Mark E. Aldrich
Janet M. Bonnefin
Robert K. Olsen
Eric G. Baron
Keith R. Forrester
Anne M. McEvilly

ALDRICH & BONNEFIN
Professional Law Corporation

Tricia E. Engelhardt
Stephanie A. Shea
Joel N. Cook

Our File Number:

CALIFORNIA BANKERS ASSOCIATION

37TH ANNUAL REGULATORY COMPLIANCE CONFERENCE

VENDOR CONTACTS AND MONITORING

OCTOBER 6-9, 2015

Anne M. McEvilly
Principal
Aldrich & Bonnefin, PLC
Counsel to the Bankers' Compliance Group®

18500 Von Karman Avenue, Suite 300 ■ Irvine, California 92612
949.474.1944 ■ Fax 949.474.0617 ■ ab@ablawyers.com ■ www.ablawyers.com

Mailing Address: P.O. Box 19686 ■ Irvine, California 92623-1029
Tax I.D. Number: 33-0027849

DISCLAIMER

This presentation is intended solely for educational purposes to provide you general information about laws and regulations and not to provide legal advice. There is no attorney-client relationship intended or formed between you and the presenters or you and the authors of these materials. Consult your institution's legal counsel for advice about how this information impacts your institution.

VENDOR CONTACTS AND MONITORING

OUTLINE

I. CONTRACT REVIEW

A. In General. After selecting a vendor, the financial institution should ensure that the specific expectations and obligations of both the financial institution and the vendor are set forth in a written contract prior to entering into the arrangement.

B. Lessons Learned: How failures in the vendor "selection process" can backfire in the contract negotiation phase.

C. Involving Legal Counsel.

1. Other instances where legal counsel may be involved. Legal counsel involvement may be warranted when a significant amount of money is at stake (*e.g.*, costly services or products) or there is significant risk exposure to the financial institution (*e.g.*, sensitive customer information is being shared or the vendor is a foreign entity).

   In such cases it may be prudent to have legal counsel review the vendor agreement in order to ensure that the financial institution is best protected and the agreement complies with the applicable guidance. Legal counsel may also be helpful when dealing with vendors that may seem to have the "upper hand" in terms of bargaining power given the vendor's size, reputation and assets.

D. Contract Provisions. The contract should clearly set forth the rights and responsibilities of each party to the contract.

E. Exhibit A – Sample Vendor Contract Checklist. Exhibit A to this Outline provides a sample vendor contract checklist that may be used to help ensure necessary contract provisions are included.

II. ONGOING MONITORING

A. In General. The extent of oversight of a particular vendor relationship depends upon the potential risks and the scope and magnitude of the arrangement.

B. Frequency. When it comes to ongoing oversight of vendors, a common question is how often must a financial institution review and monitor a particular vendor.

1. The board should oversee and review at least annually significant vendor arrangements and whenever there is a material change to the program. Additionally, management should periodically review the vendor's operations.

2. Higher risk vendors may require more frequent assessments and monitoring and may require designation of individuals or a group as a point of contact for these vendors.

C. Documentation. When it comes to ongoing oversight of a vendor, not only does documentation help demonstrate compliance with the Guidance but also helps facilitate the monitoring and management of the risks associated with vendor relationships.

The financial institution should maintain documents and records on all aspects of a vendor relationship, including valid contracts, business plans, risk analyses, due diligence and oversight activities (including reports to the board or delegated committees). Also, retain documents regarding any dispute resolution.

D. Ongoing Monitoring Items. Below are the items that the financial institution may consider including in their ongoing oversight of vendors. Note that this list is not all-inclusive and that not all of the items below may be relevant to certain vendors.

1. Effectiveness of relationship. Evaluate overall effectiveness of the vendor relationship and the consistency of the relationship with the financial institution's strategic goals.

2. Review licenses. Review any licensing or registrations to ensure the vendor can legally perform its services.

3. Insurance. Review the adequacy of the vendor's insurance coverage.

4. Audits. Review independent audit reports of the vendor, and follow-up on any needed corrective actions.

5. Vendor's internal policies and controls. Review the adequacy and adherence to the vendor's policies relating to internal controls and security issues.

