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 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.

I. INTRODUCTION

A. Introductory Remarks.

B. Supporting Materials.

II. Third-Party Risk Management : A Guide for Community Banks.

A. 2024 Joint Agency Issuance. On May 3, 2024, the OCC, FDIC, and OCC (the "Agencies") issued joint guidance titled "Third-Party Risk Management, A Guide for Community Banks" (2024 Guide).

1. Tool to aid development and implementation. The 2024 Guide is intended to help institutions develop and implement their third-party risk management programs, policies, and practices.

2. Potential considerations, resources and examples. The 2024 Guide provides potential considerations, resources, and examples through each stage of the third-party risk-management life cycle.

3. Supplements TPRM Guidance. On June 6, 2023, the Agencies issued guidance also intended to assist financial institutions in managing risks with their third-party relationships titled, "Interagency Guidance on Third-Party Relationships: Risk Management" (the "TPRM Guidance"). 88 FR 37920. The 2024 Guide is intended to supplement and not replace the TPRM Guidance.

a) Reminder: TPRM Guidance rescinded certain prior guidance. The TPRM Guidance rescinded and replaced some of the Agencies' guidance previously issued on the topic of third-party risk management. Specifically, the TPRM Guidance rescinded the following:

(1) FRB Guidance on Managing Outsourcing Risk (issued December 5, 2013, Updated February 26, 2021) (FRB SR-13-19);

(2) OCC Risk Management Guidance issued in October 2013 (OCC Bulletin 2013-29);

(3) OCC Third Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29; and

(4) FDIC Guidance for Managing Third party Risk issued in June 2008 (FIL-44-2008).

b) Other non-rescinded guidance still valid. The TPRM Guidance has not resulted in the rescission of other regulatory materials that address this topic.

c) Not applicable to credit unions. The NCUA did not participate in the issuance of the TPRM Guidance. The NCUA's Supervisory Letter No. 07-01 entitled, "Evaluating Third Party Relationships," issued in October 2007, remains valid and applicable to FCUs.

B. 2024 Guide Summary.

1. Risk management.

a) More rigor over higher-risk activities. As part of sound risk management, community banks are expected to apply more rigorous risk-management practices throughout the third-party relationship life cycle for third parties that support higher-risk activities, including critical activities.

b) Considerations illustrated in the 2024 Guide. The 2024 Guide includes considerations illustrating how a community bank may apply risk-management practices in different stages of the third-party relationship life cycle.

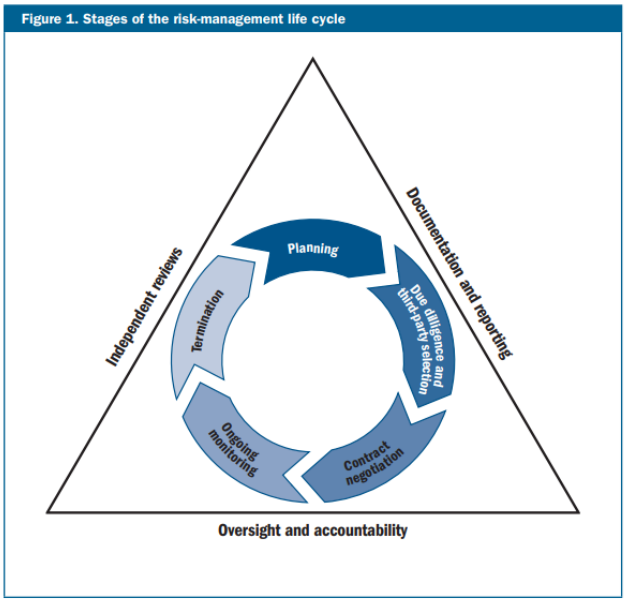
c) Initially identify relationships that support higher-risk activities. An important initial step is identifying third-party relationships that support higher-risk activities, including critical activities. In determining whether an activity is higher risk, banks may assess various factors, such as if the third-party:

(1) Has access to sensitive data (including customer data);

(2) Processes transactions; or

(3) Provides essential technology and business services.

2. Third-party relationship life cycle.



a) Planning.

