Copyright ©2024 LexisNexis and/or its Licensors.
This branded reprint, or any of the content within the branded reprint, may not be posted online, including on social media, without express written permission from LexisNexis.

The Bank Service Company Act: The Curious Late Life of an Old Law

A Practical Guidance® Practice Note by James P. Bergin and Paul Lim, Arnold & Porter

James P. Bergin
Arnold & Porter

Paul Lim
Arnold & Porter

This practice note discusses in detail the Bank Service Company Act, including its legislative history, how it has been used by federal banking regulators over time, and recent developments. In addition, this practice note provides practical considerations for financial institutions and service providers.

For more information, see Financial Services Regulations Fundamentals Resource Kit. For guidance on managing third-party technology outsourced relationships, refer to Regulation and Examination of Bank Service Companies, 12 U.S.C. § 1867 Federal Deposit Insurance Corporation (FDIC) Releases Guidance on Technology Service Provider Contracts: Client Alert Digest. For further information on evaluating and managing risks related to third-party relationships, refer to Third-Party Service Provider Risk Management Oversight: Presentation, Third-Party Vendor Management Checklist, Responding to a Data Breach Checklist (Financial Institutions) and Interagency Guidance on Third-Party Relationships: Risk Management.

Introduction

It was a time of rapid technological innovation. New technology was leading to changes in consumer preferences and, particularly, changes in the nature and scale of payments. Banks were finding that they did not have the capacity to keep up, within their own four walls. They needed to go outside to find the technological talent, the capacity, and the expertise they had to have in order to adjust to a rapidly changing environment. They ran into regulatory constraints. The traditional American boundary between banking and commerce was tested. They appealed to Congress for help.

It was 1962. The innovation was the computer, and the change in consumer preference was an exploding demand for checks. Small- and medium-sized banks found they needed computers to help them adapt to the exponential increase in data processing demanded by the post-war economy. They did not have the technological knowledge to build these machines themselves, of course, and they were finding, too, that they could not afford them. They wanted to pool together to buy computers to run their banking businesses. Regulators were okay with that idea, but they wanted to make sure that they could maintain the strict oversight of bank activities they were used to as, increasingly, nonbank third-party providers began providing these important bank services. And so, the Bank Service Company Act (BSCA)—originally the "Bank Service Corporation Act"—was born.

This practice note will look at the curious late life of this obscure law. While not the most well-known of all banking laws, the BSCA has become an important part of the bank regulatory toolkit through its 60 years of existence. It serves, among other roles, as the statutory basis of banking

agencies' examination programs for those firms that provide technological services to banking organizations. And, now in its dotage, it is proving more vital than ever. Just two years ago, it saw its first rulemaking, as the banking agencies used it to apply new, direct cyber-notification requirements on third-party service providers to banks. It is being mentioned as an important financial stability tool in Financial Stability Oversight Council (FSOC) reports. International standard-setters are eyeing it enviously, as a model to be copied by other countries as they, too, grapple with the same problem that confronted U.S. policy-makers back in 1962—how to navigate rapid technological change and consumer preferences across the timeworn banking-commerce divide.

We will first take a brief look at what led to the BSCA. Then, we will review the law itself, with an eye on what limits may lie within its short text. Next, we will examine how the statute has been used by the banking agencies over time, including the longstanding technology service provider program of the Federal Financial Institutions Examination Council (FFIEC) and the recent cyber-notification rule as highlights. After that, we will look at potentially evolving applications of the statute, as policy-makers mention it more frequently as a potential solution to knotty problems, and congressional policy-makers debate new legislation that would expand its perimeter to sharing with states. Finally, we end by offering practical guidance for both banks and service providers relating to this old but still vigorous law.

The Rationale for the Law, and Its Amendment over Time

Not unlike many other banking laws, but to a more extreme degree, the part of the text of the BSCA that is of the most current interest sits within a bed of statutory language that, while not vestigial, is mostly interesting for its evocation of a regulatory past.

The BSCA was enacted in 1962 against the backdrop of a tremendous increase in the volume of checks in circulation and other demand for bank services, 87 Pub. L. No. 856; 76 Stat. 1132 (October 23, 1962). According to a contemporaneous congressional report, it was expected that the estimated volume of checks would reach 22 billion by 1970 from only 3.5 billion checks in 1939, increasing at the rate of about one-half billion checks per year, see H.R. Rep. No. 87-2062, at 2 (1962). The report also noted that many banks found it difficult to acquire adequate personnel to handle the rapidly increasing demand.

According to the congressional debates at the time of its passage, banks felt a need for computers to handle data processing, but not all were able to afford them. Congressional debates took notice of the increasing insufficiency of manual processes and the fact that banks needed automation for check-handling and other bank services such as processing savings accounts, computing payrolls, and calculating other credits and charges, see H.R. Rep. No. 87-2062, at 5 (1962). This appears to have led to advocacy from small- and medium-sized banks for an expansion in their authority and, particularly, the ability for them to pool their investments with other smaller banks in new bank service corporations. When the bill was introduced, it was reported that big commercial banks had already purchased data-processing equipment or data-processing services from existing, private data-processing firms. The problem was that smaller banks could not afford to make similar investments, making it more difficult to compete in offering efficient banking services to their customers. The BSCA was the solution.

Some legislators expressed concerns. Some were worried about the erosion of safety and soundness that could ensue if supervised banks outsourced traditional banking activities to bank service corporations and nonbanks. This worry led to the aspects of the BSCA that carry the most current import, the authority for the banking agencies to examine the activities of nonbanks. These provisions appear to have been uncontroversial. See H.R. Rep. No. 87-2105, at 3(1962).

Other legislators were concerned about the separation of banking and commerce and the possibility that banking organizations would go into the technology business as a way to boost their profits. The proposed bill provided that a bank service corporation may perform up to one-half of its services for persons other than banks, 108 Cong. Rec. 16498 (1962). Some legislators objected to this provision because it would enable banks to engage in nonbanking activities. The bill was amended to address this concern by explicitly providing that bank service corporations may not engage in any activity other than the performance of bank services for banks, Pub. L. No. 87-856.

Some legislators, citing the attorney general, expressed concerns that the bill might lead to abuse by competing banks that invest in or utilize the services of a bank service corporation, by enabling them through the mechanism of these joint ventures to exchange confidential information for anticompetitive purposes, 108 Cong. Rec. 16502 (1962). The bank regulators promised to surveil for such abuse, 108 Cong. Rec. 20147 (1962). A compromise was thus forged, and the BSCA became law. See, e.g., H.R. Rep. No. 87-2105, at 2 (1962); 108 Cong. Rec. 20862 (1962).

