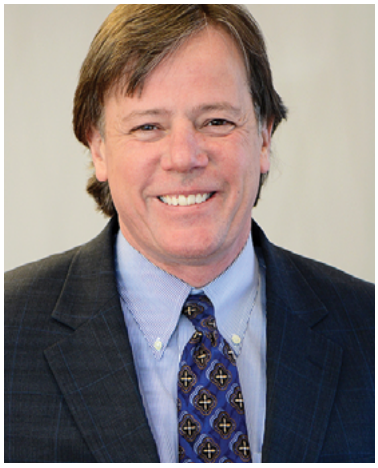
GOVERNMENT WATCH

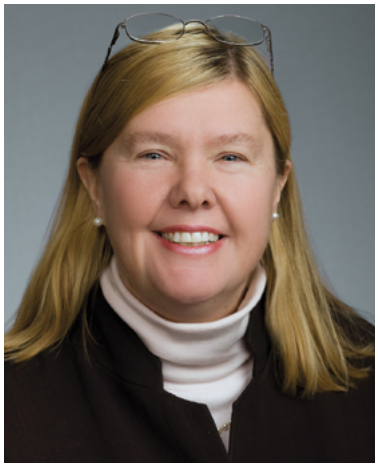
VIEWPOINT

Attention Banks and Vendors: DON'T FORGET THE CONTRACT

For banks and their third-party vendors, it's crucial to have a solid contract. Or, at least it's crucial if they want to avoid the ire of regulators and fines that could reach into the billions. In this article, two top financial services lawyers share their advice for crafting bank/vendor agreements that will withstand the scrutiny of regulators that are targeting vendor risk management and oversight by ensuring banks' contracts with third parties are clear, effective and leave no doubt about where the buck stops.



By John ReVeal, Bryan Cave



By Judith Rinearson, Bryan Cave

In Viewpoints, prepaid and emerging payments professionals share their perspectives on the industry. Paybefore endeavors to present many points of view to offer readers new insights and information. The opinions expressed in Viewpoints are not necessarily those of Paybefore.

First there was the bulletin about third-party vendors issued by the CFPB in April 2012.[1] Next, it was the FFIEC's guidance on IT service providers in October 2012,[2] followed by the FDIC's September 2013 Financial Institution Letter about payment processing relationships with high-risk merchants.[3] Then, there was the news on Oct. 30, 2013, about the OCC's Guidance on Third-Party Relationships,[4] followed shortly by the Federal Reserve Board's Guidance on Managing Outsourcing Risks in December 2013.[5]

Whew!

Let's face it, there always have been concerns about banks and their relationships with third-party service providers. Banks were expected to choose their vendors carefully and monitor their performance faithfully. And, most banks have done a reasonably good job in this regard—most of the time. As time passed, regulators raised the bar by degrees regarding banks' relationships with their third-party processors, program managers and other service providers. And, banks and vendors adapted to the gradual increased scrutiny.

But since the OCC's Guidance on Third-Party Relationships was issued last October, it's increasingly clear we're experiencing a sea change in how regulators approach the relationships between banks and their third-party vendors. Recent regulatory publications, examinations and enforcement actions suggest that the standards and expectations by which regulators evaluate banks' third-party relationships now are significantly more exacting. They're digging deeper on how banks select their third-party vendors, and the scope of their review is extending to more and more vendors.

This increased focus makes it critically important for banks and their partners to get their relationships right from the start by setting their own appropriate expectations and establishing standards for oversight, access and follow through.

And, the contract is the key.

Condor 36/Shutterstock.com

Attention Banks and Vendors: Don't Forget the Contract

Recent Regulatory Developments

The CFPB's Bulletin 2012-03 issued in April 2012 indicates that the CFPB "expects supervised banks and nonbanks to oversee their business relationships with service providers in a manner that *ensures compliance* with federal consumer financial law" (emphasis added). The accompanying press release, "CFPB to Hold Financial Institutions and their Service Providers Accountable," summarized the CFPB's position with those 10 words.