6. Compliance with laws. Monitor for compliance with applicable laws, rules and regulations.

7. Business resumption planning. Review the vendor's business resumption contingency planning and testing.

8. Changes in vendor's key personnel. Assess the effect of any changes in key vendor personnel involved in the relationship with the financial institution.

9. Training. Determine the adequacy of any training provided to employees of the financial institution and the vendor.

10. Testing vendor's interaction with customers. Administer any testing programs for vendors with direct interaction with customers.

11. Customer complaints. Review customer complaints about the products and services provided by the vendor and the resolution of the complaints.

12. Meetings and onsite visits. Meet as needed with representatives of the vendor to discuss performance and operational issues. Regular onsite visits may be useful to understand fully the vendor's operations and ongoing ability to meet contract requirements.

13. Monitor activities and performance. Management should also ensure that the financial institution's employees who directly manage vendor relationships monitor the vendor's activities and performance. The financial institution should pay particular attention to the quality and sustainability of the vendor's controls, and its ability to meet service-level agreements, performance metrics and other contractual terms, and to comply with legal and regulatory requirements.

14. Escalation. Financial institution employees who directly manage vendor relationships should escalate to senior management, and the board of directors if appropriate, significant issues or concerns arising from ongoing monitoring, such as an increase in risk, material weaknesses and repeat audit findings, deterioration in financial condition, security breaches, data loss, service or system interruptions, or compliance lapses.

15. Financial condition. Financial institutions should establish procedures to monitor the financial condition of vendors to evaluate their ongoing viability. In performing these assessments, institutions should review the vendor's most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity and operating results.

16. Subcontractors. If a vendor relies significantly on subcontractors to provide services to the financial institution, then the vendor's controls and due diligence regarding the subcontractors may also need to be reviewed.

17. Information technology services. If the vendor delivers information technology services, in addition to the independent audit reports mentioned earlier, the financial institution can request the FFIEC Technology Service Provider examination report from its primary federal regulator. Security incidents at the vendor may also trigger the financial institution's need to elevate its monitoring of the vendor.

III. VENDOR OVERSIGHT BY THE REGULATORS

A. In General. The federal financial regulators have the statutory authority to supervise all of the activities and records of a financial institution whether performed or maintained by the institution itself or by a vendor on or off of the institution's premises. Section 7(c)(1) of The Bank Service Company Act (12 USC 1867).

B. Notification to Regulators. Financial institutions should in all cases take care to comply with the Bank Service Company Act (12 USC 1867) which requires insured financial institutions to notify their appropriate federal regulator in writing within 30 days of contracts or relationships with third parties that provide certain services to the financial institution.

C. Contractual Obligations. Financial institutions should address the matter explicitly in the contract with the vendor. See Exhibit A for a sample checklist of specific contractual obligations, which includes the regulator's right to examine the vendor.

IV. RECENT INFORMAL FRB GUIDANCE

A. Vendor management has always been a concern, but historically the focus was on IT vendors.

B. FRB (and other regulators) have moved to more holistic approach to vendor management expectations.

C. Financial institution's cannot "outsource" compliance risk.

D. The vendor management program should be risk-focused, including oversight and controls commensurate with the outsourced engagements.

E. Most Common Issues:

1. No vendor management program at all.

2. Inadequate analysis/identification of critical vendors.

3. Vendors not captured in inventory.

4. Inadequate monitoring of critical vendors.

5. Vendor management program too IT-centric.

6. Vendors have overly broad access to sensitive customer information.

V. THANK YOU FOR YOUR PARTICIPATION – WE'RE ADJOURNED!

Speaker Contact Information:

Anne M. McEvilly
Principal
Aldrich & Bonnefin, PLC
18500 Von Karman Avenue, Suite 300
Irvine, California 92612
Bus: 949-474-1944
Email: **AMcEvilly@ABLawyers.com**

EXHIBIT A

SAMPLE: CONTRACT CHECKLIST

Contract provisions for Significant Level, Intermediate Level and Low Level vendors:

☐ 1. **Term.** Note initial term commitments, as well as auto-renewing notification requirements.

