CALIFORNIA BANKERS ASSOCIATION

Las Vegas, September 2023 Bankers Summit

New Interagency Guidance on Third-Party Risk Management, Compliance and Recent Consent Orders

Speakers:

Anne M. McEvilly, Esq., President & CEO, Aldrich & Bonnefin, PLC
Sean Kiester, Sr. Director, Vendor Mgmt., Fremont Bank

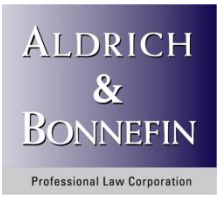
ALDRICH & BONNEFIN
Professional Law Corporation

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.

ALDRICH & BONNEFIN
Professional Law Corporation

New Third Party Risk Management Guidance



Third-Party Risk Management Guidance

- *Interagency Guidance on Third-Party Relationships: Risk Management*

- Jointly issued June 6, 2023, by the OCC, FRB and FDIC

ALDRICH & BONNEFIN
Professional Law Corporation

Rescinds Certain Prior Guidance

- Guidance rescinds:
  - FRB Guidance on Managing Outsourcing Risk (FRB SR-13-19);
  - OCC Risk Management Guidance issued in October 2013 (OCC Bulletin 2013-29);
  - OCC Third Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29; and
  - FDIC Guidance for Managing Third Party Risk issued in June 2008 (FIL-44-2008)

ALDRICH & BONNEFIN
Professional Law Corporation

Other Guidance Not Rescinded

- Not all prior guidance on this topic has been rescinded
- For example, the following are not rescinded (not exhaustive list):
  - FFIEC IT Booklets
  - Agencies' recent "*Cyber-Security Incident Notification Rule*"
  - OCC's "*Model Risk Management*" booklet, which is part of Comptroller's Handbook series; and
  - OCC's "*Third-Party Due Diligence Guide for Community Banks*"

ALDRICH & BONNEFIN
Professional Law Corporation

Scope of New Guidance

- New Guidance is intended to provide "broad, principles-based approach"
  - Agencies stated they intentionally did not revise final Guidance to address "specific topics or types" of relationships

ALDRICH & BONNEFIN
Professional Law Corporation

Future Guidance

- Agencies indicated plan to develop
  - "..*additional resources to assist smaller, non-complex community financial institutions in managing relevant third-party risks*"

ALDRICH & BONNEFIN
Professional Law Corporation

Credit Unions

- New Final Guidance does not apply to credit unions
- NCUA's Supervisory Letter No. 07-01
  - Entitled, "*Evaluating Third Party Relationships*"
  - Issued in October 2007
  - Remains valid & applicable to FCUs

ALDRICH & BONNEFIN
Professional Law Corporation

Scope

- Guidance applies to “third-party relationships”
  - “..*addresses <u>any business arrangement</u> between a financial institution and another entity, <u>by contract or otherwise</u>*”
  - Not limited to arrangements where third party is performing critical/material functions

ALDRICH & BONNEFIN
Professional Law Corporation

Scope

- Examples of covered relationships:
  - Outsourced services
  - Independent consultants
  - Referral arrangements
  - Merchant payment processing services; and
  - Services provided by institution's affiliates & subsidiaries

ALDRICH & BONNEFIN
Professional Law Corporation

Level of Due Diligence

- Guidance does not require institutions to apply same level of
  - Rigor
  - Due diligence; or
  - Risk management procedures
  - To every third-party relationship
- Instead, consider the materiality of the relationship to categorize risk and apply due diligence based on institution's size, complexity & risk profile

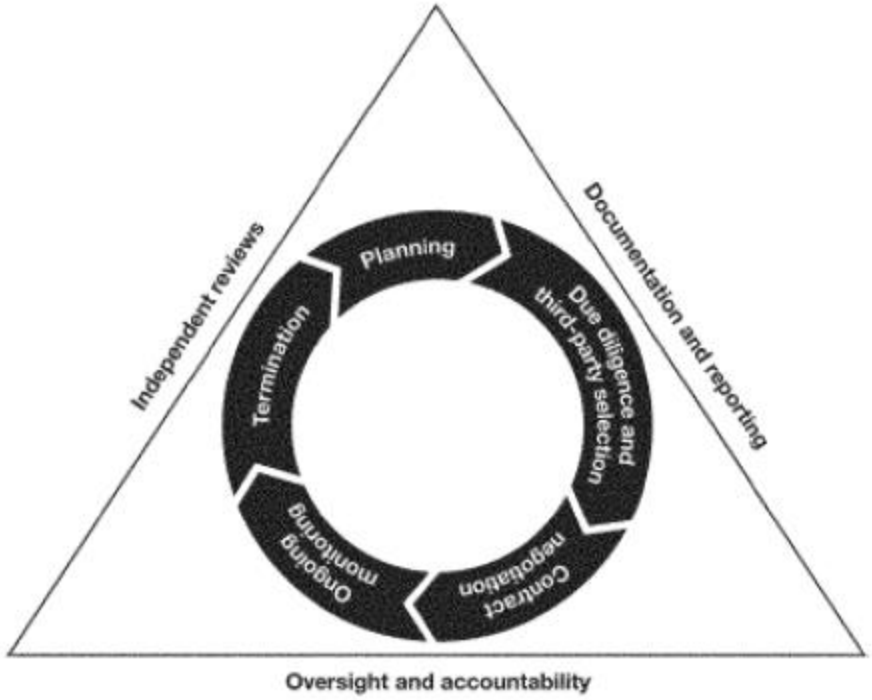
ALDRICH & BONNEFIN
Professional Law Corporation

