Published on *The National Law Review* https://natlawreview.com

FDIC Issues Guidance on Service Technology Service Provider Contracts

Article By:

Theodore R. Flo

Glen P. Trudel

On April 2, 2019, the FDIC issued Financial Institution Letter FIL-19-2019 (the "Letter") to remind financial institutions about certain contractual provisions and other requirements pertaining to technology service provider contracts. Apparently, during recent routine examinations, the FDIC found several technology service provider contracts that were inadequate under existing guidance. These contracts were missing or inadequately addressed key terms, such as:

1. Requiring the service provider to maintain a business continuity plan,

2. Establishing recovery standards,

3. Specifying the institution's remedies if the service provider misses a recovery standard,

4. Requiring the service provider to respond to security incidents by, among other things, notifying the institution, and

5. Defining key terms in the contracts relevant to business continuity and/or incident response. As noted in the Letter, the Interagency Guidelines Establishing Information Security Standards, which were promulgated pursuant to the Gramm-Leach-Bliley Act and incorporated into the FDIC's Rules and Regulations as Appendix B to Part 364, establish standards for safeguarding customer information. Such guidelines set the FDIC's expectations for managing technology service provider relationships through contractual terms and ongoing monitoring and financial institutions must account for these requirements in their contracts with technology service providers. For the reasons described above, the contracts that the FDIC saw during its examinations apparently failed to meet those expectations. Finally, the Letter highlights that depository institutions are obligated pursuant to Section 7 of the Bank Service Company Act (12 U.S.C. 1867) ("Act") to report to their respective federal bank regulatory agencies those contracts with technology service providers that provide certain types of services to the bank, as enumerated in Section 3 of the Act, and includes an FDIC-developed form as an unofficial aid in complying with that notification requirement.

The Letter serves as timely examination feedback and a good reminder to the industry that the FDIC believes that third-party providers of technology-related services can create special risks to depository institutions that need to be properly addressed in their service contracts with such entities, particularly in areas such as business continuity and incident response. The FDIC indicated that it plans to hold the board and senior management of financial institutions accountable for controlling those risks in accordance with the requirements of law and its existing regulatory guidance.

The Letter also reminds institutions that the FDIC's Guidance for Managing Third Party Risk, FIL-44-2008, discusses contract provisions that the FDIC believes should be addressed in technology service provider agreements (at a level of detail consistent with the scope and risks associated with the relationship), including those that were missing in the actual contracts the FDIC reviewed. The FDIC goes on to highlight other sources of guidance and resources available to assist bank personnel in understanding the requirements and regulatory expectations in this area.

The FDIC expects institutions to take steps to mitigate the risks posed by such gaps by getting new contract terms from vendors or modifying the institution's own business continuity program to account for the gaps.

National Law Review, Volume IX, Number 94