Reinhart

FDIC Audit Finds Banks Falling Short

Deficiencies persist in managing technology service providers

POSTED:
Feb 27, 2017

RELATED PRACTICES:
Banking and Finance
https://www.reinhartlaw.com/practices/banking-and-finance

RELATED PEOPLE:
John T. Reichert
https://www.reinhartlaw.com/people/john-reichert

On February 14, 2017, the Federal Deposit Insurance Corporations' ("FDIC") Office of Inspector General issued a 28-page report (the "Report")[1] summarizing its audit of "Technology Service Provider Contracts with FDIC-Supervised Institutions." The balance of this e-Alert summarizes the Report. The key take-away as we see it is that banks have not fully understood or implemented the myriad requirements for working with technology service providers ("TSPs"), and we expect the FDIC to respond to the audit by escalating its focus on TSPs in upcoming examinations.

Background

There is a daunting array of sources for regulatory "guidance" on the topic of managing TSPs, including Interagency Guidelines, Federal Financial Institutions Examination Council ("FFIEC") guidance, Financial Institution Letters ("FILs"), Regional Directors Memoranda, and Examination Documentation modules. The FDIC's audit focused on nine such resources.[2] The obligations of banks under this "guidance" can be summarized in three points:

1. Exercise appropriate due diligence in selecting service providers (risk assessment).
2. Contractually require TSPs to implement appropriate measures to meet the guidelines' objectives related to protecting against unauthorized access to or use of sensitive customer information.
3. Monitor contract compliance by the TSPs consistent with the institution's risk assessment including consistent review of service provider audits, test results summaries or other equivalent evaluations.

As banks work with TSPs, they need to consider how the TSP fits within and affects the bank's own Business Continuity Plan and Incident Response Program. As a refresher, the Business Continuity Plan is an enterprise-wide plan that establishes the basis "to recover and resume business processes when

operations have been disrupted unexpectedly." An Incident Response Program "specifies the actions to be taken when the [bank] suspects or detects that unauthorized individuals gained access to customer information systems, and includes providing appropriate reports to regulatory and law enforcement agencies."

Key Findings

While the 28-page Report was laden with findings and recommendations, we have highlighted 12 key findings below. In reading each, you can see how these lend themselves to enhanced scrutiny in an upcoming examination.

- Little "evidence, in the form of risk assessments or contract due diligence, that most of the FDIC-supervised FIs . . . fully considered and assessed the potential impact and risk that TSPs may have on the FI's ability to manage its own business continuity planning and incident response and reporting operations."
- Contracts "did not clearly address TSP responsibilities and lacked specific contract provisions to protect FI interests and preserve FI rights."
- ". . . almost half of the FIs lacked evidence that the FIs performed a comprehensive due diligence assessment prior or subsequent to the contract's ratification."
- 95% of the contracts reviewed "allowed service providers to subcontract assigned work." Of those, most "did not document subcontractor considerations" within the contract, risk assessment matrix or due diligence reviews.
- Identified 11 "Key Contract *Provisions*" that were frequently missing or deficient in contracts with TSPs.
- Identified 11 "Key Contract *Terms*." "Subjective terms such as potential breach, unauthorized access, containment, material impact, and timely notification may be subject to differing interpretations, and require further clarification within the contract."
- "Few contracts established or defined clear performance standards, and few of those established performance metrics and remedies for failures to meet such standards."
- "Few contracts established criteria to assess the nature and scope of potential

incidents; or to contain and control such incidents, which could preserve evidence."

- "Contracts typically did not provide remedies for the failure to meet incident response and reporting standards."
- "TSPs appear to have drafted most of the contracts . . .. Many of the contracts appeared to be based on standardized forms with generic FI customer descriptions, and high-level provisions that lacked specificity needed to protect the FI's information and resource needs." The Report concluded, "FIs may not be sufficiently engaged in writing and negotiating contracts to ensure their rights and TSP responsibilities are clearly defined. TSPs appear to be drafting the contracts and ensuring that their rights are protected more than the FIs."
- ". . . annual due diligence reviews and ongoing contract monitoring documentation appeared limited."
- "FIs may not have sufficient contracting and IT knowledge, expertise, or resources to gauge risks presented by TSPs; structure contracts to or otherwise address those risks; and oversee ongoing contracts. *Over-reliance on service providers coupled with a lack of appropriate contract management expertise weakens an FI's control environment* . . .." (Emphasis added).

Take-Away

The FDIC concurred with the Report's findings and proposed to take steps to work with banks to address the deficiencies by October 2018. As such, we believe banks have a window of opportunity to revisit their third-party risk procedures generally, but specifically the use of TSPs. As contracts mature or you evaluate and consider new engagements, consider having counsel involved to help address the contractual deficiencies cited in the Report.

For questions regarding this e-Alert, contact John Reichert at 414-298-8445 or jreichert@reinhartlaw.com.

---

[1] FDIC Office of Inspector General, Report No. EVAL-17-004.

[2] Appendix B to Part 364 - *Interagency Guidance Establishing Information Security Standards;* FFIEC IT Examination Handbook; FIL-19-2016 - *Technical Assistance Video on Outsourcing Technology Services;* FIL-55-2015 - *Cybersecurity Awareness*

Resources; FIL-28-2015 - *Cybersecurity Assessment Tool;* FIL-13-2014 - *Technology Outsourcing: Information Tools for Community Bankers Documents;* FIL-44-2008 - *Third-Party Risk Guidance for Managing Third-Party Risk;* June 2008 RD Memorandum titled, *Guidance for Managing Third-Party Risk; and* September 2014 Examination Documentation Module titled, *Third-Party Risk.*