(1) Careful planning enables a community bank to consider potential risks in the proposed third-party relationship.

(2) In addition, risk assessments are an important component of managing third-party relationships and help a bank evaluate the extent of risk-management resources and practices for effective oversight of the proposed third-party relationship throughout the subsequent stages of the third-party relationship life cycle.

b) Due diligence in third-party selection.

(1) Due diligence is the process by which a community bank assesses, before entering into a third-party relationship, a particular third party's ability to perform the activity as expected, adhere to the community bank's policies, comply with all applicable laws and regulations, and conduct the activity in a safe and sound manner.

(2) Effective due diligence assists with the selection of capable and reliable third parties to perform activities for, through, or on behalf of the community bank.

(3) If the bank cannot obtain desired due diligence information from the third party, the bank may consider alternative information, controls, or monitoring.

c) Contract negotiation.

(1) Before entering a contractual relationship with a third party, a community bank typically considers contract provisions that meet its business objectives, regulatory obligations, and risk-management policies and procedures.

(2) The community bank typically negotiates contract provisions that facilitate effective risk management and oversight, including terms that specify the expectations and obligations of both the community bank and the third party.

(3) When a community bank has limited negotiating power, it is important for bank management to understand any resulting

limitations and consequent risks. Possible actions that bank management might take in such circumstances include:

(a) Determining whether the contract can still meet the community bank's needs;

(b) Whether the contract would result in increased risk to the community bank; and

(c) Whether residual risks are acceptable.

d) Ongoing monitoring.

(1) A community bank's ongoing monitoring of the third party's performance enables bank management to determine if the third party is performing as required for the duration of the contract.

(2) The bank may also use information from ongoing monitoring to adapt and refine its risk-management practices.

e) Termination.

(1) A community bank may choose to end its relationship with a third party for a variety of reasons.

(2) A bank typically considers the impact of a potential termination during the planning stage of the life cycle. This consideration may help to mitigate costs and disruptions caused by

termination, particularly for higher-risk activities, including critical activities.

3. Governance. Community banks typically consider the following governance practices throughout the third-party relationship life cycle:

a) Oversight and accountability;

b) Independent reviews; and

c) Documentation and reporting.

III. PRIVACY AND INFORMATION SECURITY ISSUES

A. Understanding Privacy Risks: Data and Usage.

1. What type of data will the third party have access to? Prior to entering the relationship, 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.

a) The privacy risk associated with a particular third party relationship is directly correlated to the type of data being provided to the third party.

b) The 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").

c) Different laws apply to different types of Personal Data.

(1) Consumer (*i.e.* for personal, family or household use) financial data is primarily subject to specific restrictions under the Gramm-Leach Bliley Act (GLBA) and its implementing Regulation P, and the California Financial Information Privacy Act (CFIPA).

(2) "Personal information" that can be "reasonably associated" with California residents is also subject to the California Consumer Privacy Act (CCPA).

(a) Includes information on your own employees and individual information associated with business customers.

(b) The CCPA has a specific exemption for information subject to the GLBA (See Cal. Civil Code. Section 1798.145(e)). Therefore, consumer financial data is largely exempt from the CCPA.

(3) If the Personal Data of residents from other states is involved, other state privacy laws may apply. Various states have passed comprehensive privacy laws that are similar in scope to the CCPA (such as Oregon, Colorado, and Texas).

d) Specific data items viewed as highly sensitive can create an added layer of risk. Examples include:

(1) Social security numbers;

(2) Information regarding gender identity or sexual orientation (consider the CFPB's Small Business Data Collection Rule);

(3) Health information;

(4) Precise geolocation;

(5) Account credentials;

(6) Biometric information (i.e. face scans, fingerprints, voice authentication).

2. How will the third party use Personal Data?

a) The manner in which the third party uses the Personal Data will also inform the level of privacy risk associated with the third party.

b) What is the nature of the relationship?

(1) Consider the types of services the third party will be performing.

