ncontracts
Risk Management Solutions

(888) 370-5552
info@ncontracts.com
www.ncontracts.com

Vendor Risk Management:
Navigating the Evolving Regulatory Landscape

By: Michael Berman, Chief Executive Officer of Ncontracts

Vendor Relationships in the Financial Industry

Community West Bancshares, a $572 million asset commercial bank located in Goleta, California, has a relationship with 70 outside companies that provide a variety of services ranging from data processing to building services and lawn care. Some, like lawn care, are important because Community West has a network of five branches north of Los Angeles that have to look neat and well-trimmed since they are the bank's face to the public. Others, like data processing, are so critical that it could not operate without them.

These third-party arrangements play a vital role in the management of all financial institutions (FIs). The main reason is that vendor relationships enable FIs to conduct business more efficiently by outsourcing activities that are necessary but hardly critical, like lawn care removal. Critical vendor relationships, including third-party IT service providers, are essential to FIs. Community FIs often lack the internal staff and security measures to protect their customers' confidential data. Very large financial institutions will have tens of thousands of such service provider relationships. Smaller organizations have many fewer outsourcing arrangements, but they are just as important.

"They [third-party vendors] are very crucial, especially in a small community banking organization. I don't have to build the infrastructure for those things," explains Community West's EVP and COO, Chuck Kohl, on outsourcing to third-party vendors.

However, as important as they are, these vendor relationships do not come without a cost, and it is more than just their fees. Five of the nation's financial regulators – the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corp. (FDIC), the National Credit Union Administration (NCUA), the Consumer Financial Protection Bureau (CFPB) and the Federal Reserve Board (FRB) – are increasing scrutiny in examinations and audits of vendor risk management. Moreover, if there's one central message that all institutions need to understand, it is this: You can outsource the function, but you cannot outsource the risk, and the regulators will hold you accountable for having strong risk management practices and policies in place just as if you performed the activity in-house.

> Community West, which has a national banking charter and is regulated by the OCC, has certainly felt the pressure in recent years to tighten control over third-party service providers. "Vendor management has received a whole lot more attention from the regulators in the last five years," says Kohl. "They expect a lot out of you now."

The Vendor Management Plan

Developing a plan to manage the relationship is often the first step in the third-party risk management process. Assigning roles and responsibilities at both the enterprise and business unit levels are essential to help meet regulatory requirements. Standard categories that provide services to financial institutions include:

- **Third-party product providers such as mortgage brokers, credit card providers, and personal lines insurance.**
- **Loan servicing firms that handle such things as flood insurance monitoring, debt collection and loss mitigation/foreclosure activities.**
- **Disclosure preparers, such as disclosure preparation software and third-party documentation preparers.**
- **Technology providers such as software vendors and website developers.**
- **Providers of outsourced bank compliance functions such as compliance audits, fair lending reviews, and compliance monitoring activities.**
- **Data processing companies, external and internal auditing services and human resource consulting.**
- **Vendors that provide a range of less critical but necessary services, for instance, janitorial companies, landscapers, and lawn services contractors, building security and maintenance.**

Federal regulators are concerned because third-party providers have the potential to cause an institution serious harm if they are allowed to operate outside of a robust risk management structure. For example, a Texas man was awarded $1.5 million in a civil suit in 2010 over abusive phone calls he received from a debt collection agency that was under contract to Bank of America Corp. The case received national attention when ABC World News with Diane Sawyer and Nightline aired reports in separate national broadcasts. Although a $1.5 million judgment was of little financial consequence to $2.1 trillion asset Bank of America, the case was an embarrassment nonetheless and damaged the reputation of the company, which does business directly with consumers in every market where the reports aired.