Twenty years later, the BSCA was amended by the Garn-St. Germain Depository Institutions Act of 1982 (Garn-St.

Germain), Pub. L. No. 97-320, which expanded the authorized powers of bank service companies. Garn-St. Germain aimed to ease pressures on depository institutions as the Federal Reserve raised interest rates to curb the high inflation of the 1970s, Garn-St Germain Depository Institutions Act of 1982, Federal Reserve History (Nov. 22, 2013). The BSCA's restrictions on bank service companies were eased in several respects. First, any one bank could now set up a bank service company subsidiary. Second, it allowed bank service companies to offer services to the general public, as well as other types of financial institutions. Third, in what would later turn out to be the most consequential amendment, there was an expansion in the types of activities in which a bank service company may engage to include all those activities and services that can be performed by a state-chartered bank under state law, as well as the activities and services that can be engaged in by a bank holding company subsidiary as incidental to banking, as authorized under the Federal Reserve's Regulation Y. These amendments would have the collateral effect of expanding the bank regulators' examination authorities over third parties.

In addition to the Garn-St Germain Depository Institutions Act of 1982, four additional amendments were made to the BSCA, notably:

- Pub. L. No. 104-208 in 1997 renamed the Bank Service Corporation Act as the Bank Service Company Act and replaced the term "corporation" with "company" throughout the Act
- In addition, Pub. L. No. 104-208 authorized bank service companies to organize as limited liability companies
- The Financial Services Regulatory Relief Act of 2006, Pub. L. No. 109-351, amended the BSCA to allow savings associations to invest in bank service companies
- The Dodd-Frank Act, Pub. L. No. 111-203, replaced the Office of Thrift Supervision with appropriate federal banking agencies to reflect the abolishment of the Office of Thrift Supervision

An Examination of the BSCA

The most important current application of the BSCA is that it authorizes U.S. banking regulators to examine the activities of entities that provide services to banks. See Third-Party Relationships: Interagency Guidance on Risk Management, OCC Bulletin 2023-17 (June 6, 2023).

In these and prior versions of the principles, the banking regulators may evaluate third-party servicers' safety and soundness risks, the financial and operational viability of the third-party servicer to fulfill its contractual obligations, compliance with applicable consumer protection, fair lending, and anti-money-laundering laws, and whether the third-party servicer engages in unfair or deceptive acts or practices in violation of federal or applicable state law. This is striking if for no other reason that private sector entities often go to great lengths to decide whether they wish to sit within or without the banking perimeter, with all the careful oversight—and sometimes privileges—that status can entail. See 12 C.F.R. pt. 225; Ravi R. Desai, Private Equity Investment in Financial Institutions and How to Avoid Becoming a Bank Holding Company, 13 N.C. Banking Inst. 385 (2009); Chip MacDonald, "Private Equity Investments in Financial Services Firms: Threading the Regulatory Needle" (2011). The BSCA creates a means for bank regulators to reach outside of that perimeter.

The law also, as the name portends, creates a licensing, and permitted activities regime for so-called "bank service companies," entities that are established by one or more insured banks to provide certain services to banks. This type of entity may be less popular these days, after changes in law and business reality.

Examination Authority for Service Providers

Section 7 of the BSCA, 12 U.S.C. § 1867(c) and (d), contain the authority for examination of nonbank service providers. Section 7(c) states, in relevant part:

> . . . whenever a depository institution that is regularly examined by an appropriate federal banking agency, or any subsidiary or affiliate of such a depository institution that is subject to examination by that agency, causes to be performed for itself, by contract or otherwise, any services authorized under this Act, whether on or off its premises —
>
> (1) Such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the depository institution itself on its own premises, and
>
> (2) The depository institution shall notify each such agency of the existence of the service relationship within thirty days after the making of such service contract or the performance of the service, whichever occurs first.

This authorization appears to sweep broadly, both in terms of the types of bank entities and agreements that trigger the requirements thereunder. But that may be moderated, in some respect, by the limitation of the examination to the "performance" of the services rather than the entity itself.

Types of Banking Entities That Trigger the Law

The language has, as its starting point for application, a "depository institution that is regularly examined by an appropriate Federal banking agency."The term "depository

institution" is defined as an insured bank, a savings association, a financial institution subject to examination by the appropriate Federal banking agency or the National Credit Union Administration ("NCUA"), or a financial institution the accounts or deposits of which are insured or guaranteed under State law and are eligible to be insured by the FDIC or the NCUA. 12 U.S.C. § 1861(b)(4). "Appropriate Federal banking agency" includes the OCC, the FDIC, and the Board of Governors of the Federal Reserve System. 12 U.S.C. § 1813(q). By following the definitions through the BSCA and the Federal Deposit Insurance Act (FDI Act), this definition appears to capture most types of banking entities that are supervised in some way by a federal banking agency or the National Credit Union Administration Board, including federal and state-chartered depository institutions, savings associations, and probably insured and uninsured branches of foreign banks.

The definition then goes on to include services provided to "any subsidiary or affiliate of such a depository institution that is subject to examination by that agency." The term "subsidiary" means any company which is owned or controlled directly or indirectly by another company and includes any service corporation owned in whole or in part by an insured depository institution or any subsidiary of such a service corporation. 12 U.S.C. § 1813(w)(4). "Affiliate" means any company that controls, is controlled by, or is under common control with another company. 12 U.S.C. § 1841(k). This addition makes the BSCA expansive indeed—services not just to the banking entities themselves, but also one of the many subsidiaries or affiliates of such an entity are covered.

Types of Service Contracts That Trigger the Law

Section 7(c) of the BSCA applies when one of these covered banking entities "causes to be performed for itself, by contract or otherwise, any services authorized under this Act, whether on or off premises." The services need not be provided under an actual contract, so long as the entity has "cause[d them] to be performed for itself." The services can be furnished on- or off-bank premises. And, notably, there is no materiality qualifier: it applies to "any" services authorized under the BSCA. Since it is hard to get broader than "any," the language providing that the services must be "authorized" under the BSCA bears some scrutiny.

