Bloomberg BNA

BNA's Banking Report™

THIRD PARTY MANAGEMENT

Regulatory Blue Pencil: CFPB Guidance, Enforcement Actions Signal Expanding Focus on Vendor Management

BY ELIZABETH MCGINN AND MOORARI SHAH

In April 2012, the Consumer Protection Financial Bureau (the ''CFPB'' or ''Bureau'') issued Bulletin 2012-03 (the ''Service Provider Bulletin''), a guidance document setting forth the CFPB's high-level expectations related to the engagement of third party service providers by supervised financial institutions.[1] In the three years hence, the Bureau has often referenced the Servicer Provider Bulletin in subsequent guidance and enforcement actions, but has not provided much in the way of detailed requirements for managing service providers similar to those established by other prudential regulators for their respective supervised entities.[2] Despite the absence of strong guideposts, the CFPB has nonetheless sent unmistakable signals to highlight conduct which fails to meet the Bureau's expectations on a variety of vendor relationship issues.

The latest addition to the CFPB's loosely-sewn patchwork of vendor management guidance is Compliance Bulletin 2015-01 (the ''CSI Bulletin''),[3] which, among other directives, puts CFPB-supervised entities on notice that they may not invoke nondisclosure agreements to avoid complying with requests from the Bureau to produce a third party's confidential information. To drive home the point, the CSI Bulletin states: ''Failure to provide information required by the CFPB is a violation of law for which the CFPB will pursue all available remedies.''[4]

For nonbanks and service providers still coming up-to-speed on federal agency supervision and enforce-

[1] Consumer Fin. Prot. Bureau, CFPB Bull. No. 2012-03, *Service Providers* (Apr. 12, 2012), *available at* http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf. Note that the terms ''vendor'' and ''service provider'' are generally used interchangeably among regulators and practitioners, but the Dodd–Frank Wall Street Reform and Consumer Protection Act at 12 U.S.C. § 5481(26) employs the defined term ''service provider.''

Elizabeth McGinn is a partner and Moorari Shah is a counsel in the Washington, D.C. and LA offices of BuckleySandler LLP. They advise clients on consumer financial services, e-commerce, vendor management, and privacy-related issues.

[2] *See, e.g.*, Fed. Reserve Bd., Div. of Banking Supervision and Regulation & Div. of Consumer and Cmty. Affairs, FRB Supervisory Letter No. SR 13-19 (Attachment), *Guidance on Managing Outsourcing Risk* (Dec. 5, 2013), *available at* http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf; Office of the Comptroller of the Currency, OCC Bull. No. 2013-29, *Third-Party Relationships: Risk Management Guidance* (Oct. 30, 2013), *available at* http://occ.treas.gov/news-issuances/bulletins/2013/bulletin-2013-29.html; Fed. Deposit Ins. Corp., FDIC Letter No. FIL-44-2008, *Third-Party Risk: Guidance for Managing Third Party Risk* (June 6, 2008), *available at* https://www.fdic.gov/news/news/financial/2008/fil08044.pdf; Fed. Reserve Bank of N.Y., *Outsourcing Financial Services Activities: Industry Practices to Mitigate Risk* (Oct. 1999), *available at* http://www.newyorkfed.org/banking/circulars/outsource.pdf.

[3] Consumer Fin. Prot. Bureau, CFPB Compliance Bull. No. 2015-01, *Treatment of Confidential Supervisory Information* (Jan. 27, 2015), *available at* http://files.consumerfinance.gov/f/201501_cfpb_compliance-bulletin_treatment-of-confidential-supervisory-information.pdf.

[4] *Id.* at 5.

 ISSN 0891-0634

ment, the CSI Bulletin — while not exclusively directed at vendor relationships — presents another wrinkle in the ongoing effort to meet compliance obligations arising in the context of service provider contracts. Read in conjunction with the CFPB's public enforcement actions and other guidance touching upon vendor management, a pattern appears to be emerging regarding the Bureau's preference for the inclusion of certain contractual language in vendor agreements. As explored in further detail below, confidentiality obligations, audit rights, vendor training responsibilities, and remedies for vendor breaches are among the more thorny agreement provisions that may need to be enhanced in light of developing trends.