☐ 2. **Describe Products and Services.** The products or services to be provided by the vendor are sufficiently described in the contract, including (as applicable) the frequency, format and other specifications.

☐ 3. **Vendor's Use of On-Site Facility, Equipment, Employee.** Terms relating to any use of the financial institution's premises, equipment and employees, as appropriate, are included in the contract.

☐ 4. **Compliance Representations.** Requires that the vendor comply with all applicable laws, regulations and regulatory guidance, including obtaining necessary licenses and certifications. If vendor is a foreign based provider, address application of U.S. regulatory standards.

☐ 5. **Regulator's Access to Records.** Includes authorization for the financial institution and the appropriate federal and state regulatory agencies to examine the vendor and have access to the vendor's records to the extent necessary or appropriate to evaluate the vendor's compliance with laws, rules, and regulations.

☐ 6. **Subcontracting.** Addresses whether or not the vendor is permitted to subcontract or use another party to meet its obligations with respect to the contract and any notice or approval requirements. If subcontracting is permitted, address vendor's continuing liability for subcontractor's actions or inactions.

☐ 7. **Fees.** Outlines the fees to be paid, including any fixed compensation, variable charges and any fees to be paid for nonrecurring items or special requests.

☐ 8. **Outsourced Equipment, Software Cost & Maintenance.** Addresses cost and responsibility for purchasing and maintaining any equipment, hardware, software or other item related to the outsourced product or service.

☐ 9. **Default, Remedies & Cure.** Specifies what circumstances constitute default, identifies remedies and allows for a reasonable opportunity to cure a default.

☐ 10. **Termination.** Specifies each party's termination rights and allows for reasonable termination rights for the financial institution. Specifies termination rights for various conditions, such as a change in control, substantial increase in cost, failure to meet performance standards, failure to fulfill contractual obligations, inability to prevent violations of law, bankruptcy, company closure and insolvency. States termination and notification requirements, with operating requirements and timeframes to allow for the institution's orderly conversion to another entity without excessive expense. Return of the financial institution's data, records and other resources must also be addressed.

☐ 11. **Dispute Resolution.** Includes a dispute resolution process for the purpose of resolving problems expeditiously, and provides for continuation of the arrangement between the parties during the dispute.

☐ 12. **Indemnification.** Includes an indemnification provision that requires the vendor to indemnify and hold the financial institution harmless from liability as a result of the vendor's performance.

☐ 13. **Limitation on Liability.** Limits the financial institution's liability and any limitation on the vendor's liability is not unreasonable and is acceptable to the financial institution.

☐ 14. **Notification to Federal Regulator**. Addresses the financial institution's requirement to comply with Section 7 of the Bank Service Company Act (12 USC Section 1867) which requires FDIC-insured financial institutions to notify their appropriate federal banking agency in writing of contracts or relationships with third parties that provide certain services to the institution.

☐ 15. **Equal Opportunity Clauses.** If the contract may exceed $10,000 in any year, the contract includes the following equal opportunity clauses: affirmative action (41 CFR 60-1.4); and workers with disabilities (41 CFR Section 60-741.5). If the contract may exceed $100,000 in any year, the contract includes the equal opportunity clause for veterans (41 CFR Section 60-300.5).

☐ 16. **Amendments; Assignments.** Prohibits vendor's ability to unilaterally modify or assign the contract without the institution's prior written consent, including the use of and changes to subcontractors.

☐ 17. **Obtaining & Sharing Vendor Information.** Addresses the financial institution's ability to obtain and share information regarding the vendor from and with others.

☐ 18. **Choice of Law.** Includes a choice of law provision that applies California law (exclusive of conflicts of law principles). If California law is not applied, then explain in an attached document why it is appropriate to apply another state's laws and consult with out-of-state counsel as needed. If the vendor is providing services or products in part or in whole in a foreign country, the contract includes choice-of-law covenants and jurisdictional covenants that provide for adjudication of all disputes between the parties under the laws of a single, specific jurisdiction.

