1 Due Diligence in Corporate Transactions Author(s)

Due Diligence in Corporate Transactions > Publication Information

Author(s)

Due Diligence in Corporate Transactions
2026

Frank Ciatto

Randi Rubinstein

Vikram Suryavanshi

Due Diligence in Corporate Transactions

End of Document

1 Due Diligence in Corporate Transactions Questions

Due Diligence in Corporate Transactions > Publication Information

Questions

Technical Questions

Phone: (800) 223-5297

Fax: (800) 533-1645 or (518) 487-3191

E-mail: *technical.support@lexisnexis.com*

Visit Our Web Site: *http://www.lexis.com*

Editorial Questions

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call or email:

Donna Hart, J.D. at 908-673-3371

Email: ..... *donna.m.hart@lexisnexis.com*

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844

Outside the United States and Canada, please call ..... (518) 487-3385

Fax Number ..... (800) 828-8341

LexisNexis® Support Center ..... *https://supportcenter.lexisnexis.com/app/home/*

For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940

Outside the United States and Canada, please call ..... (518) 487-3385

1 Due Diligence in Corporate Transactions Copyright

Due Diligence in Corporate Transactions > Publication Information

Copyright

ISBN: 979-8-3417-0319-3 (print)

ISBN: 979-8-3417-0320-9 (eBook)

ISSN: 3070-0566 (print)

ISSN: 3070-0574 (online)

1 Due Diligence in Corporate Transactions About the General Editors

Due Diligence in Corporate Transactions > Publication Information

About the General Editors

Frank Ciatto is Co-Chair of Venable's Corporate Practice Group, where he manages offices across the country while maintaining his personal presence in Washington D.C. and New York. Frank is a business attorney who assists entrepreneurs with existing and new business ventures. His legal knowledge and practical experience are important in helping owners and investors realize the full value of their ideas and investments. He focuses on corporate and partnership structuring, mergers and acquisitions, limited liability companies, private equity investments, tax and accounting issues, business divorces, and succession planning.

Frank drafts and negotiates key business documents, such as merger agreements, limited liability company agreements, partnership agreements, stockholder agreements, executive employment agreements, severance agreements, stock-option plans, grant agreements, and other corporate agreements.

He serves as corporate counsel to entrepreneurs and individual investors in a number of industries, including hedge funds, financial services providers, auto dealerships, publishing, securities companies, professional consulting firms, software and technology providers, hospitality, law firms, and other professional service providers.

In addition to his legal work, Frank is a certified public accountant, formerly with Coopers & Lybrand (now PricewaterhouseCoopers) in New York – experience that often adds value to his clients' transactions.

Frank served as the firm's corporate counsel in its recent combination with the Fitzpatrick Cella law firm.

Randi Rubinstein is an Associate in Venable's Corporate Group in the Washington, D.C. office. She advises clients in a wide variety of transactional matters, including mergers and acquisitions, corporate governance, and commercial contracts. She has experience in drafting commercial contracts, limited liability company agreements, stockholder agreements, buy-sell agreements, and other key business documents. She also advises borrowers and lenders in debt financing transactions, including acquisition financing, working capital lines of credit, and other types of loan facilities. She has advised clients in complex transactions across a variety of industries, including real estate, healthcare, hospitality, food service, automotive, and technology.

Vikram Suryavanshi is an Associate in Venable's Corporate Group in the New York office. He advises clients on a broad range of corporate and transactional matters, with a focus on mergers and acquisitions, commercial contracts, and corporate governance. In his practice, Vikram supports partners in structuring complex transactions and works closely with specialists in tax, employee benefits, and regulatory compliance to address key diligence and deal considerations. He also has experience drafting limited liability company agreements, buy-sell agreements, and other foundational business documents.

1 Due Diligence in Corporate Transactions About the Contributing Authors

About the Contributing Authors

Taylor Beck is an Associate in the Washington, D.C. office of Venable LLP, where her practice focuses on a wide range of commercial real estate transactions, including leasing, acquisitions, dispositions, financings, joint ventures, and land conservation.

Emma Blaser is a Partner in the Washington, D.C. office of Venable LLP. She counsels clients on all aspects of compliance with privacy and data security laws, including U.S. state privacy laws, child and teen privacy laws, the Gramm-Leach-Bliley Act (GLBA), and the Video Privacy Protection Act (VPPA). She has valuable and practical experience gained from multiple secondments embedded with global corporations, working closely with her clients' legal, business, and technology teams.

Neha Dhindsa is Counsel in the Washington, D.C. office of Venable LLP. She is a member of the International Trade and Logistics Group and her practice focuses on international trade, customs, maritime, and transportation issues, including sanctions and export controls laws, U.S. import customs compliance, transportation laws and other regulations affecting cross-border transactions. Neha represents clients in compliance and due diligence reviews, disclosures, investigations, and disputes, helping companies engaged in cross-border business navigate the complex regulatory landscape governing imports, exports, and international transactions and transportation.

Audrey Distler is Counsel in the Washington, D.C. office of Venable LLP. She advises clients on domestic and cross-border transactions, including mergers and acquisitions, divestitures, joint ventures, strategic alliances, and venture capital and private equity investments. She has extensive experience negotiating transactional risk allocation, including representations and warranties insurance (RWI), both on the deal side and as underwriting counsel for RWI carriers. She also regularly drafts and negotiates key corporate and commercial agreements and advises on corporate governance matters.

Leah A. Druckerman is Counsel in the New York office of Venable LLP. Her practice focuses on data protection, data privacy, and cybersecurity in transactions, including corporate transactions such as mergers, acquisitions, strategic partnerships, and joint ventures, and technology transactions such as outsourcing, licensing, and development relationships across regulated and non-regulated industries. She also regularly assists clients with security incident response, remediation, and related matters, including crisis management, reporting and notification of security incidents, and representation in connection with resulting regulatory inquiries.

Craig Gilley is a Partner in the Washington, D.C. office of Venable LLP practicing in telecommunications and technology law. A trusted advisor for companies operating at the intersection of telecommunications, technology, regulation, and business strategy, Craig guides clients through complex regulatory and business challenges across the full spectrum of emerging technologies—from traditional telecom and broadband to cutting-edge artificial intelligence (AI), data centers, internet of things (IoT), and cloud services.

John M. Harras is Counsel in the New York office of Venable LLP, where his practice focuses on employee benefits matters arising from corporate transactions, including multiemployer pension plan withdrawal liability. Prior to joining Venable LLP, Mr. Harras was senior counsel at Bond, Schoeneck & King PLLC and a partner at Virginia & Ambinder LLP.

Hayley Klein is an Associate in Venable's Labor and Employment Group in the Tysons, V.A. office. Hayley's practice involves providing strategic counselling to employers on employment and labor issues, as well as

defending against employment-related litigation. Hayley represents private and public entities, as well as nonprofit and educational institutions, in connection with internal and governmental investigations, including those regarding discrimination, harassment, and retaliation, and various forms of other workplace misconduct. Hayley also serves as a subject matter expert in connection with complex corporate transactions, advising on employment considerations related to potential mergers and acquisitions.

Liz Barket Kremser is an Associate in Venable's Los Angeles office. She is a member of the firm's corporate Group, and her practice focuses on mergers and acquisitions, financings, and other corporate transactions.

Clayton D. Laing is an Associate in the Washington, D.C. office of Venable LLP and a member of the Firm's Commercial Real Estate Group. His practice focuses on a wide range of commercial real estate transactions including acquisition and dispositions, financings, commercial leasing, and real estate joint ventures and investment structuring.

Diz Locaria is a Partner in the Washington, D.C. office of Venable LLP. He assists government contractors and grant recipients in all aspects of doing business with the federal government. Diz has extensive knowledge of government contract and grant regulations, enabling him to help organizations qualify to become federal contractors or grantees. He represents clients in compliance with various federal procurement and grant requirements, including ethics and integrity; mandatory disclosures; False Claims Act; responsibility matters, such as suspension and debarment; small business matters; and General Services Administration (GSA) Federal Supply Schedule contracting. Diz also represents and counsels clients regarding the Homeland Security Act, including obtaining and maintaining SAFETY Act protections.

Ari J. Markenson is a Partner in the Healthcare and Corporate Practices at Venable LLP in New York. He has built his career at the intersection of healthcare, law, and business, advising industry stakeholders—including investors, lenders, providers, and suppliers—on a wide range of regulatory and corporate matters. Ari has significant experience guiding clients through complex healthcare acquisitions and financial transactions, regularly representing private equity firms and lenders in these deals. He also provides counsel on compliance and regulatory issues affecting sellers and potential borrowers working with banks and other financing sources. Ari advises healthcare organizations on matters such as conditions of participation; fraud and abuse; and survey, certification, licensure, and enforcement issues. He is a frequent speaker and author for leading healthcare organizations on topics related to healthcare law and business. An active participant in professional organizations, Ari is a Past Chair of the New York State Bar Association's Health Law Section, where he continues to serve on the Executive Committee. He is also a member of the Board of the American Health Law Association and an engaged contributor to its work. Ari holds several academic appointments: Adjunct Professor of Health Policy and Management at the Columbia University Mailman School of Public Health; Adjunct Assistant Professor of Law at Columbia Law School; Adjunct Associate Professor in Pace University's College of Health Professions; and Adjunct Professor of Law at the Elisabeth Haub School of Law at Pace University.

Kirill Y. Nikonov is a Counsel in the New York office of Venable LLP. He advises public companies on capital markets transactions, SEC reporting, and corporate governance matters. He also counsels public and private companies on securities law compliance relating to blockchain and digital assets.

Gregory W. Packer, Jr. is an Associate in the Tysons, V.A. office of Venable LLP where his practice focuses on mergers and acquisitions and general corporate matters.

Joe Schmelter is a Partner in the Tysons, V.A. office of Venable, where he often advises government contractors – including technology, aerospace, defense and services companies – in their M&A and debt and equity finance transactions.

Andrew E. Shapiro is a Partner in the New York office of Venable LLP. His practice focuses on counseling both public and private companies, as well as senior executives, on a broad range of executive compensation and employee benefits matters, including in the context of mergers and acquisitions and other corporate transactions.

About the Contributing Authors

Kelly Shubic Weiner is Chair of Venable's Commercial Real Estate Group - a national group of 40+ lawyers, while maintaining an office in Baltimore, M.D. Kelly leads the group with a focus on efficient teamwork to deliver practical guidance and effective execution on every aspect of commercial real estate activity for Venable clients. She has extensive experience offering business solutions for investors, owners, developers and operators across various types of asset classes and brings a strategic yet pragmatic approach to her work on all types of complex real estate transactions.

Due Diligence in Corporate Transactions

End of Document

1 Due Diligence in Corporate Transactions Chapter 1.syn

Chapter 1 Introduction to Due Diligence

Synopsis to Chapter 1 : Introduction to Due Diligence

End of Document

§ 1.01 Overview (What is Due Diligence?)

Due diligence refers to the investigative process through which parties evaluate all relevant legal, financial, and operational information in connection with a proposed transaction. In corporate transactions, due diligence enables the buyer to identify risks, verify material representations, and make informed decisions before entering into a definitive agreement. Through this process, the buyer gains visibility into the target company's condition and can better allocate risk, negotiate deal terms, and plan for integration.

Lawyers must treat due diligence as a structured legal analysis. They must not limit their review to collecting documents, but must examine those documents critically, identify inconsistencies or deficiencies, and assess their impact on the transaction's value and execution.