Confidentiality

The typical confidentiality section in a vendor contract precludes either party from disclosing or using the other party's confidential information, except as necessary to perform or receive the benefit of the procured services. If either party becomes legally compelled to disclose the other's confidential information through a subpoena or other legal process, most vendor contracts require, at a minimum, prompt notification to the other party and reasonable assistance in opposing such disclosure or in seeking a protective order to limit the disclosure or use by the party or governmental agency compelling production.

Read in conjunction with the CFPB's public enforcement actions and other guidance touching upon vendor management, a pattern appears to be emerging regarding the Bureau's preference for the inclusion of certain contractual language in vendor agreements.

The CSI Bulletin, however, effectively rewrites the standard confidentiality clause in much the same way a court might invoke the ''blue pencil'' rule to strike or modify an unreasonable restriction in an agreement between litigating parties.[5] The CFPB may compel disclosure of a third party's confidential information regardless of contractual obligations to the contrary and without permitting an opportunity to oppose disclosure or seek other recourse. Moreover, the CSI Bulletin reminds supervised entities that even disclosing the mere fact that a third party's confidential information has been provided to the Bureau can be neither revealed, confirmed, nor denied, absent prior written approval of the CFPB.[6]

As heavy-handed as the CFPB's approach appears, it is worth noting that regulated banks have operated under similar constraints long before the CFPB came into existence.[7] Therefore, perhaps the primary, but hardly novel, takeaway from the CSI Bulletin is that the Bureau shows no signs of relenting in its pursuit to level the playing field between bank and nonbank regulation. In terms of specific actions to be taken, the CSI Bulletin tacitly but clearly presses supervised entities to review confidentiality clauses in standard vendor contracts, as well as information-sharing policies and procedures generally. To that end, and to avoid potential breach claims and litigation, financial institutions may want to contemplate in their vendor contracts the potential for required document production to regulators without notice to the party whose confidential information is being revealed.[8] In addition, the practice of maintaining an up-to-date log of confidential and sensitive information (*e.g.*, non-public personal information) shared with third parties has become a common expectation of regulators, inclusive of contractual procedures to ensure the prompt return and/or destruction of such information once its need to render services has ended.[9] Suffice it to say that adhering to such protocols, and explicitly requiring vendors to do the same throughout the contractual relationship and beyond, is likely to prove beneficial during the course of regulatory examinations.

Audit Rights

The CFPB's repeated reprimands of supervised entities for failing to monitor vendors also signal the potential need for more contractual consideration in setting ''appropriate and enforceable consequences for violating any compliance-related responsibilities.''[10] In particular, red flags are likely to be raised by the omission of audit rights in agreements with any critical service provider to a financial institution. Such rights generally permit periodic review and confirmation of a vendor's observance of compliance responsibilities set forth in the contract. Note also that a supervised entity's failure to perform onsite audits where warranted may expose the *service provider* to direct examination by regula-

[5] The blue-pencil test is a judicial standard for deciding whether to invalidate the whole contract or only the offending words. Under this standard, only the offending words are invalidated if it would be possible to delete them simply by running a blue pencil through them, as opposed to changing, adding, or rearranging words. *Black's Law Dictionary* 1921 (10th ed. 2014).

[6] *See* CFPB Compliance Bull. No. 2015-01, *supra* note 3, at 5 (stating ''a supervised financial institution may risk violating the law if it relies upon provisions of [a non-disclosure agreement] to justify disclosing [confidential supervisory information] in a manner not otherwise permitted'').

[7] *See, e.g.*, 12 C.F.R. § 261.20(g) (making disclosure of confidential supervisory information subject to approval by the applicable prudential regulator).

[8] Note that the Bureau's position is in line with the OCC's guidance, which sets forth the expectation for service provider contracts to stipulate that the performance of activities by service providers ''is subject to OCC examination oversight, including access to all work papers, drafts, and other materials.'' OCC Bull. No. 2013-29, *supra* note 2.

[9] *See, e.g.*, Consent Order at 16, *In re JPMorgan Chase Bank, N.A., Columbus, Ohio*, No. AA-EC-13-76 (OCC Sept. 18, 2013) (identifying third party management policies and procedures to be followed including transfers of original records).

