Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

July 26, 2018

Technology Service Providers for Banks

Recent surveys indicate that convenience is the primary reason why consumers select their preferred bank or credit union. Convenience in the form of mobile and online banking has become an important contributor to consumer satisfaction. As more banking transactions are delivered through digital channels, financial institutions that lack the in-house expertise are increasingly relying upon third-party vendors, specifically technology service providers (TSPs). TSPs develop the software and customer interfaces for customer account and payment services as well as maintain the digital technology.

In light of growing reliance on TSPs, regulators are scrutinizing how banks manage their *operational risks*, the risk of loss having to do with failed internal controls, people, and systems, or from external events (as defined by the Basel Committee of Bank Supervision). Rising operational risks, specifically in the form of cyber risks (e.g., data breaches, insufficient customer data backups, and operating system hijackings), have compelled regulators to scrutinize security programs aimed at mitigating operational risk. Cyber-related disruptions can potentially weaken public trust and confidence in the financial system, thus increasing the potential of a systemic risk panic (i.e., run on bank) event. Consequently, managing cyber-related risks (relative to other types of financial risks) and the associated costs have grown in importance.

Regulatory Background

Banking regulators have a broad set of authorities to supervise third-party servicers, such as TSPs, that have contractual relationships with banks. In addition, an institution's use of a TSP does not reduce the institution's responsibility to ensure that actions are performed in a safe and sound manner. Activities taken through a TSP must meet the same regulatory requirements as if they were performed by the supervised depository institution itself.

Two laws are of interest: the Bank Service Company Act (BSCA; P.L.87-856) and the Gramm-Leach-Bliley Act (GLBA; P.L. 106-102). The BSCA provided federal depository institution regulators with authority to examine and regulate TSPs that provide services to banks, including check and deposit sorting and posting, preparation of statements, notices, bookkeeping, and accounting. Section 501 of GLBA requires federal agencies to establish appropriate standards for financial institutions to ensure the security and confidentiality of customer information. In 2001, the prudential depository regulators issued interagency guidelines requiring banks to establish information security programs that, among other things, regularly assess the risks to consumer information (in paper, electronic, or other form) and implement appropriate policies, procedures, testing, and training to mitigate risks that could cause substantial harm and inconvenience to customers. The guidance requires banks to provide continuous oversight of third-party service providers to ensure that appropriate security measures are maintained.

The regulators periodically update guidance pertaining to third-party vendors. For example, the Federal Deposit Insurance Company (FDIC) emphasized in a 2008 Financial Institutions Letter (*Guidance for Managing Third-Party Risk*) that a financial institution's management is ultimately responsible for risks arising when activities are conducted through third-party relationships. In October 2012, the Federal Financial Institutions Council (FFIEC) issued a revised *Supervision of Technology Service Providers* booklet; the Federal Reserve System, the FDIC, and the Office of the Comptroller of the Currency concurrently issued new *Administrative Guidelines for the Implementation of the Interagency Program for the Supervision of Technology Service Providers*. In April 2014, the FDIC re-issued suggested guidelines for bank directors to consider when outsourcing essential banking functions to TSPs.

Concerns Related to TSP Relationships

The Office of Inspector General at the FDIC (OIG-FDIC) frequently audits the FDIC's oversight process for identifying and monitoring TSPs used by FDIC-supervised institutions and for prioritizing examination coverage. In the recent 2017 audit, the OIG-FDIC reviewed 48 contracts negotiated between TSPs and 19 banking firms and underscored the following concerns.

- Some contracts lacked provisions that would contractually require TSPs to implement appropriate measures to meet objectives stated in the Interagency Guidelines (e.g., protecting against unauthorized access to or use of sensitive nonpublic personal information).

- Some contracts lacked provisions that would establish business continuity plans, or provisions specifying how quickly operating systems would be restored after a cyber-related disruption. Some contracts had limited information and assurance that TSPs would have sufficient recovery capabilities if their systems were compromised.

- Some contracts lacked provisions that would require TSPs to provide incident response reports after an adverse incident. Banks should be notified when incidents, such as unauthorized access or misuse of customer information stored in a TSP's data system, occur; the actions taken; the response times; and controls taken to prevent further adverse incidents.

- The TSPs drafted most of the contracts reviewed by the OIG-FDIC. As a result, some contracts' terms may not

have been clearly defined or subjective, making it difficult to understand the rights and responsibilities of both parties. Although contracts negotiated between larger banks and TSPs typically contain more detailed provisions, the OIG-FDIC noted inconsistencies.