Is there some meaningful limitation there? The language refers to the authorized activities under the BSCA for the institutions that were the original reason for the statute: the bank-owned "bank service companies" 12 U.S.C. § 1863. Section 3 of the BSCA describes such activities as check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution. Insured depository institutions may invest in bank service companies that perform these functions only for depository institutions without prior regulatory permission. These words all carry a whiff resonant of a 1960s-era paper bank statement, printed on green-striped paper stuffed inside an envelope with heavy yellow glue. Since the enactment of the BSCA, the federal banking agencies have expanded the BSCA and approved banks to invest in bank service companies that provide various types of activities including, among other things, data-processing services, electronic funds switching and processing, real estate investment advisory activities, insurance underwriting, and mortgage banking activities. *See, e.g.*, FDIC, Technology Service Provider Contracts, FIL-19-2019 (April 2, 2019); Board, *Orders Issued Under Section 5 of Bank Service Corporation Act the Indiana National Bank, American Fletcher National Bank and Trust Company, and Merchants National Bank and Trust Company* (March 1984).

Section 4 of the BSCA expands the limits of what "bank service companies" are authorized to do for other persons, by reference to relevant laws for state banks and savings associations, on the one hand, and national banks and savings associations, on the other—essentially making their powers almost equivalent to those wielded by their potential bank investors if they receive prior approval from the federal banking agencies, 12 U.S.C. § 1864(b) through (d). Section 4(f), as added by Garn-St. German, takes this to the furthest logical extension, by stating that bank service companies may "perform . . . any service, other than deposit-taking, that the Board has determined, by regulation, to be permissible for a bank holding company under Section 4(c)(8) of the Bank Holding Company Act as of the day before the enactment of the Gramm-Leach-Bliley Act." This brings in the list of activities that have been determined to be closely related to banking—a fairly expansive list—as services that are covered by the BSCA.

The federal banking agencies noted the fairly broad sweep of Section 4(f) in the adopting release for the recent cyber-notification rule, for purposes of determining covered services under the BSCA, see 86 Fed. Reg. 2299 (Jan. 12, 2021). Under the BSCA, such services must be permissible for bank holding companies under Section 4(c)(8) of the Bank Holding Company Act of 1956, as amended, and Section 225.28 of the Board's Regulation Y. 12 U.S.C. § 1841 et seq.; 12 C.F.R. § 225.28. Rather than responding to comments that they should articulate the services covered by the rule, so as to put service providers clearly on notice that they would be subject to the notification requirement, they simply defined covered services as services under the BSCA, without restating what those were and were not. A number of comments urged the Agencies to limit the scope of covered services and service providers beyond the outer limits of

what the BSCA covers, but the Federal banking agencies declined this invitation. *See e.g.*, ABA, BPI, IIB, SIFMA, OCC-2020-0038-0024 (April 12, 2012).

When the federal banking agencies were actively reviewing applications by bank service companies to engage in certain activities, there was sometimes a discerning eye cast on what was and was not an activity authorized by the BSCA. *See, e.g.*, Board, *Orders Issued Under Section 5 of Bank Service Corporation Act Louisiana National Bank* (December 1983). Now, with the possibility that there is less focus on the BSCA as a means of finding permissibility for bank subsidiary activities, the regulatory incentives may work the other way, toward reading such services more expansively.

At the same time, the congressional history of the BSCA indicates that not all services rendered to banks were originally meant to be covered, suggesting that covered services should be limited to the outsourcing of core banking functions. Note this extract from the 1962 Senate report, which seems to carve out, among others, lawyers, accountants, and armored cars:

> Banks have always employed others to do many things for them, and they will have to continue to do so, and the bill is not intended to prevent this or to make it more difficult. For example, banks have employed lawyers to prepare trust and estate accounts and to prosecute judicial proceedings for the settlement of such accounts. Banks have employed accountants to prepare earnings statements and balance sheets. Banks have employed public relations and advertising firms. And banks have employed individuals or firms to perform all kinds of administrative activities, including armored car and other transportation services, guard services and, in many cases, other mechanical services needed to run the banks' buildings. It is not expected that the bank supervisory agencies would find it necessary to examine or regulate any of these agents or representatives of a bank, except under the most unusual circumstances.

It is not clear whether the federal banking agencies would view the BSCA as so limited now, but it is noteworthy, nonetheless, S. Rep. No. 2105, 87th Cong. 3 (1962).

Such Performance

There lurks another limiting factor contained in the statute's limitation of examination and regulation authority to "such performance" of services to banking organizations. The banking regulators' statutory authorities for oversight of other subject entities generally allow them to go wherever they want, whenever they want, to look at whatever they want, to assure themselves of the overall safety and soundness and compliance with law of the entity that they are examining. It has to be assumed that the regulation and examination of "performance" will be narrower, but how much narrower has yet to be tested. A 1989 interpretive letter from the Office of the Comptroller of the Currency (OCC) suggested that the "performance" qualifier meant that their authority over service providers was "probably narrower" than its general authority over banks. OCC, Interpretive Letter (July 26, 1989) (unpublished), available in LEXIS, Bankng Library, ALLOCC File. It is informative to consider how the FFIEC has implemented its program for the oversight of technology service providers, to understand the line between performance and entity regulation. We will study this in further depth below.

Regulation and Examination

In any case, the performance of the activities will be subject to "regulation and examination," according to Section 7(c), "as if such services were being performed by the depository institution itself." For service providers that are not familiar with the intrusive nature of bank supervision, this may bring the biggest surprise, as the word "examination" implies that bank regulators may do what they ordinarily do with bank entities—visit, ask questions, and possibly criticize. The courts, in the limited case law of the BSCA—none of which involves third parties protesting the jurisdiction of the federal banking agencies—have affirmed that it provides for oversight. See Reyn's Pasta Bella, LLC v. Visa U.S.A., 259 F. Supp. 2d 992, 1003 (N.D. Cal. 2003), holding that the BSCA "provides an enforcement mechanism by explicitly subjecting each bank service company to regulation by the Board of Governors of the Federal Reserve System and the appropriate federal banking agency of its principal investor"; Sawyer v. Bill Me Later, Inc., 23 F. Supp. 3d 1359 (D. Utah 2014), holding that loans serviced through contracts with third parties are expressly subject to federal regulation and oversight.

The intent of the language, as described above, is to make sure that the outsourcing of banking functions does not lead to any diminution in their safety and soundness, and the supervisors' authority over same.

