CALIFORNIA BANKERS ASSOCIATION

2024 Bank Counsel Seminar

THIRD-PARTY RISK MANAGEMENT: LATEST GUIDANCE, INSIGHTS & A LOOK AHEAD

Presented By:
Anne M. McEvilly, Esq. and John M. Davis, Esq.
Aldrich & Bonnefin, PLC

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.

Third-Party Risk Management: A Guide for Community Banks

- OCC, FDIC and FRB Joint “Third-Party Risk Management, A Guide for Community Banks” (Guide) (May 2024)
  - Supplements 2023 “Interagency Guidance on Third-Party Relationships: Risk Management”

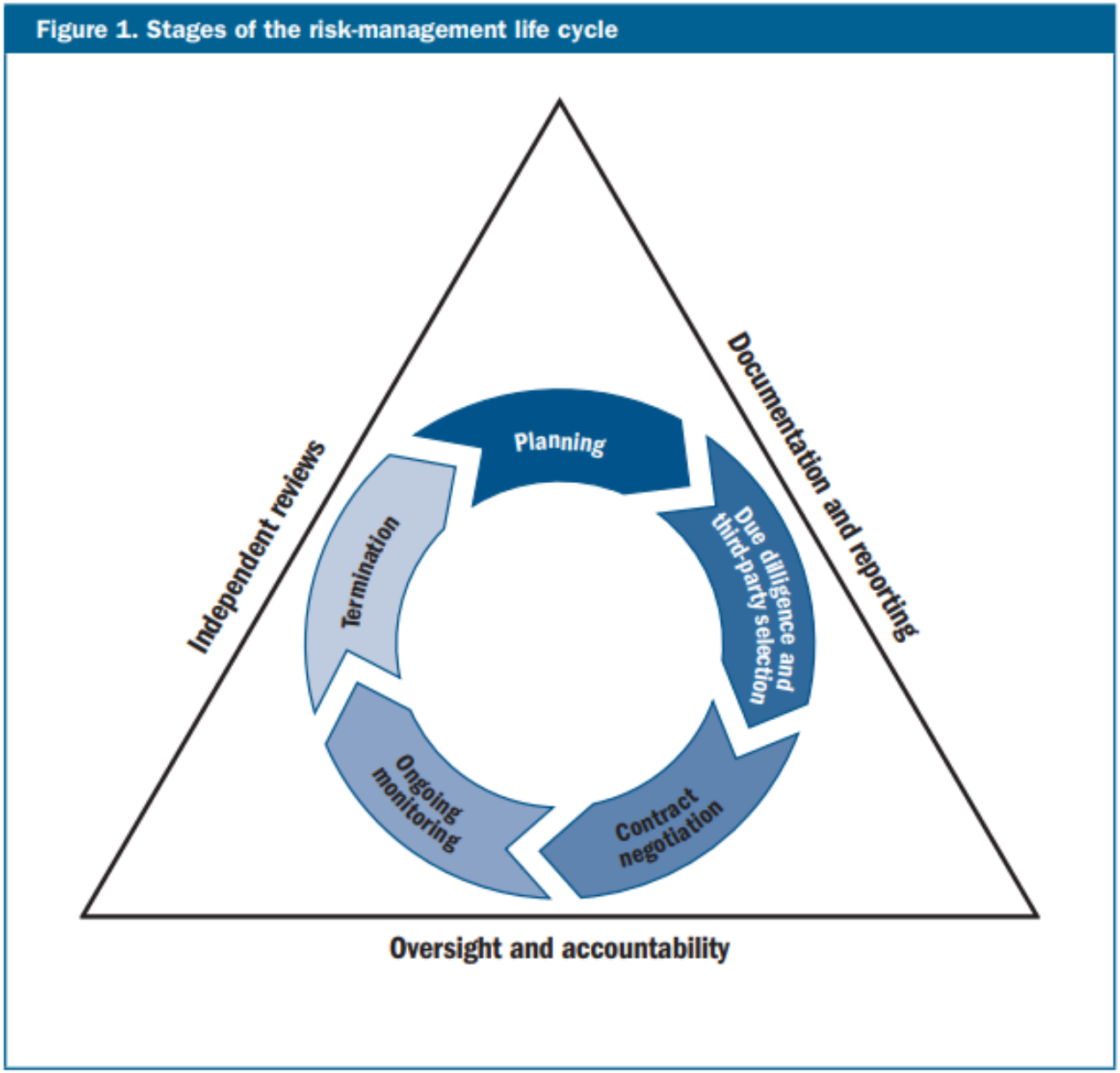
Third-Party Risk Management: A Guide for Community Banks

- Potential considerations, resources and examples
  - Guide provides potential considerations, resources, and examples through each stage of the third-party risk-management life cycle

