FinTech Webinar Series: Vendor Management Principles

Evolving Best Practices of Bank Service Providers

February 14, 2013

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Speakers

Russell Bruemmer
Partner
WilmerHale

Eric Mogilnicki
Partner
WilmerHale

Jeffrey Hydrick
Special Counsel
WilmerHale

Jonathan McKernan
Senior Associate
WilmerHale

Overview

- Recent developments
  - Evolving regulatory landscape
  - Regulatory guidance
  - The new regulator: the CFPB
- Legal requirements
  - General requirements
  - Special application to technology service providers
- Regulatory supervision
  - Bank examinations
  - Technology service provider examinations
  - CFPB examinations
  - Enforcement authority
- Case studies

Recent Developments

Evolving Regulatory Landscape

- Banks continue to refine their vendor management programs.
- Changes driven in part by bank regulators.
- Recent enforcement actions have targeted compliance and other issues involving service providers.
- Regulators also have revised regulatory guidance.

Regulatory Guidance

- Guidance applicable to financial institutions
  - OCC
    - OCC Advisory Letter 2000-9: Third-Party Risk
    - OCC Bulletin 2001-47: Third Party Relationships
    - OCC Bulletin 2002-16: Bank Use of Foreign-Based Third-Party Service Providers
  - FDIC
    - FIL-49-99: Bank Service Company Act
    - FIL-50-2001: Bank Technology Bulletin: Technology Outsourcing Information Documents
  - Federal Reserve
    - SR 00-4 (SUP): Outsourcing of Information Technology and Transaction Processing
  - FFIEC
    - Examination Booklet on Outsourcing Technology Services Risk (Jun. 2004)
    - Risk Management of Outsourced Technology Services (Nov. 2000)

Regulatory Guidance (cont.)

- Guidance applicable to both financial institutions and TSPs
  - CFPB Bulletin 2012-03: Service Providers
  - FFIEC IT Examination Booklet on the Supervision of Technology Service Providers (Oct. 2012)
    - Guidance for examiners and banks on supervising TSPs.
    - Uniform Rating System for Information Technology (URSIT).
- Guidance applicable to TSPs
  - FFIEC Administrative Guidelines – Implementation of Interagency Programs for the Supervision of Technology Service Providers (Oct. 2012)
    - Describes the interagency supervisory process.

The New Regulator: the CFPB

- Expansive jurisdiction
- New perspectives
- New authority
- New energy

Recent Enforcement Activity

- Capital One consent orders targeted high pressure telemarketing sales tactics by vendor call centers in marketing credit card add-ons. $60 million in penalties and $150 million in customer redress.
- Discover consent orders also targeted telemarketing sales tactics by vendor call centers in marketing credit card add-ons. $14 million in penalties and $200 million in customer redress.
- Amex consent orders targeted deceptive and other unlawful credit card practices arising out of ineffective oversight of affiliated service providers. $27.5 million in penalties and $85 million in customer redress.
- First Bank of Delaware consent order targeted AML violations arising out of inadequate oversight of vendor payment processors that processed fraudulent transactions. $15 million in civil money penalties, $500,000 in customer redress, and loss of charter.

Legal Requirements

General Requirements

- Banks must take appropriate steps to ensure that their service provider relationships are conducted in safe and sound manner and in compliance with law.
  - Special application of risk management principles.
- Specific vendor management requirements are risk-based.
- One size does not fit all. Different for each service provider relationship.
- Supervision by risk
  - Operational risk - the risk of loss due to failures of people, processes, systems, and external events.
  - Operational risk is “currently at the top of the list of safety and soundness issues” and might have “eclipse[d] credit risk as a safety and soundness challenge.” Comptroller Curry speech (May 2012).

Vendor Management Components

- Four components to vendor management program:
  - Risk assessment
  - Due diligence of potential service providers
  - Negotiation of appropriate contractual terms
  - Ongoing monitoring of service providers
- Strong policies, procedures, and contracts are not enough.
- Banks must enforce policies, procedures, and contract rights.
- CFPB has looked closely at the training of bank *and servicer provider* personnel in relevant bank policies and procedures.
- Vendor management programs are bank-specific.
- Special considerations when applied to TSPs.

Component 1: Risk Assessment

- Risk assessment should *identify and measure* risks associated with the proposed service provider relationship.
  - Risks include operational, strategic, compliance/legal, transaction, credit, and reputation risks.
- The risk assessment should also result in the identification of contractual and other measures necessary to *monitor and control* these identified risks.
- “Headline risks”
  - Data security and privacy risks
  - UDAAP risks
  - AML/BSA
  - FCPA and other country risks

Component 2: Due Diligence

- Diligence review must evaluate proposed service provider's expertise, operations and controls, and financial condition.
  - Data security program
  - Business continuity program
  - Customer complaints
  - Training of personnel
  - Compliance with law
  - Insurance coverage
  - Backgrounds of principals and key personnel
- Diligence review should extend to any material sub-contractors and diligence process in selecting those sub-contractors.

Component 3: Contractual Terms

- Contracts must address the risks identified in the risk assessment and due diligence phases.
- Specific terms will vary for each arrangement.
  - Clear specification of the services / SLAs
  - Appropriate termination rights and transition assistance provisions
  - Audit rights or other provisions facilitating bank's oversight
  - Reporting obligations to enable the bank to monitor the service provider's performance and financial condition
  - Appropriate business continuity program requirements
  - IP and data ownership provisions
  - Indemnity and insurance provisions
- Not enough to have good contracts. Banks must ensure contract rights are enforced.
- Red lights – visible departures from the bank's form GSA

Component 4: Ongoing Monitoring

- After signing an agreement, the bank must proactively monitor the service provider's performance, internal controls, and financial condition.
- Monitoring often accomplished through audits by the bank's internal auditors.
  - In some cases sufficient monitoring is possible through audits by the service provider's own auditors or by third parties.
- Banks should confirm remediation of audit-disclosed deficiencies within a reasonable period of time.
- There should be penalties for deficiencies and failures to remediate deficiencies.
- Monitoring must extend to any sub-contractors.