- The OIG-FDIC noted that 41 of the 48 contracts allowed TSPs to use subcontractors, further increasing the possibility of compliance, operational, and reputational risks. In June 2008, however, the FDIC stated that contracts should prohibit TSPs from subcontracting unless the same due diligence standards used to select the TSP are met by subcontractors. The OIG-FDIC did not find sufficient evidence that comprehensive due diligence was performed by some banking firms.

Coordination Among Regulators

Collaboration among financial regulators arguably facilitates detection of potential financial risks. Federal, state, and self-regulatory organizations have entered into information-sharing agreements to facilitate oversight responsibilities and coordinate compliance challenges. U.S. federal financial regulators on the Financial Stability Oversight Council share information to detect systemic risks to the U.S. financial system. H.R. 3626, the Bank Service Company Examination Coordination Act, would clarify the authority of state regulators to examine certain TSPs in coordination with federal regulators. The bill also provides for information sharing between state and federal regulators with respect to TSPs, thus facilitating the detection of operational risks related to cyber disruptions.

Challenges for Financial Institutions

Despite concerns pertaining to an operational risk event, enhanced compliance standards may still pose challenges particularly for community banks and small credit unions.

- Greater due diligence in selecting TSPs and improved contract structuring may still be costly for institutions lacking sufficient contracting and IT knowledge expertise to gauge potential TSP risks. Some banks may also lack the resources to monitor contract compliance to insure that the TSPs are adhering to GLBA and other regulatory requirements.

- Although the industry consists of many TSPs, only a few large TSPs currently provide the majority of digital products to the financial industry. Some bankers suspect that the large TSPs may practice oligopolistic pricing. Banks' vendor choices may be limited, however, to the extent operational risks may be greater with some smaller and perhaps less experienced TSPs.

- Given lower transaction volumes and costly digital services, some industry observers report that community banks have adopted digital processing technology at slower rates relative to larger banking and fintech firms, possibly inhibiting the ability to compete in various niche product markets. Additional requirements placed on TSP contracts will likely increase the costs and, therefore, the difficulty for some of the small depository institutions to close existing technology gaps.

Additional Resources

Michael B. Benardo, Kathryn M. Weatherby, and Robert J. Wirtz, "Managing Risks in Third-Party Payment Processor Relationships," *Supervisory Insights*, Summer 2011.

Office of Inspector General—Federal Deposit Insurance Corporation, *Technology Service Provider Contracts with FDIC-Supervised Institutions*, Office of Audits and Evaluations, Report No. EVAL-17-004, February 2017.

Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 C.F.R. Part 364, February 2001, at https://ithandbook.ffiec.gov/media/resources/3530/occ-12cfr30_ap_b_inter_guid_estab_stand_safe_info.pdf.

Interagency Guidelines Establishing Standards for Safeguarding Customer Information, Federal Reserve System Examiner Guidance, at https://www.federalreserve.gov/boarddocs/srletters/2001/sr0115a1.pdf.

International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version, Basel Committee on Banking Supervision, June 2006, at https://www.bis.org/publ/bcbs128.pdf.

Federal Deposit Insurance Corporation, *Guidance for Managing Third-Party Risk*, FIL-44-2008, June 6, 2008.

Federal Deposit Insurance Corporation, *Technology Outsourcing: Informational Tools for Community Bankers*, FIL-13-2014, April 7, 2014.

Government Accountability Office, *Better Information Sharing Among Financial Services Regulators Could Improve Protections for Consumers*," GAO-04-882R, June 29, 2004, at https://www.gao.gov/products/GAO-04-882R.

Government Accountability Office, *Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight*," GAO-18-254, March 2018, at https://www.gao.gov/assets/700/691290.pdf.

Penny Crosman, "*Can Big Four Core Banking Vendors Oligopoly Be Broken?*" American Banker, October 7, 2013.

Bryan Yurcan, "*Automation is Leveling the Commercial Lending Playing Field*," American Banker, October 19, 2017.

CRS InFocus CRS In Focus IF10163, *Cybersecurity and Information Sharing*, by N. Eric Weiss.

CRS Report R44429, *Financial Services and Cybersecurity: The Federal Role*, by N. Eric Weiss and M. Maureen Murphy.

Darryl E. Getter, dgetter@crs.loc.gov, 7-2834

IF10935