(2) Will the third party need ongoing access to Personal Data or is it just a one time transfer?

c) A third party's use of Personal Data needs to be consistent with any privacy disclosures or other legal notices an institution has provided to its customers or other individuals (such as its GLBA privacy notice or the CCPA Notice at Collection).

d) Extensive reuse or complex processing of Personal Data by a third party can increase the privacy risk because it might allow the third party to use the Personal Data in a way the individual may not reasonably expect.

(1) Will the third party be analyzing the Personal Data to create inferences or outputs that the institution will rely on to make a decision?

(2) Will the third party be incorporating Personal Data into its own proprietary technology, such as data analytic models or artificial intelligence (AI) technology?

e) A third party that heavily relies on subcontractors can also increase the privacy risk.

(1) If the subcontractor has access to Personal Data the institution will need to consider if additional controls are necessary to manage the risk.

(2) High risk associated with subcontractors located outside of the United States.

B. Understanding Information Security Risks: Data (again) and Integration.

1. Consider the type of data the third party will have access to.

a) The type of information a third party has access to also impacts the information security risk associated with a third party.

b) Personal Data also creates an 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).

c) If there is a breach, Personal Data also impacts whether the institution will have an obligation under federal and state laws to notify customers.

d) However, other types of data and information (beyond just Personal Data) can create additional information security concerns.

(1) Proprietary information, such as information related to the institution's financial condition, or technology or models the institution relies on to provide services.

(2) Internal policies, procedures or controls for addressing fraud prevention or AML/CFT programs.

(3) Access credentials to the institution's internal communication systems, payment networks and other operational technology.

2. Consider how the third party will be accessing or integrating with the institution's internal information systems.

a) Will the third party need to directly integrate its technology with the institution's internal applications and software?

b) Many institutions are starting to shift away from on-premise technological solutions and moving towards cloud service providers.

c) 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.

d) Consider if the third party will be provided access credentials.

C. Due Diligence. Information revealed during the due diligence phase will also inform the privacy and information security risk associated with the third party.

1. Reputation. What is the third party's reputation when it comes to privacy and information security issues?

a) Consider if there any publicly reported on complaints (from customers or regulators) about the third party. A quick google search can be useful.

b) Are there any ongoing or has there been prior regulatory complaints filed against the third party?

c) Has the third party suffered an information security breach in the past which triggered notice under applicable breach notification laws.

2. Review results of audit reports and independent testing related to privacy and information security controls.

3. Review the third party's privacy and information security program.

a) What are its policies, procedures and controls (or do they have any)?

b) Incident response programs.

c) Assess the third party's data, infrastructure, and application security programs.

4. History of doing business with financial institutions.

5. Assess the third party's knowledge and familiarity with applicable privacy and information security laws.

6. Insurance coverage for privacy and information security issues.

D. Important Contract Provisions to Address Privacy and Information Security Risks.

1. Confidentiality and Use Restrictions. It is critical that the contract include provisions which address the confidentiality and use of the institution's data (particularly when it comes to Personal Data).

a) 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.

b) The CCPA specifically requires contracts with entities viewed as "service providers" or "contractors" to include the following provisions:

(1) A prohibition on "selling" or "sharing" Personal Data;

(2) Identification of the specific purpose or reason the third party is being provided the Personal Data, and a corresponding agreement by the third party to use the Personal Data for no other reason;

(3) An express requirement by the third party to comply with the CCPA;

(4) A right to audit the third party for specific compliance with the CCPA;

(5) An obligation to notify the financial institution if the third party determines it can no longer satisfy its obligations under the CCPA, and a right for the financial institution rectify the violation once being notified;

(6) An agreement by the third party to assist the financial institution comply with consumer requests made pursuant to the CCPA (referred to as "Data Subject Requests").

Note, if the contract does not satisfy these specific requirements the third party will not be viewed as a "service provider" or "contractor" under the CCPA. See 11 CCR Section 7050(e).

c) The GLBA does not impose a similar requirement on contracts with service providers that have access to Personal Data subject to the GLBA. However, 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.

d) If Personal Data is involved, 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.