[10] CFPB Bull. No. 2012-03, *supra* note 1, at 3.

  BBR ISSN 0891-0634

tors.[11] The Bureau's emphasis in this area raises two key contract issues.

First, typical vendor agreements include a requirement that the vendor ''comply with all laws'' – a nice catch-all but likely insufficient in and of itself to establish ''clear expectations about compliance'' in the eyes of regulators.[12] For example, the CFPB's allegations against a telecommunications provider in December 2014 stated that such a contract clause may provide ''breach-of-contract remedies, but did little to protect customers'' that were unfairly charged for services without prior authorization.[13] According to the Bureau's complaint, the failure to specify compliance-related responsibilities and the lack of oversight created ''blind spots'' for the telecommunications provider, which enabled vendors to add unauthorized charges onto customer bills.[14] The CFPB's assessment that the contracts entered into with service providers were inadequate is indicative of growing regulatory scrutiny of vendor contracts to identify important laws and regulations applicable to the services being provided, and also to specify the procedures to be followed and remedial actions to be taken should a violation occur during the provision of services.[15]

. . . [T]he Bureau has frequently voiced its dissatisfaction with supervised entities that fail to create sufficient contractual and operational structure to enforce such audit rights.

Second, the CFPB has been steadfast in requiring as part of its enforcement actions that vendor contracts contain rights for financial institutions to conduct periodic onsite audits to verify that vendors are actually carrying out their compliance obligations.[16] To be sure, audit rights are not a new concept for outsourcing arrangements. The right to audit has been a standard contract fixture for more than a decade since the passage of the Sarbanes-Oxley Act, which, in pertinent part, required public companies to certify that adequate controls were in place to safeguard the accuracy and integrity of financial data, including data derived from third-party systems.[17] Typically, therefore, audit sections in vendor contracts cover an obligation for vendors to maintain complete and accurate records of services rendered, which is subject to audit by an independent auditor at least once per year. Such an audit right, however, may not be sufficient to meet current regulatory expectations, even if considered ''market'' for certain outsourcing contracts.[18] To wit, the Bureau has frequently voiced its dissatisfaction with supervised entities that fail to create sufficient contractual and operational structure to enforce such audit rights:

> Where such situations have occurred, the CFPB has directed financial institutions to develop and implement a comprehensive program that ensures the service providers' compliance with Federal consumer financial law. Such programs typically include consistent, risk-based procedures governing the retention and monitoring of service provider relationships, as well as policies and procedures to monitor and test for compliance with Federal consumer financial law by service providers acting on behalf of the financial institution[19].

Recent enforcement actions show no weakening of the CFPB's resolve in this regard, typically requiring robust contractual audit rights oriented to focus on compliance with consumer protection laws, and detailed internal policies and procedures to facilitate periodic reviews at the service providers' places of business.[20]

Vendor Training

Further evidence of the Bureau's attentiveness to specific terms and conditions of vendor contracts is appar-

[11] *Id.* at 2 (noting that ''[The Dodd-Frank Act] also grants the CFPB supervisory and enforcement authority over supervised service providers, which includes the authority to examine the operations of service providers on site'').

[12] *Id.* at 3.

[13] Complaint ¶ 22, *Consumer Fin. Prot. Bureau v. Sprint Corp.*, No. 14-cv-9931 (S.D.N.Y. Dec. 17, 2014), ECF No. 1.

[14] *Id.* ¶ 23.

[15] *See, e.g.*, Stipulated Order for Permanent Injunction and Monetary Judgment, *F.T.C. v. T-Mobile USA, Inc.*, No. 2:14-cv-00967-JLR (W.D. Wash. Dec. 22, 2014), ECF No. 18 (requiring a telecommunications provider to establish a process for refunding unauthorized charges incurred by customers as part of $90 million settlement reached with the Federal Trade Commission); Stipulated Order for Permanent Injunction and Monetary Judgment, *F.T.C. v. AT&T Mobility, LLC*, No. 1:14-cv-3227-HLM (N.D. Ga. Oct. 8, 2014), ECF No. 2 (requiring a telecommunications provider to resolve allegations that the company billed customers for unauthorized third-party charges, a practice known as ''mobile cramming,'' as part of a joint Federal Trade Commission, Federal Communications Commission, and State Attorney General's $105 million settlement).

