Regulatory Requirements and the Third-Party Threat

How Third Parties Increase Risk in the Financial Sector and What Organizations Can Do to Reduce Vulnerability

A LexisNexis® White Paper

Introduction

"Just as ripples spread out when a single pebble is dropped into water, the actions of individuals can have far-reaching effects." The Dalai Lama doubtless meant those words to inspire, but those words are also a good reminder of the third-party risk potential. As the financial sector has discovered with growing frequency, ripples emanating from third-party performance lapses can quickly develop into a tsunami of problems. In spring 2014, Attorney General Eric Holder announced investigations into a number of banks which enabled third-party payment processors to fraudulently remove funds from consumers' bank accounts. And Citigroup Inc., is under investigation for possible U.S. Foreign Corrupt Practices Act violations related to bad loans made by a Mexican subsidiary.[1]

Faced with an increasing number of anti-corruption regulations like the UK Bribery Act, Brazil's Clean Companies Act and Germany's Act on Combating International Bribery (IntBestG), the financial industry must conduct even deeper due diligence on third parties to ensure compliance and avoid the costly investigations, potential financial penalties and reputational damage when third parties fail to meet expectations.

While managing and monitoring risk has always been an important business practice, organizations' growing reliance on outsourcing to third parties has amplified the need—and led to an even more complex, regulatory environment. Speaking at the Risk Management Association's Governance, Compliance and Operational Risk Conference in May 2014, Thomas J. Curry, Comptroller of the Currency, noted, "One reason we feel it is so necessary to establish heightened expectations for risk management, internal audit, and governance capabilities at large institutions is that risk today, in an interconnected world, is qualitatively different—and far more difficult to manage—than it was even a few years ago."[2]

Perception or Reality— Is Risk Really on the Rise?

There are a number of trends serving to highlight the risks of outsourcing to third parties. In the last few years, a number of high-profile hacking scandals have originated from third-party providers. In fact, the 2013 Trustwave Global Security Report, which analyzed 450 global data breach investigations, found that 63 percent of the security failures could be attributed to a third-party component of IT system administration.[3] As financial organizations outsource more and more sensitive functions—customer support centers, marketing, social media or mobile banking—their risk exposure increases. Likewise, a growing number of technology solutions, such as cloud storage and Software as a Service (SaaS) used to manage and store sensitive data, multiply the risk.

Regulatory requirements are also forcing financial organizations to focus more attention on third-party relationships. In the highly competitive financial industry, third-party providers can enable organizations to achieve their strategic objectives by delivering products or services that require special expertise

[1] http://www.fiercecfo.com/story/reported-citibank-investigation-latest-vigilant-fcpa-enforcers/2014-03-03-0

[2] http://www.occ.gov/news-issuances/speeches/2014/pub-speech-2014-69a.pdf

[3] http://www2.trustwave.com/rs/trustwave/images/Trustwave_GSR_ExecutiveSummary_4page_Final_Digital.pdf

or by conducting activities with greater efficiency than could be achieved in-house—all while helping to increase revenues or reduce costs.

But in the aftermath of what former Chairman of the Federal Reserve, Ben Bernanke, called "the worst financial crisis in global history" in the fall of 2008, scrutiny on these third-party relationships increased exponentially. In its "Guidance for Managing Third-Party Risks" shared with financial institutions that same year, the FDIC emphasized that "A bank can outsource a task, but it cannot outsource the responsibility."[4] More recently, the topic of third-party risk was addressed in the *Federal Reserve Guidance on Managing Outsourcing Risks,* issued in December 2013. The Federal Reserve notes that risk is not limited to the "outsourced activity itself" but can also be introduced strictly through involvement with a third-party provider.[5] In reaction to practices that contributed to the financial crisis, government oversight ranging from rules safeguarding customer interactions and the privacy of customer data to anti-corruption laws demand greater attention be paid to the code of conduct within organizations—and their suppliers.

Industry expert Linda Tuck Chapman states that "effective third party risk management is a natural evolution in the maturation of disciplined sourcing and procurement in the financial services sector. All financial services companies—large and small—have hundreds or thousands of third party relationships, all of which must be evaluated and managed. Robust third party risk management programs bring consistency to identify, assess, control, and monitor about twenty different categories of third party risk throughout the life of each relationship. Simplifying complexity, risk-adjusting processes and controls, and implementing enabling technologies and solutions all create a strong foundation for effective third party risk management. After you develop the program, one of the biggest challenges is the scarcity of internal resources to execute. Acquiring proven solutions from partners like LexisNexis allows buyers to stay current with changes to third party risk profiles, enabling executives to make informed decisions.[6]"

Categories of Risk

No two regulators categorize risk in precisely the same way, but there are several categories that recur with great frequency. **Strategic risk**—If a third-party provider fails to meet the terms of a contract or return on investment, it can be considered a strategic risk.

Reputation risk—Whether a third-party provider deals directly with customers or offers a service that can indirectly impact customers, it's your reputation on the line if the third party drops the ball.

Operational risk—When a third-party provider is integrated into internal processes, such as through the use of a cloud-based, customer relationship management solution, it increases operational complexity and risk.

Transaction risk—From insufficient capacity that prevents transactions from being completed to security lapses that lead to unauthorized access and misuse of data, transaction risk is one of the most commonly encountered—and highly publicized—risks a financial institute faces.