The ultimate nightmare scenario might be a version of what happened to the giant retailer Target Corp., which operates a nationwide chain of retail stores when hackers broke into its network in 2013 and stole credit and debit card data from 40 million accounts. The investigation later determined that the intruders gained their initial access to Target's network by first penetrating the network of Fazio Mechanical Services, an HVAC contractor that did work for Target. The hackers succeeded in stealing network credentials that gave Fazio access to Target's network, which they then used to penetrate the giant retailer's network. (Fazio had access to Target's network for electronic billing, contract submission, and project management.) The hackers later installed malware on a majority of Target's point-of-sale devices and surreptitiously collected customer account information. Target eventually agreed to pay $10 million to the customers whose data was stolen. Although the security-conscious financial services industry might have more robust cyber defenses than most retailers (or most retailers had before the highly publicized cyber-heist at Target), there's no reason to believe that a bank can also experience a breach through a vendor's access to confidential data in the same manner.

The Target case, and a subsequent data intrusion at retailer Neiman Marcus, certainly captured the attention of federal regulators and accounts for some of the increased focus placed on vendor risk management. Comptroller of the Currency Thomas Curry spoke to this issue directly when he addressed one large industry trade group in March 2014.

"Many community banks look to third-party service providers for IT services, in the area of data security, among others," Curry said. "That can be an effective tool, but while you can outsource the activity, you cannot outsource the risk. It is good because third-party relationships help you acquire and leverage the specialized expertise that you cannot afford to develop on your own. However, these relationships bring significant risk management considerations with them. Third-party relationships have to be closely monitored. Third parties can be the weak link in your information systems security and resiliency; and especially where that third party is providing security services, you'll want to make sure they are up to the task and performing to your expectations."

Curry cited other concerns as well, including "the extent to which service providers are consolidating, which means that more financial institutions are dependent upon a single vendor," and the increased reliance on foreign-based subcontractors to support critical activities. Moreover, most importantly, the comptroller said he was worried "about the access third parties have to large amounts of sensitive bank or customer data. For an industry in which reputation means everything, a single data breach involving confidential customer information can be extremely costly. Banks are particularly vulnerable to events that erode trust, and once an institution's reputation is damaged, it can take years to repair."

It is not uncommon for financial institutions to grant certain third-party service providers access to their internal networks for specific reasons. For example, ORNL Federal Credit Union, a $1 billion asset institution located in Eastern Tennessee, has outsourcing arrangements with 212 vendors. Keeping track of all those relationships is the responsibility of Wayne Hood, ORNL's senior vice president and chief legal officer. Hood works directly with the credit union's various business line managers and senior executives to track vendor contracts when they come up for renewal, perform due diligence on new or renewing contracts and keep tabs on how all those service providers are performing.

Historically, some of these vendors have had access to ORNL's internal network, but that is now perceived to be a tremendous risk given the frequency with which U.S. companies are experiencing cyber-attacks by hackers in recent years. Moreover, another part of Hood's job is to lessen that risk as much as possible. "I've been working with our IT security department to minimize the number of vendors that are allowed to go through our credit union with unrestricted access," he says.

In March 2015, National Credit Union Administration (NCUA) Chairman Deborah Matz appealed to Congress to give the NCUA the authority to scrutinize and control vendors that serve credit unions. "Vendors are such an integral part of the financial services industry," Matz said, "We feel like our hands are really tied." The NCUA provides very specific guidelines for vendor management for credit unions in Supervisory Letter Number 07-01, but it is the only federal banking regulator that does not have the muscle to examine third-party vendors.

Categorizing Vendor Risks

There are a variety of vendor risk categories that financial institutions need to be aware of beginning with compliance risk, which is the danger that a vendor might knowingly or unknowingly violate a state or federal law. Although the inappropriate action or behavior might have been the fault of the vendor, the consequences will come back to the institution. Another is reputation risk, which is a threat to the good name or standing of the institution because of the actions of a third-party. The $1.5 million judgment against Bank of America because of the actions of the debt collection agency is an example of reputation risk. Operational risk is the risk of loss from inadequate or failed internal processes, people, and systems, or from external events. An example of operational risk would be an inability to complete customer transactions because of a problem with the institution's third-party data processor.