[16] *See, e.g.*, Consent Order ¶ 21(b)(iii), *In re U.S. Bank Nat'l Assoc.*, No. 2014-CFPB-0013 (CFPB Sept. 25, 2014), ECF No. 1 [hereinafter ''U.S. Bank Consent Order''] (requiring that written contracts entered into with service providers grant authority to the supervised entity to conduct periodic onsite reviews of the service provider's controls, performance, and information systems).

[17] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (requiring, under Section 404, publication in annual reports of information concerning the scope and adequacy of internal control structure and procedures for financial reporting, as well as attestation from an external auditor in regards to the effectiveness of internal controls and procedures).

[18] *See, e.g.*, OCC Bull. No. 2013-29, *supra* note 2 (''A bank should include in the contract the types and frequency of audit reports the bank is entitled to receive from the third party (e.g., financial, SSAE 16, SOC 1, SOC 2, and SOC 3 reports, and security reviews). . . . Audit reports should include a review of the third party's risk management and internal control environment as it relates to the activities involved and of the third party's information security program and disaster recovery and business continuity plans.'').

[19] Consumer Fin. Prot. Bureau, *Supervisory Highlights: Fall 2012* 5 (Oct. 31, 2012), *available at* http://files.consumerfinance.gov/f/201210_cfpb_supervisory-highlights-fall-2012.pdf.

[20] *See, e.g.*, U.S. Bank Consent Order, *supra* note 16, ¶ 21(c); Consent Order ¶ 29(f), *In re Am. Express Centurion Bank, Salt Lake City, Utah*, No. 2012-CFPB-0002 (CFPB Oct. 1, 2012) [hereinafter ''American Express Consent Order'']; Consent Order ¶ 44(c), *In re Synchrony Bank*, No. 2014-CFPB-0007 (CFPB June 19, 2014), ECF No. 1; Consent Order ¶ 20(c), *In re JP Morgan Chase Bank, N.A.*, No. 2013-CFPB-0007 (CFPB Sept. 19, 2013), ECF No. 1.

ent in expectations related to vendor training programs. The Service Provider Bulletin states that supervised institutions should request and review ''the service provider's policies, procedures, internal controls, and training materials to ensure that the service provider conducts appropriate training and oversight of employees or agents that have consumer contact or compliance responsibilities.''[21] On the surface, the guidance appears to be focused on due diligence performed on vendors *prior* to contract execution. However, the CFPB has insisted in several enforcement actions subsequent to issuance of the Service Provider Bulletin that vendor contracts themselves contemplate training for service provider personnel in applicable consumer protection laws.[22] In fact, the CFPB has even gone so far as to require supervised entities to develop policies and procedures to deliver training directly to service providers regarding compliance with consumer protection laws.[23]

Simply put, requiring vendors to maintain updated training materials, while good practice, may not insulate covered entities from regulatory fines that arise as a result of vendor's failure to comply with applicable laws and regulations.

While regularly vetting vendor training materials may seem to be a natural extension of vendor oversight procedures, the burden on supervised entities and their service providers could become a significant imposition on the overall relationship. For instance, depending on the integration necessary to ensure that existing service provider systems and processes appropriately incorporate applicable legal and regulatory requirements, the development and delivery of training materials may, in some cases, require extensive joint efforts by the financial institutions and their service providers, regardless of typical contractual provisions that assign this responsibility to vendors. After all, a logical next step to requiring vendors to maintain adequate training materials is the ability to review such materials as part of regular audits and dictate changes to content to ensure compliance with the then-current state of consumer protection laws and regulations. Furthermore, to the extent violations of consumer financial laws do occur on the vendor's watch, indemnification clauses designed to protect supervised entities from vendor failures in this regard are often nullified by another common feature in CFPB enforcement cases: Supervised entities subject to consent orders in a number of instances have not been able to seek reimbursement or indemnification from any source (including insurance policies) with regard to civil money penalties imposed for legal violations, even if the violations are purely the fault of the service provider.[24]

