Third-Party Risk Management:

Busting Myths and Telling Truths

Richik Sarkar, Esq.
McDonald Hopkins LLC
600 Superior Avenue, East, Suite 2100
Cleveland, OH 44114
(216) 430-2009
rsarkar@mcdonaldhopkins.com

Myth 1: CFPB Bulletin 2012-03 changed the regulatory landscape regarding third-party risk management

- For more than a decade, regulators have been providing guidance about third-party risk management:
  - "Outsourcing Financial Services Activities: Industry Practices to Mitigate Risk," Federal Reserve Bank of New York, October 1999
  - "Third-Party Relationships: Risk Management Principles," OCC Bulletin 2001-47
  - "Third-Party Risk: Guidance for Managing third Party Risk," FDIC Financial Institution Letter FIL-44-2008

Myth 2: Institutions can "contract away" their third-party risk

- CFPB Bulletin 2012-03 makes clear that institutions cannot simply rely upon their third-party vendors to "supervise" themselves. Banks are directed to:
  - Conduct due diligence to verify compliance
  - Review third-party policies, procedures, controls, and training materials
  - Set clear compliance expectations and consequences in contracts
  - Establish internal controls, policies, and plans to monitor and address third-party risk
  - Take prompt action to remediate compliance failures
- Examination Manuals have specific procedures, objectives, and assessment checklists directed towards third-party risk management:
  - CFPB Manual (Version 2)
  - FDIC Compliance Manual (December 2012)

Myth 3: Penalties for failing to properly address third-party risk will only be assessed against the institution

- Regulatory materials make clear that the "board of directors and senior management" of institutions 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." (FDIC Compliance Manual (December 2012) at VII-5.1).
- Moreover, a bank's "use of third-parties to achieve its strategic goals does not diminish the responsibility of the board of directors and management to ensure the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws. (OCC Bulletin 2001-47).

Truth 1: Institutions must conduct a complete risk assessment (compliance risk, reputational risk, operational risk, strategic risk, etc.) of its existing third-party vendors

- Emphasis should be placed on identifying "significant" vendors; especially if they deal directly with consumers
  - Examples of significant vendors:
    - Vendors whose activities affect an institution's revenue
    - Vendors performing critical regulatory functions
    - Vendors with access to sensitive customer or payment information
  - Examples of vendors who deal directly with consumers:
    - Mortgage brokers
    - Automotive dealers
    - Credit card providers
    - Loan servicers

Truth 1: Continued

- Institutions should investigate and evaluate potential vendors to ensure they can adequately provide contracted services, have appropriate policies, controls, and training materials, and will not increase an institution's risk profile
- Independent reports (SAS 70, SSAE 16, SOC 1-3) provided by third-party vendors are not certifications, but such audits and/or attestations can be used to evaluate third-party vendor control activities and processes
- Boards and senior management need to be advised about third-party risk assessment programs so they can provide proper oversight, assess and control risk, and ensure internal controls are adequate to protect the institution

Truth 2: Institutions must examine the policies and procedures of third-parties to ensure they understand and are capable of complying with regulatory requirements

- As the regulators expect institutions to "supervise" third-party vendors, the best examination tools are the regulator's examination manuals (CFPB, OCC, FDIC) and the detailed checklists
- Institutions should also be prepared to assist third-parties with the development of internal controls and procedures

Truth 3: Contracts with third-parties need to specifically address compliance and risk management issues

- Regulators will likely examine third-party contracts to ensure contracted responsibilities and expectations are clearly defined and enforceable
- As part of that process, contracts should include clear expectations, benchmarks, and requirements for, among other things:
  - Scope
  - Performance
  - Communication plans
  - Risk assessment and audit rights (perhaps with triggers for same)
  - IP rights
  - Data security

Truth 3: Continued

- Indemnification
- Response to consumer complaints
- Regulator oversight
- Insurance
- Termination

- Compensation provisions should be structured in a way to promote compliance and avoid incentives that could ultimately injure consumers

Truth 4: Institutions must regulate and examine their third-party vendors

- Institutions must have vendor monitoring programs in place
- Institution staff must be trained with respect to the vendor relationship and monitoring procedures
- Such programs should be documented (again, regulator checklists can be excellent tools)
- Policies and procedures to document and address consumer complaints must be in place so risks can be identified
- Risk assessments should be updated based upon complaints and monitoring results
- Vendor risk management is not an event, it is a process