Buyers conduct due diligence to assess the legal and business implications of acquiring a target company. This review includes evaluating how the target company will integrate into the buyer's operations and whether the transaction aligns with the buyer's strategic goals. Lawyers assist in this evaluation by identifying legal risks, analyzing contractual restrictions, and confirming whether the target company holds the rights, approvals, and assets required for its business.

The buyer uses the results of the diligence review to determine whether to proceed, to renegotiate deal terms, or to decline the opportunity. The buyer must ensure that the transaction will create future value and must analyze whether the target company presents potential synergies, such as cost reductions, new revenue sources, or market expansion. If the review reveals material deficiencies such as regulatory exposure, unresolved litigation, or improper governance, the buyer may modify the transaction structure or require additional protections.

§ 1.02 Due Diligence Process Overview

[1] Staffing the Due Diligence Team

The due diligence team must include lawyers with the subject-matter expertise required to evaluate all relevant legal aspects of the transaction. The size and composition of the team depend on the scope and intensity of the review. For a limited diligence review, such as one conducted in connection with a minority investment, the team may consist of only a few corporate lawyers. For a full acquisition involving multiple business lines, jurisdictions, or regulatory exposures, the team must include lawyers from the firm's specialized practice groups.

The corporate lead lawyer must assess the transaction structure and target profile to determine which practice areas must participate. For example, if the target company operates internationally, the team must include international trade and cross-border regulatory lawyers. If the target company owns or operates real estate or holds environmental permits, the team must include lawyers from the real estate and environmental groups. Other common areas requiring specialist review include tax, intellectual property, employee benefits, data privacy, antitrust, and labor and employment.

As diligence progresses, the corporate lead lawyer may identify new issues that require additional expertise. The team must remain adaptable and expand as needed to address specific risks. Each participating lawyer must understand their role, complete their assigned review efficiently, and report material findings in a timely and coordinated manner. The corporate team must ensure that the diligence process proceeds in a structured, disciplined, and comprehensive manner consistent with the client's strategic and risk objectives.

[2] Selected Diligence Team Responsibilities

Each lawyer assigned to the diligence team must review the materials relevant to their area of responsibility and communicate their findings clearly and promptly. A corporate lead lawyer, typically a senior transactional attorney, coordinates the overall review, maintains the diligence timeline, and ensures consistent reporting to the client.

Lawyers must facilitate active communication across disciplines. Each team member must understand the scope of their assignment, track progress, and escalate issues that affect other workstreams. For example, if a regulatory lawyer identifies a potential enforcement issue involving the target company's core product, the corporate and litigation teams must assess how that issue affects valuation, indemnification terms, and closing conditions.

[3] Timeline and Budget

The timeline and budget for due diligence depend on the complexity, size, and structure of the transaction. Lawyers must tailor both the schedule and the scope of the review to reflect the level of diligence required. A straightforward transaction, such as a discrete asset purchase, may require only a limited review over a short period. In contrast, a complex transaction—such as an entity or asset acquisition involving multiple jurisdictions, heavily regulated business lines, or a disorganized data room—requires more time, greater coordination, and a larger budget.

Key factors that influence the due diligence timeline and budget include the structure of the transaction (asset acquisition, stock acquisition, or merger), the number of jurisdictions in which the target company operates, the regulatory environment governing the target company's business, the volume and quality of materials produced

by the seller, and the buyer's tolerance for legal risk. The responsiveness of the seller and the organization of the virtual data room also significantly affect timing and cost. Where the seller delays production or provides incomplete or inconsistent responses, lawyers must extend the review and allocate additional resources to address the deficiencies.

If lawyers identify red flags during the due diligence process, they must conduct additional investigation and may need to involve other specialists within the firm. This further review increases both the timeline and the budget. Lawyers must alert the client as soon as they identify material issues that will expand the scope of diligence. Early communication allows the client to make informed decisions about risk allocation, resource deployment, and potential deal modifications.

[4] Documenting Due Diligence

The diligence process begins with the preparation of a tailored request list. Lawyers must identify the categories of documents and information needed to complete the review. The seller populates a virtual data room in response, and lawyers track the production and review status using a diligence tracker.

The diligence tracker must identify the status of each request, note open items, and assign responsibility for review. The team should record follow-up questions, unresolved risks, and additional requests based on the documents produced. Lawyers must use the tracker to monitor completion and to identify issues that require client input or escalation.

At the conclusion of the review, lawyers prepare a due diligence memorandum or report. The format may vary depending on the transaction and client preference. The report may take the form of a comprehensive narrative, a summary of material issues, or a structured table with annotations. Regardless of format, the report must identify unresolved risks, explain the potential consequences of those risks, and recommend specific actions or contractual protections. The report must also summarize the scope of the review and document any limitations based on incomplete disclosures or timing constraints.

§ 1.03 How Due Diligence Informs the Acquisition Agreement and Deal Terms

[1] Introduction

Lawyers conduct due diligence not merely to assess the legal condition of the target company but to identify, measure, and allocate risk. The due diligence process provides the factual and legal basis upon which transaction counsel can structure the acquisition agreement. Although parties may begin drafting the agreement concurrently with due diligence, the final terms often depend heavily on the diligence findings. Lawyers must therefore understand how to translate those findings into specific adjustments to deal terms, contract language, and closing mechanics.

[2] Strategic Outcomes of Due Diligence

Due diligence findings can lead to several outcomes. In rare cases, the reviewing party identifies no material issues, and the acquisition agreement proceeds as initially negotiated. More commonly, lawyers identify issues that require adjustment of specific provisions within the agreement. In some cases, due diligence uncovers material risks that cannot be resolved through contractual mechanisms, which may lead the buyer to terminate the transaction or the parties to mutually abandon the deal.

The primary outcomes of due diligence can include:

1. Proceeding without changes (uncommon),
2. Adjusting the purchase price,
3. Modifying specific provisions of the acquisition agreement,
4. Terminating or walking away from the transaction.

Among these, the most frequent outcome involves tailoring the acquisition agreement to reflect the risks uncovered. Lawyers accomplish this by drafting, modifying, or expanding representations and warranties, preparing comprehensive disclosure schedules, negotiating indemnification protections, and structuring financial adjustments.

[3] Tailoring Disclosure Schedules to Due Diligence Findings

The acquisition agreement typically requires the seller to prepare disclosure schedules that qualify the representations and warranties. Lawyers identify issues that the seller must disclose to avoid potential breach. For example, if the seller represents that no material litigation exists, but due diligence reveals a pending employment lawsuit, the seller must disclose the claim in the schedule to the litigation representation. The process of preparing disclosure schedules operates in parallel with legal due diligence and frequently leads to iterative negotiation and clarification.

[4] Adjusting Representations and Warranties

Lawyers will often need to respond to due diligence findings by revising the scope, specificity, or materiality qualifiers in the acquisition agreement's representations and warranties. If due diligence reveals specific vulnerabilities, such as a lack of IP ownership documentation or prior regulatory noncompliance, lawyers may tailor the relevant representations to address those risks directly or include knowledge qualifiers or exceptions.

Buyers may also request the addition of new representations tailored to deal-specific findings, such as representations regarding government investigations, data privacy, or compliance with particular industry laws.

[5] Negotiating Indemnification Protections

Indemnification provisions allocate post-closing risk and are frequently informed by due diligence. If due diligence reveals risks that cannot be entirely mitigated before closing, the parties may allocate those risks through special indemnities, escrow arrangements, or holdbacks. For example, if the target company's tax filings are incomplete or under audit, the buyer may negotiate a tax-specific indemnity or set aside a portion of the purchase price to cover any future liability. Similarly, unresolved litigation or potential employee classification issues may give rise to dedicated indemnity baskets or extended survival periods for specific representations.

[6] Purchase Price Adjustments

Some due diligence findings directly affect the valuation of the target company. If the financial due diligence reveals unexpected liabilities, overstatement of revenue, or underfunded obligations, the buyer may seek a reduction in purchase price. In some cases, the parties agree to a closing date adjustment based on a working capital calculation or net debt position, both of which may be refined based on diligence findings. The parties may also increase the escrow amount or delay a portion of the consideration through earnouts, or contingent payments tied to post-closing performance.

[7] Refining Working Capital and Net Debt Calculations

Buyers frequently base closing payments on estimated working capital or net debt. These estimates require a detailed understanding of the target company's financial condition. Legal due diligence can inform these calculations by identifying off-balance sheet liabilities, accounting irregularities, or disputes affecting accruals and reserves. For example, due diligence may uncover material uncollected receivables, aged payables, or contingent liabilities that the buyer must factor into the working capital peg. Adjustments to these calculations may become a focal point of the purchase agreement and may necessitate post-closing true-ups.

[8] Walking Away from the Transaction

In some cases, due diligence uncovers issues so fundamental or irreparable that proceeding with the transaction would expose the buyer to unacceptable risk. This may occur when the target company lacks clear ownership of core assets, operates without required regulatory licenses, or faces undisclosed material litigation. If the seller cannot cure the deficiency and the buyer cannot adequately protect itself through contract terms, the buyer may withdraw from the transaction. Although rare in negotiated deals, the walk-away option remains a critical outcome that lawyers must preserve and evaluate based on the facts uncovered during diligence.

Throughout this book, we will examine how due diligence informs disclosure schedules, representations and warranties, indemnification provisions, working capital adjustments, and other contractual mechanisms. Each chapter will highlight how lawyers identify and respond to legal risks within specific subject areas and translate those risks into actionable revisions to the acquisition agreement.

§ 1.04 Conducting the Legal Due Diligence Investigation

[1] Scope and Common Topics of Review

A due diligence investigation consists of multiple components, each of which serves a distinct function in evaluating the transaction. The core areas of due diligence typically include legal due diligence, financial due diligence, and operational due diligence. Legal due diligence focuses on the corporate, contractual, regulatory, and compliance aspects of the target company's business and is conducted by lawyers. Financial due diligence assesses the financial health, tax obligations, and accounting practices of the target company and is conducted by accountants and financial experts. Operational due diligence addresses the business functionality of the target company and is typically performed by the business team to evaluate the target company's operations, assets, and organizational infrastructure.

Each component of due diligence contributes essential information to the overall assessment. Legal diligence focuses primarily on risk identification, compliance verification, and validation of authority, while financial and operational diligence assess the target company's viability, performance, and integration potential. Although lawyers focus principally on legal matters, they must maintain awareness of financial and operational diligence findings to ensure a holistic review of risks and obligations.

[2] Legal Due Diligence

[a] Entity and Affiliate Overview

Before beginning substantive document review, lawyers must develop a foundational understanding of the target company's structure, operations, and ownership. A preliminary review of organizational charts, summaries of operations, and lists of subsidiaries and affiliates enables lawyers to frame the subsequent diligence in context and ensures that no material entities or relationships are overlooked.

[b] Organization

Evaluating the target company's organization requires a careful review of how the entity was formed, structured, and managed. Lawyers must confirm that the target company's formation complies with applicable law and that its internal governance structure, including decision-making authority and approval processes, aligns with legal and contractual requirements. Understanding the basic organizational framework is critical for identifying potential governance gaps, undisclosed liabilities, or procedural defects that could impact the transaction.

[c] Company and Industry Profile

Effective due diligence requires a strong working knowledge of the target company's industry. Lawyers must identify the regulatory framework governing the industry, assess any licenses, permits, or certifications required for lawful operation, and consider industry-specific risks. For example, target companies operating in heavily regulated sectors such as healthcare, financial services, or environmental industries often present unique compliance risks that must be analyzed carefully. Lawyers must tailor diligence requests based on the industry context and must understand the types of documents and information necessary to assess both legal compliance and operational risk.