In the context of vendor management, credit risk is the danger that a vendor can no longer fulfill the terms of the contractual arrangement or financially perform as agreed. Strategic risk arises when a vendor that is being relied upon to perform an activity critical to the performance of the institution is no longer able to do so. Transaction risk stems from the failure of a third party to perform as expected, which has an adverse impact on the institution or its customers. Cyber risk is the risk of financial loss, disruption or reputational damage resulting from the intrusion of a hacker. The Target data breach is an example of cyber risk.

Regulatory Mandates

Vendor, risk management had been the focus of U.S. regulators since at least 2004 when the Federal Financial Institutions Examination Council (FFIEC) – an interagency group comprised of the FRB, OCC, FDIC, NCUA, and CFPB – included vendor risk management in its examination manual.

> "An institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution." – As summarized by the FDIC in FIL-44-2008.

However, it was the April 13, 2012, publication of CFPB Bulletin 2012-03 that really caught the attention of the financial services community. This bulletin clearly stated that financial institutions "may be held responsible for the actions of the companies with which they contract. The Bureau will take a close look at the service providers' interactions with consumers. It will hold all appropriate companies accountable when legal violations occur." It was made very clear that ongoing oversight and close monitoring of third-party services provider activities would be expected going forward.

Each of the five regulatory agencies has issued separate guidance that applies to the institutions under their

direct supervision. (The FRB supervises bank holding companies and state-chartered banks that are members of the Federal Reserve system, the OCC oversees nationally chartered banks, the FDIC supervises state-chartered banks that are not members of the Federal Reserve, the NCUA oversees national credit unions and the CFPB is responsible for consumer protection in the financial sector, with jurisdiction over a wide range of providers including banks and credit unions.) As of March 2016, the most recent guidance to financial institutions regarding third party risk for primary federal regulator is listed below:

FRB: http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf

OCC: http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

FDIC: https://www.fdic.gov/news/news/financial/2014/fil14013.html

NCUA: http://www.ncua.gov/resources/documents/lcu2007-13enc.pdf

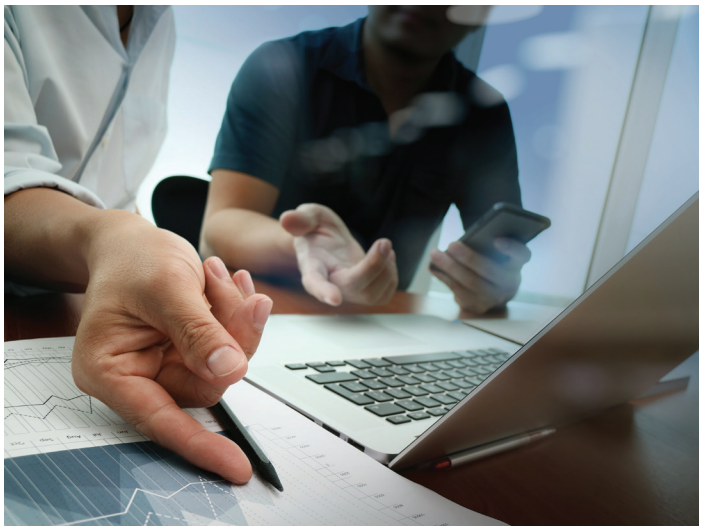
CFPB: http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf

Although each agency's mandates are somewhat different, they all advocate a similar framework for vendor risk management. These guidelines divide the process into four categories: Risk assessment, due diligence in selecting a vendor, contract structuring and review, and monitoring. The guidance also spells out the responsibilities of management and the board of directors. A review of the guidance issued by the OCC provides a precise overview of the regulatory expectations in this area. "The OCC is concerned that the quality of risk management over third-party relationships may not be keeping pace with the level of risk and complexity of these relationships," the agency said when the guidance was released. Specific shortcomings that the OCC identified include a failure to properly assess and understand the risks and direct and indirect costs involved in third-party relationships, a failure to perform adequate due diligence and ongoing monitoring of third-party relationships, entering into a contract without adequately assessing the vendor's risk management practices – or sometimes using the services of a vendor on an informal basis without a contract. Lastly, the OCC says that a national bank's vendor risk management process should fit the size and complexity of the institution and the critical nature of the activity that a third party is performing. In short, the larger and more complex the financial institution is, and the more critical the outsourced function, the more robust the risk management process needs to be.