2. Audit rights.

a) The contract should establish the institution's right to audit the third party specifically for privacy and information security issues (this is also expressly required in certain instances under the CCPA).

b) The level and degree of an institution's contractual right to audit will be informed by the level of risk associated with the third party.

c) Most contracts include provisions that provide for periodic, independent audits of the third party and its relevant subcontractors.

d) However, in some cases boilerplate audit right provisions do not specifically reference whether the institution's audit right extends to privacy and information security issues.

e) Thus, an institution often needs to negotiate to address these issues.

(1) 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).

(2) 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.

f) This can often be one of the most heavily negotiated provisions in a contract.

3. Ownership of Personal Data.

a) The contract should clearly define who owns any Personal Data accessed or used by the third party.

b) This can be complicated when Personal Data with technology or software providers that will be extensively processing or analyzing Personal Data to make inferences or create outputs.

c) When Personal Data is processed by a model or a different type of sophisticated analytic system, the question often is who owns the output?

4. Incident Reporting By Third Party.

a) It is critical that the contract specifies when and how the third party will disclose, in a timely manner, information security breaches or unauthorized intrusions.

b) The contract should clearly define when the third party is obligated to notify the financial institution of a breach, incident or intrusion.

(1) A more broad definition of will better protect the institution.

(2) 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.

c) Provisions addressing incident reporting should be included in contracts with almost any third party, not just those that have access to Personal Data.

5. 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.

a) The contract should give the institution the right to know who the subcontractors are (particularly if those subcontractors will have access to Personal Data).

b) The contract should give the institution the right to know where those subcontractors are located.

c) Consider addressing the right of the institution to audit the subcontractor for compliance with applicable privacy and information security obligations.

d) It is a good idea to reserve the institution's right to terminate the agreement if the third party uses a subcontractor that the institution disapproves of. However, not all third parties will agree to this.

6. 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.

a) CCPA Data Subject Requests.

(1) 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 (RTD) of Personal Data collected about them.

(2) The RTK, RTD, and RTC rights extend to Personal Data maintained by a third party on behalf of a financial institution.

(3) Therefore, the contract should appropriately address the third party's obligation to assist the institution in responding to these Data Subject Requests.

b) The GLBA does not grant consumers these types of rights over Personal Data, that is subject to the GLBA.

c) However, the CFPB's Open Banking Rule issued under Section 1033 (discussed in Section IV. below) will grant consumers the right to request access to their Personal Data, once that rule is finalized.

7. Indemnification and Limitation on Liability.

a) 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.

b) In general, institutions should not be liable if a privacy or information security breach was solely the result of the third party's negligence.

c) However, 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.

d) The 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.

e) 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).

8. Insurance Coverage.

a) Make sure the contract requires the third party to have appropriate insurance policies in place with appropriate policy limits.

b) 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.

E. New Artificial Intelligence Risks.

1. 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").

a) 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.

b) 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.

2. 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

a) AI technology integration;

b) Data privacy;

c) Data retention policies;

d) AI model validation;

e) AI model maintenance; and

f) 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.

3. 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:

a) Notify the financial institution if the third party makes changes or updates to products or services that use AI systems;

b) Disclose the scope of AI system use in their products or services and notify them of material changes;

c) Describe the model and data lifecycles, when an AI system is significant to a product or service;

d) 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;

e) Describe the implemented security practices, including patch management and the vulnerability assessment process, of the infrastructure hosting the AI system; and

f) Describe any incorporated underlying third-party AI models.

IV. SECTION 1033 DATA SHARING (OPEN BANKING)

A. Section 1033. Section 1033 of the Consumer Financial Protection Act of 2010 (CFPA) provides that subject to rules prescribed by the CFPB, a covered person must make information in their control or possession concerning consumer financial products or services to that consumer upon request. Although Section 1033 was enacted over thirteen years ago, it has no effect until such time that the CFPB issues a rule or regulation implementing the statutory requirements.

B. CFPB's Proposed Rule. On October 19, 2023, the CFPB took a big first step towards implementing Section 1033 of the CFPA by publishing a notice of proposed rulemaking to enact its requirements. The proposed rule contemplates that the CFPB would implement Section 1033 through the introduction of a new set of regulations in 12 CFR Section 1033.