☐ 19. **Notice to Parties.** Includes specific provisions governing notice to each party, including whether electronic communications may be used, timing of notices and effect of non-delivery.

Additional contract provisions for Significant Level and Intermediate Level vendors:

☐ 20. **Customer Disclosures.** Identifies which party will be responsible for delivering any required customer disclosures (as applicable).

☐ 21. **Legal/Audit Expenses.** Addresses which party is responsible for payment of any legal or audit expenses.

☐ 22. **Vendor's Insurance.** Addresses the insurance coverage to be maintained by the vendor.

☐ 23. **Periodic Performance Monitoring and Reviews.** Includes an authorization for the institution to monitor and periodically review the vendor for compliance with the contract.

☐ 24. **Performance Standards and Service Levels.** Clearly defines performance standards for the vendor, including as appropriate service level requirements and applicable benchmarks.

☐ 25. **Notice of Changes to Fees/Contracted Activities.** Requires sufficient notification to the financial institution before making significant changes to the fees or contracted activities, including acquisition, mergers, joint ventures, divestitures, subcontracting, off-shoring, management or key personnel changes, or implementing new or revised policies, processes, and information technology. May trigger need to have right to terminate contract without liability or cost.

☐ 26. **Modifying or Adding Services.** Specifies the contracting parties' rights in modifying existing services performed under the contract (*e.g.*, "vendor to provide services to client at least as favorable to client as those provided by vendor to vendor's most favored client"), and guidelines for adding new or different services and for contract re-negotiation. Also include notice requirements pertaining to the same.

☐ 27. **Vendor's Notification of Material Events.** Requires the vendor to promptly notify the financial institution of the vendor's financial difficulty, catastrophic events and significant incidents (such as information breaches, data loss, service or system interruptions, compliance lapses, enforcement actions or other regulatory actions), and includes the materiality thresholds and procedures for notifying the financial institution in writing of such events.

☐ 28. **Reports.** Specifies the type and frequency of management information reports that the vendor must provide, including (check those included in the contract): ___ performance reports; ___ audits reports; ___ financial reports; ___ security reports; ___ business resumption testing reports; ___ exception-based reports serving as notification of any changes or problems; ___ consumer complaint reports; and ___ regulatory or law enforcement actions reports.

☐ 29. **Access and Use of Institution's Data & Systems.** Addresses the ability of the vendor to resell, assign or permit access by other entities to the financial institution's data and systems.

☐ 30. **Customer Complaint Handling.** Specifies whether the financial institution or the vendor has the duty to respond to any complaints received by the vendor from the financial institution's customers. If the vendor is responsible for responding, then a copy of any complaint and the vendor's response should be forwarded to the financial institution. The contract also provides for periodic summary reports detailing the status and resolution of complaints. If the institution is responsible for responding to customer complaints the vendor receives, the contract defines the procedures the vendor is to communicate any complaints (including the timeframe in which the vendor must communicate complaints) to the institution.

☐ 31. **Property Ownership.** Addresses ownership issues and the vendor's right to use the financial institution's property, including data, equipment, software and intellectual property, such as the institution's name and logo, trademark and other copyrighted material.

☐ 32. **Work Product Ownership.** Addresses ownership and control of any records generated by the vendor.

☐ 33. **Vendor's Technology Representations & Warranties.** Requires the vendor to provide representations and warranties to protect against viruses, malware, spyware, phishing, malicious codes and other unauthorized intrusions as applicable to electronic services that are provided by the vendor and data transmitted between the vendor and the financial institution.

☐ 34. **Vendor's Intellectual Property Representations & Warranties, Including Indemnification.** If any intellectual property is shared between the vendor and the financial institution, then representations and warranties with respect to the intellectual property are included in the contract. Additionally, indemnification provisions for the vendor's breach of the warranties are included in the contract, as well as other potential remedies that may be appropriate.

☐ 35. **No Management Functions & Decisions; Vendor Not Employee/Partner/Joint Venturer.** With regard to the services or products provided, the vendor will not perform management functions or make management decisions, or act in the capacity of an employee, or of any partner or joint venturer of the financial institution.