The OCC guidance provides a framework for what it describes as the "risk management life cycle," beginning with the development of a management plan for each of the financial institution's third-party relationships, particularly those that involve a critical activity for data processing. Elements to include in this plan are:

- **A review of the risks inherent in the outsourced activity**
- **A discussion of its strategic purpose (like cutting costs, for example)**
- **An assessment of the complexity of the arrangement**
- **A determination of whether the potential financial benefits of the arrangement outweigh the costs required to control risk**
- **An assessment of potential information security implications including access to the financial institution's systems by the vendor**
- **And a contingency plan should it become necessary to terminate the relationship and engage with another vendor, or bring it in-house**

Regulatory guidance requires financial institutions to conduct a thorough due diligence of all vendors before entering into a contract. This process should not only apply to prospective new vendors, but also vendors with which the institution is currently doing business. The degree of due diligence should be commensurate with the complexity of the relationship. Critical qualifications the guidance recommends including the third party's track record of legal and regulatory compliance, its financial condition, its business experience and reputation, fee structure and incentive, and the effectiveness of its risk management processes and information security program.



Contract Negotiation

Following the selection of a third party, the financial institution's management should negotiate a contract that clearly spells out the rights and responsibilities of each party, limits the institution's liability, and each contract should receive board approval when it involves a critical activity. The contract should also include provisions for periodic independent internal or external audits, and the financial institution must be able to monitor the vendor's performance and require the remediation of any problems. The third party must agree to comply with all laws and regulations that apply to the activity involved.

Vendor Monitoring and Relationship Termination

The institution is expected to closely monitor the vendor's performance commensurate with the level of risk associated with the relationship. It is especially important to assess the vendor's internal controls, its ability to meet service-level agreements and performance metrics and compliance. Additionally, the institution should assess any significant changes to the vendor's business strategy, financial condition or key personnel essential to the activity being performed. It is important that institutions have a process in place to track all contracts as they come up for renewal so they can be reviewed and the service provider's performance evaluated. To ensure that adequate monitoring is established, management should dedicate staffing resources with the necessary expertise, authority, and accountability to monitor the third party.

Moreover, finally, the financial institution should ensure that its third-party relationships are terminated in an efficient manner, and it should have a contingency plan that spells out how the activity will be handled once the contract has been terminated, whether it be discontinued or brought in-house or transferred to another vendor. Having a well thought out exit strategy will serve to protect your company and your customers.

Governance of Vendor Risk Management

The institution's board of directors and senior management team are equally responsible for its vendor management program, although they have a different set of duties consistent with their respective roles. It is the responsibility of the board to ensure that a sound program is in place, and it should be very proactive in the case of critical outsourced activities – reviewing and approving management plans for the use of third parties to provide critical services, approving contracts for critical services and reviewing the results of all critical activity monitoring.

Management's responsibility is to develop and implement the vendor risk management program, ensure that appropriate due diligence is conducted on all third-party providers before the execution of a contract, review and approve all vendor contracts and terminate all agreements that no longer meet their performance expectations.

Ncontracts® is a leading provider of risk management software and services to financial institutions. While we started with our industry-leading vendor management platform, our portfolio offerings have evolved to feature enterprise risk management, business continuity risk management, compliance management, findings management, and cybersecurity management. More than 600 financial organizations use Ncontracts to manage risk more efficiently and effectively using our integrated suite of software and services.

ncontracts
Risk Management Solutions

(888) 370-5552
info@ncontracts.com
www.ncontracts.com