Third-Party Risk Management: A Guide for Community Banks

- Risk management
  - More rigor over higher-risk activities
  - Considerations illustrated throughout the Guide
  - Initially identify relationships that support higher-risk activities, such as:
    - Has access to sensitive data
    - Processes transactions; or
    - Provides essential technology and business services

Third-party Relationship Life Cycle



Resources: Cloud Services

- Financial Services Sector Coordinating Council (FSSCC) and Financial and Banking Information Infrastructure Committee (FBIIC) issued Resources to Enhance Relationships with Cloud Service Providers (July 2024)
  - Cloud Outsourcing Issues and Considerations
  - Cloud Risk Assessment Framework
  - Principles for Security and Resilience in Cloud Environments
  - Cloud Lexicon

Request for Information

- OCC, FRB, & FDIC Joint Request for Information Bank-Fintech Arrangements Involving Banking Products & Services Distributed to Consumers and Businesses (July 2024)

Proposed Recordkeeping for Custodial Accounts

- FDIC's Proposed Recordkeeping for Custodial Accounts (Oct 2024)
  - "Custodial deposit account with transactional features"
    - Established for the benefit of beneficial owners
    - Comingles deposits of multiple beneficial owners; and
    - Beneficial owners may authorize or direct transfers to third parties
  - Banks would be required to maintain detailed records to identify: beneficial owners, balances attributable to each beneficial owner, and ownership categories
  - Subject to specific electronic file formatting

Guidance on Third-Party Deposit Products and Services Arrangements

- FRB, OCC & FDIC Joint Guidance on Banks' Arrangements with Third Parties to Deliver Bank Deposit Products and Services (July 2024)
  - Potential Risks
    - Operational & Compliance
    - Growth
    - End User Confusion and FDIC Insurance Misrepresentation
  - Risk Management and Governance

PRIVACY AND INFORMATION SECURITY ISSUES

Understanding Privacy Risks: The Data

- What type of data will the third party have access to?
  - It is critical to have a clear understanding of the type of data or information you will be providing or making available to the third party
  - The privacy risk is directly correlated to the type of data being provided to the third party
  - Level and degree of risk management needed to address privacy issues from a particular third party relationship will largely depend on whether the third party has access to information associated with individuals (referred to in this Outline as “Personal Data”)

Understanding Privacy Risks: The Data

- Different laws apply to different types of Personal Data
  - Consumer financial data is primarily subject to the GLBA and CFIPA
  - "Personal information" that can be "reasonably associated" with California residents is also subject to the California Consumer Privacy Act (CCPA)
    - Includes information on your own employees and individual information associated with business customers
    - The CCPA has a specific exemption for information subject to the GLBA (See Cal. Civil Code. Section 1798.145(e))
    - Consumer financial data is largely exempt from the CCPA
  - Other state privacy laws may apply
    - Check if you do business with residents of states other than California

Understanding Privacy Risks: The Data

- Specific data items viewed as highly sensitive can create an added layer of risk

- Examples include
  - Social security numbers
  - Information regarding gender identity or sexual orientation (consider the CFPB's Small Business Data Collection Rule)
  - Health information
  - Precise geolocation
  - Account credentials
  - Biometric information (*i.e.* face scans, fingerprints, voice authentication)

Understanding Privacy Risks: Usage

- How will the third party use Personal Data?
  - The manner in which the third party uses the Personal Data will also inform the level of privacy risk associated with the third party
  - What is the nature of the relationship?
    - Consider the types of services the third party will be performing
    - Ongoing access vs. one time transfer
  - Use of information needs to be consistent with any privacy disclosures or other legal notices an institution has provided to its customers or other individuals (to the extent applicable)

Understanding Privacy Risks: Usage

- Extensive reuse or complex processing of Personal Data can increase the privacy risk because
  - It might allow the third party to use Personal Data in a way the individual may not reasonably expect
  - Will the third party be creating inferences or outputs that the institution will rely on to make a decision?
  - Will the third party be incorporating Personal Data into its own proprietary technology, such as data analytic models or artificial intelligence (AI) technology?

Understanding Privacy Risks: Usage

- A third party that heavily relies on subcontractors can also increase the privacy risk
  - If the subcontractor has access to Personal Data the institution will need to consider if additional controls are necessary to manage the risk
  - High risk associated with subcontractors located outside of the United States

Understanding Information Security Risks: Data (again) and Integration

- Consider the type of data the third party will have access to
  - Type of information also impacts the information security risk associated with a third party
  - Personal Data can increase the information security risk because Personal Data is often targeted by fraudsters and other bad actors in order to perpetrate various crimes (such as identity theft)
  - If there is a breach, Personal Data also impacts whether the institution will have an obligation under federal and state laws to notify customers