1. Making information available to consumers and authorized third parties. The proposed rule would require depository and non-depository entities to make available to consumers and authorized third parties certain data relating to consumers' transactions and accounts.

2. Obligations on third parties accessing data. The proposed rule would establish obligations for third parties accessing a consumer's data, including important privacy protections for that data.

3. Standards for accessing data. The proposed rule would also provide basic standards for data access; and promote fair, open, and inclusive industry standards.

C. Covered Data Provider. A "covered data provider" would be a covered person (as defined in 12 USC 5481) that:

1. Is a financial institution, as defined in Regulation E and controls or possesses covered data concerning a covered consumer financial product or service;

2. Is a card issuer, as defined in Regulation Z and controls or possesses covered data concerning a covered consumer financial product or service; or

3. Controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person, and also controls or possesses covered data concerning any covered consumer financial product or service.

D. Covered Data. Covered data would mean:

1. Transaction information, including historical transaction information in the control or possession of the data provider;

2. Account balance;

3. information to initiate payment to or from a Regulation E account;

4. Terms and conditions (e.g., applicable fee schedule, any annual percentage rate or annual percentage yield, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement);

5. Upcoming bill information (e.g., information about third party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider); and

6. Basic account verification information (limited to the name, address, email address, and phone number associated with the covered consumer financial product or service).

E. Excluded as Covered Data. Covered data would not include:

1. Confidential commercial information;

2. Information collected by the data provider for the sole purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct;

3. Information required to be kept confidential by any other provision of law; or

4. Information that the data provider cannot retrieve in the ordinary course of its business.

F. Establishing and Maintaining Interfaces.

1. A covered data provider would be required to have a consumer interface and a developer interface (an interface that a data provider establishes and maintains to receive requests for covered data and make covered data available to authorized third parties).

2. Both the consumer interface and developer interface would have to make available, upon request, covered data in a machine-readable file that can be retained by a consumer or authorized third party and transferred for processing into a separate information system that is reasonably available to and in the control of the consumer or authorized third party.

3. The developer interface would have to satisfy additional standardized format, performance, and security requirements set forth in the proposed rule.

G. Third Party's Certification Obligations. A third party would have to certify its agreement to certain third party obligations in order to be an authorized third party. These third party obligations would include:

1. Adhering to the proposed limitations on the collection, use, and retention of covered data;

2. Establishing, maintaining, periodically reviewing, and updating (as appropriate) policies and procedures to ensure that covered data is accurately transmitted;

3. Applying an information security program that satisfies Section 501 of the Gramm Leach Bliley Act to its systems for the collection, use, and retention of covered data;

4. Providing consumers with copies of their authorization disclosures, information about the third party's access to their covered data, and third-party contact information;

5. Providing a mechanism that the consumer can use to revoke the third party's authorization to access covered data. The mechanism must be as easy to access and operate as the initial authorization; and

6. Additionally, a third party with authorization to access to covered data would have certify that it will contractually require other third parties to comply with certain obligations (including limits on collection, use, and retention of covered data) before providing covered data to them.

H. Fees Prohibited. A covered data provider would be prohibited from imposing any fees or charges on a consumer or authorized third party in connection with:

1. Establishing or maintaining the interfaces required by the proposed rule; or

2. Receiving requests or making available covered data in response to requests as required by the proposed rule.

I. Proposed Compliance Dates. Depository institutions as data providers would have to comply according to the following:

1. Approximately six months after the date of publication of the final rule in the Federal Register for depository institutions that hold at least $500 billion in total assets.

2. Approximately one year after the date of publication of the final rule in the Federal Register for depository institutions that hold at least $50 billion in total assets but less than $500 billion in total assets.

3. Approximately two and a half years after the date of publication of the final rule in the Federal Register for depository institutions that hold at least $850 million in total assets but less than $50 billion in total assets.

4. Approximately four years after the date of publication of the final rule in the Federal Register for depository institutions that hold less than $850 million in total assets.

V. CONCLUSION & CONTACT INFORMATION

Anne M. McEvilly, Esq.
CEO & Principal
Aldrich & Bonnefin, PLC
(949)474-1944
Amcevilly@ablawyers.com

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