The FDIC's September 2013 letter focused on banks that facilitate payment processing services, either directly *or* through a third party, for merchant customers engaged in "higher-risk activities." Again, the regulators reinforced the position that banks not only are expected to perform proper risk assessments and conduct due diligence, but they are expected to determine whether "merchant customers are operating in accordance with applicable law." That's a significant responsibility and difficult to achieve—especially when there's a third party involved.

In October 2013, the OCC published Risk Management Guidance regarding third-party relationships, OCC Bulletin 2013-29. The bulletin is broader in scope than the CFPB's, because it focuses on all "third-party relationships involving critical activities," a concept addressed below, *in addition to* consumer protection.

Following suit, the Federal Reserve issued its guidance in December 2013 that almost echoed the OCC bulletin point for point. Other than the fact that the CFPB focuses on consumer products and services and the OCC and Fed approach vendor risk management more broadly, the bulletins issued by the three regulators show similar regulatory expectations, including:

- Thorough due diligence of the service provider, which the OCC notes could call for on-site visits depending on the risks of the relationship.
- Clear contractual expectations for the service provider, including enforceable consequences for violating contractual requirements (see more below).
- Establishment and maintenance of internal controls and ongoing monitoring of the service provider.

Bank Board and Management Requirements

The OCC and Fed bulletins are detailed and include significantly more strongly stated expectations of the bank's board and management. In fact, the OCC stated that "a bank's failure to have an effective third-party risk management process … may be an unsafe and unsound banking practice."[6] For example, under the OCC's guidance, a supervised bank's board of directors has the following specific responsibilities:

- Ensure an effective process is in place to manage risks

CFPB BULLETIN RECAP

The CFPB bulletin applies to "supervised banks and nonbanks." CFPB-supervised banks are all banking institutions and their affiliates with total assets exceeding $10 billion. CFPB-supervised nonbanks are certain nonbank businesses, regardless of size, that do business in the following markets: mortgages (originators, brokers, and servicers, and loan modification or foreclosure relief services); payday lenders; and private education lenders.

cfpb Consumer Financial Protection Bureau

The CFPB also supervises all nonbanks that are "larger participants" with respect to other consumer financial products or services as determined by the CFPB. The "service providers" of concern are those persons that provide a material service to a covered institution in connection with the offering or providing of a consumer financial product or service.

According to the CFPB bulletin, the CFPB expects all of its supervised banks and nonbanks to have an effective process for managing the risks of service provider relationships. It's very important to note that the CFPB intends to apply these standards even if the supervised bank or nonbank doesn't have a direct relationship with the service provider. This would seem to mean that a bank or nonbank is responsible for its vendor's service providers if those service providers perform a material service relating to the bank's or nonbank's consumer products or services. Similarly, the OCC and Fed expect a bank's contract with its third-party vendors to address the third-party's use of subcontractors and the responsibilities for and monitoring of those subcontractors.

Attention Banks and Vendors: Don't Forget the Contract

related to third-party relationships in a manner consistent with the bank's strategic goals, organizational objectives and risk appetite.

- Approve the bank's risk-based policies that govern the third-party risk management process and identify critical activities.
- Review and approve management's plans for using third parties that involve critical activities.
- Review summary of due diligence results and management's recommendations to use third parties that involve critical activities.
- Approve contracts with third parties that involve critical activities.
- Review the results of management's ongoing monitoring of third-party relationships involving critical activities.
- Ensure management takes appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring.
- Review results of periodic independent reviews of the bank's third-party risk management process.

Contractual Requirements

The OCC bulletin also includes a comprehensive list of issues the OCC expects to be addressed in each bank's contracts with its third-party vendors. If your company provides services to a bank, don't be surprised when the bank demands these contractual provisions, even if they weren't required before.

Matters the OCC will expect banks to include in their contracts are:

Nature and scope of arrangement. Contracts for complicated or highly technical services have not always included the detail that now is expected. Future contracts need to be absolutely clear on issues, such as the specific nature and scope of the arrangement; the frequency, content, and format of the service, product or function to be provided; where the services are to be performed; and the use of the bank's information, facilities, personnel, systems and equipment, as well as access to and use of the bank's or customers' information.

Performance measures or benchmarks. Contracts should specify clear and verifiable performance measures. The bulletin notes that such measures can be used to motivate the third party's performance, penalize poor performance or reward outstanding performance.