[3] Legal Organizational Matters

[a] Introduction

Transitioning from preliminary understanding to document-based verification, lawyers must conduct a systematic review of all material organizational records.

[b] Organizational Structure, Key Affiliates, and Subsidiaries

Lawyers must first identify the target company's legal entity type, whether corporation, limited liability company, partnership, or another form, because this classification dictates the applicable statutes and the types of governance documents that must be reviewed. They must map out the relationships among the target company, its subsidiaries, and any affiliates, and must assess whether these relationships materially affect operations, ownership rights, or risk allocation. Where subsidiaries contribute significantly to the target company's business, lawyers must ensure that the transaction properly includes ownership of those subsidiaries.

Lawyers must also identify key individuals involved in the management and control of the target company, including directors, officers, members, shareholders, and partners. Understanding the roles and authorities of these individuals is critical for validating corporate actions and assessing approval rights.

[c] Formation Documents

Formation documents, including certificate of incorporation or formation and articles of organization, establish the target company's legal existence. Lawyers must confirm that the entity properly filed its formation documents with the appropriate governmental authority and that the documents remain consistent with current operations. In many jurisdictions, the formation documents identify initial ownership interests and designate the individuals authorized to act on behalf of the entity.

Reviewing formation documents enables lawyers to assess compliance with statutory formation requirements and to identify any governance provisions embedded within them, such as voting rights, indemnification clauses, and liability limitations. Lawyers must also order certificates of good standing, or their jurisdictional equivalents, to confirm that the entity maintains legal compliance and continues to exist in good standing at the time of the transaction. Subsidiaries and affiliates that form part of the transaction require the same level of review.

[d] Bylaws, Operating Agreements, and Governance Documents

Lawyers must obtain and review the entity's governing documents, which vary depending on the entity type. For corporations, these documents include the bylaws and, where applicable, shareholder agreements. For limited liability companies, the governing document is the operating agreement.

The operating agreement governs a limited liability company's ownership structure, internal management, decision-making processes, and member rights. It also addresses transfer restrictions, such as rights of first refusal, drag-along rights, and consent rights, which may affect the transaction structure or timing. The operating agreement identifies whether the LLC is member-managed or manager-managed and specifies how the company must approve material actions.

Bylaws govern the internal operation of a corporation, including director and officer appointments, shareholder voting, quorum requirements, and approval procedures. Reviewing the bylaws allows lawyers to verify authority for material actions, assess compliance with governance requirements, and anticipate any legal or procedural barriers to completing the transaction. Where applicable, shareholder agreements provide critical information about voting rights, transfer restrictions, and rights associated with different classes of stock.

[e] Minutes, Written Consents, and Other Governance Records

Meeting minutes and written consents provide a contemporaneous record of decisions made by the entity's governing bodies. Lawyers must review these records to confirm that the entity properly approved all major corporate actions, including equity issuances, mergers, financings, and key contractual arrangements.

Minutes should reflect compliance with quorum and voting requirements and must document material approvals. Written consents, when properly executed, carry the same legal effect as approvals made during formal meetings. Reviewing these documents enables lawyers to verify that the entity followed proper corporate formalities and to identify any irregularities or missing approvals that could impair enforceability.

Based on the target company's corporate history, lawyers must assess whether the minutes and consents cover the entity's major milestones and whether gaps in the records require remedial action.

[f] Capitalization and Equity Records

Lawyers must conduct a detailed review of the target company's capitalization records, including stock ledgers, capitalization tables, and records of equity issuances and transfers. This review confirms the ownership interests the buyer will acquire and ensures that no undisclosed claims or disputes exist.

Understanding the capitalization structure is also critical for confirming whether the entity obtained the required consents for prior actions, particularly where stockholder or member votes depended on ownership percentages. Lawyers must assess dilution risks, liquidation preferences, conversion rights, and voting thresholds embedded within different classes of equity.

Failing to verify capitalization can expose the buyer to claims of defective issuance, unauthorized ownership transfers, or unenforceable equity rights post-closing.

[g] Certificates of Good Standing, Foreign Qualifications, and Other Permissions

Confirming the legal standing of the target company and its subsidiaries is a critical diligence step. Lawyers must obtain certificates of good standing from each entity's jurisdiction of formation and from every jurisdiction in which the entity conducts business.

Foreign qualification is required where an entity operates outside its formation state. For example, a Delaware corporation with its principal office and operations in Texas must maintain foreign qualification in Texas. Lawyers must review whether the target company maintains good standing in each relevant jurisdiction and must address any lapses through corrective measures before closing.

Failure to maintain good standing or proper foreign registration may expose the entity to fines, impair contract enforceability, and delay closing.

[h] Tax Permits, Licenses, Certificates, and Registrations

As part of the due diligence investigation, lawyers must review the target company's tax permits, business licenses, certificates of authority, and regulatory registrations. Verifying the existence and validity of these documents ensures that the target company operates lawfully and that no outstanding compliance risks exist.

Understanding which licenses and permits are required depends on the jurisdictions in which the target company operates. Lawyers must cross-reference the target company's business activities and locations with local, state, and federal licensing requirements. This diligence not only identifies compliance issues but also supports post-closing operational integration by highlighting transfer or renewal obligations.

Comprehensive due diligence on tax and licensing matters builds upon the organizational diligence foundation and ensures that lawyers assess the transaction's risks holistically.

[4] Financial Matters

[a] Introduction

Transitioning from legal structure to financial reporting, lawyers must review indebtedness, liens, and related financial obligations that may affect the target company's value or the mechanics of the transaction.

[b] Indebtedness

Lawyers must identify all indebtedness of the target company, including secured loans, unsecured notes, and any other credit facilities. These documents frequently contain change-of-control restrictions, requiring lenders' consent before a sale or merger. Early identification of these restrictions enables transaction parties to allocate responsibility for obtaining consents and to assess the timing and certainty of closing.

Lawyers must also confirm the amount and terms of outstanding indebtedness. In many transactions, the parties agree to apply a portion of the purchase price to pay off outstanding debt obligations at closing. Failure to account for such indebtedness may materially alter the purchase price allocations and distribution mechanics.

[c] Security Interests, Pledges, Liens, and Other Encumbrances

Lien diligence is essential for understanding encumbrances on the target company's assets. Lawyers must order lien searches to identify active liens, review security agreements, and assess whether the target company must discharge or subordinate liens before closing.

In asset purchases, buyers must ensure that the seller conveys assets free and clear of liens. Failure to release liens may result in the buyer acquiring encumbered assets with impaired value. In equity transactions, buyers assume all liabilities, including secured obligations, making it critical to identify and evaluate liens before consummating the sale.

Clear title to assets, or a clear understanding of retained liabilities, is a necessary condition for closing in any well-structured transaction.

[5] Real and Personal Property

[a] Real Property

The due diligence review of real property interests in a corporate transaction should focus on:

1. understanding what rights the seller has to convey,
2. understanding what obligations may be associated with such rights,
3. understanding what, if any, third party consents may be required for the intended transaction with respect to such real estate interest, and
4. confirming that the buyer's intended use of the real property will be permitted. The appropriate scope of the real property diligence is often driven by considerations like the buyer's view of relative value of the real property interests versus other business assets, how material the real property interests may be given the nature of the business, risk tolerance or intended use of the real property interests. Therefore, it is important to connect with the buyer regarding its needs, intentions, and expectations generally before beginning a more detailed review.

As a threshold matter it is necessary to determine whether the seller has a fee interest or leasehold interest in the real property that is the subject of transaction.

Typically, the due diligence for a fee interest will be more in-depth given that the buyer will be acquiring full legal ownership of the subject property. The scope of this review typically covers matters such as:

1. title and survey,
2. zoning,
3. permits,
4. property insurance,

5. leases or occupancy agreements,

6. appraisal,

7. physical property inspection,

8. a property condition report and

9. environmental reports

Title and survey review is a common umbrella term for the review of the legal description of the property, any recorded encumbrances or mortgages, any existing title insurance documents, as well as existing and new surveys.

Under a leasehold interest, the buyer will not be acquiring a fee ownership interest in the subject property, but rather the buyer will acquire a leasehold interest which affords possessory rights to use the property pursuant to a lease agreement with the owner of the subject property. Leasing review will entail reviewing the relevant lease agreement and understanding the related terms, including, but not limited to, each party's obligations, use limitations, the lease term, rents, termination requirements, and any consents required with respect to the transfer of a direct or indirect interest in the subject property.[1]

[b] Equipment and Other Personal Property

[i] Introduction

In every corporate transaction, lawyers must conduct a comprehensive due diligence review of the target company's personal property, including both tangible and intangible assets. This review plays a critical role in confirming ownership, determining asset value, identifying liens or encumbrances, and ensuring the adequacy of documentation, maintenance, and insurance. Lawyers must approach this analysis with precision to protect against unanticipated liabilities and valuation inaccuracies. In addition to intellectual property,[2] lawyers must also review tangible assets and other intangible personal property.

[ii] Tangible Assets

Lawyers must closely examine all tangible personal property, such as equipment, machinery, vehicles, tools, and fixtures. During this process, lawyers should confirm that the target company maintains accurate and complete asset schedules supported by ownership documents and physical inspection reports. They must verify that the target company holds clear title to each asset and has not encumbered the assets with undisclosed liens or security interests. Lawyers must review maintenance records to ensure that the target company has preserved the condition and functionality of key equipment. They must also evaluate warranty information, depreciation schedules, and insurance coverage to determine whether the target company has properly accounted for asset value and replacement cost.

When lawyers uncover deficiencies—such as outdated schedules, inconsistent valuation methods, or missing maintenance documentation—they must assess how these issues affect the deal. Such deficiencies may require purchase price adjustments, post-closing remediation, or supplemental representations and warranties. Lawyers must advise clients on these matters early in the transaction to preserve negotiation leverage.

[iii] Intangible Personal Property

---

[1] Real property due diligence is discussed in *Chapter 6*.

[2] Intellectual property due diligence is discussed in *Chapter 8*.

In addition to tangible assets, lawyers must conduct a detailed review of intangible personal property. Although intellectual property usually garners primary attention, lawyers must also examine leases, licenses, permits, databases, and other contractual rights. Lawyers must confirm that the target company has secured all necessary rights through valid and enforceable agreements and that those agreements remain current and assignable. They must verify key terms, renewal provisions, and any restrictions on transferability. Where applicable, lawyers must identify and obtain third-party consents required to assign or novate agreements in connection with the transaction.

Intangible assets frequently present legal risks that affect transaction feasibility or integration. Common issues include non-transferable licenses, expired permits, undisclosed termination rights, or burdensome restrictive covenants. Lawyers must identify these risks early and develop strategies to mitigate them. These strategies may involve obtaining consents, renegotiating key terms, or supplementing disclosure schedules to allocate risk appropriately. Lawyers must communicate these findings to the client clearly and advise on whether to proceed, restructure, or adjust transaction terms in response.

[6] Labor and Employment Matters

A pivotal component of the due diligence process is an evaluation of labor and employment matters affecting the target corporation and ultimately the transaction. From the labor and employment perspective, due diligence involves a comprehensive review of the target company's workforce and a thorough assessment of its labor and employment-related practices, including legal compliance at the global, federal, state, and local level. Accordingly, labor and employment due diligence not only helps the parties identify and mitigate potential risks and liabilities but also to ensure post-transaction integration and success. This chapter provides an overview of labor and employment due diligence, including its objectives, core components, and the potential risks that may be uncovered as a result. Overall, labor and employment due diligence is one essential piece of a larger process to evaluate the legal, financial, and strategic implications of the human capital in a corporate deal.

