ARHMF | Avila Rodriguez Hernandez Mena & Ferri LLP

VENDOR MANAGEMENT: Responsibilities and Risk Mitigation

Saltmarsh Compliance Funnel

Patricia M. Hernandez

September 22, 2016

ARHMF

TODAY'S OBJECTIVES

- Review vendor management guidance issued by the FED, OCC, FDIC, and CFPB
- Discuss considerations for a vendor management program
- Understand best practices for reviewing legal agreements involving third-party relationships
- Review recent vendor management enforcement actions
- Questions

VENDOR MANAGEMENT OVERVIEW

ARHMF

Background: Trends

- Banks continue to increase the number and complexity of relationships with both foreign and domestic vendors, such as:
    - Outsourcing entire bank functions, outsourcing lines of business or products, relying on third party to perform multiple activities, working with third parties that engage directly with customers
- Concern is that the quality of risk management is not keeping pace with risk and complexity of vendor relationship

ARHMF

Background: Trends

- Trends include:
  - Failure to properly assess and understand risks and direct and indirect costs involved in vendor relationships;
  - Failure to conduct proper due diligence and ongoing monitoring
  - Entering into contracts without properly assessing risks; and
  - Engaging in informal vendor relationships without contracts.

ARHMF

What are the Risks?

Potential risks arising from vendor relationships include:

1. Strategic Risk
   - Adverse business decisions
2. Reputation Risk
   - Negative public opinion
3. Operational Risk
   - Inadequate or failed internal processes, people and systems or from external events
4. Transaction Risk
   - Problems with service or product delivery
5. Credit Risk
   - Unable to meet the terms of contractual arrangements with the financial institution or to otherwise financially perform as agreed
6. Compliance Risk
   - Violations of laws, rules, or regulations or from non-compliance with policies, procedures, or business standards
7. Other Risks

ARHMF

Federal Reserve Board (FED)

- Supervision and Regulation Letter 13-19, "Guidance on Managing Outsourcing Risk" (December 2013)
- Provides guidance on managing outsourcing risks (mirrors OCC Bulletin 2013-29)
- Effective vendor risk management programs include the following core elements:
    1. Risk assessments;
    2. Due diligence and selection of service providers;
    3. **Contract provisions and considerations**;
    4. Incentive compensation review;
    5. Oversight and monitoring of service providers; and
    6. Business continuity and contingency plans.
- Additional risks include Suspicious Activity Report (SAR) reporting functions, foreign-based vendors, internal audit, and risk management activities