Responsibilities for providing,receiving and retaining information. Ensure that the contract requires the third party to provide and retain timely, accurate and comprehensive information, such as records and reports that enable bank management to monitor performance, service levels and risks. The contract also should stipulate the frequency and type of reports required, including, for example, performance reports, control audits, financial statements, security reports, BSA/AML and Office of Foreign Asset Control (OFAC) compliance responsibilities and reports for monitoring potential suspicious activity, reports for monitoring customer complaint activity and business resumption testing reports.

In addition, the contract should address the responsibilities and reports regarding such matters as catastrophic events, data loss, service or systems interruptions, significant changes to the vendor's systems or key personnel, and significant business changes such as result from changes in ownership, among other things.

The right to audit and require remediation. The contract should ensure that the bank has a right to audit, monitor performance and require remediation when issues are identified. For certain types of services, such as technology services, the audits should specifically address applicable technology and security standards. Audit reports also 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.

Responsibility for compliance with applicable laws and regulations. The contract must address compliance with the specific laws, regulations, guidance and self-regulatory standards applicable to the activities involved and clearly specify the parties' respective obligations for compliance.

Costs and compensation. The contract must be clear on all aspects of costs and compensation, including which party is responsible for costs of system changes necessitated by changes in laws or other circumstances and costs for audits and similar requirements.

Ownership and license. The contract should clearly address each party's rights to use the information, technology and intellectual property of the other and include appropriate warranties on the part of the third party related to its ac-

Attention Banks and Vendors: Don't Forget the Contract

quisition of licenses for use of any intellectual property developed by other third parties. If the bank purchases software, establish escrow agreements to provide for the bank's access to source code and programs under certain conditions (e.g., insolvency of the third party).

Confidentiality and integrity.
A contract must prohibit the third party and its subcontractors from using or disclosing the bank's information, except as necessary to provide the contracted activities or comply with legal requirements. If the third party receives bank customers' personally identifiable information, the contract should ensure that the third party implements and maintains appropriate security measures to comply with privacy regulations and regulatory guidelines.

Business resumption and contingency plans.
The contract must provide for continuation of the business function in the event of problems affecting the third party's operations, including degradations or interruptions resulting from natural disasters, human error or intentional attacks. The contract also should require the third party to provide the bank with operating procedures to be carried out in the event business resumption and disaster recovery plans are implemented. Include specific time frames for business resumption and recovery that meet the bank's requirements and, when appropriate, regulatory requirements.

Indemnification.
A contract must carefully assess indemnification clauses that require the bank to hold the third party harmless from liability.

Insurance.
A contract must require the third party to maintain adequate insurance, notify the bank of material changes to coverage and provide evidence of coverage, where appropriate.

Dispute resolution.
Consider whether the contract should establish a dispute resolution process (arbitration, mediation or other means) to resolve problems between the bank and the third party in an expeditious manner and whether the third party should continue to provide services to the bank during the dispute resolution period.

"Banks must recognize that if regulators' concerns about contract terms aren't dealt with according to the standards expressed in the recent OCC and Fed bulletins, they might face harsh examinations when existing and new arrangements are reviewed."

Limits on liability.
Determine whether the contract limits the third party's liability and whether the proposed limit is in proportion to the amount of loss the bank might experience because of the third party's failure to perform or to comply with applicable laws. While not specifically stated in the OCC bulletin, we suggest caution in agreeing to terms that cap liability based on the amount of fees paid.

Default and termination.
Of course, every contract should be clear on what constitutes an event of default, the remedies for such default and the consequences of termination of the contract. The OCC bulletin also states that the bank should determine whether the contract includes a provision that enables the bank to terminate the contract, upon reasonable notice and without penalty, in the event that the OCC formally directs the bank to terminate the relationship.

Customer complaints.
Specify whether the bank or third party is responsible for responding to customer complaints, how complaints are handled and how complaint information is provided to the bank.

Subcontracting.
If the vendor will be allowed to use subcontractors, specify the activities that can or cannot be subcontracted and address the third party's liability for activities or actions by its subcontractors and which party is responsible for the costs and resources required for any additional monitoring and management of subcontractors. Reserve the right to terminate the contract without penalty if the third party's subcontracting arrangements do not comply with the terms of the contract.