Understanding Information Security Risks: Data (again) and Integration

- Other types of data and information (beyond just Personal Data) can create additional information security concerns
  - Proprietary information, such as information related to the institution's financial condition, or technology or models the institution relies on to provide services
  - Internal policies, procedures or controls for addressing fraud prevention or AML/CFT programs
  - Access credentials to the institution's internal communication systems, payment networks and other operational technology

Understanding Information Security Risks: Data (again) and Integration

- Consider how the third party will be accessing or integrating with the institution's internal information systems
  - Will the third party need to directly integrate its technology with the institution's internal applications and software
  - Many institutions are starting to shift away from on-premise technological solutions and moving towards cloud service providers
    - Cloud service providers can often offer more flexible technological solutions, but often require a deeper level of integration with the institution's internal information systems
  - Consider if the third party will be provided access credentials

Due Diligence

- Information revealed during the due diligence phase will also inform the privacy and information security risk associated with the third party
- Reputation
  - Consider if there any publicly reported complaints (from customers or regulators) about the third party
    - A quick google search can be useful
  - Any ongoing or prior regulatory complaints
  - Has the third party suffered an information security breach in the past which triggered notice under applicable breach notification laws

Due Diligence

- Review results of audit reports and independent testing related to privacy and information security controls
- Privacy and information security program
  - Policies, procedures and controls (do they have any?)
  - Incident response programs
  - Assess third party's data, infrastructure, and application security programs
- History of doing business with financial institutions
- Knowledge and familiarity with applicable privacy and information security laws
- Insurance coverage for privacy and information security issues

Important Contract Provisions to Address Privacy and Information Security Risks

Confidentiality and Use Restrictions

- Critical that the contract include provisions which address the confidentiality and use of the institution's data (particularly when it comes to Personal Data)
  - Effective contracts typically prohibit the use and disclosure of information by a third party and its subcontractors, except as necessary to provide the contracted activities or comply with legal requirements
    - Look for special carve outs in the contract
  - Privacy laws (such as the CCPA) may require contracts to includes specific provisions
  - For instance, under the CCPA if a contract does not satisfy specific requirements the third party will not be viewed as a "service provider" or "contractor"

Confidentiality and Use Restrictions

- GLBA
  - Unlike the CCPA, the GLBA does not impose a similar requirement on contracts with service providers that have access to Personal Data
  - There generally needs to be representation and warranty from the service provider that they have an information security program that meets certain information security standards issued under the GLBA

Confidentiality and Use Restrictions

- Storage
  - The contract should also appropriately limit where the third party may store the Personal Data
  - In most cases, institutions do not want third parties storing Personal Data outside of the United States

Audit Rights

- Contract should establish the institution's right to audit the third party specifically for privacy and information security
- Level and degree of an institution's contractual right to audit will be informed by the level of risk associated with the third party
- Most contracts include provisions that provide for periodic, independent audits of the third party and its relevant subcontractors
- In some cases boilerplate audit right provisions do not specifically reference whether the institution's audit right extends to privacy and information security issues
- An institution often needs to negotiate to address these issues
  - Assess whether the types of reports an institution is entitled to receive from the third party address privacy and information security issues (such as SOC reports)
  - Consider whether the institution feels it is necessary to reserve a right to conduct its own audit of the third party's privacy and information security controls
- This can often be one of the most heavily negotiated provisions in a contract

Ownership of Personal Data

- Contract should clearly define who owns any Personal Data accessed or used by the third party
- This can be difficult when Personal Data will be extensively processed or analyzed to make inferences or create outputs
- When Personal Data is processed by a model or a different type of sophisticated analytic system, the question often is who owns the output?

Incident Reporting By Third Party

- It is critical that the contract address notice obligations in the event of a data breach or other incident
- The contract should clearly define when the third party is obligated to notify the financial institution of a breach, incident or intrusion
  - Broader definition and scope is more protective of the institution
  - Even if the incident doesn't trigger a customer notice obligation under applicable law, the institution will want to be informed of any incident impacting a third party and the institution's data
- Provisions addressing incident reporting should be included in contracts with almost any third party, not just those that have access to Personal Data

Subcontractors

- The contract should address when and how the third party should notify the financial institution of its use or intent to use a subcontractor and whether the institution prohibits the use of specific subcontractors
  - The contract should give the institution the right to know who the subcontractors are (particularly if those subcontractors will have access to Personal Data)
  - The contract should give the institution the right to know where those subcontractors are located
  - Consider addressing the right of the institution to audit the subcontractor for compliance with applicable privacy and information security obligations
  - It is a good idea to try and reserve the institution's right to terminate the agreement if the third party uses a subcontractor that the institution disapproves of--but
    - Not all third parties will agree to this