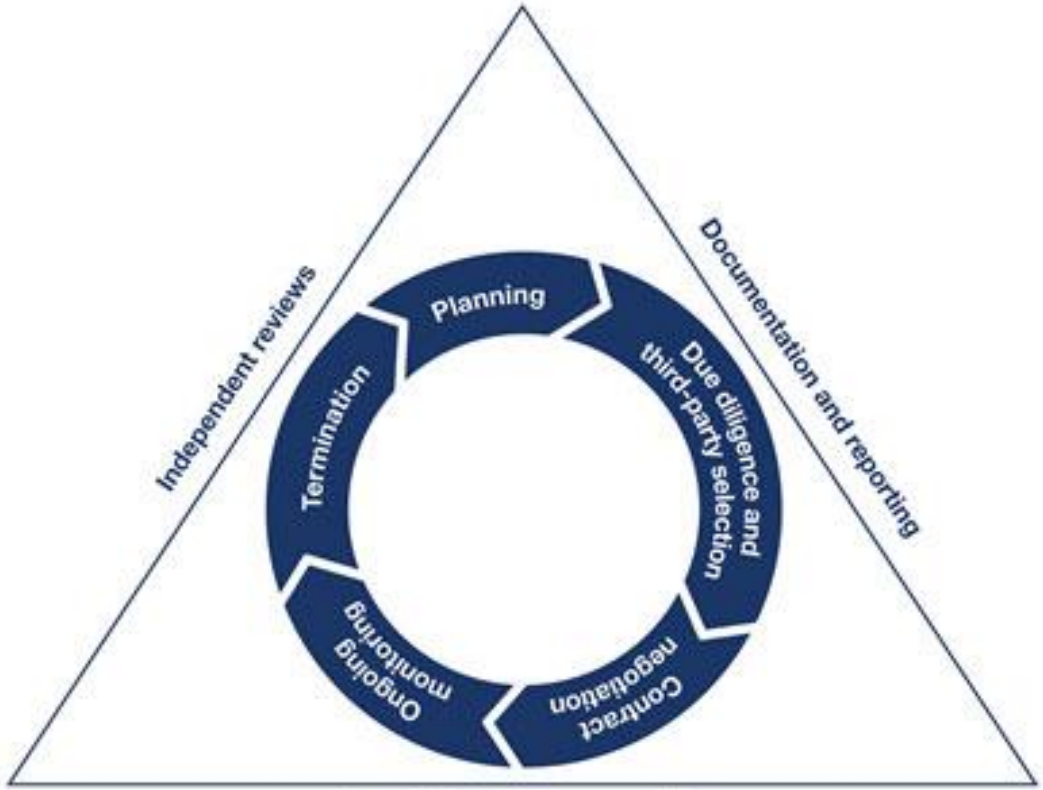
ARHMF

Office of the Comptroller of the Currency (OCC)

- OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance" (October 2013)
- Provides most comprehensive guidance for effective risk management
- Makes clear that failure to have an effective risk management process commensurate with the level of risk and complexity of third-party [vendor] relationships may be an "*unsafe and unsound banking practice*"
- Effective risk management process "follows a continuous life cycle for all relationships," and includes the following phases:
    1. Planning
    2. Due Diligence and Third-Party Selection
    3. **Contract Negotiation**
    4. Ongoing Monitoring
    5. Termination

ARHMF

Risk Management Life Cycle



Source: OCC

ARHMF

Consumer Financial Protection Bureau (CFPB)

- CFPB Bulletin 2012-03, "Service Providers" (April 2012)
- Expects banks to oversee their business relationships with vendors
- Expect banks to have an effective process for managing and protecting against "unwarranted risk", for example:
  1. Conduct due diligence to verify that vendors comply with law;
  2. Request and review vendor's policies, procedures, internal controls, and training materials;
  3. **Include clear expectations about compliance in contracts and consequences for non-compliance;**
  4. Establish internal controls and on-going monitoring to monitor compliance; and
  5. Take prompt action to address problems in monitoring process.

ARHMF

Federal Deposit Insurance Company (FDIC)

- FDIC Letter FIL-44-2008, "Guidance for Managing Third-Party Risks" (June 2008)
- An institution's board of directors and senior management are ultimately responsible for vendor activities
- Risk management process dependent on vendor relationship, scope and magnitude of activity, and risk identified
- Provides four main elements of an effective vendor risk management process:
  1. Risk assessment;
  2. Due diligence in selecting a vendor;
  3. **Contract structuring and review**; and
  4. Oversight
- Review of vendor relationships contributes to the FDIC's overall evaluation of management and its ability to control risk

ARHMF | Vendor Management Summary

Therefore, before entering into a vendor relationship, a bank should:

1. Conduct a thorough risk assessment;
2. Develop a plan to manage vendor relationship;
3. Conduct due diligence appropriate to the level of risk in vendor relationship;
4. Negotiate and review all contracts; and
5. Develop a monitoring program with proper oversight and accountability, documentation and reporting, and independent reviews

Contract Negotiation

ARHMF

Contract Negotiation

Upon selecting a vendor, what should the bank's management do?

...

1. Negotiate a contract that clearly specifies the rights and responsibilities of the bank and vendor.
2. Review contract provisions with legal counsel prior to execution.
3. Obtain board approval.
4. Review existing contracts periodically, and renegotiate (if necessary).

ARHMF

What Should the Contract Address?