Critical Activities

- May include activities that could:
  - Cause institution to face significant risk if third party fails to meet expectations
  - Have significant customer impact; or
  - Have significant impact on institution's financial condition or operations

ALDRICH & BONNEFIN
Professional Law Corporation

Figure 1: Stages of the Risk Management Life Cycle



Source: Board, FDIC, and OCC

ALDRICH & BONNEFIN
Professional Law Corporation

Stages of Third-Party Relationships

- Five stages of managing risks with third-party relationships:
  - Planning
  - Due diligence & third party selection
  - Contract negotiating
  - Ongoing monitoring; and
  - Termination

ALDRICH & BONNEFIN
Professional Law Corporation

Planning

- Institutions consider the following factors when developing a plan to address its third-party relationships:
  - Strategic purpose
  - Identification of benefits and risks
  - Nature of relationship
  - Expected costs
  - Impact on employees
  - Impact on customers
  - Information security implications
  - Physical security implications
  - Ongoing oversight; and
  - Contingency plans

ALDRICH & BONNEFIN
Professional Law Corporation

Due Diligence & Third-party Selection

- Due diligence at the selection phase may include review of third party's ability to:
  - Perform activity as expected
  - Adhere to policies related to activity
  - Comply with all applicable laws and regulations; and
  - Conduct activity in safe & sound manner

ALDRICH & BONNEFIN
Professional Law Corporation

Inability to Obtain Information

- When unable to obtain desired due diligence information from third party
- For example, third party
  - May not have long operational history
  - Prohibit on-site visits; or
  - May refuse to share information that institution requests

ALDRICH & BONNEFIN
Professional Law Corporation

Inability to Obtain Information

- In these situations, Guidance indicates it is important to:
  - Identify & document any limitations of its due diligence process
  - Understand risks created by those limitations; and
  - Consider alternatives as to how to mitigate risks

ALDRICH & BONNEFIN
Professional Law Corporation

Inability to Obtain Information

- For example, institution
  - May obtain alternative information to assess third party
  - Implement additional controls on or monitoring of third party to address information limitation; or
  - Consider using different third party

ALDRICH & BONNEFIN
Professional Law Corporation

Relevant Due Diligence Factors

- Institution would consider the following factors:
  - Strategies and goals
  - Legal and regulatory compliance
  - Financial condition
  - Business experience
  - Qualifications and background of key personnel
  - Risk Management
  - Information security
  - Management of information systems
  - Operational resilience
  - Incident reporting and management processes
  - Physical security
  - Reliance on subcontractors
  - Insurance coverage; and
  - Contractual arrangements with other parties

ALDRICH & BONNEFIN
Professional Law Corporation

Relevant Contractual Provisions

- Institutions consider a number of other factors when negotiating a contract:
  - Nature and scope of arrangement
  - Performance measures
  - Responsibilities for receipt and handling of information
  - Audit right and remediation
  - Compliance with applicable law
  - Costs and compensation
  - Ownership and license
  - Confidentiality and integrity
  - Operational resilience and business continuity
  - Indemnification and limits on liability
  - Insurance
  - Dispute resolution
  - Customer complaints
  - Subcontracting
  - Foreign-based third parties
  - Default and termination; and
  - Regulatory supervision;

ALDRICH & BONNEFIN
Professional Law Corporation

Ongoing Monitoring

- Effective third-party risk management includes ongoing monitoring throughout duration of third-party relationship
  - May be conducted on periodic or continuous basis
  - The greater the risk, the more frequent the monitoring

ALDRICH & BONNEFIN
Professional Law Corporation

Relevant Factors that Impact Ongoing Monitoring Activities

- The following factors when assessing appropriate ongoing monitoring activities to apply to its third-party risk management program:
  - Effectiveness of third party
  - Changes to third parties business strategy
  - Changes in financial condition
  - Insurance coverage
  - Audit results
  - Compliance with applicable law (…)

ALDRICH & BONNEFIN
Professional Law Corporation

Relevant Factors that Impact Ongoing Monitoring Activities

- Change to key personnel
- Subcontractors
- Training
- Incident response
- Confidentiality and integrity
- Business continuity
- External factors; and
- Customer complaints

ALDRICH & BONNEFIN
Professional Law Corporation

Termination

- Termination considerations may vary depending on degree of risk & complexity of relationship, and may include:
  - Transition options
  - Managing capabilities & resources
  - Costs
  - Data & systems control
  - Joint intellectual property; and
  - Failure by third party to meet expectations

