Current Issues Facing Financial Institutions

New Hampshire Bankers Association
2016 Annual Meeting

June 23, 2016

Presented By:
Lawrence M.F. Spaccasi, Esq.
lspaccasi@luselaw.com
Gary A. Lax, Esq.
glax@luselaw.com
Luse Gorman, PC
www.luselaw.com

Who We Are

Luse Gorman, PC is a Washington, D.C. based law firm that specializes in representing community banks and other financial institutions.

We are a national leader in representing community banks in mergers and acquisitions, capital raising transactions, corporate governance, executive compensation, regulatory and enforcement and general corporate and securities law.

We represent over 250 financial institutions nationwide. Most are community banks ranging from $100 million to $20 billion in assets.

Who We Are

- Top 10 law firm in M&A every year since 2001
  - No. 1 in 2009, 2011, 2012 and 2015
- No. 1 law firm nationally in community bank capital raising transactions since 2000
- Largest practice group nationally dedicated exclusively to representing financial institutions
  - 25 Attorneys, including 5 attorneys specializing in executive compensation/employee benefits
  - Represent 250+ financial institutions, 100+ mutual institutions, 90+ SEC reporting companies

Agenda for Discussion

1. Bank Secrecy Act/Anti-Money Laundering
2. Consumer Compliance
3. Data Security
4. Enterprise Risk Management
5. Vendor Management
6. Corporate Governance
7. Emerging Supervisory Issues

BSA/AML

BSA/AML - Overview

- BSA/AML compliance still being focused upon by regulators

- Program must be written and address (at a minimum):
  1. Internal Controls
  2. Qualified Responsible Individual (named BSA Officer)
  3. Testing
  4. Training

- Supervisory expectation: full compliance with 4 pillars, if not or failure to correct a BSA/AML related MRA - formal enforcement order typically follows

- Program must also include Customer Identification Program (CIP) with risk-based procedures which demonstrate "reasonable belief" of customers true identity

BSA/AML Program – Internal Controls

- Management must determine BSA/AML risks and establish internal controls based on that risk assessment

- Internal controls manage, monitor and control risk through policies, procedures and processes

- Internal controls ensure compliance with BSA regulations, include recordkeeping and reporting requirements as well as compliance with OFAC rules

BSA/AML Program – Qualified BSA Officer

- Must be "qualified and knowledgeable" person
- Must be appointed by Board of Directors
  - Board record should address qualifications and vetting
- Must possess resources, authority and access across product/service lines to perform their job
  - Cannot "silo" BSA Officer or restrict crossing departments
- Should be involved assessing BSA/AML implications of new products and services and involve them early in process

BSA/AML Program – Testing

- Testing (whether performed by third-party or in-house) must be independent

- No statutory time frame for testing, but supervisory expectation is that it will be performed every 12 – 18 months depending on the risk profile of the bank

- Testing should be well-documented and reported to board with evidence of Board review

BSA/AML Program – Training

- Should be provided to directors and executive officers
- Should be provided to all employees, but tailored to their specific job duties
- Training ties in policies, procedures and processes to regulatory requirements
- Should be provided on an on-going basis and updated for new products and services
- Training must be documented

BSA/AML Program – Supervisory Expectations

- Achieve full (100%) compliance with regulatory requirements (4 pillars)
- Timely address all (100%) criticisms/suggestions in Reports of Examination, including MRAs
- Timely address all (100%) criticisms/suggestions in Audit Report
- Transparent and timely reporting to senior management and Board
- Review and revise BSA Program at least annually, but more frequently based on risk profile

BSA/AML Program – Emerging Issues

- Increased BSA/AML Enforcement Orders:
  - Bank of China New York Branch
  - Meetinghouse Bank
  - Carver Bank
  - OCC Bulletin 2016-16
- CIP requirement for beneficial owners of corporate entities
- CIP for pre-paid cardholders
- Increased scrutiny of OFAC compliance

Consumer Compliance

Consumer Compliance - Overview

- Long shadow of CFPB has caused other regulators to act more quickly and forcefully in area of consumer compliance
- More regulatory monitoring and scrutiny of consumer complaints and mitigation efforts
- Fair Lending, HMDA data and CRA
- UDAAP enforcement actions at all time high - direct result of new consumer bias by regulators (driven by CFBP)
- System should address consumer complaints and resolutions
- System should designate "compliance officer" with authority to cross departments, make corrections and with accountability
- System should monitor and identify possible problems and "unfairness" to consumers before they happen
- System should address periodic review of disclosures and training

Consumer Compliance - Management Program

- Board and senior management oversight – needs to set the tone at the top
- Board should appoint "Consumer Compliance Officer"
- Elements of Compliance Program:
  - Policies, Procedures & Limits
  - Training
  - Monitoring
  - Response to consumer complaints
- Compliance Audit