Although the exact scope of labor and employment due diligence may vary depending on the industry involved and the transaction's structure, there are key areas that should typically be evaluated in any transaction to provide a complete picture of the target company's workforce-related legal and operational posture. Each of the areas comprising labor and employment due diligence will be explored in greater detail in the chapter that follows. At the outset, information should be evaluated so that there is a clear understanding of the company's overall workforce composition and structure (*i.e.,* its employees and engagement of third-party labor). An early step in that process is often to request and review detailed censuses of employees and independent contractors engaged by the company. For example, an employee census should typically be obtained identifying key details regarding the employment relationship between the target company and each of its employees, including the employee's classification (*i.e.,* full-time/part-time, exempt/non-exempt), position, tenure, compensation, *etc.* Likewise, an independent contractor census should typically be obtained providing details regarding the company's engagement of each third-party contractor or consultant,[3] such as the contracting entity (*i.e.,* whether the engagement is direct or through a corporate entity), duration of the engagement, work location, services provided, rate of pay, *etc.* This information provides a framework within which to review the other areas that make up labor and employment due diligence, including the jurisdictions and specific labor and employment laws that may be implicated as a result of the company's workforce.

In addition, information concerning the company's historic and current relationship with any labor unions and obligations under any collective bargaining agreement should typically be obtained early during the diligence process, as it speaks to the overall composition of the workforce, impacts the review of other key labor and employment diligence areas, and directly relates to overall compliance. For companies that currently have unionized employees, this includes, for example, obtaining copies of and analyzing the obligations under any applicable agreements governing the terms and conditions of union employees' employment and receipt of benefits. For companies without union employees, this includes gaining an understanding of historic efforts or

[3] Many companies use the terms "contractor" or "consultant" interchangeably. For clarity, the information sought concerns those individuals or entities receiving a 1099 tax form from the company for the services provided.

threats to unionize. Other information relating to labor matters should also be requested and reviewed as a part of this effort, such as any unfair labor practice charges that the company has received, and audits or investigations of the company conducted by governmental authorities concerning labor matters.

With that background information on the overall workforce composition and structure, other areas that should typically be assessed as part of the labor and employment due diligence effort include executive compensation; employment practices and procedures; health and safety compliance; employment, independent contractor, and other employment-related agreements; immigration; employee separations; and pending, actual, or threatened employment-related litigation. Though broad, each of these areas is intended to focus the due diligence effort on specific aspects of the company's employment-related operations and legal compliance. Sufficient information relating to each these general areas and more specific subtopics captured therein should be procured and analyzed in terms of both operational best practices and legal compliance. For example, within employment practices and procedures, information on subtopics to be reviewed and analyzed, include the company's classification of its employees and independent contractors, administration of leave and other legal entitlements, and policies governing its workforce. This chapter explores each of these areas in terms of the information that may, potential implications of that information, and strategies for using that information during the diligence process.

Labor and employment due diligence is a multidimensional review and analysis of a company's operations and legal compliance. It is critical to identify, assess, and mitigate potential risks that could impact the value of the transaction, to facilitate a smooth transition and integration of the workforce following the transaction, and to ensure subsequent legal compliance. Thorough diligence into the areas outlined in the chapter to follow and others that may be specific to a particular transaction help to uncover liabilities, anticipate integration challenges, and shape the strategy for achieving the broader goals of a corporate transaction.

[7] Employee Benefit Matters

Lawyers must also examine employee benefits during the due diligence process to ensure the appropriate representations, warranties, and disclosures are included in the transaction.

In transactions where employees are transferred from seller to purchaser, the due diligence process must include a review of any pending litigation claims arising from violations of employment laws, such as wage and hour laws, laws prohibiting discrimination, and laws prohibiting hostile work environments and harassment, including the Fair Labor Standards Act, Title VII of the Civil Rights Act of 1964, and state employment. This review should also determine whether any of seller's existing policies could result in such an employment law violation. The due diligence process must also determine whether any employees, especially executives, have employment agreements entitling them to certain relief upon a change in control of the entity, such as a severance payment or a parachute payment. The due diligence procedure should also ensure that the seller has complied with its payroll tax obligations and its contribution obligations to unemployment insurance, short-term disability insurance funds, and paid family leave funds, if applicable.

Transactions involving the transfer of employees often also involve the transfer of employee benefit plans, such as a defined contribution plan organized pursuant to *sections 401(k)* or *403(b) of the Internal Revenue Code*, defined benefit pension plans, and welfare plans providing medical insurance coverage to employees. Accordingly, the due diligence process involves a review of the employee benefit plans' benefits obligations to their participants and beneficiaries, their funding status and funding sources, their administrative structure, and their compliance with the Employee Retirement Income Security Act of 1974 ("ERISA"). For welfare plans, there are additional items to review, as those plans must also comply with the Patient Protection and Affordable Care Act, the Mental Health Parity and Addiction Equity Act, COBRA, and other such statutes. Moreover, welfare plans can either be self-insured or fully-insured, with the former structure paying participants' medical claims directly and with the latter structure paying an insurance premium to an insurer who pays the participants' medical claims. These types of welfare plans are subject to different laws and have significantly different liability exposure. Accordingly, the structure of the welfare plan transferred in a transaction must be scrutinized.

Even if the transaction does not involve a transfer of employee benefits plans, the due diligence process must, nonetheless, focus on these plans if they are to be terminated through the transaction. Each type of employee

benefit plan has specific rules governing the termination of the plan. Failure to terminate an employee benefits plan in conformity with these rules could result in significant liability for the contracting parties.

If the transaction involves the transfer of a unionized work force, then there is another layer of diligence that must be performed. Regarding labor law diligence, the due diligence process must examine whether the purchaser has any duty to bargain with the labor organization representing the seller's employees or any liability for the seller's labor obligations under seller's collective bargaining agreement as a successor or alter ego of the seller. Regarding employee benefits diligence in the unionized workforce context, the seller, in connection with its collective bargaining agreement, may have an obligation to contribute to an ERISA multiemployer pension plan. In which case, careful diligence must be implemented to determine whether the transaction implicates withdrawal liability under Part IV of ERISA, which is a penalty assessed on companies that cease to have a contribution obligation to an ERISA multiemployer pension plan due to either a cessation of operations covered by the relevant collective bargaining agreement or the termination of the collective bargaining agreement requiring the contribution to the ERISA multiemployer pension plan. The penalty is equal to the seller's allocable share of the ERISA multiemployer pension plan's unfunded vested benefits, which is often a significant amount. If exposure to ERISA withdrawal liability is identified during the due diligence process, then the language can be included in the transaction document to avoid the assessment of ERISA withdrawal liability by the ERISA multiemployer pension plan.[4]

[8] Executive Compensation Matters

Executive compensation plays a crucial role in corporate transactions, impacting both the structure and success of the transaction. Buyers and their counsel must carefully examine a target company's executive compensation arrangements – not only to understand the financial and legal obligations they may inherit, but also to ensure ongoing compliance with tax, securities, employee benefit, and employment laws. If executive compensation arrangements are not thoroughly understood and addressed, it can lead to unintended acceleration of payments or benefits, tax liabilities, negative accounting outcomes, and issues with employee retention.

Executive compensation arrangements, such as employment and severance agreements, retention bonuses, deferred compensation, equity incentive awards, and change-in-control plans, are typically unfunded. This means they represent unsecured promises by the target company to pay employees or service providers future compensation. The acquiring company must thoroughly review these arrangements to identify and account for any potential obligations that may survive the transaction. In addition to providing the acquiror with a better understanding of potential liabilities, an analysis of the change-in-control provisions of these arrangements, such as accelerated vesting or cash-out requirements, or for the obligation to provide an enhanced level of benefits following the transaction help the acquiror identify opportunities and obstacles in retaining key employees.[5]

[9] Privacy Matters

Data privacy and data security have become increasingly important during due diligence as regulatory frameworks evolve and are vigorously enforced. Acquisition targets across many industries process confidential, sensitive, and/or personal information to run their businesses and conduct their operations. The goal of data privacy and data security due diligence is to identify the privacy and security obligations that apply to the target company and identify any gaps between these obligations and the target company's practices.

These obligations may vary depending on factors like the nature, sensitivity, and volume of the data the target company processes; the purposes for which the data is processed, including whether the data is used to train artificial intelligence or machine learning models; the industries and jurisdictions in which the target company operates; the customers or consumers the target company serves; the products and services the target

---

[4] Employment, employee benefits, and labor due diligence is discussed in *Chapter 7*.

[5] Executive compensation due diligence is discussed in *Chapter 7*.

company provides; how the target company markets its products and services; the terms of contracts the target company has signed; and the representations the target company has made in privacy policies or other public statements.

In addition to evaluating the target company's data privacy and data security compliance measures and materials, diligence also generally includes review and evaluation of any privacy or security incidents, complaints, and investigations, which can pose risks to both the target company and the buyer post-closing.[6]

[10] Intellectual Property Matters

Not long ago, we could accept that the target company in a corporate transaction has no intellectual property, and therefore no intellectual property due diligence is needed. Today virtually all companies are "IP companies" to varying degrees. Intellectual property due diligence now often starts with a basic assessment of the materiality and substantiality of the target company's owned and licensed intellectual property, and the extent of due diligence follows from that assessment. On one extreme, intellectual property due diligence may be limited to confirming that the target company owns no registered intellectual property or that the target company is the record owner of the limited registered intellectual property it does own. On the other extreme, due diligence may be quite extensive, involving multiple subject matter experts to review patents and trademarks, inquiring into the development history of intellectual property, extensive review of development and licensing agreements, and other detailed analysis as required. The strategy must be adapted to fit the nature of the target company's business, the size of the transaction, and the relative value of the intellectual property to the rest of target company's assets.

While intellectual property due diligence will vary for each matter, the scope will typically involve some degree of investigation of certain key elements:

1. Registered intellectual property: Patents and patent applications, issued trademark registrations and applications therefore, issued copyright registrations and applications therefor, and domain names.
2. Unregistered intellectual property: Material unregistered marks and logos that identify the target company or its products or services, material unregistered copyrights (e.g., software, publications, etc.), and material trade secrets.
3. Licensed intellectual property: Third party intellectual property that is used in the target company's business and the corresponding license agreements. This includes open source and other "free" software.
4. Protection of intellectual property: The target company's policies and procedures to protect its and third parties' intellectual property, including contracts with employees and contractors regarding confidentiality of trade secrets and assignment of intellectual property.
5. Intellectual property disputes: Any claims or allegations involving the use of intellectual property by the target company. These may include claims by third party licensors and current or former employee or contractors, particularly where an individual's departure was contentious.
6. AI technologies: AI technologies are not a separate type of intellectual property, but due to the increased attention and value placed on them, and increased risk associated with them, focused AI-related due diligence is often warranted. AI concerns cover many legal disciplines, requiring coordination between specialist teams.