ALDRICH & BONNEFIN
Professional Law Corporation

Oversight and Accountability

- Structure of third-party risk management processes may vary
  - Some institutions may disperse accountability for third-party risk management processes among their business lines
  - Others may consolidate processes under their
    - Compliance
    - Information security
    - Procurement; or
    - Risk management functions

ALDRICH & BONNEFIN
Professional Law Corporation

Discussion & Practice Points

ALDRICH & BONNEFIN
Professional Law Corporation

Discussion & Practice Points

- Due diligence documents vendors are reluctant to provide
  - Financials for private companies
  - Business continuity plans & tests
  - Audit reports (SOCs/SSAE)
  - Other security items

Penetration tests	Encryption policies
Security training	Third-party relationships

Discussion & Practice Points

- Vendor management process challenges
  - Scope of “business arrangements”
  - Business unit review/sign-off/approval
  - Complementary Entity User Controls
  - Cloud vendors
  - Ad-hoc vendors
  - Consultants
  - Certificate of Insurance v. Insurance Policy
  - 4th Party SOC Reports

Discussion & Practice Points

- Contract review
  - When does Compliance need to review?
  - When does Information Tech need to review?
  - When does Information Security need to review?
  - When does Legal need to review?

ALDRICH & BONNEFIN
Professional Law Corporation

Discussion & Practice Points

- Contract review
  - How much review does a new engagement for SOW require?
  - What about online agreements that vendor's change?
  - Dealing with a lack of negotiation leverage
  - How to cut ties with a bad vendor, mid-contract?

ALDRICH & BONNEFIN
Professional Law Corporation

Discussion & Practice Points

- Vendors who use Artificial Intelligence

ALDRICH & BONNEFIN
Professional Law Corporation

CALIFORNIA BANKERS ASSOCIATION

Noteworthy Resent Consent Orders

(Including Beyond Scope of Vendor Management)

ALDRICH & BONNEFIN
Professional Law Corporation

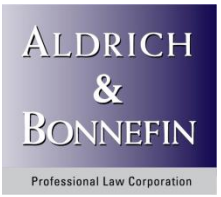
Noteworthy Consent Orders

- OCC American Express National Bank, Sandy, Utah (July 2023)
  - Consent Odder for engaging in unsafe or unsound practices regarding governance and oversight of its third-party affiliates
  - $15 million dollars in civil money penalties

ALDRICH & BONNEFIN
Professional Law Corporation

Noteworthy Consent Orders

- American Express National Bank, Utah, Failures
  - To properly govern and oversee third-party affiliate's call monitoring and documentation processes, including tracking and monitoring of customer complaints
  - To obtain EINs for certain small business customers and properly maintain records regarding compliance with CIP regulations; and
  - To properly maintain records related to its effort to retain such customers and, later, produce them in response to the OCC requests



Noteworthy Consent Orders

- CFPB Wells Fargo Bank Consent Order (Dec 2022)
  - $1.7 billion penalty (plus consumer redress)
  - Auto loan financing
    - Loan payments misapplied, erroneous fees/charges, incorrect repos, failed refunds on cancelled debt collection products
  - Home mortgage servicing
    - Qualified borrowers' modifications denied
  - Consumer deposit accounts
    - Improper freeze/closed, improper OD fees, failed to waive fees consistent with disclosures

ALDRICH & BONNEFIN
Professional Law Corporation

Noteworthy Consent Orders

- OCC MUFG Consent Order (June 2023)
  - $15 million civil money penalty
  - Alleged UDAP violations for fee waiver practices
  - Failed to disclose customer's affirmative request for waiver and corresponding account linking was condition precedent to waiver
- CFPB Supervisory Highlights (April 2023) noted recent fee waiver exam findings as raising UDAAP concerns, including back-end practices that did not match customer-facing disclosures

ALDRICH & BONNEFIN
Professional Law Corporation

Noteworthy Consent Orders

- CFPB and OCC Bank of America Consent Orders
  - CFPB and OCC assessed civil money penalties of $150 million and $60 million, respectively.
  - Alleged
    - “Multiple NSF” fees for same underlying transaction
    - Opening unauthorized consumer credit card accounts and deceptively advertising certain credit card-related rewards

ALDRICH & BONNEFIN
Professional Law Corporation

Noteworthy Consent Orders

- In summary….
  - Penalties are increasing
  - UDAP/UDAAP as basis for violations expanding
  - Back-end practices not mirroring front-end disclosures
  - Even with sufficient disclosure, the practice itself may be called into question under UDAP/UDAAP analysis
  - Emphasis on need for better oversight and controls

ALDRICH & BONNEFIN
Professional Law Corporation

CALIFORNIA BANKERS ASSOCIATION

We're adjourned!

Anne McEvilly, Esq.
President & CEO
Aldrich & Bonnefin, PLC
(949) 474-1944
AMcEvilly@ABLawyers.com

Sean Kiester
Sr. Director, Vendor Mgmt.
Fremont Bank
(510) 792-2300
Sean.Kiester@fremontbank.com

ALDRICH & BONNEFIN
Professional Law Corporation