PAUL HASTINGS
STAY CURRENT
A CLIENT ALERT FROM PAUL HASTINGS

April 2014

Bank Vendor Management – An Aspirin to Prevent a Headache or Just a Headache?

BY LAWRENCE D. KAPLAN & KEVIN L. PETRASIC

A flurry of recent regulatory guidance, pronouncements and enforcement actions by federal regulators demands that banks must be keenly aware of their obligations when retaining third-party service providers. Similarly, third-party service providers must understand the types of regulatory and supervisory obligations they undertake when they provide services to banks. In particular, third-party service providers must be aware of, understand and be able to apply and comply with the laws and regulations to which their bank customers are subject. Failing to do so will expose both a service provider and its bank customers to potential supervisory and enforcement actions.

As the banking industry's dependence on outsourcing of activities by financial institutions has proliferated, the federal banking agencies,[1] and now, the Consumer Financial Protection Bureau ("CFPB"), continue to discuss and publish guidance to address regulatory expectations for managing third-party service providers.[2] The federal banking agencies' guidance essentially implements the agencies' authority set forth in the Bank Service Company Act ("BSCA"),[3] which governs situations where a bank arranges, by contract or otherwise, for another party to perform its applicable functions. While the BSCA is the provision typically referenced for the federal banking agencies' jurisdiction of third-party vendor relationships, the agencies' historically have maintained their ability to oversee these activities in an even broader construct. In this regard, federal laws, regulations and agency guidance reference various requirements imposed on banks to oversee the activities of their service providers,[4] and the federal banking agencies have exercised their existing safety and soundness authority to compel the same.[5]

Under the BSCA, the federal banking agencies have the authority to examine and regulate the activities, functions and operations performed by third-party service providers to the same extent as if these were performed by the bank itself.[6] Moreover, banking regulators are authorized under the BSCA to review service providers' operations and initiate enforcement actions against both a bank and its service provider for violations of any law, which frequently has included Section 5 of the Federal Trade Commission Act addressing unfair or deceptive acts or practices. The CFPB's authority to examine banks and nonbanks subject to its jurisdiction extends to the entity's service providers under authority derived from Title X of the Dodd Frank Wall Street Reform and Consumer Protection Act.[7]

Recent regulatory guidance also supplements multiple enforcement actions taken in the last few years against banks as well as their service providers – imposing civil money penalties and significant restitution payments to impacted-customers.[8] The existing regulatory guidance, coupled with numerous speeches and comments from various federal and state bank regulators, is a clear and

critical warning to banks that outsourcing requires intensive oversight and vendor management, and reiterates the view of all regulators that the use of third-party service providers does not release a bank from liability for actions taken by its third-party service providers. Similarly, service providers should heed the warning that they have an independent obligation to comply with all laws, regulations, and guidance that their counterparty banks are subject to, with no allowance or concessions provided for failing to fully understand these requirements, even where the bank customer fails to do so.

Regulatory Guidance

The federal banking agencies and the CFPB have each issued guidance addressing regulatory expectations for when a bank or supervised nonbank outsources operations.[9] All of the issuances underscore a clear and unambiguous expectation that management of third-party risk be commensurate with the level of risk and complexity of the third-party relationship and a bank's operations and organizational structure. As noted by the OCC, a bank must have more comprehensive and rigorous oversight and management of third-party relationships that involve critical activities. These include critical core functions and operations (e.g., cybersecurity, privacy and data protection), significant bank functions (*e.g.,* payments, clearing, settlements and custody), significant shared services (*e.g.,* information technology and marketing initiatives), as well as other activities that could:

- Cause a bank to face significant risk if a third party fails to meet the obligations and expectations imposed on it;
- Have significant customer impact;
- Require significant investment in resources to implement the third-party relationship and manage the risk; or
- Have a major impact on bank operations if the bank has to find an alternate third party or if the outsourced activity has to be brought in-house.

As described by the OCC, regulators expect that an effective third-party risk management process will follow an ongoing and continuous "life cycle" that incorporates the following important phases:

- Planning to identify the services to be outsourced;
- Due diligence and third-party selection of firms to perform the outsourced services;
- Contract negotiation with the service provider;
- Ongoing monitoring of the service provider's activities and operations, including periodic reporting requirements, as appropriate;
- Termination of the relationship, including protections for the institution and its customers, where appropriate;
- Contingency planning to move activities to a third party, bring activities in-house, or discontinue activities and outsourcing operations when a contract expires, is in default, or in response to a change in the bank's business strategy;
- Vendor oversight and accountability;