The bank regulators may also engage in regulation of such activities, according to both 12 U.S.C. § 1867(c) and (d), which allow them to issue "such regulations . . . as necessary." It is not clear how far this reaches. One form of regulation, as suggested by the structure of the statute, could be the application of regulations that would otherwise be applicable to bank activities that have been outsourced. Another form could be devising new regulatory requirements for the

services provided, specifically designed for service providers. As discussed further below, this is what the Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers represents. A final form might be to try to go one step further and aim safety and soundness regulations at certain service providers, on the basis that bank regulators have an interest in knowing whether a service provider has the financial or operational wherewithal to weather negative events and keep providing essential services. Some of the recent federal financial agency reports expressing serious concerns about the role of cloud service providers in modern banking operations might make you wonder if this type of regulation could be in consideration at some point. This form may not be consistent with the statutory language—that is, the "performance of such activities" and the regulatory construction of the agencies over time. Courts have found that the regulation of the federal banking agencies is, moreover, not meant to be exclusive, D.C. v. Elevate Credit, Inc., 554 F. Supp. 3d 125 (D.D.C. 2021); FTC v. CompuCredit No. 1:08-cv-1976-BBM-RGV, 2008 U.S. Dist. LEXIS 123512 (N.D. Ga. Oct. 8, 2008).

Enforcement

The statute implies that the federal banking agencies have enforcement authority under the BSCA. A "regulation" is, by its nature, binding on those who are regulated, but how it will be made binding is a bit of a question. See, e.g., Atkins v. Rivera, 477 U.S. 154 (1986). Section 7(d) states that "the Board and the appropriate Federal banking agencies are authorized to issue such . . . *orders* as may be necessary to enable them to administer and carry out the purposes of this chapter and to prevent evasions thereof." 12 U.S.C. § 1867(d). The federal banking agencies have entered into a number of consent orders with third-party service companies over time. *See* Lender Processing Services, Inc., DOCX, LLC, LPS Default Solutions, Inc., OCC No. 2011-053 (April 13, 2011); Fundtech Corporation, BServ, Inc., FDIC No. 2013-193 (December 5, 2013); Higher One, FRB No. 15-026-E-I, 15-026-CMP-I (December 23, 2015).

At the same time, it is at least curious that Section 7(b) of the BSCA explicitly states that "bank service companies" (again, the bank-owned service companies, not the third-party service companies that are covered under the BSCA) are subject to the provisions of Section 1818 of the FDI Act—from where the bank regulators' formal enforcement powers derive—while not mentioning the nonbank service providers that are discussed in the following paragraph. 12 U.S.C. § 1867(b). Whether the ellipsis is meaningful is ambiguous. The consent orders that the federal banking agencies have entered into with third parties are usually careful to delineate that the third-party service providers are "institution-affiliated parties" (IAPs) as well as service providers under the BSCA, and thus subject to the FDI Act's enforcement provisions. See, e.g., Fundtech Corporation, BServ, Inc., FDIC No. 2013-193 (December 5, 2013).

Notification Requirement

Under Section 7(c) of the BSCA, a depository institution that is regularly examined by an appropriate federal banking agency, or any subsidiary or affiliate of such a depository institution that is subject to examination by that agency, must notify the agency of the existence of the service relationship within 30 days after the making of such a service contract or the performance of the service, whichever occurs first. From a bank regulatory perspective, this notice is important because it allows the banking agencies to understand how to examine the banking entity's third-party risk management and whether to undertake the supervision of the third party itself under the BSCA. The Federal Deposit Insurance Corporation (FDIC) has remonstrated the industry for not filing such notices in at least one instance. See FDIC, Required Notification for Compliance with the Bank Service Company Act, FIL-49-99 (June 3, 1999).

Bank-Owned Bank Service Companies

The BSCA creates an authorization regime for the establishment of "bank service companies." A "bank service company" is a corporation or a limited liability company "organized to perform services authorized by this chapter" by "1 or more" insured depository institutions. We have examined the services authorized by the BSCA already. Bank service companies may not take deposits. 12 U.S.C. § 1864(a). "1 or more" comes from the circumstances that led to the BSCA's creation, as amended by Garn-St. Germain. In the 1960s, computers were beyond the budget of small- to medium-sized banking institutions, which led to a desire to team up with other institutions to make the investment. See, e.g., H.R. Rep. No. 87-2062, at 8 (1962). The investment that banks are allowed to make in "bank service companies" is limited to (1) not more than 10% of their paid-in and unimpaired capital and unimpaired surplus in a single bank service company and (2) not more than 5% of their total assets in bank service companies in general. 12 U.S.C. § 1862.

Banks need prior approval from their appropriate federal banking regulator to make investments in bank service companies that engage in activities other than those authorized by Section 3, or the Board of Governors of the Federal Reserve System (Board), in the case of investments authorized only as activities closely related to banking, although all such applications will be deemed approved after 90 days. 12 U.S.C. § 1865(a), (b), and (d). Similar to other

statutes governing the expansion of banking organizations, the agencies are authorized to consider the effects on the "financial and managerial resources and future prospects" of the investing bank and the bank service company itself. In addition, consistent with the debates in Congress at the time of its passage, the agencies may also consider "possible adverse effects such as undue concentration of resources, unfair or decreased competition, conflicts of interest, or unsafe or unsound banking practices." 12 U.S.C. § 1865(c).

Bank service companies are not allowed to "unreasonably discriminate in the provision of any services authorized under this chapter" against competitors. It will not be considered "unreasonable discrimination" to provide services only at a price that fully reflects all the costs, including the cost of capital and a reasonable rate of return. 12 U.S.C. § 1866. Bank service companies may refuse to provide services to a non-stockholding or nonmember institution if comparable services are available from another source at competitive overall costs, or if the providing of services would be beyond the practical capacity of the service company. 12 U.S.C. § 1867(b).

Bank service companies are fully subject to the regulation, examination, and enforcement powers of the banking agencies, without any of the limitations or ambiguities discussed above in the context of nonbank service providers. A bank service company is subject to "regulation and examination" of the appropriate federal banking agency of its principal investor to the same extent as its principal investor; there is no limitation to performance, rather than entity, regulation, whatever that means, as there is for nonbank service providers. 12 U.S.C. § 1867(a). A bank service company is "subject to the provisions of section 1818" of the FDI Act, including the customary bank enforcement authorities, "as if the bank service company were an insured depository institution."

It is hard to be sure from the regulatory record, but the popularity of the "bank service company" as a corporate form may have waned over time. There was a profusion of orders allowing the formation of bank service corporations in the wake of Garn-St. Germain, but the regulatory record of new approvals tails off by the late 1980s. A search conducted on Lexis-Nexis for "Bank Service Corporation" orders in the Federal Reserve Regulatory Service reveals 503 orders between 1984 and 1989, ending in April 1989.

Uses of the BSCA over Time

The federal bank regulators' most prominent use of the authority granted by the BSCA over service providers has been through their program for the supervision of technology service providers (TSPs) to banks. This supervision has, in a handful of cases, led to consent agreements with supervised entities. While harder to observe from the outside, the federal bank regulators have indicated that they will sometimes invoke the BSCA for other purposes as well, such as exerting power with respect to entities engaged in the infrastructure for payments. More recently, the cyber-notification rule applied an affirmative notification requirement to service providers.