Intellectual property due diligence relies primarily on narrative responses and document production by the target company. But a review of public records, the target company's public website and other marketing materials, and private deal materials (such as the target company's confidential information memorandum and financials and acquirer's internal business justification) can help guide the diligence. Targeted due diligence requests based on the target company's business and responses to other due diligence questions can aid the

[6] Privacy due diligence is discussed in *Chapter 9*.

prompt and efficient production of material due diligence items to identify and assess potential intellectual property related risks.[7]

[11] Environmental Matters

[a] Introduction

Corporate transactions can involve environmental risk, including for parties seeking to acquire real property or an ownership stake in an existing business. These risks can take the form of ongoing compliance obligations, fines or penalties for regulatory non-compliance, liability for past or future site assessment or cleanup, or liability to third parties for exposure to or harm caused by releases of hazardous substances or materials. Liability for environmental releases, exposures, and damages is not limited to parties directly responsible or even aware of the underlying action or inaction; in many instances facility owners or operators could face substantial liability based on their owner or operator status—even for releases of chemicals which pre-date their involvement with a site, facility, or business.

A carefully thought-out environmental diligence can help identify, evaluate, and mitigate environmental liabilities in corporate transactions. There is no one-size-fits-all approach to environmental due diligence, and transaction-specific factors will dictate the appropriate scope and depth of the diligence approach. For most corporate transactions, the following key areas should be considered as part of a baseline environmental diligence plan.

[b] Evaluate Past Compliance with Environmental Laws, Regulations, and Permit Requirements Regarding Chemicals and Hazardous Materials

This could include, for example, requirements governing management and disposal of solid and hazardous wastes under the Resource Conservation and Recovery Act (RCRA); pesticides under the Federal Insecticide, Fungicide and Rodenticide Act (FIFRA); chemicals regulated by the Toxic Substances Control Act (TSCA); discharges of pollutants into waters of the United States regulated by the Clean Water Act; air emissions governed by the Clean Air Act; hazardous materials transportation requirements; and equivalent state requirements governing the manufacture, use, storage, transportation, sale, and disposal of hazardous substances or materials. Other relevant considerations may include requirements governing the installation, operation, removal, and/or closure of aboveground or underground storage tanks, groundwater wells, natural gas pipelines, boilers, electrical equipment, and underground injection wells.

[c] Consider Disclosure, Labeling, Warning, and Notification Requirements

Environmental diligence may also focus on whether a company has complied with requirements like the registration requirements for pesticides under FIFRA; labeling or notification requirements under TSCA; reporting the release of a hazardous substance to the National Response Center under the Comprehensive Environmental Response, Compensation and Liability Act (CERCLA); reporting on substances governed by the Emergency Planning and Community Right-to-Know Act (EPCRA); and analogous state requirements. The diligence plan can also consider forward-looking requirements that may be relevant to business plans or operational considerations.

[d] Personal Injury and Tort Liability

Environmental liability can arise under common-law, such as toxic tort claims, trespass, negligence, and nuisance, and may therefore involve evaluation of any outstanding, pending, or threatened claims arising from a past operation or environmental issue (such as an alleged spill or release). The diligence plan might also assess the likelihood that past or ongoing operations could give rise to such liability in the future.

---

[7] Intellectual property due diligence is discussed in *Chapter 8*.

[e] CERCLA and Cleanup Liability Considerations

A common component of environmental diligence is evaluation of potential liability under the federal Comprehensive Environmental Response, Compensation and Liability Act (CERCLA), *42 U.S.C. § 9601 et seq.*, also known as Superfund. CERCLA imposes strict, retroactive, joint and several liability for releases of hazardous substances for parties falling within four statutorily defined categories:

1. current facility owners,
2. facility owners at the time a release occurred,
3. transporters of hazardous substances, and
4. parties who arrange for the disposal of hazardous substances.

The diligence step can help assess existing liability under CERCLA and state analogs and can also address measures to be taken to establish eligibility for certain statutory defenses to liability (for example, the "bona fide prospective purchaser" or BFPP defense for parties newly acquiring real property).

[f] Wetlands, Endangered Species, and Wildlife and Ecosystem Considerations

Diligence related to these issues may focus on compliance with the consultation requirements and take prohibitions under Sections 7, 9, and 10 of the Endangered Species Act; the requirements and take prohibitions of the Marine Mammal Protection Act; permitting requirements for discharging material to or obstructing wetlands under Section 404 of the Clean Water Act and Section 10 of the Rivers and Harbors Act; and analogous state endangered species, marine mammal, and wetland protection laws. These considerations may be more relevant for real property transactions and/or transactions involving proposed development or infrastructure projects or funding.

[g] The National Environmental Policy Act (NEPA) and State Counterparts

This aspect of diligence examines whether an activity requiring agency approval has undergone or is subject to the requirements of NEPA and state counterparts. These laws do not directly regulate private conduct but are instead focused on ensuring that federal and state agencies consider and disclose the environmental effects of actions that agencies take directly or issue approval for. However, current or threatened litigation under these laws can delay or threaten private activities that rely on agency approvals. These considerations are most relevant for transactions involving infrastructure or other projects requiring compliance with NEPA or its state counterparts.

[h] Deal-Specific Issues

Issues unique to a particular company or operation may require special attention during the diligence process. The facts, circumstances, and procedural posture of enforcement actions or litigation against a target company may also raise specific questions or issues.

As with other types of diligence, environmental diligence will rely heavily on documentation provided by the target company. But a thorough environmental diligence plan will often involve retention of independent consultants (including, for example, of an environmental professional to conduct a Phase I Environmental Site Assessment prior to a property acquisition) and may need to go beyond the data room to properly understand the risks that a target company's assets and operations present. Contract terms, including representations and warranties of the target company and indemnification provisions, should be informed by the information identified in the course of environmental due diligence. Finally, there is a robust market for environmental insurance, which can help mitigate many known and unknown environmental risks.[8]

[12] Diligence of Customer and Supplier Agreements

---

[8] Environmental due diligence is discussed in *Chapter 5*.

An essential component of the due diligence process involves reviewing the target company's customer and supplier agreements. From a business standpoint, these agreements support the company's revenue generation and operational continuity. From a legal perspective, these agreements often contain provisions that directly affect the transaction, including restrictions on assignment, change-of-control clauses, and termination rights.

Lawyers must identify whether any customer or supplier agreement requires third-party consent as a result of the transaction. If the parties fail to obtain the required consent, the target company may be in breach following closing. The review should also determine whether any agreement includes a termination-for-convenience clause, which allows the counterparty to terminate the agreement at any time and for any reason. If a counterparty becomes dissatisfied with the buyer post-closing, it may invoke this clause and terminate the relationship. Where multiple agreements contain this provision, the buyer may face the risk of significant post-closing attrition in business relationships it expected to acquire.

In addition, lawyers must review other material provisions, including indemnification obligations, express warranties, and limitations of liability. These terms define the nature and scope of the liabilities the buyer may assume through the transaction. Warranties merit particular attention. If the target company's customer or supplier agreements contain warranties that differ materially from the buyer's existing contractual standards, the buyer may face unexpected liabilities or elevated service obligations post-closing.

When the target company maintains a large number of customer and supplier agreements, lawyers typically limit the scope of review to material agreements. Where the target company uses standardized form agreements across numerous counterparties, lawyers should identify the relevant form and confirm that review of a representative sample adequately captures the applicable risk. This approach ensures efficiency while maintaining focus on legal exposure.

[13] Regulatory Compliance

Lawyers must assess whether the target company complies with the regulatory framework applicable to its industry. This analysis enables the buyer to evaluate legal risk accurately and determine whether the company operates lawfully under federal, state, and industry-specific laws. Regulatory noncompliance may result in fines, penalties, business disruptions, or required remedial measures, any of which may affect valuation and closing risk.

Regulatory compliance concerns arise frequently in industries such as healthcare, environmental services, data privacy, financial services, and defense. Lawyers must evaluate whether the target company has complied with applicable regulatory obligations and whether any governmental inquiry, investigation, or enforcement action is pending. Where the target company fails to maintain required compliance programs or has a history of regulatory violations, the buyer may face inherited exposure post-closing.

In certain transactions, regulatory approvals may be required as a condition to closing. These include antitrust approvals for transactions exceeding Hart-Scott-Rodino ("HSR") thresholds and foreign investment approvals under the Committee on Foreign Investment in the United States ("CFIUS"). Lawyers must determine early in the process whether such approvals apply and coordinate filings or notifications accordingly.

In many industries, the target company must hold licenses or permits to conduct its business. Lawyers must confirm that the company holds all required authorizations, that those authorizations remain current and unexpired, and that they cover the full scope of the company's operations. Where permits or licenses are non-transferable, the buyer may need to obtain new approvals before or immediately after closing. If the target company lacks required authorizations, the buyer should evaluate whether to require corrective action pre-closing or seek protection through representations, covenants, or closing conditions.

[14] Cross-Border and International Matters

Cross-border transactions have become an unavoidable aspect of modern commercial activity, driven by the globalization of markets, expansion of multinational enterprises, and the ongoing search for new investment opportunities and strategic partnerships. As business operations increasingly span continents and legal systems, the complexity of conducting transactions across borders has correspondingly increased. Legal

professionals and business advisors are now tasked with navigating a dynamic landscape characterized by disparate regulatory regimes, differing standards of corporate governance, ever-evolving compliance requirements, national security concerns and a rapidly changing geopolitical landscape. The stakes for successful cross-border transactions are high: beyond the immediate commercial objectives, these transactions often shape long-term business relationships, determine access to new markets, and create reputational and organizational risk.

At the core of any successful cross-border transaction lies a comprehensive due diligence process. International due diligence serves not only to validate the commercial premises of a deal, but also to uncover latent legal, regulatory, and operational risks that might otherwise undermine the transaction's value and completion. Practitioners must be prepared to address a range of issues, from ownership structures and contractual obligations to regulatory notifications and tax implications. For example, when engaging in transactional due diligence involving foreign investment in the United States, practitioners must be acutely aware of the scrutiny imposed by regulatory bodies such as the Committee on Foreign Investment in the United States ("CFIUS"). CFIUS review has become a standard aspect of cross-border deals, with the Committee having the power to recommend suspension, prohibition, or even unwinding of transactions deemed to pose risks to national security.

Moreover, foreign investors seeking to acquire U.S. real property or invest in American enterprises encounter unique statutory and regulatory considerations. The Foreign Investment in Real Property Tax Act ("FIRPTA") imposes specific tax withholding and reporting obligations on foreign sellers of U.S. real property interests, requiring careful structuring and planning to mitigate unexpected tax exposure.

Conversely, U.S. entities investing abroad—whether establishing wholly-owned subsidiaries, joint ventures, or acquiring controlling stakes in foreign enterprises—must be cognizant of a different set of regulatory hurdles, including the necessity of compliance with increasing U.S. outbound investment restrictions like the Outbound Investment Security Program ("OISP"), which restricts U.S. persons from investing in certain Chinese or Chinese-owned companies that engage in specified activities related to artificial intelligence, quantum information technology, semiconductors, and microelectronics.

In addition to U.S.-centric considerations, practitioners must also be mindful of cross-jurisdictional issues arising from foreign regulatory regimes, particularly in regions such as the European Union. EU and UK merger notification requirements, for example, can trigger multi-jurisdictional filings, necessitating an integrated approach to regulatory, antitrust and competition law analysis. The practical consequence is that cross-border transactional teams must coordinate the timing, scope, and substance of notifications to avoid inadvertent violations and regulatory delays. Failure to do so can result not only in delays but also penalties and, in some rare cases, the unwinding of consummated transactions.

