service providers in order for such providers to qualify for consideration to do business with the covered entity. *See, Id.,* §500.11(a)(2). Moreover, the rules require the establishment of due diligence processes used to evaluate the adequacy of cybersecurity practices of such third-party service providers. Lastly, companies must engage in a periodic assessment of such providers based on the risk they present and the continued adequacy of their cybersecurity practices.

The rules also require that covered entities have relevant guidelines for due diligence to evaluate third-party cybersecurity practices and/or contractual protections that bind third parties. While engaging in due diligence or drafting contractual obligations, companies must consider the risk the third party presents to the company and obtain appropriate assurances, through due diligence and/or contractual controls, that the third party will protect the company's nonpublic information.

The guidelines must address the following four areas: 1) the third party's use of authentication, including multifactor authentication for access to internal networks from external networks; 2) encryption of nonpublic information, both at rest and in transit; 3) breach notification by the third party to the covered entity; and 4) representations and warranties regarding the third party's cybersecurity policies and procedures. The rules contain a limited exception for an agent, employee, representative or designee of a covered entity who is itself a covered entity. *See, Id.,* §500.11(c). In these cases, the third party need not develop its own third-party information security policy if the agent, employee, representative or designee follows the policy of the covered entity that is required to comply with the rules.

Key Components of a Third-Party Service Provider Risk Management Program

The FRB guidelines and DFS regulations provide separate helpful standards that companies should reference when creating their own third-party risk mitigation procedures. Likewise, the OCC supplemental procedures assist in

evaluating the "strategic risk" of third-party service provider relationships against the cost of in-house systems. Viewed together, these publications create a framework with several key requirements. Below are the key considerations that companies should examine and include when crafting their own third-party service provider risk management programs.

Analyze Internal Company Security and Disclosure Policies for Nonpublic Information

When performing due diligence on a third-party service provider, companies should scrutinize the effectiveness of the third party's security measures to protect against exposing nonpublic consumer information. Measuring the scope of system access, device access, security protocols, and the efficacy of the third party's security event plans, will allow companies to effectively evaluate and protect against their own exposure risks. Additionally, companies should turn to the OCC bulletin to help assess whether third-party relationships are worth the potential risk and cost.

Consult External Counsel for Compliance/Best Practices and Develop an Internal Cybersecurity Group

Companies should partner with external security legal experts while also developing their own internal security group to both insure compliance with applicable legal expectations and to protect sensitive information. Companies should consult external counsel, turning to the FRB and DFS cybersecurity requirements as instructional benchmarks for appropriate security measures.

Develop Articulated Standards for Third-Party Service Provider Risk Assessment

When performing due diligence on third-party service providers, companies should rely on consistent and defined criteria to determine the security risks. Companies can look to both the OCC issues lists and DFS for guidance, and should consider factors like encryption, staff training, contingency planning, access and authentication, and overall system security.

Contractually Require Third-Party Service Providers to Adhere to Information Security Terms

Third-party service providers with access to nonpublic consumer information should be contractually bound to abide by defined and enforceable security protocols (regardless of the service provider's internal policies) in order to guarantee information security and protect the company should provider policies shift. Companies should have a plan of action that prioritizes information security when entering into a third-party contract negotiation or renewal, and should seek cybersecurity addenda to their existing third-party contracts to ensure compliance with legal expectations.

Establish Mandatory Breach Notification and Event Response Plans

Third-party service provider contracts should require immediate company notification in the event of a third-party security breach. Additionally, both companies and providers should have response plans in the event of a breach that mitigates exposure and protects against losing consumer data. Failure to notify the company of a breach should be considered a material breach and should insulate the company from any further liability created by the third-party service provider.

Contractually Mandate Periodic Audits for Both Internal and Third-Party Cybersecurity Programs

Third-party contracts should include mandatory audits to ensure compliance with adequate security standards. Both the FRB and the DFS regulations require continuous third-party cybersecurity oversight, and even companies not bound by those standards should contract for periodic audits to ensure that nonpublic information is not exposed to undue risk. The OCC supplemental procedures may also be instructive in developing due diligence procedures.

Develop and Update System Monitoring Policies

Companies and third-party service providers should implement monitoring systems to detect breaches of their information, and should periodically test to ensure the systems' effectiveness. When necessary, policies and software should be updated and staff should be trained to securely use the updated systems.

Maintain a Company Record of Risk Assessment Protocols and Security Efforts

Companies should create detailed records of their risk assessments, security protocols, and other action taken to advance security of nonpublic consumer information to protect against information breach and to mitigate the company's potential legal exposure in the event of a breach.

Conclusion

Customers will need to develop risk mitigation strategies as they increase dependencies on third-party service providers. Organizations outside of the financial services industry can develop their risk management programs by looking to established financial services guidance for a viable framework and path forward in developing effective service provider diligence programs. The core components of this framework center on the organization's approach to pre-contract due diligence, effective contract negotiations, and strong ongoing risk oversight, all for purposes of limiting risk as much as reasonably possible. Customers that can effectively utilize these resources will be better able to manage their corporate fiduciary duties and protect valuable assets against harm.

—❖—