Data Subject Requests

- Recently enacted privacy laws (such as the CCPA) have granted consumers various rights to request and control the Personal Data institution's obtain on them
- The contract should require the third party to assist or cooperate with the institution as necessary to comply with a Data Subject to Request received
  - CCPA Data Subject Requests
    - Grants California residents the right to request access (referred to as a "Right to Know" or "RTK"), to request the deletion (RTD) and to request the correction (RTC) of Personal Data collected about them
    - These rights extend to Personal Data maintained by a third party on behalf of a financial institution
    - Therefore, the contract should appropriately address the third party's obligation to assist the institution in responding to these Data Subject Requests
  - The GLBA does not grant consumers these types of rights over Personal Data, that is subject to the GLBA
  - However, the CFPB's Open Banking Rule issued under Section 1033 (discussed in below) will grant consumers the right to request access to their Personal Data, once that rule is finalized

Indemnification and Limitation on Liability

- Need to consider the extent to which the institution will be liable under the contract resulting from the failure of the third party or its subcontractor to comply with its own privacy or information security obligations
- In general, institutions should not be liable if a privacy or information security breach was solely the result of the third party's negligence --but
  - Many software and technology providers will not agree to indemnify the institution for damages resulting from their own negligence or will limit their liability resulting from such damages to a specific cap. These can be difficult negotiations
- Monetary damages resulting from just one information security breach can be significant. Therefore, it is critical that an institution clearly understand whether it will be held liable under the contract for the third party's own negligence with respect to privacy or information security issues
- If the third party will not agree to make the institution whole (even for its own failure) the institution will need to consider alternative ways to address the gap (such as insurance coverage)

Insurance Coverage

- Make sure the contract requires the third party to have appropriate insurance policies in place with appropriate policy limits
- Depending on the arrangement it may be appropriate to require the third party to have separate policies that specifically address privacy and information security problems, such as cyber insurance

New Artificial Intelligence Risks

- On March 27, 2024, the Treasury released a report entitled “Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector” (the “AI Risk Report”)
  - The AI Risk Report provides an overview of the state of artificial intelligence in the financial services sector (including banks and credit unions) and identifies various security and resiliency challenges that AI presents
  - The AI Risk Report also addresses certain best practices institutions should consider adopting when dealing with vendors or third parties that provide AI tools
  - Thus, it can be a helpful resource for institutions learning to deal with this new technology

AI-specific Due Diligence Issues

- In addition to common third-party risk-related questions, when dealing with an AI vendor, financial institutions should consider inquiring about
  - AI technology integration
  - Data privacy
  - Data retention policies
  - AI model validation
  - AI model maintenance
  - Consider asking their vendors if they rely on other vendors for data or models and if so, how they manage and account for these factors

Specific Questions or Requests

- The AI Risk Report indicates that financial institutions should consider making the following types of requests to vendors that utilize AI:
  - Notification to the financial institution if the third party makes changes or updates to products or services that use AI systems
  - Disclose the scope of AI system use in their products or services and notify them of material changes
  - Describe the model and data lifecycles, when an AI system is significant to a product or service
  - Explain the impact the AI systems could have on the financial institution's customers and how the financial institution can explain this impact to their customers
  - Describe the implemented security practices, including patch management and the vulnerability assessment process, of the infrastructure hosting the AI system
  - Describe any incorporated underlying third-party AI models

Section 1033 Data Sharing

- CFPB's Required Rulemaking on Personal Financial Data Rights
  - October 19, 2023, CFPB issued a Notice of Proposed Rulemaking
    - Must make financial information in institution's control available to consumers and their authorized third parties
    - Third parties will be subject to access requirements
      - Including privacy protections for the data
    - Goal to promote fair, open & inclusive industry standards
    - No opportunity for fees here
  - More detail provided in the outline

Notable Recent Enforcement Actions

- **Piermont Bank and Sutton Bank FDIC C&D and Consent Orders (Feb 2024)**
  - Safety and Soundness concerns regarding insufficient oversight, controls and Board supervision of BAAS and fintech third-party relationships
  - BSA compliance issues a theme
- **American Express Nat'l Bank OCC Consent Order (July 2023)**
  - OCC Consent Order and $15 million dollars in civil money penalties
  - Unsafe or unsound practices regarding governance and oversight of its third-party affiliates
- **Evolve Bancorp and Evolve Bank & Trust FRB C&D and Consent Order (June 2024)**
  - Bank offered deposit accounts & payment processing services to fintech companies which in turn offered financial products and services to end-user customers
  - FRB identified deficiencies in Bank's risk management of the Fintech Partner Program, including in the areas of AML compliance

CALIFORNIA BANKERS ASSOCIATION

We're adjourned!

Speaker Contact Information:

Anne M. McEvilly, Esq.
Principal
Aldrich & Bonnefin, PLC
(949) 474-1944
AMcevilly@ABLawyers.com

John M. Davis, Esq.
Associate
Aldrich & Bonnefin, PLC
(949) 474-1944
JDavis@ABLawyers.com