- Documentation and reporting of services performed and issues requiring the attention of the bank and/or its regulators; and
- Independent reviews to validate that the services provided are being performed in a legal and contractually required manner.[10]

These supervisory and regulatory obligations imposed on banks mandate that banks outsourcing critical services have in place a detailed management process to oversee their third-party service provider relationships. A bank's failure to properly manage its third-party vendor relationships will almost certainly be adversely reflected in the bank's management component in its report of examination.[11]

Federal and state bank regulators, including the CFPB, expect that supervision of third-party service providers occur at all levels of a bank's management structure, including: (i) the board of directors; (ii) senior bank management; and (iii) employees interacting with the third-party vendor. Moreover, a bank's written policies should specify that third-party vendor management and oversight must occur (i) prior to retention through a detailed due diligence process; as well as (ii) periodically throughout the term of the bank's written agreement with the service provider. Regulators now expect to see written confirmation of all levels of outsourcing and third-party vendor involvement with a bank to be documented in the bank's books and records, including, as appropriate, in its board minutes.

Application to Third-Party Service Providers

While bank regulators have generally directed agency guidance to the banks they supervise, such guidance applies equally to each third-party service provider to a bank. Thus, to avoid the penalties and enforcement actions[12] that bank regulators are authorized to issue against both banks and their service providers, service providers must understand and be able to comply with the obligations they undertake that are imposed on their bank counterparties. More importantly, service providers must continually be prepared to demonstrate that they have active and diligent compliance programs that minimize material risks to the banking system. Recently, the Comptroller of the Currency cautioned that each vendor and subcontractor retained by a bank provides potential access points into the banking system, introducing complexity as well as new and different potential weaknesses into the banking system.[13] According to the Comptroller, banks should conduct appropriate due diligence to mitigate risks posed by relying upon a third party.[14]

While federal bank regulators have clear and specific enforcement authority over the banks they supervise,[15] their authority and jurisdiction over third-party service providers is less clearly spelled out.[16] Nonetheless, the federal bank regulators maintain the view that their authority, which stems from their supervision and oversight of the bank itself, as well as the BSCA, is unequivocal. As noted above, the BSCA authorizes the regulation and examination of third-party service providers to the same extent as if such services were being performed by the depository institution itself on its own premises.[17] While a third-party service provider most commonly would be viewed as an independent contractor of a bank, it is also important to recognize that the Federal Deposit Insurance Act ("FDI Act"), federal banking agency policy, and court rulings generally impose a higher standard on enforcement actions against independent contractors. Specifically, under the enforcement provisions of the FDI Act, federal banking agencies only can bring actions against "institution affiliated parties" ("IAP"), a term defined in pertinent part as:[18]

> any shareholder … consultant, joint venture partner, and any other person as determined by the appropriate Federal banking agency (by

> regulation or case-by-case) who participates in the conduct of the affairs of an insured depository institution; and any independent contractor (including any attorney, appraiser, or accountant) who knowingly or recklessly participates in --
>
> - any violation of any law or regulation;
> - any breach of fiduciary duty; or
> - any unsafe or unsound practice;
>
> *which caused or is likely to cause more than a minimal financial loss to, or a significant adverse effect on, the insured depository institution.*[19]

FDIC policy addressing who is deemed to participate in the affairs of a bank also explicitly provides that:

> [T]ypically, an independent contractor does not have a relationship with the insured institution other than the activity for which the insured institution has contracted. Under 12 U.S.C. § 1813(u), *independent contractors are institution-affiliated parties if they knowingly or recklessly participate in violations, unsafe or unsound practices or breaches of fiduciary duty which are likely to cause significant loss to, or a significant adverse effect on, an insured institution.*[20]

In *Grant Thornton v. Office of the Comptroller of the Currency*, the D.C. Circuit found that a contractor must be involved in the "business of banking" to meet the statutory jurisdictional requirements to be deemed an IAP.[21] As a result of such legal obstacles, in 2013, the OCC's Deputy Chief Counsel testified at a Congressional hearing that the OCC would welcome a legislative change in this area to facilitate the agency's ability to take enforcement actions directly against independent contractors that engage in wrongdoing.[22] As the OCC Deputy Chief Counsel noted "such a legislative change would be useful not only with respect to the use of independent contractors in an enforcement context but also, and perhaps more importantly, in cases where a bank has chosen to outsource significant activities to an independent contractor."[23]

Accordingly, absent consent,[24] in order to bring a formal enforcement order against a third-party service provider to address some type of wrongdoing, federal banking agencies must demonstrate that: (i) the third-party service provider knowingly or recklessly participated in violations, unsafe or unsound practices, or breaches of fiduciary duty; and (ii) the third-party service provider's actions are likely to cause a significant loss to or a significant adverse effect on an insured institution and that the activities of the third party were akin to engaging in the business of banking.[25] In practice, however, it rarely gets this far; instead, for a host of reasons including, most importantly, minimizing reputation risk, a service provider will most likely negotiate and consent to a settlement rather than challenging an agency enforcement action in court.