☐ 36. **IT Provisions.** If the contract is for information technology services, the contract addresses:

☐ a. Customer service support, including who will provide end-user "help" functions.

☐ b. What oversight and control will the financial institution have and what reports will it receive from the vendor.

☐ c. Financial institution support (including response times for requests to the vendor).

☐ d. Completion dates for installation and full functionality (including consideration of penalties for vendor-induced delays).

☐ e. Pricing on upgrades and on new releases.

☐ f. Assurances from the vendor that no new release is contemplated within a specified period following installation.

☐ g. Security issues associated with information technology, which include as appropriate (check those that are addressed in the contract): ___ network access; ___ application access; ___ data access; ___ physical access; ___ security monitoring techniques; and ___ security escalation procedures.

☐ h. Security issue performance standards, which include as appropriate (check those that are included in the contract): ___ frequency, form and transmission systems for reports; ___ how minor and major breaches are distinguished; ___ what will be done, how frequently and who will receive reports; and ___ the time period between event and report.

☐ i. Require Source Code escrow provision for software contracts, as appropriate.

☐ j. Obtain warranty from vendor against using self-help or disabling remedies in the event of a dispute.

☐ 37. **Data Control.** Addresses the following (check those included in the contract): ___ data destruction (pre- and post-termination, including hardware disposal); ___ encryption of communications; ___ responsibility for communication, authorization and notification; and ___ proxy or test data usage.

☐ 38. **Data Retention**. Specifies which records must be maintained by the vendor, the retention period and access to the records by the institution and its regulatory agencies. Costs of access to these records, including under legal compulsion (*e.g.*, subpoena) is also included.

☐ 39. **Tax Implications.** Addresses any tax implications, including any deductibility of start-up or upfront costs.

☐ 40. **Anti-Trust Restraints.** If there are any antitrust issues raised by restraints on pricing or other restraints on trade, then the contract addresses such issues.

☐ 41. **Insider/Affiliate Transactions.** Addresses insider or affiliate transaction issues, if applicable.

Additional contract provisions for Significant Level vendors:

☐ 42. **Background Checks.** Provides that the vendor and its employees agree to background checks at the vendor's expense. May also be appropriate to address areas requiring dual control, and other reconciliation measures.

☐ 43. **Performance of Banking Functions.** Addresses setting and monitoring of parameters relating to any banking functions, such as payment processing and any extensions of credit on behalf of the institution.

☐ 44. **Disaster Recovery and Business Continuity.** Addresses the vendor's responsibility for continuation of services provided for under the contract in the event of an operational failure, including both man-made and natural disasters. Ensures that the vendor has appropriate protections for backing up information and also maintain disaster recovery and contingency plans with sufficiently detailed operating procedures. The vendor agrees to permit financial institution to participate in periodic testing and agrees to provide the results of the periodic testing of these plans to the financial institution.

☐ 45. **Right to Audit.** Specifies the financial institution's right to audit the vendor (or engage an independent auditor) as needed to monitor the vendor's performance under the contract, including auditing the vendor's internal control environment as it relates to the product or service being provided. Also provides the types and frequency of audit reports the financial institution is entitled to receive from the vendor (*e.g.*, financial, internal controls, SSAE 16, SOC 1, SOC 2, and SOC 3 reports, and security reviews) and specifies whether internal or external audits, as appropriate, are acceptable to the financial institution.

☐ 46. **Privacy & Security of Personally Identifiable Data.** To the extent covered data (personally identifiable financial information) is accessible by the vendor, the contract includes vendor's compliance with the Gramm-Leach-Bliley Act, the California Financial Information Privacy Act and other customer information protection requirements, including audit, secure destruction and security incident notification.

Speaker Contact Information:

Anne M. McEvilly
Principal
Aldrich & Bonnefin, PLC
18500 Von Karman Avenue, Suite 300
Irvine, California 92612
Bus: 949-474-1944
Email: **AMcEvilly@ABLawyers.com**