Foreign-based third parties.
If your vendor is based in a foreign country, be sure to address choice-of-law and jurisdictional matters. And, if your bank is not familiar with the laws of the foreign country, seek appropriate legal guidance before entering into the contract.

OCC supervision.
All contracts with service providers should provide federal bank regulators with access to the service provider, including access to all work papers, drafts and other

Attention Banks and Vendors: Don't Forget the Contract

materials. The OCC generally has the authority to examine and regulate the functions or operations performed or provided by third parties to the same extent they were performed by the bank itself on its own premises.

Practical Advice and Next Steps

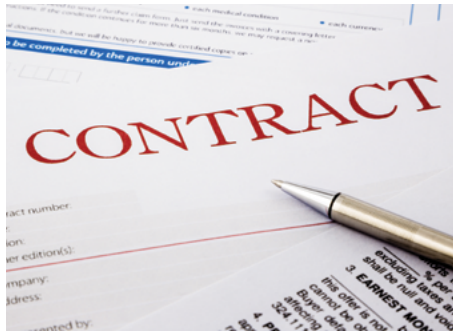
We've had the opportunity to share concerns with and ask questions of OCC staff in Washington, D.C., on a number of occasions. During those conversations, the OCC staff suggested that regulatory expectations of banks haven't actually changed, while acknowledging that their focus going forward will be on contractual relationships between banks and their third-party vendors, including contracts entered into *prior* to the OCC bulletin. That may seem like business as usual to the regulators, but—for many banks—the focus on contracts—especially preexisting contracts—seems like a new and difficult aspect of regulation and regulatory review. And banks must recognize that if regulators' concerns about contract terms aren't dealt with according to the standards expressed in the recent OCC and Fed bulletins, they might face harsh examinations when existing and new arrangements are reviewed.

In that regard, the OCC noted that each bank should do the following:

- Prioritize their review of existing third-party relationships, focusing on those involving critical activities.
- Review each contract to ensure that critical terms described above are addressed, including:
  - Clear expectations about compliance, as well as appropriate and enforceable consequences for violating any compliance-related responsibilities;
  - Rights to audit the vendor at reasonable times and with reasonable frequency for compliance with the contract and compliance related responsibilities; and
  - Rights to terminate contracts for material violations.
- Amend or update any contracts that fall short of these standards.
- For contracts that cannot be renegotiated or amended, a bank will need to "step up its risk management game internally," i.e., until such time that necessary contractual protections can be added, the bank will need to increase monitoring and other oversight activities to address the higher risk.

As noted above, the OCC bulletin purports to focus on third-party relationships involving "critical activities." What this might mean in practice is anybody's guess, and the OCC's judgment ultimately will determine that. But, the OCC bulletin itself states that critical activities include: "significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology) or other activities that:

- Could cause a bank to face significant risk if the third party fails to meet expectations.
- Could have significant customer impacts.
- Require significant investment in resources to implement the third-party relationship and manage the risk.



- Could 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."

With this broad definition, if a bank ultimately is embarrassed or criticized by customers or the media for activities performed by a third party, virtually any activity that previously seemed non-critical could, with hindsight, later be deemed to have been "critical." In the meantime, banks have few options but to comply with these high standards with respect to third-party processors, service providers and vendors.

John ReVeal *and* ***Judith Rinearson****, who lead Bryan Cave's payments group, are partners in the firm's Washington, D.C., and New York City offices, respectively.* *They would like to gratefully acknowledge the assistance of Karen Louis, an associate in Bryan Cave's Atlanta office, in reviewing and finalizing this article.* *John and Judith may be reached at john.reveal@bryancave.com and judith.rinearson@bryancave.com.*

ENDNOTES

1 www.consumerfinance.gov/newsroom/consumer-financial-protection-bureau-to-hold-financial-institutions-and-their-service-providers-accountable/

2 www.ffiec.gov/press/pr103112.htm

3 www.fdic.gov/news/news/financial/2013/fil13043.html

4 www.occ.treas.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

5 www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf

6 www.occ.treas.gov/news-issuances/bulletins/2013/bulletin-2013-29.html