What appears then at first blush to be a rather straight-forward task of obligating vendors to maintain training materials may, in fact, require fundamental changes to contractual responsibilities to develop and enhance training materials depending on the scope of services and potential for consumer harm. Moreover, while indemnification and limitation of liability provisions in vendor contracts may help financial institutions avoid liability for legal violations committed by vendors *vis à vis* other third parties, such provisions will not necessarily provide complete protection to financial institutions. Simply put, requiring vendors to maintain updated training materials, while good practice, may not insulate covered entities from regulatory fines that arise as a result of vendor's failure to comply with applicable laws and regulations.[25] As such, a vendor's contractual obligation to maintain training materials and educate employees to comply with consumer protection laws may need to be customized and enhanced based on the particular risks attendant to the services provided. In addition, supervised entities may be well-advised to maintain the right to closely monitor service providers in their training efforts to ensure that the vendors have the wherewithal to adequately develop and provide such training throughout the term of the agreement.

System Warranties, Remedies

Based on the foregoing review of CFPB enforcement actions involving vendors, it may seem that the Bureau is focused primarily on vendors that directly interface with customers as they likely represent the highest risk for violations of consumer protection laws. In particular, mortgage servicing companies, debt collection agencies, and product marketing companies have all generated considerable focus from the CFPB.[26] Unfortunately, just as great a risk for consumer harm may lie with vendors that never actually interact with the customer at all, such as large technology service providers (''TSPs'') that store and process large amounts of sensitive customer information and regularly transmit such information to other systems and service providers. The

[21] CFPB Bull. No. 2012-03, *supra* note 1, at 3.

[22] *See, e.g.*, Stipulation and Consent Order ¶ 34(b)(ii), *In re Capital One Bank, (USA) N.A.*, No. 2012-CFPB-0001 (CFPB July 18, 2012); U.S. Bank Consent Order, *supra* note 16, ¶¶ 21(b)(ii), 21(g).

[23] *See, e.g.*, American Express Consent Order, *supra* note 20, ¶ 29(h).

[24] *See, e.g.*, U.S. Bank Consent Order, *supra* note 16, ¶ 49(b).

[25] *See Supervisory Highlights: Fall 2012*, *supra* note 19, at 5 (stating ''[d]epending upon the circumstances, responsibility for legal violations by a service provider may lie with the financial institution as well as with the service provider'').

[26] *See, e.g.*, Consumer Fin. Prot. Bureau, CFPB Bull No. 2012-06, *Marketing of Credit Card Add-On Products* § C (July 18, 2012), *available at* http://files.consumerfinance.gov/f/201207_cfpb_bulletin_marketing_of_credit_card_addon_products.pdf; Consumer Fin. Prot. Bureau, CFPB Bull. No. 2013-07, *Prohibition of Unfair, Deceptive, or Abusive Acts or Practices in the Collection of Consumer Debts* § C (July 10, 2013), *available at* http://files.consumerfinance.gov/f/201307_cfpb_bulletin_unfair-deceptive-abusive-practices.pdf; Consumer Fin. Prot. Bureau, CFPB Bull. No. 2014-01, *Compliance Bulletin and Policy Guidance: Mortgage Servicing Transfers* § A (Aug. 19, 2014), *available at* http://files.consumerfinance.gov/f/201408_cfpb_bulletin_mortgage-servicing-transfer.pdf.

  BBR ISSN 0891-0634

CFPB's enforcement action against a nonbank finance company ostensibly provides a case-in-point.[27]

The Bureau alleged in August 2014 that a Texas-based auto finance company ''showed careless disregard for its customers' financial lives by knowingly distorting their credit profiles for years.''[28] The CFPB's allegation suggests brazen illegality on the part of the auto finance company. In fact, however, the conduct in question was largely the result of flaws in a TSP's computer system that the auto finance company had relied upon to report consumer credit information to credit reporting agencies.[29] True to its word that it would hold supervised entities responsible for legal violations caused by vendors, CFPB Director Richard Cordray in comments about the action stated, ''[C]ompanies cannot pass the buck by blaming a computer system or vendor for their mistakes.''[30]

True to its word that it would hold supervised entities responsible for legal violations caused by vendors, CFPB Director Richard Cordray in comments about the action stated, "[C]ompanies cannot pass the buck by blaming a computer system or vendor for their mistakes."