It is also essential to recognize the increasing interplay between domestic policy objectives—such as the protection of critical infrastructure and sensitive technology—and cross-border investment reviews. As governments worldwide refine their foreign investment review mechanisms, the risk environment continues to evolve, placing greater emphasis on proactive due diligence, comprehensive risk assessments, and early engagement with relevant authorities. Practitioners must remain abreast of these trends and anticipate regulatory responses to emerging industries and geopolitical developments.

In sum, effective due diligence in cross-border transactions demands a sophisticated understanding of both the legal framework and the practical realities of operating across multiple jurisdictions. It is not merely a matter of compliance, but a strategic exercise in risk management, value protection, and deal execution. The following chapter provides a detailed roadmap for navigating these challenges, including practical guidance on CFIUS review, FIRPTA implications, outbound U.S. investment concerns, and EU and UK investment controls, all within the broader context of international transactional due diligence. By anticipating and addressing the unique legal and regulatory issues presented by cross-border transactions, practitioners can better position their clients to achieve successful outcomes in the global marketplace.[9]

---

[9] Cross-border issues will be *covered in Chapter 10*.

[15] Export Rules, National Security, and International Trade Regulations Matters

The intersection of international trade, national security, and regulatory compliance presents one of the most challenging environments for companies engaged in cross-border business. The expansion of international supply chains, the proliferation of dual-use technologies, and the increased scrutiny of global transactions by regulatory authorities have created a landscape where even minor lapses in compliance can lead to severe penalties, operational disruptions, and reputational damage. As such, effective due diligence related to trade controls has become an indispensable component of risk management for multinational corporations, investors, and their advisors.

The framework governing trade controls is multifaceted, encompassing U.S. laws and regulations as well as those of foreign jurisdictions. At the forefront of U.S. regulatory oversight are sanctions and export control regimes administered by the Department of the Treasury's Office of Foreign Assets Control ("OFAC"), the Department of Commerce's Bureau of Industry and Security ("BIS"), and the Department of State's Directorate of Defense Trade Controls ("DDTC"). These agencies collectively administer broad and frequently updated restrictions on the export, reexport, and transfer of goods, technology, and services to designated countries, entities, and individuals. The scope and complexity of these regimes demand careful diligence to identify whether a transaction, party, or destination is subject to controls or prohibitions, and whether any licenses may be required to complete the proposed transaction.

International trade due diligence begins with a thorough understanding of the products, technology, or services involved, and an assessment of their classification under the relevant export control regimes, such as the Export Administration Regulations ("EAR") or the International Traffic in Arms Regulations ("ITAR"). This process may include technical analysis to determine the appropriate export controls classifications and associated controls, as well as an evaluation of end-use, end-user, and ultimate destination. In parallel, parties to cross-border transactions must consider the impact of U.S. sanctions programs, which are expansive and extend extraterritorially and restrict direct and indirect dealings with sanctioned individuals and entities and also entities owned or controlled by such parties— often even when such dealings occur outside U.S. territory.

A further dimension of diligence involves compliance with U.S. Customs and Border Protection ("CBP") import regulations, which govern the lawful entry of goods into the United States. Practitioners must ensure the target has systems and processes in place to satisfy all customs valuation, marking, and country-of-origin requirements are satisfied, and must also be prepared to address issues relating to tariff classification, tariffs, antidumping and countervailing duties, forced labor in the supply chain. Increased enforcement by CBP has heightened the importance of thorough reviews of the import practices of entities in order to mitigate the risk of significant penalties and investigations down the line.

Of equal significance in international business transactions is the need for vigilance under anti-corruption statutes, chief among them the Foreign Corrupt Practices Act ("FCPA"). The FCPA prohibits U.S. persons and companies from offering or providing anything of value to foreign government officials for the purpose of obtaining or retaining business. The FCPA's reach is global with violations subject to criminal and civil penalties. Due diligence under the FCPA extends to evaluating the target's or business partner's historical conduct, internal controls, and third-party relationships—particularly in jurisdictions with high corruption risk or in industries with heightened vulnerability. Effective anti-corruption diligence may include forensic reviews, interviews, and contract analysis, as well as an assessment of policies, procedures, and compliance culture.

Trade regulations are an increasingly popular vehicle to address national security concerns and policy objectives such as the protection of sensitive technologies, the safeguarding of critical infrastructure, and the prevention of proliferation and terrorist financing are all driving the ongoing expansion of export controls and sanctions. Recent legislative and regulatory changes have further broadened the scope of review, particularly in emerging areas such as cybersecurity, artificial intelligence, and biotechnology. As a result, companies and their advisors must remain attentive to the evolving regulatory landscape, anticipate potential policy shifts, and engage with regulators where necessary to obtain guidance or authorizations.

In practice, due diligence in trade controls is both a legal and a strategic exercise. It requires multidisciplinary coordination among legal, compliance, operations, finance, technical and product teams. Timely identification of regulatory risks, gaps in compliance, or red flags can mean the difference between a smooth transaction and one that presents the risk of a costly enforcement action. Moreover, integrating robust trade and compliance

due diligence into transaction planning not only mitigates legal risk but also fosters a culture of compliance that can be leveraged in future business activities.

This chapter offers a comprehensive guide to the practical and legal issues at the heart of trade controls due diligence. It covers the foundational principles of international trade due diligence— the impact of sanctions and export controls, the nuances of U.S. Customs and import regulations, and the critical importance of anti-corruption compliance under the FCPA. By equipping practitioners with both the legal framework and practical tools necessary for effective diligence, this chapter seeks to empower those engaged in cross-border transactions to anticipate challenges, avoid pitfalls, and achieve successful outcomes in the increasingly complex realm of global trade.[10]

[16] Litigation, Investigations, and Legal Proceedings

[a] Introduction

Litigation due diligence requires lawyers to conduct a comprehensive review of all legal proceedings involving the target company. These proceedings include active, pending, threatened, and historical litigation. Lawyers must examine each matter carefully to determine how existing or potential legal exposure may affect transaction value, timing, and post-closing operations.

[b] Active and Pending Litigation

Lawyers must obtain a complete list of all active and pending litigation matters. They should analyze each case in detail, including the nature of claims, asserted defenses, procedural posture, and the potential range of liability. To complete this analysis, lawyers must review court filings, pleadings, motions, and court orders. They must also evaluate whether the target company has established adequate reserves and secured appropriate insurance coverage to address existing exposures.

When lawyers identify gaps in disclosures, undervalued liabilities, or inadequate coverage, they must advise clients to assess how these deficiencies impact valuation and deal structure. Lawyers should recommend protective measures, such as indemnification provisions, closing conditions, or price adjustments, and they must collaborate with insurance counsel to verify that policy exclusions, coverage limits, and historical claims activity align with the transaction's risk profile.

[c] Threatened Litigation

Lawyers must treat litigation threats with equal scrutiny. They must collect and review all written and oral communications that suggest potential claims, including demand letters, cease-and-desist notices, and contentious exchanges. They must also examine the target company's settlement history to identify patterns that may signal future liability or regulatory exposure.

To determine whether the target company has properly prepared for such risks, lawyers must confirm the existence and sufficiency of any reserves or insurance policies covering unresolved threats. When lawyers uncover material threats, they must advise clients to consider requiring supplemental representations and warranties, special indemnities, or adjustments to the purchase price. They must also investigate whether recurring threats stem from underlying business practices or compliance failures that warrant broader diligence or remediation.

[d] Historical Litigation

Lawyers must carefully review the target company's historical litigation, even if resolved, to identify operational weaknesses or governance deficiencies. They must examine final judgments, settlement agreements, and consent decrees to determine whether the target company continues to face ongoing

---

[10] International trade matters will be *covered in Chapter 11*.

obligations. These obligations may include deferred payments, confidentiality terms, or restrictive covenants that could affect post-closing operations.

In addition, lawyers must assess whether past litigation reveals patterns of conduct—such as repeated employment claims or product liability disputes—that may indicate systemic legal risk. They should evaluate the continuing impact of past litigation on the target company's reputation, commercial relationships, and market position.

Where the history of litigation raises concerns, lawyers must recommend enhanced due diligence in related functional areas and advise clients to negotiate risk-shifting mechanisms, such as targeted indemnities, escrow arrangements, or disclosure supplements. Lawyers must ensure that the transaction documentation fully reflects the legal and financial exposure arising from the target company's litigation history.

[e] Regulatory and Compliance Investigations

Lawyers must thoroughly investigate all regulatory inquiries and compliance investigations involving the target company, particularly those initiated by the SEC, the DOJ, or relevant industry-specific agencies. These investigations often reveal material risks that directly affect transaction value, timing, and structure. To conduct an effective review, lawyers must identify every current and historical investigation or inquiry, including those that occurred before the commencement of formal enforcement proceedings.

Lawyers should obtain and analyze all correspondence between the target company and regulatory authorities. This includes subpoenas, deficiency letters, formal responses, and internal memoranda addressing regulator communications. A thorough review of the target company's compliance framework remains essential. Lawyers must examine compliance policies, employee training materials, internal audit reports, and any remedial steps the target company has taken in response to prior regulatory deficiencies.

When reviewing regulatory matters, lawyers should give heightened attention to investigations concerning financial reporting practices, anti-bribery and anti-corruption controls, environmental compliance programs, and consumer protection obligations. These areas frequently generate contingent liabilities and may signal broader operational weaknesses. In light of such risks, lawyers must advise clients to implement targeted compliance improvements prior to closing or to design post-closing integration plans that strengthen oversight and reduce exposure.

[f] Strategic Considerations in Litigation and Investigations

Litigation and regulatory investigations significantly influence the structure, timing, and risk allocation of corporate transactions. Lawyers must assess the cumulative impact of all identified legal issues and develop protective strategies that address those risks directly. When high-risk litigation or unresolved investigations arise, lawyers should recommend that clients include special indemnities, establish purchase price holdbacks, or fund escrow accounts to shield against adverse outcomes.

To address specific risks uncovered during due diligence, lawyers should revise representations and warranties to include appropriate knowledge qualifiers and materiality thresholds. When pending matters create uncertainty, lawyers should advise clients to adjust transaction timelines or modify closing conditions to account for necessary resolutions.

Lawyers must proactively guide clients through the negotiation of risk-shifting mechanisms. These may include obtaining representation and warranty insurance, incorporating covenants that mandate post-closing cooperation, or requiring the target company to complete specific compliance or remediation steps before closing. To implement a comprehensive risk mitigation strategy, lawyers must coordinate closely with litigation, regulatory, and insurance counsel and ensure that the transaction structure reflects the full scope of the target company's legal exposure.

§ 1.05 Conducting Financial Due Diligence

[1] Introduction

Lawyers oversee the financial due diligence process to identify exposures that affect transaction structure, valuation, and risk allocation. Although accountants and financial advisors conduct technical analyses, lawyers interpret the results to ensure the client receives appropriate legal protection.

[2] Verification of Financial Statements

At the outset, lawyers review the target company's financial statements to confirm that they present historical performance and comply with applicable accounting standards, such as U.S. GAAP or IFRS. They examine auditor reports for material qualifications and evaluate whether any deficiencies require changes to representations, warranties, purchase price adjustments, or closing conditions. If they do not conform to a particular accounting standard, representations and warranties need to be revised, or exceptions need to be noted or explained in the disclosure schedules.

[3] Assessment of Revenue, Profitability, and Cash Flow

During financial diligence, lawyers analyze the target company's revenue sources, profitability, and cash flow trends. They evaluate customer concentration, recurring revenues, and cash generation to identify risks that could affect valuation. Where irregularities or concentrations arise, lawyers recommend structuring contractual protections, earnouts, or price adjustments.