Supervision of Technology Service Providers

The federal banking agencies have had a joint program for the TSPs for banking institutions since at least 1978. After a number of iterations, the FFIEC has been in charge of overseeing this program since 2012. The FFIEC is a formal interagency body empowered to examine significant service providers to financial institutions. The member agencies of the FFIEC include the Board, FDIC, OCC, NCUA, and CFPB.

Current Supervisory Programs for TSPs

The FFIEC maintains certain uniform standards and report forms for the federal examination of financial institutions, including the Information Technology Examination Handbook (IT Handbook), which covers a variety of technology and technology-related risk management guidance for financial institutions and examiners. In October 2012, the FFIEC published the supervision of technology service providers booklet (TSP Booklet) as part of the IT Handbook. Concurrently, the federal banking agencies issued administrative guidance (supervisory guidance) to implement interagency programs for the supervision of TSPs. The TSP Booklet was created under the agencies' statutory authority under the BSCA to supervise third-party service providers that enter into contractual arrangements with regulated financial institutions. FFIEC, *Supervision of Technology Service Providers*, 1 (October 2012).

The agencies conduct IT-related examinations of financial institutions and their TSPs based on the guidelines contained in the IT Handbook, including the TSP Booklet. Examination responsibility for a given TSP is determined based on the class and type of servicer as well as the class and type of insured financial institutions being serviced (e.g., the OCC examines TSPs of national banks and the Federal Reserve examines the TSPs of state member banks). If more than one class of insured institutions is serviced, the examination is conducted jointly and on a rotated basis, as agreed to among the responsible federal financial institution regulators.

The TSP Booklet describes four current supervisory programs: (1) Multi-Regional Data-Processing Services (MDPS) Program, (2) Regional TSP Program, (3) Foreign-Based TSP Program, and (4) Shared Application Software Review (SASR) Program.

The MDPS Program covers the largest, systemically important TSPs. A TSP is considered for examination under the MDPS Program when the TSP processes mission-critical applications for a large number of financial institutions that are regulated by more than one agency, or when the TSP provides services through a number of technology service centers located in diverse geographic regions. See, FFIEC, *Supervision of Technology Service Providers*, fn. 9 (October 2012). TSPs subject to the MDPS Program are subject to special monitoring and collaborative interagency supervision at the national level based on the agencies' recognition that the companies in the MDPS Program may pose a significant risk to the banking system. For example, major cloud service companies that provide cloud services to financial institutions through data centers in multiple geographic regions would be subject to the MDPS Program. Indeed, the Federal Reserve Bank of Richmond conducted a formal examination of Amazon facility in Virginia. *See* Liz Hoffman, Dana Mattioli, Ryan Tracy, Banks' Cloud Practices Face Fed's Scrutiny, WALL ST. J. (August 2, 2019).

The Regional TSP Program is applicable to TSPs that are local and smaller in size or complexity. The agencies' district or regional offices are responsible for the administration, coordination, oversight, and implementation of the supervision of TSPs that are subject to the Regional TSP Program. Although these TSPs are not subject to the MDPS Program, they are supervised in a similar manner and under the guidelines of the TSP Booklet and the supervisory guidance. The Foreign-Based TSP Program applies to foreign-based TSPs and domestic TSPs that outsource to or subcontract foreign-based TSPs. If circumstances warrant, the agencies may obtain information related to the services provided to U.S.-regulated financial institutions or conduct on-site supervision of foreign-based TSPs through the appropriate foreign regulatory agencies.

Finally, the SASR Program involves reviews of software programs or systems in use at financial institutions, including specialty software products, such as those used for asset management, BSA/AML, consumer compliance, and retail credit. The SASR Program is designed to identify potential systemic risks and reduce the time and resources needed to examine the financial institutions using the products. Accordingly, a SASR report from these reviews is meant for the agencies' internal use only, and such a report is not shared with the TSP or user financial institutions.

Nature of TSP Supervision

The identification and selection of TSPs for supervision is ongoing and risk-based. The TSP Booklet provides for examination coverage of selected TSPs, including core application processors, electronic fund transfer switches, internet banking providers, item processors, managed security servicers, and data storage servicers. Examinations focus on the following underlying risk issues that affect the client financial institutions or their customers: (1) management of technology; (2) integrity of data; (3) confidentiality of information; (4) availability of services; (5) compliance with applicable laws, rules, regulations, and policies; and (6) financial stability.

The agencies use the Risk-Based Examination Priority Ranking Program (RB-EPRP) to determine the level of scrutiny to which TSPs should be subject. The RB-EPRP determines the overall level of risk presents based on its business lines, controls, and risk management processes. TSPs with higher risk rankings are subject to more frequent and extensive examinations, with examination cycles of 24 months, 36 months, or 48 months. As part of the supervision of a TSP, examiners can conduct interim supervisory reviews or unscheduled site or service examinations for areas of evolving supervisory interest or concern, and all examined TSPs will receive at least one interim supervisory review during each examination cycle.

Ratings of TSPs and Distribution of Examination Reports

The agencies use the Uniform Rating System for Information Technology (URSIT) to assess and rate the IT-related risks of financial institutions and their TSPs. This rating is based on a risk evaluation of four critical components: (1) audit, (2) management, (3) development and acquisition, and (4) support and delivery. Each TSP examined by the agencies is assigned a composite rating based on the overall results of the evaluation on a scale of 1 through 5, with 1 being the highest and 5 being the lowest.

The agencies have a uniform examination format, with an open and confidential section. The open section includes all significant findings, conclusions, and Matters Requiring Attention. The confidential section includes the rating, matters of a proprietary or competitive nature, comments that support operating and procedural deficiencies, internal control weaknesses, and financial information.

Examination reports are distributed to the federal banking agencies, the supervised TSP, and the serviced financial institutions. In addition, the agencies provide the Consumer Financial Protection Bureau (CFPB) with access to the Report of Examination (ROE) in accordance with the provisions of the Dodd-Frank Act. See 12 U.S.C. § 5512(c)(6)(B)(i). The supervised TSP and the serviced financial institutions have access to the open section only, and the agencies distribute automatically all ROEs with a composite URSIT of 4 or 5. Depending on the circumstances, the agencies may also distribute ROEs with a composite URSIT of 3; however, as a general rule, ROEs with a composite URSIT

of 1, 2, or 3 are provided to client financial institutions upon their request.