1. **Nature and Scope of Arrangement**
   - Clearly define rights and responsibilities of each party
2. **Performance Standards**
   - Clearly defined performance standards (industry standard or customized standard) that define expectations and responsibilities for both parties
3. **Required Notifications**
   - Require vendors to provide and retain timely, accurate, and comprehensive information that allow bank to monitor performance
4. **The Right to Audit and Subject to Supervision**
   - Establish bank's right to audit, monitor performance, require remediation if issues are identified, and access audit reports
   - Require independent internal or external audits of vendor consistent with bank's in-house functions to monitor performance
   - Stipulate that vendor's performance is subject to OCC, FDIC, and CFPB examination oversight

ARHMF

What Should the Contract Address? (Cont'.)

5. **Legal and Regulatory Compliance**
   - Address compliance with specific laws and regulations applicable to the contemplated activities (GLBA, BSA/AML, OFAC, and Fair Lending, etc.)
   - Require vendor to maintain policies and procedures that address bank's right to monitor performance
6. **Cost and Compensation**
   - Outline fees to be paid, costs and responsibility for purchasing and maintain equipment, software, or other item related to activity
   - Responsible party for payment of any legal or audit expenses
   - Ensure that contract does not provide potential incentives to take imprudent risks
7. **Ownership and License**
   - How and when does the vendor have the right to use bank's information and intellectual property?
   - Address ownership of control of any information generated by vendors

ARHMF

What Should the Contract Address (cont'd.)

8. **Confidentiality**
   - Prohibit vendors and its agents from using or disclosing the bank's information, except as necessary
   - Nonpublic customer information needs to be handled in a similar manner consistent with bank's own privacy policy and in accordance with laws and regulations
   - Require potential breach to be fully and promptly disclosed
9. **Contingency Plans**
   - Address the continuation of services provided by vendor in the event of operational failures
   - Include provisions for transferring the bank's accounts or activities to another vendor "without penalty" in the event of initial vendor's bankruptcy, business failure, or business disruption
   - Vendor responsibility to back up information and maintain disaster recovery plan (results testing plans should be given to the bank)
10. **Indemnification and Insurance**
   - To what extent will the bank be held liable for failure of vendor's performance?
   - Vendors should have adequate insurance, provide proof of insurance to banks, and notify banks of any material changes in policies

ARHMF

What Should the Contract Address (Cont'd.)

11. **Limits on Liability**
    - Vendors may want to contractually limit their liability
    - Board of directors and senior management should determine whether the proposed limitations are reasonable when compared to the potential risks if vendor fails to perform
    - Would the contract subject the bank to undue risk of litigation?
12. **Default and Termination**
    - Stipulate what constitutes a default, provide notification requirements, identify remedies, and allow opportunities to cure defaults
    - Provision that enables the bank to terminate the contract, upon reasonable notice and without penalty, in the event the bank is formally directed to terminate relationship
    - Assign all costs and obligations association with transition and termination

ARHMF

What Should the Contract Address (cont'd.)

13. **Customer Complaints**
    - Specify the responsibilities of banks and vendors related to responding customer complaints
    - If vendors are responsible for consumer complaint resolution, then vendors should provide timely summary reports to banks
14. **Subcontracting**
    - Stipulate when and how the vendor must notify the bank of its intent to use a subcontractor
    - Specify limits to the vendor's ability to subcontract the services

ENFORCEMENT ACTIONS

ARHMF

Enforcement Actions: A Case Study

- January 2014: (**FDIC** and **OCC**) **BServ** and **FUNDtech Corporation**
  - Joint cease-and-desist order due to "unsafe or unsound banking practices"
    1. Lacked an internal auditor or an integrated risk-focused audit program;
    2. Lacked a comprehensive due diligence program;
    3. Lacked an enterprise-wide risk assessment to determine related risks and vulnerabilities of assets throughout the company;
    4. Lacked an effective business continuity or disaster recovery plan;
    5. Lacked effective patch management procedures to identify and address software vulnerabilities; and
    6. Lacked an effective log review program to detect, identify, and act on potential threats in a timely manner.