Credit risk—While credit risk is most frequently considered in terms of a third party's own financial condition, credit risk also stems from the use of third parties for loan origination, underwriting or business solicitation.

Compliance risk—As more laws, rules and regulations are put into place to protect consumers, the level of compliance risk also increases. Non-compliance due to lapses by a third-party provider does not indemnify a financial organization against penalties.

Country risk—Whenever a financial institution engages a third-party provider based in a foreign country, it is exposed to potential economic, social and political conditions related to the provider location.

Legal risk—The activities of a third-party provider can expose a financial institution to legal expenses and possible lawsuits.

[4] https://www.fdic.gov/news/news/financial/2008/fil08044.html

[5] http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf

[6] Linda Tuck Chapman is a recognized expert in third party risk management and outsourcing governance. She is President, ONTALA Performance Solutions Ltd. and former Chief Procurement Officer in three major banks—BMO Financial Group, Fifth Third Bank and Scotiabank Group.

What Defines a Significant Third-Party Relationship?

Not *every* third-party provider constitutes a high risk. As a standard practice, your organization should vet any third party prior to entering into a new relationship, however many third parties should be subjected to greater levels of oversight and risk management. The FDIC suggests that a third-party provider should be considered significant if the relationship has the potential to impact revenues or expenses. In addition, third-party providers are engaged to implement activities related to:

- Storing, accessing, transmitting or performing transactions using sensitive customer information
- Marketing bank products or services
- Offering services related to subprime lending or card payment transactions

In addition, the interconnected, global nature of the financial services industry means that potential geo-political risks of third parties also merit consideration. If a third-party provider engages in transactions in countries—or with individuals—that are on official sanction or watch lists, it can have a negative impact even if those transactions aren't made on behalf of your organization.

"Simplifying complexity, risk-adjusting processes and controls, and implementing enabling technologies and solutions all create a strong foundation for effective third party risk management "

Linda Tuck Chapman—President, ONTALA Performance Solutions Ltd. and former CPO of BMO Financial Group

Effectively Reducing Third-Party Risk

Given the potential for damage, financial services organizations need to implement an efficient, methodical approach to managing significant third-party relationships. The challenge is executing a risk-management process that is comprehensive and timely. While regulatory guidance varies between the OCC, FDIC and the Federal Reserve, they all agree that vigorous due diligence and on-going monitoring of third parties are crucial steps toward reducing third-party risk.

Due Diligence Research

A superficial evaluation is not sufficient to proactively assess and mitigate risk. Organizations must vet potential third-party providers beyond financial stress scores in order to capture an accurate picture of potential third parties. This information may include:

- Financial, legal and business information on private, public and international entities
- Company profiles and information beyond typical self-reported data
- Negative news and litigation history
- Politically Exposed Persons, global sanctions and warnings

According to a 2014 research study by The Aberdeen Group, one method best-in-class organizations use to gain deeper insights into the companies they want to do business with is through the use of third-party data. Relying exclusively on the open Web does not provide the level of visibility needed to adequately mitigate risk.

On-Going Monitoring

Once the contract is signed, financial services organizations must remain vigilant. To minimize exposure to risk, organizations need to implement a consistent monitoring program to ensure that third-party operations continue to meet performance and compliance standards set forth in the original contract. A visual dashboard and alerting tool can help organizations:

- Monitor risk categories including financial, legal, political, societal/reputation and technical/operational
- Uncover hidden risks using global media sourced from leading news, business, legal and analytical content providers
- Keep pace with breaking news or trends that may impact your business

Armed with a more up-to-date perspective, organizations are empowered to make more informed, more confident decisions regarding third-party providers. In today's global financial industry, outsourcing and third-party relationships are essential to conducting business—despite the inherent exposure to risk ranging from regulatory action and litigation to financial and reputational losses. Financial organizations must develop proactive due diligence and third-party monitoring strategies that provide reliable, real-time insights to reduce vulnerability.

LexisNexis®

As a leading provider of information-enabled workflow solutions, LexisNexis can empower your organization to work more efficiently and safeguard business assets—an increasing difficult undertaking given the global, widely distributed nature of the financial services industry. As Carolyn DuChene, the OCC's Deputy Comptroller for Operational Risk, has noted, "In the same way that a chain is only as strong as its weakest link, the security of financial services is only as strong as its weakest participant."[7] LexisNexis can help financial services organizations strengthen their due-diligence processes, enhance regulatory compliance and conduct on-going third-party monitoring to better manage risk.

[7] http://www.occ.treas.gov/about/who-we-are/occ-for-you/alumni/supervisions/top-stories/sup-apr-2014-operational-risk-division-trio.html

For more information

Visit www.lexisnexis.com/supply-management
Email supply@lexisnexis.com

@LexisNexisBiz

LexisNexis®

About LexisNexis® Legal & Professional

LexisNexis Legal & Professional is a leading global provider of content and technology solutions that enable professionals in legal, corporate, tax, government, academic and non-profit organizations to make informed decisions and achieve better business outcomes. As a digital pioneer, the company was the first to bring legal and business information online with its Lexis® and Nexis® services. Today, LexisNexis Legal & Professional harnesses leading-edge technology and world-class content, to help professionals work in faster, easier and more effective ways. Through close collaboration with its customers, the company ensures organizations can leverage its solutions to reduce risk, improve productivity, increase profitability and grow their business. Part of Reed Elsevier, LexisNexis Legal & Professional serves customers in more than 100 countries with 10,000 employees worldwide.