Notably, the agencies do not provide a copy of a TSP's ROE to financial institutions that are either considering outsourcing services to the examined TSP or that enter into a contract after the date of the examination because the agencies' statutory authority is limited to examining a TSP that enters into a contractual relationship with a regulated financial institution. Lastly, the FDIC is responsible for providing copies of TSP ROEs to the state regulatory agency that has authority to examine the TSP, has supervisory interest in the TSP, and/or participated in the examination of the TSP.

As part of the supervisory process, the agencies require the TSPs to produce a list of regulated financial institutions with which the servicer has entered into a contractual arrangement, and the services that the TSP provides. This customer list is solely for the internal use of the agencies to validate and correctly identify the financial institutions that are entitled to a copy of the ROE or that may be affected by the TSP's operations.

BSCA Enforcement Activity

There have been a number of enforcement action taken by the federal banking agencies under the BSCA over the past several decades. These consent orders do not indicate that the federal banking agencies see their BSCA powers as especially limited; at the same time, they all rely on IAP authority as well. Some of these grew out of the technology service program, and some did not. These included the following:

- In 1999, the Board, FDIC, OCC, National Credit Union Administration (NCUA), and Office of Thrift Supervision (OTS) entered into a Written Agreement with a third-party electronic funds transfer service provider. The regulators found that the company had not satisfied the requirements stated in the Year 2000 readiness guidelines issued by the FFIEC for the review, renovation, testing, remediation, management, and contingency planning of mission-critical systems. The agencies directed the company to, among other things, take necessary actions to provide its financial institution customers with Year 2000 testing service in a timely manner, submit a project plan addressing the company's proposed actions to comply with the agreement, and prepare and submit to the agencies various progress reports. See TransAlliance L.P., FDIC 5-21-99 (May 14, 1999).
- In 2006, the FDIC entered into a Written Agreement with a third-party service company that provided marketing and servicing of various loan products, including payday loan products, for certain state nonmember banks. The FDIC identified regulatory issues, substantive violations of law, ineffective procedures, and other safety and soundness concerns with the banks' loan programs marketed and serviced by the third-party company. The FDIC required that the company provide the FDIC with written notice prior to entering into an agreement with a state nonmember bank to market or serve any payday loan products. See Advance America, Cash Advance Centers, Inc., FDIC-06-144WA (August 22, 2006).
- In 2011, the OCC, the Board, FDIC, Federal Housing Finance Authority (FHFA), and OTS entered into a Consent Order with a third-party service company that provided various services to financial institutions related to tracking and registering residential mortgage ownership and servicing, acting as mortgagee of record in the capacity of nominee for lenders, and initiating foreclosure actions. The agencies found that the company, with its residential mortgage and foreclosure-related services, failed to exercise appropriate oversight, management supervision, and corporate governance. In addition, the agencies found that the company failed to establish and maintain adequate internal controls, policies and procedures, compliance risk management, and internal audit with respect to the administration and delivery of services to serviced financial institutions. The agencies ordered the company to, among other things, establish a compliance committee, submit a comprehensive action plan to remedy the identified deficiencies, and strengthen board and management supervision. See MERSCORP, Inc., and the Mortgage Electronic Registration Systems, Inc., OCC No. AA-EC-11-20 (April 13, 2011).
- In 2015, the Federal Reserve entered into a Consent Order with a service company that provided financial aid and reimbursement services to colleges and universities and deposit account services to students through contractual relationships with depository institutions. The Federal Reserve found that the service company engaged in deceptive acts or practices by inducing students to receive their financial aid refund to the account offered by the bank service company and its affiliated banks. The Federal Reserve also found that the company failed to disclose information related to various fees associated with such accounts. The Federal Reserve required the service company to, among other things, submit an acceptable written plan to enhance the consumer compliance risk management program and retain an independent auditor. Notably, in addition to corrective actions, the Federal Reserve assessed a restitution of $24 million and civil money penalty of approximately $2.2 million. See Higher One, FRB No. 15-026-E-I, 15-026-CMP-I (December 23, 2015).

Payment System Oversight

Federal bank regulators have referred to their authority under the BSCA in other contexts. The Federal Reserve has referred to the BSCA as part of the Federal Reserve's toolkit for overseeing aspects of the payments system that involve nonbanks, but have a nexus to supervised banks. Governor Brainard has said that while the Federal Reserve does not have plenary authority over payment systems, as do supervisors in other nations, the BSCA provides the Federal Reserve with some reach. Lael Brainard, The Digitalization of Payments and Currency: Some Issues for Consideration (February 5, 2020). For example, The Clearing House, a consortium of banking organizations that provide payment services, is made subject to examination and regulation by the federal banking agencies by the BSCA, and asserts that such regulation is "extremely broad." RTP Frequently Asked Questions, The Clearing House. The federal banking agencies indicated that the SWIFT, a consortium of banking organizations that engage in the transmission of messages to facilitate financial transactions, is also made subject to examination by the federal banking agencies by the BSCA. *See* U.S. General Accounting Office, Report to the Chairman, Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce, House of Representatives, Electronic Funds Transfer: Oversight of Critical Banking Systems Should Be Strengthened (Jan. 1990).

A more recent invocation of the BSCA came in Project Cedar, a test-run of a shared ledger for commercial and central bank digital currency conducted under the auspices of the Federal Reserve Bank of New York. The legal paper issued in connection with Project Cedar pointed to the BSCA as a means for the official sector to exercise oversight powers over the utility behind the shared ledger. The old law seems to be up for learning new tricks.

Computer-Security Incident Notification Rule

On November 23, 2021, the agencies published a final rule (the "Notification Rule") that imposes new notification requirements on banking organizations and service companies following significant cybersecurity incidents. 86 Fed. Reg. 66424–66444. The rule supplements banking organizations' existing obligations to provide notification for cybersecurity incidents under various laws and regulations. However, the Notification Rule directly applies notification requirements to service companies in addition to banking organizations.

A "bank service provider" is defined under the rule as a bank service company or other person that performs services that are subject to the BSCA. 12 C.F.R. § 225.301(b)(2); 12 C.F.R. § 304.22(b)(2); 12 C.F.R. § 53.2(b)(2). The rule requires a bank service provider to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible after determining that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours. 12 C.F.R. § 225.303; 12 C.F.R. § 304.24; 12 C.F.R. § 53.4. A computer-security incident means an event that results in actual, rather than potential, harm to information and systems. 12 C.F.R. § 225.301(b)(4); 12 C.F.R. § 304.22(b)(4); 12 C.F.R. § 53.2(b)(4).