ARHMF

Enforcement Actions: A $225 Million Settlement

- June 2014: (**CFPB** and **DOJ**) **GE Capital Retail Bank** (Synchrony Bank), $225 million in relief and $3.5 civil money penalty for deceptive and discriminatory credit card practices
- Bank did not require customer service to follow scripts and bank's monitoring of compliance and service providers was inadequate
- Bank's telemarketers misrepresented credit card add-on products:
    1. Marketed the product as free of charge so long as the consumer paid off the monthly balance in full;
    2. Failed to disclose consumers' ineligibility for "key benefits" of the products;
    3. Failed to disclose that consumers had to pay for the product; and
    4. Falsely marketed products as a limited-time offer.

ARHMF

Vendor Management Regulatory Action

- Criticism in reports of examinations
- Matters requiring attention
- Violations of law
- Formal/informal enforcement actions
- Civil money penalties

ARHMF

Enforcement Actions: Additional Cases

- Each case below involved deceptive sales practices by third-party vendors while marketing a bank product:
  - April 2016: (**OCC** and **CFPB**) **HSBC Bank USA, N.A.**, $35 million civil money penalty
  - July 2015: (**OCC** and **CFPB**) **Citibank, N.A.**, $35 million civil money penalty and $700 million in consumer relief
  - September 2014: (**OCC** and **CFPB**) **US Bank**, $48 million in refund to consumers, $4 million civil money penalty (OCC), and $5 million civil money penalty (CFPB)
  - September 2013: (**CFPB**) **J.P. Morgan Chase**, $309 million in restitution and $20 million civil penalty
  - December 2013: (**CFPB**) **American Express**, $59.5 million in restitution and $9.6 million civil money penalty

ARHMF

Observations

- Banks should review their vendor risk management policies and processes to ensure that the bank is able to exercise sufficient oversight in each stage of risk management life cycle
    - Banks may need to update risk management policies or reassess risk management policies depending on the level of risk and complexity of relationship
- An emphasis on “independent” reviews
- Bank’s board of directors should approve contract with vendors, and review the ongoing monitoring of vendor activities
- Be aware of vendor’s vendors

Questions?

PATRICIA M. HERNANDEZ, PARTNER

Patricia M. Hernandez
Partner, ARHMF
tel 305.779.3566
phernandez@arhmf.com
arhmf.com

A founding partner of ARHMF, Patricia M. Hernandez focuses on corporate and financial services, particularly in counseling businesses, including banks and financial services companies, in varied legal issues. Ms. Hernandez has extensive experience in representing domestic and international financial institutions and other financial businesses in all aspects of regulatory, compliance, lending, mergers and acquisitions, and other transactional matters.

Ms. Hernandez regularly represents clients before the Office of the Comptroller of the Currency (OCC), the Federal Reserve, the FDIC, the Florida Office of Financial Regulation and other regulatory agencies and assists banks in negotiating and complying with enforcement actions. She has extensive knowledge in privacy and compliance with the requirements of the Gramm-Leach-Bliley Act and has achieved specific expertise in lending transactions, including asset-backed, trade-finance, factoring and Ex-Im Bank financing. She also has extensive practice in counseling U.S. and foreign clients on the effects of Regulations of the Office of Foreign Assets Control (OFAC) regarding Cuba and other embargoes. For the last three years, Ms. Hernandez has served as General Counsel to the Florida International Bankers Association. She also serves on the Banking Law Advisory Panel for the ALI-CLE of the American Law Institute, as well as a Board Member of the South Florida Banking Institute..


BANKING & FINANCE
CORPORATE, MERGERS & ACQUISITIONS
IMMIGRATION
LITIGATION & ARBITRATION
REAL ESTATE
TAX, TRUSTS & ESTATES
ARHMF
305.779.3560
ARHMF.COM