FDIC GUIDANCE – TECHNOLOGY SERVICE PROVIDER CONTRACTS

I. INTRODUCTION

The Federal Deposit Insurance Corporation (FDIC), has issued a Financial Institution Letter to remind its member banks with less than $1 billion in total assets to ensure that they account for risk posed by the use of technology service providers in the event of a cessation of operations or a data breach.

The Financial Institution Letter notes that examiners have cited in recent FDIC reports of examination that some financial institution contracts with technology service providers do not adequately define rights and responsibilities regarding business continuity and incident response or provide sufficient detail to allow financial institutions to manage those processes and risks. The FDIC cautions that such contracts should require the service provider to maintain a business continuity plan, establish recovery standards, and define contractual remedies if the service provider misses a recovery standard. Such agreements with fintech companies should also sufficiently detail the technology service provider's security incident responsibilities such as notifying the financial institution, regulators, or law enforcement.

II. BACKGROUND

Financial institutions often contract with technology service providers for services to the institution and its customers. Technology outsourcing relationships frequently integrate the systems and processes of the service provider and financial institution. This integration can impact how financial institutions manage their own processes such as business continuity and incident response.

When services are outsourced, a financial institution's board of directors and senior management are responsible for managing the risks posed by those services as if they were performed within the institution. Contracts are a critical tool for documenting agreement between financial institutions and their technology service providers on the levels of service required.

III. REQUIREMENTS

through contractual terms and ongoing monitoring. Financial institutions must account for these requirements in contracts with technology service providers.

A. Financial Institution Considerations

The FDIC encourages financial institutions, as part of their due diligence and ongoing monitoring, to ensure that business continuity and incident response risks are adequately addressed in service provider contracts. Long-term contracts and contracts that automatically renew may be at higher risk for coverage gaps.

When contracts leave gaps in business continuity and incident response, it is prudent for the financial institution to assess any resultant risks and implement compensating controls to mitigate them. For example, a financial institution may obtain supplementary business continuity documentation from the service provider, or modify the financial institution's own business continuity plan to address contractual uncertainties.

Institution management may refer to the FFIEC IT Examination Handbook, Business Continuity Booklet, or the FDIC’s Guidance for Managing Third-Party Risk for additional information. These materials describe practices that can be used to mitigate risk in third-party relationships.

The FFIEC IT Examination Handbook provides guidance for business continuity management, information and cyber security, and outsourcing technology services. The guidance addresses key financial institution risk management considerations such as the need for risk assessments, due diligence, strong contract provisions, and ongoing monitoring.

B. Bank Service Company Act Notification Requirements

Section 7 of the Bank Service Company Act (Act) (12 U.S.C. 1867) requires depository institutions to notify, in writing, their respective federal banking agency of contracts or relationships with technology service providers that provide certain services. Services covered by Section 3 of the Act include check and deposit sorting and posting, computation and posting of interest, preparation and mailing of checks or statements, and other clerical, bookkeeping, accounting, statistical, or similar functions such as data processing, Internet banking, or mobile banking services. The form is optional, and the information requested on this form may be submitted to the FDIC in any format. Notifications should be sent to the institution’s FDIC regional office. The FDIC has developed an optional form to allow its member banks to make this notification.


The foregoing Compliance Update is for informational purposes only and does not constitute legal advice. As a reminder, the NBA general counsel is the attorney for the Nebraska Bankers Association, not its member banks. The general counsel is available to assist members with finding resources to help answer their questions. However, for specific legal advice about specific situations, members must consult and retain their own attorney.