The notification to the bank-designated contact should use an email address, phone number, or any other contact information previously provided to the service provider by the customer (or, if none was previously provided, to contact the CEO and CIO of the banking customer, or two individuals of comparable responsibilities, through any reasonable means). 12 C.F.R. § 225.303(a); 12 C.F.R. § 304.24(a); 12 C.F.R. § 53.4(a). These flexible notice requirements are designed to ensure regulators and banking organizations receive notification on as expedited a timeline as possible so they can quickly address any matters of concern. Lastly, this notification requirement does not apply to any scheduled maintenance, testing, or software update previously communicated to a banking organization customer.

In their rulemaking, the agencies first noted that cyberattacks targeting the financial services industry have increased in frequency and severity. The agencies voiced their concern that banking organizations have become increasingly reliant on third parties to provide essential services and that the impact of computer-security incidents at bank service providers can flow through to their bank customers. As a result, the rule is designed to provide banking organizations with prompt notification of computer-security incidents and help banking organizations assess the extent to which an incident may impact them and determine whether their own notification requirement has been triggered.

The BSCA into the Future

With the rule and the increase in enforcement activity indicating increased momentum for the use of the BSCA in recent years, it is worth considering where the ambit of the BSCA may spread next. The conditions that led to the passage of the BSCA—the increasing reliance of banking organizations on technology organizations—are only stronger now, and policy-makers are taking note. In fact, Governor Michelle Bowman of the Federal Reserve (Governor Bowman) noted in her speech that the BSCA is "a potentially underused tool" that could be used to address the "flow of risk between the permeable boundary separating regulated banks and other companies." In the U.S., three developments are notable: (1) the FSOC is contemplating the BSCA as a means to manage cloud provider risks, (2) relatedly, third-party risk management has re-emerged as a major regulatory emphasis, and (3)

Congress is considering new legislation that would expand regulatory sharing about third-party service providers. Abroad, multilateral standard-setting organizations are taking stock of regulatory authority for third-party service providers, and the European Union is implementing new means for overseeing such providers.

Cloud Service Provider Risks

The FSOC identified the risks posed by financial sector relationships with cloud service providers as a financial stability risk to monitor in its 2022 annual report, and recommended legislation to empower the FHFA and the NCUA with authority similar to that provided bank regulators under the BSCA. According to the FSOC report, the pace of adoption of the cloud by financial institutions has increased markedly over the past several years. Financial institutions cite a number of factors driving them to adopt cloud environments, including increased resilience, speed, and ease of innovation. U.S. Dept. of Treasury, The Financial Services Sector's Adoption of Cloud Services 19 (2023).

By its nature, financial institutions need to partner with third parties when they enter the cloud, and usually with one of a small number of the large technology providers that provide such services. The FSOC report seems especially concerned with two risks emanating from such partnerships. First, such partnerships are characterized by shared responsibility models, where the contracting entities need to establish parameters for configuration that are appropriate for that user. The FSOC report noted that malefactors have been found to scan for misconfiguration by cloud users as a means for penetrating the systems of potential victims. Relatedly, the FSOC report, and another report issued by Treasury in 2023, expressed concerns that financial institutions lacked the human capital to properly implement cloud services and applications. FSOC, *2022 Annual Review* 71 (2022). Small- and medium-sized financial institutions, in particular, complain of not being able to attract and retain skilled professionals needed to manage their side of the cloud relationship, noting that the information technology skills required for usual banking are not a match for the needs of the cloud (this is an echo back to 1962). U.S. Dept. of Treasury, *The Financial Services Sector's Adoption of Cloud Services* 52 (2023). To manage these risks, the FSOC supported the continued development of third-party service provider supervision, as authorized by the BSCA, and the continued sharing of information among federal and state authorities. The FSOC also recommended that Congress pass legislation that would give the FHFA and the NCUA such third-party supervision authority.

Third-Party Risk Management Guidance

The banking agencies have long had supervisory expectations regarding the outsourcing of services by banking organizations, for many of the reasons that have been described in this practice note. The expectations that the agencies have had for banks has remained the same—that a bank should not take more risk because of an outsourcing arrangement and should know about and manage the relevant risks of any activity as if it is conducting the business itself. In 2023, the banking agencies published *Interagency Guidance on Third-Party Relationships: Risk Management*, for the management of third-party risk by banking organizations. 88 Fed. Reg. 37920 through 37937. This new guidance built on similar guidance that the banking agencies had published over the years. Together with the publication of this guidance, the agencies articulated third-party risk as an increasing focus for examination, describing management of cybersecurity and resilience as areas of focus.

Governor Bowman voted against adopting the guidance on the basis that it imposed too burdensome a compliance regime on smaller banks. Later, Governor Bowman suggested that one way to ameliorate these concerns is for bank regulators to make more robust use of the BSCA: " . . . we should consider the appropriateness of shifting the regulatory burden from community banks to more efficiently focus directly on service providers. The BSCA gives the federal banking agencies significant regulatory authority over outsourced banking services. In a world where third parties are providing far more of these services, it seems to me that these providers should bear more responsibility to ensure the outsourced activities are performed in a safe and sound manner." Statement on Third Party Risk Management Guidance by Governor Michelle W. Bowman (June 06, 2023). The governor pointed to the rule as a good example of allocating responsibility to service providers and away from banks. Some in the industry agree it would be appropriate for the federal banking agencies to direct more of the focus toward service providers and away from the banks themselves. See Innovation, Payments and Banking Technology (icba.org).

Bank Service Company Examination Coordination Act

Legislation has been introduced in both the Senate and the House to amend the BSCA. Draft bills entitled the "Bank Service Company Examination Coordination Act" would amend the BSCA to recognize that state supervisors may have authority to examine third-party service providers and that information can and should be exchanged with federal supervisors while still maintaining its confidential character. *Bank Service Company Examination Coordination Act, H.R. 1109, 118*th Cong. (2023). The legislation would also require federal supervisors to coordinate their examination of such service providers with their state counterparts. It would not grant any new authority. The Conference of State Bank Supervisors has endorsed the legislation, noting that "more and more, banks are outsourcing their core

business functions." The Bank Service Company Examination Coordination Act, Explained, Conference of State Bank Supervisors (Mar. 8, 2023). In addition, a number of state banking regulators have the authority to examine bank service corporations under the respective state banking law. *See, e.g.*, S.D. Codified Laws § 51A-9-5; Ala. Code § 5-3A-1(b); Me. Rev. Stat. Ann. tit. 9-B, § 221(5); Md. Code Ann., Fin. Inst. § 5-406; Or. Rev. Stat. § 708A.145(4).