Consumer Compliance - Compliance Officer

- Should know consumer protection laws and regulations and have understanding of bank's products and services
- Should have authority and independence to cross departmental lines and take corrective action
- Should have access to all areas of operations
- Responsible for developing, reviewing and updating compliance policies and procedures and training personnel
- Should provide reports to Board and management
- Responsible for responding to consumer complaints and ensuring corrective actions have occurred

Consumer Compliance – Policies and Procedures

- Program tailored to the bank
- Policies establish goals and objectives
- Procedures establish the method for meeting goals and objectives
- Policies and procedures become source documents for training
- Reviewed and updated as business and regulatory environment changes

Consumer Compliance - Training

- Training should address directors, officers and staff
- Specific training for line staff on laws, regulations, and internal policies and procedures that directly affect their jobs
- Can be conducted in-house or with third-party provider
- Training tailored to bank's products and services
- Once trained, compliance officer should assess knowledge base
- Training program should be updated for current, complete and accurate information and new products and services

Consumer Compliance - Monitoring

- Monitoring identifies procedural or training weaknesses so as to avoid regulatory violations
- Monitoring includes planning, development and implementation stages for new products and services
- In addition to real-time transaction monitoring, there should be regularly scheduled reviews of:
  - Disclosures and calculations
  - Document filing and retention procedures
  - Posted notices, marketing and advertising materials
  - State consumer protection laws/regulations
  - Third-party service provider operations
  - Internal compliance communication system to management and staff for legal updates and changes

Consumer Compliance - Consumer Complaints

- Establish Complaint Log
- Establish procedures to address complaints, including identification of persons or departments to handle them
- Ensure review of complaints by compliance officer to ensure they are not systemic

Consumer Compliance - Audit

- Independent review of compliance with consumer protection laws/regulations and adherence to policies and procedures
- Board should determine frequency and scope (but at least annually)
- May be conducted in-house or by qualified third-party
- Board and management should review compliance report and act promptly to address deficiencies
- Compliance Officer charged with overseeing corrective action noted in compliance report
- Follow-up procedures should be established to verify that corrective actions were effective and sustained

Enterprise Risk Management

Risk Management

Enterprise Risk Management Systems:

- Integration of risk management and compliance systems into overall "enterprise risk management"
- Board should establish risk management system with accountability and designated "Chief Risk Officer"
- Chief Risk Officer should not be involved in business operations or decisions (i.e. cannot be reviewing own work)
- Board should assess and establish "risk tolerance" in writing, taking into account regulatory environment, long-term interests, risk exposure and realistic ability to manage risks
- Should include how risk and compliance with policies will be monitored and updated
- Should demonstrate active review of critical operating policies and procedures, record of annual review and approval and response to changes (regulatory and market)
- OCC Guidelines Establishing Heightened Standards ($50B banks)

Vendor Management

Vendor Management - Overview

Vendor Management Systems:

- "Know your vendor" – can no longer "assume" vendor is compliant, must demonstrate diligence procedures in writing
- Written policies regarding diligence and monitoring now required
- Must assess potential impact of vendor relationship on customers, including access to or use of customer information
- Must assess extent to which vendor activities are subject to specific laws and regulations (e.g., BSA/AML, fiduciary rules)
- Must detail selection, assessment and oversight process
- Regulatory expectation is that Board (or committee) will be responsible for overseeing third-party risk management
- Cannot "blame" third-party for non-compliance, buck stops with the Board/bank and it must prove it had reason to believe vendor's abilities and compliance

Vendor Management - Overview

- IT, data security and data processing service providers are typically highest level of risk and focus but *all third party relationships involve risk*
- Customer facing providers now involve even greater risk and potential scrutiny due to focus on "consumer compliance"
- Understand that you have power to negotiate provider contracts and reject "that is our standard contract" pitch
- Even large providers (with relative monopolies) will negotiate and address reasonable concerns
- Reasonable management is key, not overreaction or setting impossible approval and monitoring goals or systems

Vendor Management - Regulatory Guidance

- FFIEC IT Examination Handbook – "Outsourcing Technology Services," "Supervision of Technology Service Providers" and "Appendix J – Strengthening the Resilience of Outsourced Technology Services"
- CFPB Bulletin 2013-03 - "Service Providers"
- FDIC FIL 44-2008 - "Guidance For Managing Third-Party Risk"
- PA - "Suggested Cybersecurity Tactics For Regulated Entities"
- **OCC Bulletin 2013-29 – "Third Party Relationships"**

Vendor Management - Regulatory Guidance

- All guidance recognizes need for banks to outsource and rely upon third parties but also note banks may bear ultimately responsibility for failures

