April 5, 2019

Technology Service Provider Contracts with Banks

Attorneys
Mark V. Nuccio
Edward G. Black
Mike Tierney

Mindful of the growing reliance by financial institutions on technology service providers, the Federal Deposit Insurance Corporation (FDIC) issued a Financial Institution Letter this week identifying gaps, particularly involving business continuity and incident response risks, that some examiners had noted in their review of contracts between banks and technology services vendors. These gaps may require banks to take additional steps to mitigate the risks that arise from them. The FDIC took the opportunity to reiterate regulatory requirements for these contracts, noting that banks remain ultimately responsible when contracts do not adequately address certain risks. Cybersecurity threats remain at or near the top of risks of concern to federal banking regulators.

The FDIC letter is likely to cause banks and their technology service providers to sharpen their focus on contractual provisions, particularly those that address business continuity and incident response risks. Based on what examiners saw, the FDIC highlighted the possible need to add provisions requiring a particular vendor to establish a business continuity plan, establish recovery standards, and define remedies for failing to meet a recovery standard. Otherwise, the bank will have to implement other compensating controls to mitigate these risks, such as obtaining supplementary business continuity documentation from the service provider, outside the scope of the applicable contract, or modifying its existing business continuity plan to address contractual shortcomings.

The FDIC suggested that undefined and unclear contract terms in these areas contribute to uncertainty around bank rights and vendor responsibilities. Such uncertainty in the face of business disruptions or security incidents can impair bank operations and compromise customer information. The letter noted that long-term contracts and those that automatically renew "may be at higher risk" for coverage gaps, suggesting that good vendor relationships and the contracts' perennial nature may contribute to less frequent review.

The letter reminds banks about interagency guidelines setting information security standards, which were issued under the Gramm-Leach-Bliley Act and the notification requirements under Section 7 of the Bank Service Company Act.

The FDIC letter was issued more than two years after, and echoes risks identified in, the FDIC's Office of Inspector General (OIG) report evaluating Technology Service Provider (TSP) contracts with FDIC-supervised institutions (FI). The OIG report identified a number of potential risks that call into question the sufficiency of FI contracts with TSPs, as follows:

1. Despite regulatory guidance reiterating that the FI retains responsibility for activities performed through third-party relationships, a risk exists that an FI will transfer or delegate its risk management responsibilities to a service provider. Some FIs appear to have risk management procedures that they do not follow or fully implement.

2. 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, which may call into question business continuity and incident response planning efforts.

3. 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 better protected than FIs'. FIs and TSPs should anticipate these new points of emphasis and adjustments to the TSP contract strike zone in upcoming examinations and would be wise to prepare for them.

For further information about how the issues described in this Alert may impact your interests, please contact Mark Nuccio, Ed Black, or Mike Tierney, or your usual contact at Ropes & Gray LLP.