Once again, the fact that the contract actually permitted the company to assign blame to the TSP for flaws in its system, as many technology-based contracts do, was of no consequence to the CFPB. Under the consent order, the auto finance company could not avail itself of warranty or indemnification provisions to hold the TSP accountable for fundamental system flaws.[31] Interestingly, the Bureau also contended that the ''Respondent's failure to require its *service provider to correct the issues causing inaccuracies within a reasonable time once Respondent learned of them* all demonstrate Respondent's failure to implement reasonable policies and procedures regarding the accuracy and integrity of the information relating to consumers that it furnishes to a consumer reporting agency . . . .'' (emphasis added).[32]

The CFPB's posture in this case suggests, at a minimum, its expectation of increased vigilance on the part of supervised financial institutions in negotiating warranties related to system compliance with consumer protection laws. Moreover, supervised entities may want to consider insisting upon prompt repair guarantees to the extent programming errors are identified after contract execution and adversely impact consumers. Finally, depending on the criticality of the system and the potential for shortcomings in complying with consumer protection laws, financial institutions may need to give additional thought to triggering termination and transition rights in the event a TSP is not able to promptly remedy system flaws. Of course, seeking such contractual protections can make for difficult negotiations, and TSPs that provide mission-critical software and systems often have significant leverage to resist such demands. To that end, although the Bureau did not take action against the service provider in the case of the auto finance company, the CFPB's ability to do so[33] may be the best bargaining chip that financial institutions have to secure durable warranties and prompt remediation of system flaws in negotiations with TSPs.[34]

Conclusion

The CFPB's continued focus on vendor management has increasingly shown a pattern of prescribing more exacting terms and conditions in service contracts to protect consumers from unwarranted harm. In much the same fashion that courts have historically invoked the blue-pencil rule to modify contracts, recent guidance and enforcement actions signal the Bureau's willingness to disregard rights and obligations negotiated at arms-length by sophisticated parties, thereby forcing supervised entities to re-think standard provisions in vendor contracts.

[27] Consent Order, *In re First Investors Fin. Servs. Grp., Inc.*, No. 2014-CFPB-0012 (CFPB Aug. 20. 2014), ECF No. 1 [hereinafter ''First Investors Consent Order''].

[28] Press Release, Consumer Fin. Prot. Bureau, *CFPB Takes Action Against Auto Finance Company for Distorting Borrower Credit* (Aug. 20, 2014), http://www.consumerfinance.gov/newsroom/cfpb-takes-action-against-auto-finance-company-for-distorting-borrower-credit-reports/.

[29] First Investors Consent Order, *supra* note 27, ¶¶ 11-27.

[30] *See* Press Release, *supra* note 28.

[31] First Investors Consent Order, *supra* note 27, ¶ 43(b) (not permitting target to seek indemnification per contract or use insurance proceeds to pay civil money penalties).

[32] *Id.* ¶ 32.

[33] *See* 12 U.S.C. §§ 5531(a), 5536.

[34] *See, e.g., Agreement By and Between Jack Henry & Associates, Inc. and the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Federal Reserve Bank of St. Louis*, No. 2013-181 (OCC Dec. 4, 2013) (subjecting a TSP to a formal agreement with federal regulators to resolve allegations of unsafe and unsound practices relating specifically to the software company's disaster recovery and business continuity planning and processes. The enforcement action resulted from delays caused by the TSP in reestablishing full operations at its New Jersey processing center that was shut down in the wake of Hurricane Sandy in 2012); Consent Order ¶ 20, *In re Dealers'Fin.Servs., LLC, Lexington, Ky.*, No. 2013-CFPB-0004 (CFPB June 25, 2013) (establishing the CFPB's jurisdiction over an ancillary product provider that marketed and sold auto GAP coverage to customers of a financial institution); Consent Order ¶ 6, *In re Cont'l Fin. Co., LLC*, No. 2015-CFPB-0003 (CFPB Feb. 4, 2015) (asserting the CFPB's jurisdiction over credit card originator, marketer, and servicer as both a ''covered person'' and ''service provider'' under the Dodd-Frank Act).