- All guidance emphasizes same themes/phases for vendor management systems:
  1. Planning – having a process and written plan
  2. Due diligence – robust selection process and vetting
  3. Contracts - negotiation of key terms and responsibilities
  4. Monitoring - reporting from and access to vendor
  5. Termination - procedures, costs and alternatives

Vendor Management – SSAE 16 Reports

- SSAE 16 replaced SAS 70 as standard for "audits" of "service organizations" (entities that provide services to end users)
- 2 types of SSAE audits, 3 types of SSAE reports
- SSAE reports should be part of vendor management system but are not appropriate for every vendor
- When is an SSAE report appropriate?
  - When vendor is holding something of value in trust (like assets, cash or data)
  - You need an assessment of vendor's "controls"
  - You need evidence of external assessment (i.e., their auditor)
- What if vendor will not provide an SSAE report?
  - You may have to "audit" for yourself and implement greater controls in the area of that vendor
  - You may want to find another vendor who will provide reports

Vendor Management – Vendor Plans

Each vendor plan should:

- Consider vendor's affect on strategic initiatives (large technology projects, organizational changes or mergers)
- Assess potential impact of relationship on customers, including vendors access to or use of confidential information
- Set forth contingency plan if transition is required (other vendors, in-house or discontinuation)
- Assess extent to which activity is subject to specific laws and regulations (e.g., privacy, BSA, AML, fiduciary laws) and how vendor maintains compliance
- Detail due diligence, selection and oversight of vendor
- Be reviewed and approved by **board of directors** when "critical activities" are involved

Vendor Management - Due Diligence

- Some level of due diligence should occur on all vendors
- Should not rely solely on "word of mouth" or trade association's "stamp of approval"
- Diligence should be commensurate with level of risk, complexity of relationship and potential exposure to risk
- Some diligence already done (i.e. public or regulated entities)
- Should consider:
  - Vendor's access to sensitive bank or customer data
  - Systematic risk due to industry consolidation
  - Reliance (directly and indirectly) on foreign-based subcontractors – can you "reach" the vendor or assets

Vendor Management – Contracts

- Know location of all material contracts, including exhibits, addendums, amendments
- Know when and how they renew
- Know costs and timing to get out of contract
- Contract should address:
  - Indemnification
  - Insurance
  - Dispute resolution
  - Limits on liability
  - Assignment
  - Default and termination
  - Subcontracting
  - Foreign-based third-parties

Vendor Management - Monitoring

- Is the vendor complying with what they promised?

- Bank should dedicate sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the third-party commensurate with the level of risk and complexity of the relationship

Data Security

Data Security

Cyber/Data Security:

- Government-wide emphasis
- New cyber security assessment tools at FDIC and FFIEC (should demonstrate that bank has done assessment)
- Focus is not just on "security" of data and systems but preparedness and contingency plans in aftermath of breach
- Need to understand role and contractual liability of/to vendors
- Need to understand cyber insurance policies and limitations:
  - Cyber security insurance is developing market
  - Most commercial polices exclude data breaches from coverage
  - Underwriting process can help identify problems
- Many larger institutions considering Board members with cyber security and/or technology experience
- Regulators now expect Board level attention to address concerns and preparedness

Corporate Governance

Corporate Governance – New FDIC Guidance

Board needs to have policies which cover:

- Safeguarding confidential information
- Integrity of records
- Strong internal controls
- Candor in dealing with regulators, auditors and advisors
- Avoidance of self-dealing and acceptance of favors
- Observation of laws and regulations
- Implementing back-ground checks
- Internal auditor monitoring of conduct and ethics
- Reporting questionable activity
- Periodic training, acknowledgement and updating of policies

Corporate Governance – Minimums

- Annually update strategic business plan
- Board executive sessions (at least 2x annually)
- Clawback compensation policies
- Majority of "independent" board members and "independence" testing
- Independent key committees (Audit, Comp, Nominating)
- Independent compensation consultants and annual review
- Risk assessment of all incentive compensation
- Whistleblower hotline and protections
- Written corporate governance guidelines
- Code of ethics/conduct (applicable to Board as well)
- Annual risk assessment and tolerance statement
- Written charters for all key committees

Emerging Issues

Emerging Supervisory Issues

- CRE Lending
- Credit Concentrations
- Interest Rate Risk
- MLO Compensation
- Consumer Compliance Rating System (FFIEC proposal)

LUSE GORMAN, PC

ATTORNEYS AT LAW

5335 Wisconsin Avenue, NW
Washington, DC 20015

TELEPHONE (202) 274-2000
FACSIMILE (202) 362-2902
www.luselaw.com