Suggested Best Practices

Given that the potential consequences of a regulatory order against third-party service providers could involve financial penalties, and the loss of a banking relationship and/or the inability to establish a new banking relationship, third-party service providers must understand and take action to implement policies and procedures to implement regulatory expectations to minimize the risk of a regulatory enforcement action. Recent enforcement actions against third-party service providers provide

significant instruction to guide service providers in establishing relationships with banks. Regulatory guidance suggests that service providers should implement a written compliance management system, requiring that the service provider take the following actions:

1. Hire a qualified compliance officer (and necessary staff) with the knowledge and experience to implement an effective compliance program, and implement an effective reporting program to the service provider's board of directors and senior management, as well as have accountability for the compliance program to the bank;

2. Identify and comply with all applicable consumer protection laws (including updating for changes to such laws) relating to the products and services outsourced by the bank;

3. Understand the products and services outsourced by the bank and review related marketing materials to avoid the possibility of making misleading or deceptive representations, statements, or omissions;

4. Require that the bank review all marketing, advertising, solicitation materials, and other information provided to bank customers, including agreements, privacy policies, and statements, as well as any amendments thereto;

5. Require that the bank approve all materials related to policies and procedures concerning third-party collection activities and monitor third-party collection calls on a regular basis;

6. Promptly address and resolve consumer inquires and complaints and notify the bank of any regulatory or legal actions by any customer or potential customer;

7. Maintain records of approved materials, customer solicitation materials, administrative materials, service provider materials, complaints, and responses;

8. Regularly meet with the bank and sub-service providers, and maintain written minutes of all such discussions;

9. Conduct onsite diligence and oversight visits (accompanied by the bank, as appropriate) to all material sub-service providers;

10. Maintain records demonstrating compliance with any service level standards in any material contracts with the bank;

11. Implement procedures to promptly notify the bank of (and escalate within the bank, as appropriate) significant regulatory inquires or consumer complaints;

12. Be responsive to regulatory, supervisory or examiner inquiries about particular issues and potential compliance, operational and similar vulnerabilities and

13. Develop an audit program that is approved by the service provider's board to ensure effective and independent review of integral policies and procedures and be prepared to share such information with the bank counterparty and its examiners.

Conclusion

The rapidly evolving supervisory, regulatory, and enforcement landscape for banks and bank service providers requires firms to continually monitor, maintain and update the integrity and effectiveness of their operations. The consequences of failing to do so are significant; thus, both banks and their service providers must dedicate sufficient resources and staffing to avoid potential regulatory or supervisory issues. A critical issue for both banks and their service providers is understanding regulatory expectations, as well as implementing the changes required to comply with regulators' rapidly evolving compliance standards in numerous areas of the law. Implementing the best practices described above is a good first step for the service provider, but perhaps the most important step for both a bank and its service provider is to develop an ongoing dialogue regarding what both parties need in order to maintain an effective compliance mechanism that furthers their common interests, and that satisfies regulatory and supervisory expectations.

✧ ✧ ✧

Paul Hastings attorneys have been advising clients on third-party service provider issues and guidance issued by federal and state banking and consumer financial protection regulators, and we have also represented various clients subjected to regulatory enforcement actions. If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Atlanta

Todd W. Beauchamp
1.404.815.2154
toddbeauchamp@paulhastings.com

Chris Daniel
1.404.815.2217
chrisdaniel@paulhastings.com

Erica Berg Brennan
1.404.815.2294
ericaberg@paulhastings.com

Heena A. Ali
1.404.815.2393
heenaali@paulhastings.com

Kevin P. Erwin
1.404.815.2312
kevinerwin@paulhastings.com

Meagan E. Griffin
1.404.815.2240
meagangriffin@paulhastings.com

Palo Alto

Cathy Beyda
1.650.320.1824
cathybeyda@paulhastings.com

San Francisco

Tom Brown
1.415.856.7248
tombrown@paulhastings.com

Samuel Zun
1.415.856.7206
samuelzun@paulhastings.com

Washington, D.C.