[4] Review of Indebtedness and Contingent Liabilities

In reviewing indebtedness, lawyers must examine all credit facilities, promissory notes, guarantees, and other debt instruments. They should identify contingent liabilities, including potential warranty claims or indemnity obligations, and assess whether these exposures require disclosure or special protections in the purchase agreement.

[5] Analysis of Working Capital

Lawyers must evaluate the target company's working capital components, including accounts receivable, accounts payable, inventory, and prepaid expenses. They must ensure that the purchase agreement includes appropriate working capital targets and adjustment mechanisms to account for changes between signing and closing. Where lawyers identify unusual trends or risks, they must raise those concerns during deal negotiations and revise the acquisition agreement accordingly.

[6] Tax Compliance and Exposure

For tax diligence, lawyers must coordinate with tax specialists to review tax returns, audit histories, payment records, and outstanding assessments. They must verify compliance with federal, state, local, and international tax obligations. Where lawyers discover material tax exposures, they must recommend contractual protections, such as targeted indemnities, purchase price holdbacks, or specific closing deliverables to address the liability.

End of Document

§ 1.06 Conducting Operational Due Diligence / Material Contracts

[1] Introduction

Operational due diligence allows lawyers to assess the target company's infrastructure, contracts, workforce, and operational risks to support a seamless transaction. Lawyers approach operational diligence systematically to minimize disruption at closing and to preserve or enhance the target company's value post-acquisition.

[2] Review of Key Contracts and Commercial Relationships

Lawyers conduct due diligence on the target company's material contracts to identify risks that may affect the transaction or the company's post-closing operations. This review typically focuses on customer agreements, supplier contracts, service arrangements, and other commercial relationships that are central to the target company's business. Lawyers must confirm that these contracts are valid and enforceable, identify any provisions that may be triggered by the transaction, and assess whether the counterparty has rights that could disrupt the transaction or impose burdensome obligations on the buyer.

Particular attention should be paid to change-of-control clauses, anti-assignment provisions, exclusivity arrangements, non-compete clauses, termination rights, and automatic renewal terms. Lawyers must also identify any contracts that generate a disproportionate share of the target company's revenue or impose unusual liabilities or performance obligations. The findings of this review often inform the acquisition agreement by prompting updates to disclosure schedules, targeted representations, indemnification protections, or adjustments to working capital calculations. Contract review requires both legal and commercial judgment and serves as a critical step in allocating operational risk in the transaction.

[3] Evaluation of Operational Systems and Infrastructure

Lawyers next review the target company's operational systems, focusing on IT infrastructure, enterprise software, logistics operations, manufacturing facilities, service contracts, and supply chain management arrangements. They examine whether the target company maintains enforceable licenses, valid maintenance agreements, and assignable service contracts. Lawyers identify vulnerabilities in system maintenance, cybersecurity, and continuity that could impair the buyer's use or integration of the systems post-closing. When gaps arise, lawyers work with technology and operations specialists to recommend corrective measures, negotiate transitional services agreements, or secure additional assurances. Lawyers also identify whether any material systems or service providers may terminate, degrade, or alter their services as a result of the transaction, and they propose protections to mitigate these risks.

[4] Workforce and Organizational Structure

Lawyers analyze the target company's organizational structure and workforce stability to evaluate operational risks tied to human capital. They obtain and review organizational charts, key employee lists, employment agreements, consulting agreements, non-competition agreements, restrictive covenants, and incentive arrangements. Lawyers confirm whether the target company has secured enforceable agreements with key personnel and whether employment contracts contain change-of-control or termination triggers. They assess retention risks, severance obligations, non-compete enforceability, and compliance with labor laws. Where workforce vulnerabilities exist, lawyers advise on appropriate transaction protections such as retention bonuses, pre-closing employment covenants, or seller indemnities. Lawyers coordinate closely with labor and

employment specialists to ensure that workforce diligence addresses both operational continuity and compliance risk.

[5] Strategic Fit and Integration Planning

Finally, lawyers evaluate how the target company's operations align with the buyer's business strategy and integration plans. They review whether operational processes, supply chains, technology platforms, employee structures, and geographic footprints complement or conflict with the buyer's business. When lawyers detect incompatibilities, they propose transaction solutions such as transitional services agreements, delayed closings for certain business units, or standalone operating structures. Lawyers ensure that the diligence record identifies integration risks early so that the buyer can plan mitigation strategies, build contingency reserves, or adjust the deal structure as necessary. They collaborate with business, human resources, and technology teams to ensure that legal advice on integration fits the client's broader strategic objectives.

§ 1.07 The Role of Executives, Owners, Advisors, and Key Persons during Due Diligence

[1] Executives

Executives play a central role in the due diligence process by providing operational knowledge, controlling access to information, and validating corporate approvals. Lawyers rely on executives to coordinate the collection of documents, explain the target company's business model, describe operational risks, and assist in identifying material contracts. Executives must verify that the company has properly maintained governance records, financial statements, regulatory licenses, and material agreements. When lawyers encounter incomplete disclosures or inconsistencies, they must engage executives directly to clarify facts and supplement the disclosure schedules. Lawyers must also interview executives to gain context around the company's operations, dependencies, competitive position, and strategic risks. Through these engagements, lawyers test the reliability of management's representations and assess whether additional diligence is necessary to validate critical issues.

[2] Owners

Owners must assist lawyers in verifying the target company's ownership structure, authority for corporate actions, and compliance with transfer restrictions. Lawyers depend on owners to provide accurate capitalization records, disclose any outstanding equity claims, and confirm voting and approval rights necessary for the transaction. In closely held companies, lawyers must pay particular attention to ownership disputes, undocumented transfers, or shareholder agreements that restrict transferability. Owners must also disclose any side agreements, rights of first refusal, or buy-sell arrangements that could affect the transaction's execution. Lawyers must review these materials carefully, confirm that ownership records align with organizational documents, and identify whether additional consents, waivers, or notices are necessary to proceed.

[3] Advisors

Advisors, including the target company's accountants, tax consultants, and internal counsel, provide critical support in documenting and explaining material aspects of the target company's business. Lawyers must coordinate directly with these advisors to verify financial statements, tax filings, regulatory compliance, and corporate governance. Advisors must cooperate in providing reports, certifications, and responses to diligence questions within their areas of responsibility. Lawyers must validate the reliability of advisor-supplied information through document review and direct inquiries. Where advisors disclose potential exposures—such as unresolved tax audits, compliance gaps, or accounting irregularities—lawyers must assess the materiality of those issues and recommend appropriate contractual protections or conditions to closing.

[4] Key Persons

Key persons, such as senior operational managers, technical leaders, and critical employees, possess institutional knowledge that lawyers must incorporate into the diligence process. Lawyers must interview key persons to understand the target company's internal operations, intellectual property development, customer relationships, and regulatory practices. Management must identify these individuals early in the diligence process and facilitate access. Lawyers must test whether key persons have made undisclosed commitments, whether critical dependencies exist, and whether the target company's business could sustain departures or changes in leadership. Lawyers must document these risks and advise clients on the need for retention

agreements, transition planning, or additional representations to mitigate key person risks identified during diligence.

End of Document

§ 1.08 Due Diligence Topic Checklist

As previewed so far in this chapter, lawyers conducting corporate due diligence must complete a comprehensive review across all material legal disciplines relevant to the transaction. The following checklist identifies the core topical areas for review. Lawyers should tailor this list to the specific facts, industry, and structure of each transaction.

1. Organizational Matters
2. Capitalization and Equity Structure
3. Material Contracts
4. Real Estate
5. Financial Matters
6. Intellectual Property
7. Privacy and Data Security
8. Labor and Employment
9. Employee Benefits and Executive Compensation
10. Environmental Matters
11. Litigation and Regulatory Investigations
12. Cross-Border and International Matters
13. Export Controls, Sanctions, and International Trade Compliance
14. Tax Matters
15. Insurance
16. Industry-Specific Regulatory Matters

1 Due Diligence in Corporate Transactions Chapter 2.syn

Chapter 2 The Due Diligence Team

§ 2.01 Overview

Due diligence in corporate transactions requires more than general understanding of corporate law. It requires in-depth knowledge of corporate governance from corporate lawyers as well as specialist expertise in specific areas of applicable law to review the target company thoroughly. This chapter explains the role specialists play in the broader context of a corporate transaction.

§ 2.02 Specialists

[1] Introduction

The specialist lawyers described below handle specific legal areas critical to due diligence. They analyze the target's operations and contracts, check compliance, and identify risks based on their specialist expertise. These specialists do not work in isolation; they are part of the larger transaction process. During the due diligence process, corporate lawyers will rely on the specialists' due diligence to shape the deal's terms, price, and risk allocation. Additionally, corporate lawyers will ask specialists to advise on walk-away points, negotiate warranties, or draft conditions precedent.

As the specialists conduct their due diligence, it is important for corporate lawyers to be responsible for coordinating the due diligence review, setting goals, and managing deadlines. The goal of the due diligence process should be to create a due diligence report that provides a legal, financial, and operational review of the target company. Corporate lawyers will use this report to advise the client on whether to proceed with the deal, renegotiate terms, or walk away.[1]

[2] Intellectual Property

Once lawyers identify the documented and registered intellectual property (IP) of a target company, they can begin a detailed due diligence process to assess the company's rights to own or utilize that IP. These rights differ based on factors such as the context in which the IP was developed, the manner and location of its use by the company, and the specifics of any applicable licensing agreements. To thoroughly evaluate these aspects, the review might involve examining contracts related to consulting, purchases, or other arrangements through which the company acquired its IP. The review should also include analyzing agreements with employees and independent contractors to clarify ownership of IP they created, as well as investigating any claims of infringement tied to the company's intellectual property.

Beyond this, IP due diligence often extends to performing searches to confirm the recorded ownership of registered IP, both in the United States and internationally. These searches help validate the legal standing of the IP and ensure there are no discrepancies in ownership records. Additionally, the process should explore the scope of protection afforded to the IP, potential expiration dates of registrations, and any third-party rights that could limit its use. This comprehensive approach not only verifies the target company's control over its IP assets but also highlights any risks or constraints that could impact the transaction, providing a clear foundation for strategic decision-making in the deal.

[3] Real Estate

When examining real property assets involved in a transaction, lawyers typically review title records, the property's legal description, any recorded liens or restrictions, zoning regulations, permits, title insurance policies, surveys, property insurance paperwork, mortgages, and lease agreements. The primary objectives of this evaluation are to clarify the seller's legal rights and their ability to transfer those rights to the buyer, to identify any encumbrances, easements, or other limitations affecting the property, and to ensure that the buyer's intended use of the property aligns with applicable laws and regulations.

---

[1] See chapter 3 for a detailed review of the due diligence report.

Additionally, this review helps uncover potential risks, such as undisclosed claims or disputes that could impact ownership or value. For example, a survey might reveal boundary issues, while zoning analysis could highlight restrictions on development or commercial activities. By addressing these elements, lawyers confirm the legitimacy of the transaction as well as provide the buyer with a clearer picture of what they are acquiring, enabling informed decision-making, and reducing the likelihood of post-transaction surprises.