International Developments

The same conditions that are driving interest in third-party management and the BSCA in the United States also apply abroad, and international supervisors are paying attention. The Financial Stability Board recently published a consultation document on "Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities" (toolkit). This toolkit document followed several years of review of this topic by the Financial Stability Board and the Basel Committee for Banking Supervision, amid heighted concern about the outsourcing of "critical services" to technology companies.

While the bulk of the toolkit is aimed at the supervision and management of third parties by banks, the toolkit conducts a short survey of supervisory authorities' ability to examine service providers directly. It determines that most jurisdictions do not have these authorities. It describes the United States' BSCA as a model that other jurisdictions could consider adopting. The toolkit points to the European Union's recent Digital Operational Resilience Act (DORA), which provides for the creation of an oversight framework for critical Information Communication Technologies (ICT) third-party service providers to European financial institution. DORA would give European supervisors the ability to designate critical ICT third-party service providers for supervision, with the possibility of examination and penalties for noncompliance, including suspension and termination. *See* European Commission, Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Section (Sept. 24, 2020); Financial Stability Board, *Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities* 51 (June 22, 2023). The toolkit also notes that the United Kingdom is considering legislation that would give them similar powers—which legislation has been subsequently enacted. See The Financial Services and Markets Act 2023 (June 29, 2023). Enhancing Third-Party Risk Management and Oversight A toolkit for financial institutions and financial authorities, the final toolkit, was published by the Financial Stability Board on December 4, 2023.

Practical Guidance and Conclusion

The BSCA was born at a time when technological change was pushing traditional banks beyond what they could do within their own four walls, and they needed to look to arrangements with third parties to keep up. The BSCA was a means of assuring supervisors that they would get what they needed as these arrangements developed. More than 60 years on, it is clear that the pace of change has only increased, and supervisors' reliance on this slender tool to look outside their normal ambit has only become more pronounced.

It is important for both parties to service contracts—the bank and the service provider— to remain conscious of this supervisory "third eye" as they document their agreements. The banking agencies have significant expectations for banking organizations to manage their third-party relationships and consider third-party management a substantial supervisory priority. Supervisory priority and increased examination have a way of manifesting themselves in observed issues. Observed issues tend to lead to a look for solutions, and the BSCA is a tool that is available to supervisors looking for solutions. The Treasury and FSOC reports focusing on the BSCA as a pressure valve for evolution in financial services are a harbinger.

Service providers to banks should be aware that the agencies have this tool at their disposal and plan appropriately. Providers, especially those of services or software that could lead to safety and soundness for individual banks or stability problems for the system at large, should consider the FFIEC examination programs that the banking agencies have employed thus far for service providers and weigh whether they would be ready for such an examination. Providers will need to be ready to comply with the Cyber Rule and may need to keep an eye out for other requirements that bank regulators may impose now that they have put the BSCA back in the regulation business.

Banks, for their part, should keep the BSCA in mind as they prepare themselves for third-party risk examinations, document their third-party relationships, and comply with new requirements, such as those of the Cyber Rule. Supervisory knowledge gained in a TSP examination may lead to further questions from supervisors to those who use the services of an examined entity. Further, banks struggling with performing assessments of third parties from whom they need essential technological services might look to the BSCA as a form of relief, pressing their regulators to share information about service providers earlier and

more robustly than they do now, and to focus some of their concern for safety and soundness and stability onto the service providers directly rather than the banks indirectly.

Finally, as fintech developments drive the infrastructure of finance in new directions—into tokenized deposits and distributed ledger settlement, for example—it can be sure that there will be a need for nonbanks to play an important role in this evolution. The BSCA will be a way for the bank regulators to follow along.

Jim P. Bergin, Partner, Arnold & Porter

Jim Bergin, former acting co-general counsel, deputy general counsel and chief of staff of the Federal Reserve Bank of New York, is a member of the firm's Financial Services practice. He advises clients as they navigate the complex and ever-changing financial and banking landscape.

As a member of the leadership team at the New York Fed over many years, Jim interacted with a wide variety of domestic and foreign supervisory authorities and central banks.

As acting co-general counsel, Jim served as part of the New York Fed's executive management and oversaw the activities of the Legal Group, including the legal, compliance, and bank applications functions. He advised senior management on a wide range of matters, including regulation and supervision of financial institutions; monetary policy and implementation; financial services and accounts matters; and corporate governance and risk management.

In his role as deputy general counsel, Jim was responsible for both markets and regulatory matters. He led the legal team that advised on matters relating to the New York Fed's implementation of monetary policy, lending, foreign exchange, U.S. Treasury, reference rate, and other market-facing activity. Jim was also responsible for advising supervisors and others on matters relating to the New York Fed's regulation and oversight of financial institutions, and oversaw the New York Fed's bank applications function.

Jim joined the New York Fed in January 2005 as an attorney. He moved to its Supervision Group in 2011 to serve as head of the Legal Compliance & Risk Department. Jim became chief of staff to President William C. Dudley in 2012 and held the position until the end of 2015 when he became deputy general counsel.

Prior to joining the New York Fed, Jim was a lawyer in private practice at an international law firm in New York where he focused his practice on energy and infrastructure finance.

Paul Lim, Associate, Arnold & Porter

Paul Lim assists in advising bank and nonbank financial institutions on a wide range of regulatory, transactional, and general corporate matters, including matters within the supervisory jurisdiction of the Federal Reserve Board, the OCC, the FDIC, and the CFPB as well as state financial regulatory agencies. Paul also assists in advising clients in the acquisition and sale of financial institutions and non-bank financial service companies.

His pro bono work includes assisting clients in immigration and asylum cases, defending victims of domestic violence, and assisting non-profit organizations in connection with formation and tax-exemption.

Paul earned his J.D. from Columbia University School of Law, where he was a Harlan Fiske Stone Scholar and served as Student Attorney at the Environmental Law Clinic, a member of Morningside Heights Legal Services. Prior to law school, he served as a Staff Sergeant for the Republic of Korea Air Force.

This document from Practical Guidance®, a comprehensive resource providing insight from leading practitioners, is reproduced with the permission of LexisNexis®. Practical Guidance includes coverage of the topics critical to practicing attorneys. For more information or to sign up for a free trial, visit lexisnexis.com/practical-guidance. Reproduction of this material, in any form, is specifically prohibited without written consent from LexisNexis.

LexisNexis.com/Practical-Guidance

LexisNexis®

LexisNexis, Practical Guidance and the Knowledge Burst logo are registered trademarks of RELX Inc.
Other products or services may be trademarks or registered trademarks of their respective companies. © 2024 LexisNexis