V. Gerard Comizio
1.202.551.1272
vgerardcomizio@paulhastings.com

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Kevin L. Petrasic
1.202.551.1896
kevinpetrasic@paulhastings.com

Lawrence D. Kaplan
1.202.551.1829
lawrencekaplan@paulhastings.com

Ryan A. Chiachiere
1.202.551.1767
ryanchiachiere@paulhastings.com

Michael A. Hertzberg
1.202.551.1797
michaelhertzberg@paulhastings.com

Amanda Kowalski
1.202.551.1976
amandakowalski@paulhastings.com

Helen Y. Lee
1.202.551.1817
helenlee@paulhastings.com

[1] The Federal banking agencies are the Board of Governors of the Federal Reserve Service ("Federal Reserve"), the Federal Deposit Insurance Corporation ("FDIC") and the Office of the Comptroller of the Currency ("OCC").

[2] *See, e.g.*, OCC Bulletin 2013-29 (Oct. 30, 2013) *available at:* http://www.occ.treas.gov/news-issuances/bulletins/2013/bulletin-2013-29.html#.

FDIC Guidance for Managing Third-Party Risk, *available at*: http://www.fdic.gov/news/news/financial/2008/fil08044a.pdf.

Federal Reserve SR 13-19, *Guidance on Managing Outsourcing Risk* (Dec. 5, 2013), *available at*: http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf.

CFPB Bulletin 2012-03 (Apr. 13, 2012) *available at*: http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf.

[3] *See* 12 U.S.C. § 1867(c).

[4] *See, e.g.*, OCC Bulletin 29, Appendix B (Oct. 30, 2013) *available at*: http://www.occ.treas.gov/news-issuances/bulletins/2013/bulletin-2013-29.html#; and OCC Bulletin 2008-12 (April 24, 2008) *available at* http://www.occ.gov/news-issuances/bulletins/2008/bulletin-2008-12.html.

[5] *See, e.g., JP Morgan Chase Bank, N.A., et al.*, OCC Consent Order AA-EC-13-76 (Sept. 18, 2013).

[6] This authority also extends to nonbanks and service providers to nonbanks under the CFPB's jurisdiction.

[7] *See* 12 U.S.C. §§ 5514(e), 5515(d), 5516(e) and 5564.

[8] *See e.g., Higher One, Inc.*, FDIC-11-700b, FDIC-11-704K (2012) (FDIC Consent Order, Order for Restitution, and Order to Pay Civil Money Penalty), *available at*:http://www.fdic.gov/news/news/press/2012/pr12092.html; FDIC The Bancorp Bank, FDIC-11-698b, FDIC-11-703K (2012) (FDIC Consent Order and Order to Pay Civil Money Penalty), *available at:* http://www.fdic.gov/news/news/press/2013/pr13045.html.

See also Meridian Bank, Inc., FDIC-12-367b(2012) (FDIC Consent Order), available at: https://www5.fdic.gov/edo/DataPresentation.html.

Achieve Financial Services, LLC, FDIC-13-048b, FDIC-13-049K (2013) (FDIC Consent Order, Order for Restitution, and Order to Pay Civil Money Penalty), available at; First California Bank, FDIC-13-046b, FDIC-13-047K (2013) (FDIC Consent Order, Order for Restitution, and Order to Pay Civil Money Penalty), available at: http://www.fdic.gov/news/news/press/2013/pr13045.html.

In re Capital One Bank (U.S.A.) N.A., 2012-CFPB-0001 (2012) (CFPB Consent Order), available at: http://www.consumerfinance.gov/pressreleases/cfpb-capital-one-probe/; In re Capital One Bank (U.S.A.) N.A.; AA-EC-2012-62 (2012) (Dept. of Treasury and Comptroller of the Currency Consent Cease and Desist Order), available at: http://occ.gov/news-issuances/news-releases/2012/nr-occ-2012-110.html.

See CFPB Orders American Express to Pay $85 Million Refund to Customers Harmed by Illegal Credit Card Practices (Oct. 1, 2012) available at: http://www.consumerfinance.gov/pressreleases/cfpb-orders-american-express-to-pay-85-million-refund-to-consumers-harmed-by-illegal-credit-card-practices/.

See CFPB Orders American Express to Pay $59.5 Million for Illegal Credit Card Practices (Dec. 24, 2013) available at: http://www.consumerfinance.gov/newsroom/cfpb-orders-american-express-to-pay-59-5-million-for-illegal-credit-card-practices/.

U.S. Bank N.A., 2013-CFPB-0003 (2013) (CFPB Consent Order), available at: http://www.consumerfinance.gov/pressreleases/cfpb-orders-auto-lenders-to-refund-approximately-6-5-million-to-servicemembers/; Dealers' Financial Services, LLC, 2013-CFPB-0004 (2013) (CFPB Consent Order), available at: http://files.consumerfinance.gov/f/201306_cfpb_enforcement-order_2013-0589-02.pdf.