Application to TSPs

- As discussed, bank controls over outsourced operations must ensure activities are conducted in a safe and sound manner and in compliance with law.
- Controls should be risk-based.
- Unique risks presented by TSPs tend to require risk controls unique to TSPs.
  - TSP risk assessments
  - TSP contracts

TSP Risk Assessments

- A bank's risk assessment generally should identify and measure risks associated with a vendor relationship.
- For TSPs, risk assessment should particularly focus on:
  - sensitivity of data accessed or controlled;
  - criticality of outsourced functions;
  - experience and reliance on subcontractors;
  - ability to maintain business continuity;
  - redundancy and reliability of communication lines; and
  - scalability and ability to accommodate growth.
- The RFP process – including the requirements definition – is particularly important for TSP outsourcing.

TSP Contracts

- Service provider contracts must address the risks identified in risk assessment and due diligence phases.
- TSP contracts are subject to the same requirements that are applicable to service provider contracts generally.
- Some contract terms are of heightened importance in the TSP context, e.g.:
  - restrictions on subcontracting;
  - restrictions on foreign-based operations; and
  - indemnity.
- TSP contracts should ensure bank has a viable exit strategy.

Regulatory Examinations

Dual Examinations

- Bank regulators evaluate risk management primarily through direct examination of financial institutions.
  - As a result, service providers' primary concern will be complying with banks' vendor management programs.
- However, regulators may also conduct examinations of service providers. 12 U.S.C. § 1867(c).
- Regulators coordinate interagency programs to supervise TSPs through FFIEC.
  - Interagency examinations reduce need for separate examinations of TSPs that service financial institutions supervised by more than one regulator.

Bank Examinations

- Examinations assess bank process for identifying and managing technology outsourcing risks.
  - Process-focused: RFP process; service provider selection process; contracting process; and monitoring process.
  - Also reviews policies governing periodic ranking of service providers by risk to set monitoring priorities.
- Examination also evaluates individual contracts.
  - For selected contracts, examiners assess the RFP, the service provider diligence, the terms of the contract, and the actual monitoring activities.
  - This requires that banks maintain records of the diligence, contract negotiations, and monitoring activities.

TSP Examinations

- Examinations are on-site risk-based assessments covering a wide variety of servicer activities.
- Objective is to identify risks that can adversely affect serviced financial institutions. Focused on IT risks.
- Exam frequency depends on risks presented.
  - 24-month, 36-month, and 48-month cycles.
  - One full and one interim review during each cycle.
  - Interim reviews identify changes in IT risk management and confirm remediation of weaknesses identified in last ROE.
- Examination results in a Report of Examination (ROE) and an assignment of an URSIT rating.

TSP Examinations (cont.)

- Four stages to an exam by a bank regulator.
  - Pre-exam planning and information requests
  - Exam kickoff meeting
  - Actual examination
  - Close of exam
- Pre-exam planning and information requests
  - Regulator will deliver an information request
  - Privileged documents will need to be delivered
  - TSP should request confidential treatment
- Exam kickoff meeting
  - Regulator might conduct an introductory presentation of the team
  - TSP's exam team should attend
  - Attendance by an executive conveys that TSP understands importance of the exam

TSP Examinations (cont.)

- Actual examination
  - Exam manager should meet daily with regulator's exam team
  - Regulator may provide feedback informally during the exam
  - Important to take feedback seriously and establish a cooperative spirit
  - For major findings, TSP should consider scheduling a presentation to address the examiners' concerns
  - TSP should notify employees that they should cooperate fully if contacted by examiners
  - TSP should prepare likely interviewees in advance
- Close of exam
  - Preliminary findings discussed
  - URSIT rating will be assessed
  - Poor rating may require board meeting with examiners

URSIT Ratings

- Examination results in rating (scale of 1 through 5)
- Rating scores the management of IT-related risks to determine the degree of supervisory attention needed and to ensure weaknesses are addressed.
  - Used to rate IT risks at both banks and TSPs.
- Components
  - Audit – internal controls relating to IT and ability to independently assess risk exposures.
  - Management – ability of the board and management with respect to IT acquisition, development, and operations.
  - Development and acquisition –ability to identify, acquire, install, and maintain IT solutions.
  - Support and delivery – ability to provide technology services in a secure environment.

CFPB Examinations

- Expansive jurisdiction
- Consumer-centric paradigm
- Coordination with enforcement
- Privilege and scope issues

Enforcement Actions

- Regulators have a range of actions to resolve issues identified in a bank or TSP examination.
- Issues may be:
  - noted orally or generally discussed in ROE;
  - identified in ROE as a matter requiring management attention or remediation;
  - cited in ROE as a violation of law or unsafe or unsound practice;
  - subject to memorandum of understanding contemplating specific remedial actions;
  - subject to public enforcement actions contemplating specific remedial actions; and/or
  - subject to civil monetary penalties.

Case Studies

Case Studies

- Data breach
- Post-contract developments
- Services for multiple institutions
- Multi-jurisdictional issues

Questions?

Russell Bruemmer
+1 202 663 6804
Russell.Bruemmer@wilmerhale.com

Jeffrey Hydrick
+1 202 663 6567
Jeffrey.Hydrick@wilmerhale.com

Eric Mogilnicki
+1 202 663 6410
Eric.Mogilnicki@wilmerhale.com

Jonathan McKernan
+1 202 663 6803
Jonathan.McKernan@wilmerhale.com