In re Bank of America, N.A. and FIA Card Services, N.A. AA-EC-2014-6 (April 7, 2014) Comptroller of the Currency Consent Order and Consent Order for a Civil Money Penalty), available at:. http://www.occ.gov/static/enforcement-actions/ea2014-027.pdf and *http://www.occ.gov/static/enforcement-actions/ea2014-028.pdf.*

[9] *See supra* at footnote 1.

[10] OCC Bulletin 2013-29 (Oct. 30, 2013) *available at*: http://www.occ.treas.gov/news-issuances/bulletins/2013/bulletin-2013-29.html#.

[11] *Id.*

[12] Under the Federal Deposit Insurance Act ("FDI Act") banking regulators have the authority to issue a panoply of written orders ranging from memoranda of understanding to cease and desist orders and can assess civil money penalties ranging up to $1.0 million per day for certain types of violations. *See* 12 U.S.C. § 1818(b) and (i).

[13] *See* Remarks of Thomas J. Curry before the Independent Community Bankers of America, (March 4, 2013) *available at:* http://occ.gov/news-issuances/news-releases/2014/nr-occ-2014-30.html.

[14] Among the concerns recently raised by the Comptroller was the consolidation of third-party service providers, as compliance deficiencies at a service provider to multiple banks poses a larger risk to the banking systems. The Comptroller also noted that service providers with foreign operations mandate specific contractual arrangements to ensure compliance with applicable law, including cross-border data transmission requirements, as well as an ability for the bank (and presumably regulators) to enforce the agreement. *Id*.

[15] *See* 12 USC §§ 248, 481, 1463 and 1820.

[16] Bank regulators' authority over service providers should be contrasted with the clear articulated authority granted to the CFPB over service providers of supervised banks and nonbanks. Specifically, the Dodd-Frank Act grants the CFPB supervisory authority over supervised service providers, defined as "any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service." 12 U.S.C. § 5481(26).

[17] 12 U.S.C. § 1867(c)(1).

[18] The omitted sections from the definition address: (1) any director, officer, employee, or controlling stockholder (other than a bank holding company or savings and loan holding company) of, or agent for, an insured depository institution; and (2) any other person who has filed or is required to file a change-in-control notice with the appropriate Federal banking agency under section 7(j).

[19] 12 U.S.C. § 1813(u) (emphasis added).

[20] FDIC Statements of Policy for Section 19 of the FDI Act (emphasis added), *available at*: http://www.fdic.gov/regulations/laws/rules/5000-1300.html.

[21] 514 F.3d 1328 (D.C. Cir. 2008).

[22] *See* Testimony of Daniel Stipano before the Subcommittee on Financial Institutions and Consumer Protection of the U.S. Senate Committee on Banking, Housing & Urban Affairs (April 11, 2013), *available at:* :http://occ.treas.gov/news-issuances/congressional-testimony/2013/pub-test-2013-61-written.pdf.

[23] *Id.*

[24] Most bank regulatory enforcement actions involve the respondent consenting to the issuance of the order rather than a formal administrative proceeding, primarily due to the significant costs necessary for a party to prevail against a government agency in an administrative action. Moreover, most consent orders are entered into without admitting or denying liability, which helps thwart collateral or derivative actions claiming the bank or third party has admitted liability to a particular infraction.

[25] Any party facing a potential consent order with a regulatory authority must consider and evaluate the consequences; if a third-party service provider does not have an alternative bank to offer its services through, a challenge to regulatory authority would require significant resources and effectively force a third-party service provider out of business before the matter could be fully resolved.

Regulators have significant powers when negotiating with a third-party service provider. For example, a determination that a party engaged in an unsafe or unsound practice is a determination granted to regulators, and would be granted significant deference by both administrative law and article III courts. Moreover, while the FDI Act requires that regulators demonstrate that a third-party service provider's conduct caused "more than a minimal financial loss" or a "significant adverse effect for a bank" if a third-party service provider is contractually obligated to hold its bank-counterparty harmless, making restitution or indemnification payments to address any regulatory issues, arguably arguable there could not be more than a minimal financial loss to the bank. An issue remains, however, as to whether a bank could suffer a significant adverse effect due to the third-party service provider's actions. Clearly, the public nature of an enforcement action arguably would create a "reputational risk" to the bank but such adverse effect, arguably, would be a regulatory-induced self-fulfilling prophecy. This adverse risk could, however, be cited by regulators if no other factor is available to bootstrap a third party into the definition of an IAP.