[4] Labor and Employment

When conducting due diligence on labor and employment issues, labor and employment lawyers typically analyze employment contracts, severance packages, collective bargaining agreements, and employee benefit programs—such as health and welfare plans, medical and life insurance policies, vacation policies, pension schemes, profit-sharing arrangements, and employee handbooks or manuals. Additionally, they examine compensation structures and retirement plans. The main objectives of this process are to understand the rights and responsibilities tied to the workforce, pinpoint any benefits or limitations that might be activated by the transaction, and assess the target company's potential exposure to liabilities stemming from violations of relevant labor laws or regulations.

Furthermore, if the buyer employs a comparable workforce, it becomes critical to compare the target company's employee compensation and benefits with those of the buyer's staff to identify disparities or alignment. The diligence process may also extend to investigating recent or ongoing employee claims related to benefit plans, as well as reviewing correspondence, filings, or documentation associated with regulatory audits, inspections, or reviews. This in-depth analysis helps uncover hidden risks, such as unresolved disputes or compliance gaps, which could affect the transaction's value or future operations. By thoroughly exploring these aspects, buyers can better anticipate integration challenges, ensure fair treatment across the combined workforce, and mitigate unforeseen legal or financial burdens in the evolving landscape of corporate acquisitions.

[5] Tax

The primary objectives of tax due diligence are to uncover the target company's tax-related assets and liabilities while gathering critical data to provide critical advice on how to structure the deal to reduce tax liability resulting from the transaction. Typically, tax lawyers will examine tax returns, supporting work papers, and key documents tied to ongoing or previous tax audits.

In addition to these core activities, tax lawyers may extend tax due diligence to assess the target's compliance with applicable tax laws, identifying any outstanding tax obligations, and evaluating potential risks such as unreported liabilities or aggressive tax positions that could trigger future disputes with tax authorities. This review might also explore the availability of tax credits, deductions, or incentives that could enhance the transaction's value, as well as the implications of cross-border tax issues if the deal involves multiple jurisdictions. By delving into these areas, tax lawyers not only quantify the client's tax exposure, but they also inform strategies—such as choosing between an asset purchase or stock purchase—to optimize the tax outcome.

[6] IT/Privacy

As cyber threats continue to escalate, IT, privacy, and cybersecurity are a critical focus for companies involved in M&A. A target company's exposure to digital risks can pose a substantial liability for a buyer, especially when the target's operations or worth heavily rely on collecting and storing sensitive data. Lawyers might vary the scope of cybersecurity due diligence depending on the types of data central to the target's business, but broadly, its key aims are to pinpoint the company's most critical information and technology assets, examine how these assets are safeguarded and maintained, and assess the target's contingency plans for restoring operations if vital systems or data are breached. This evaluation often involves investigating any past cyber incidents that significantly disrupted the target's activities, collecting details on the administrative, technical, and physical measures in place to secure information, and reviewing the oversight of cybersecurity risk management. It may also include analyzing findings from internal and external audits of adherence to the company's security policies. These steps help gauge both the present and potential future risks of a security

breach, allowing the buyer to estimate the possible effects on the target's operations, reputation, and overall value.

Additionally, privacy considerations are increasingly integral to this process, particularly when the target handles personal or regulated data. Privacy lawyers might explore compliance with privacy laws—such as GDPR, CCPA, or industry-specific regulations—by reviewing data protection policies, consent mechanisms, and procedures for handling data breaches. Understanding how the target collects, processes, and shares personal information can reveal liabilities tied to privacy violations or fines, which could impact the transaction's cost and structure.

[7] Cross-Border Transactions

Cross-border transaction lawyers are essential when a transaction spans multiple countries and requires expertise in navigating the complexities of foreign legal systems and regulatory frameworks. They begin by reviewing the target company's operations in each relevant jurisdiction, ensuring compliance with local laws related to corporate governance, taxation, labor, and industry-specific regulations. This review involves analyzing licenses, permits, and filings to confirm the target's legal standing abroad, as well as assessing the impact of international trade rules, currency exchange controls, and economic sanctions that could restrict the deal's feasibility or profitability. By identifying jurisdictional nuances—such as restrictions on foreign ownership or repatriation of profits—lawyers can help the acquiring party understand potential risks and liabilities that might not be evident in a domestic transaction.

In addition to compliance, lawyers with cross-border transactional experience focus on harmonizing the transaction with the broader cross-border context, coordinating with local counsel when needed to address region-specific issues like data privacy laws (e.g., GDPR in Europe) or anti-corruption statutes (e.g., the U.S. Foreign Corrupt Practices Act). They scrutinize contracts with foreign suppliers, customers, or partners to uncover hidden obligations or termination risks triggered by the deal, and evaluate tax implications, including double taxation treaties and transfer pricing rules, to optimize the transaction structure. Their work also extends to flagging geopolitical risks—such as political instability or upcoming regulatory changes—that could affect the target's value or operations post-closing. By providing a comprehensive risk profile and tailored strategies, cross-border transactions lawyers ensure the buyer can confidently proceed, minimizing legal surprises and aligning the deal with global business goals.

[8] Employee Benefits

Employee benefits specialist lawyers review and analyze documents such as employment contracts, severance agreements, health and welfare plans, retirement schemes (like 401(k) or pension plans), stock option programs, and other compensation-related arrangements. They assess whether these plans comply with applicable laws, such as the Employee Retirement Income Security Act (ERISA), the Internal Revenue Code, and other federal or state regulations. By identifying potential liabilities—such as underfunded pension plans, non-compliant benefit structures, or unresolved employee claims—they help the acquiring party understand the financial and legal risks tied to the target's workforce benefits, ensuring these factors are accounted for in the transaction's valuation and terms.

Beyond compliance and risk assessment, employee benefits specialists also advise on the strategic implications of integrating or transitioning the target's benefits programs post-transaction. They examine how the target's offerings compare to the buyer's existing plans, flagging disparities in compensation, vacation policies, or health benefits that could affect employee retention or morale after the deal closes. Additionally, they review collective bargaining agreements, if applicable, to evaluate obligations to unionized workers, and scrutinize any pending audits or litigation related to benefits. By providing detailed insights and recommendations—such as suggesting adjustments to the deal structure or drafting specific indemnities—these specialists ensure the buyer can navigate the complexities of benefits integration, mitigate unforeseen costs, and align the transaction with broader business objectives.

[9] Industry-Specific Specialists

Certain transactions involve target companies operating within heavily regulated or technically complex industries. In these instances, corporate lawyers must collaborate closely with specialists who possess expertise in the relevant regulatory and legal frameworks.

For example, transactions involving pharmaceutical companies, medical device manufacturers, or dietary supplement businesses require consultation with regulatory lawyers specializing in FDA compliance. These specialists review critical areas such as product classification, marketing authorizations, and labeling compliance under the Federal Food, Drug, and Cosmetic Act. Additionally, they assess promotional materials to ensure substantiation of product claims and compliance with regulatory standards.

Similarly, if a target is a product manufacturer, corporate lawyers should engage product liability specialists to evaluate exposure to consumer claims and litigation. These specialists analyze product warranties, safety protocols, and historical product claims. Furthermore, they assess the adequacy and appropriateness of insurance coverage relative to the company's risk profile.

If the corporate lawyer identifies potential issues with the target's advertising practices, they should work with the firm's advertising lawyers. These lawyers conduct due diligence with a focus on advertising and consumer protection laws. They analyze advertising campaigns, marketing disclosures, and digital content, and then flag unsupported claims or promotions that could trigger regulatory scrutiny or potential litigation.

These are just a few examples of when corporate lawyers should consult industry-specific lawyers during the due diligence process. In the next chapter, we will provide a deeper analysis on the highly regulated healthcare, telecommunications, federal government contracting, and cannabis industries.

§ 2.03 External Specialists

[1] Introduction

Most deals require due diligence from outside experts with technical or industry-specific skills beyond the firm's scope.

[2] Investment Bankers

Investment bankers play a critical role in corporate transactions by conducting financial and operational analyses that support the due diligence process. Corporate lawyers work closely with investment bankers to align legal and financial assessments, ensure consistency across findings, and evaluate how financial risks may affect the legal terms of the transaction. Investment bankers examine the target company's historical and projected financial performance, assess the viability of its business model, and evaluate industry trends that may influence the deal. They test key assumptions in the financial statements, analyze valuation metrics, and identify risks or discrepancies that could impact pricing or structure. Based on these findings, corporate lawyers may revise contractual provisions, adjust representations and warranties, or negotiate price adjustments.

[3] Accountants

External accountants deliver an independent and detailed analysis of the target company's financial health and reporting accuracy. They examine financial statements, tax returns, general ledgers, and supporting documentation to confirm the accuracy of the target's earnings, assets, liabilities, and cash flows. Additionally, they will analyze the target's accounting policies to ensure consistency with applicable standards (such as GAAP or IFRS), flag irregularities like off-balance-sheet liabilities or revenue recognition issues and test the strength of internal controls. External accountants will quantify potential financial risks, including unrecorded obligations or inflated valuations, and provide corporate lawyers with an understanding of the target's economic position. The accountants' analysis will inform purchase price negotiations, reveal issues that may warrant deal adjustments, and support financial forecasting for post-transaction integration and long-term profitability.

§ 2.04 Confidentiality of Due Diligence Information

Oftentimes, before due diligence even begins, the buyer and the seller of a transaction are likely to enter into a confidentiality agreement or nondisclosure agreement, sometimes referred to as an "NDA". This agreement will protect the confidentiality of any information shared by the parties during the diligence phase of the transaction, especially if the parties do not consummate the transaction.

As described above, most of the specialists conducting due diligence for the transaction are lawyers who are subject to attorney-client privilege. Therefore, lawyers must already treat the information exchanged during due diligence as confidential, even without a separate agreement.

However, when external specialists are brought on to conduct due diligence and assist with the transaction, they are not subject to the same types of privileges and do not owe an obligation of confidentiality. Therefore, it is important to make sure that all external specialists also sign an NDA to ensure that non-public information shared during due diligence remains confidential.

A unilateral NDA form agreement between the target company and external specialist is provided in the Appendix. The NDA imposes clear obligations on the specialist to protect confidential information, restrict its use to the scope of their engagement, and prevent unauthorized disclosure to third parties. This safeguard allows corporate lawyers to collaborate effectively with external specialists, while maintaining the confidentiality standards required by the client and the transaction.

Appendix A: Confidentiality and Non-Disclosure Agreement

1 Due Diligence in Corporate Transactions Chapter 3.syn

Chapter 3 Conducting the Due Diligence Investigation

End of Document

§ 3.01 Overview

Conducting due diligence in corporate transactions is a critical process of the deal that involves a comprehensive investigation and analysis of a target company's financial, legal, operational, and strategic components to verify information, identify risks, and ensure compliance with legal and financial obligations. The primary objective of due diligence is to identify potential risks and liabilities that could impact that transaction's value or structure. Effective due diligence enables a buyer to make informed decisions regarding whether to move forward with a transaction; negotiate favorable terms during the negotiation phase of the deal process; and ensure that there are no hidden issues in the business which could impact the success of the business post-closing.

Due Diligence in Corporate Transactions

§ 3.02 Key Preliminary Tasks

[1] Introduction

Before transaction lawyers can begin the due diligence investigation, it is critical that the scope of the diligence is defined, the due diligence team has access to the due diligence materials, and there is a working group list created.

[2] Scope Discussions

The scope of the due diligence investigation in a corporate transaction is largely tailored and dependent on the nature and complexity of the deal. The depth of the due diligence investigation in each transaction is different for each transaction and depends on a wide array of factors. Factors that may influence the scope of the due diligence investigation may include: (i) the size and type of the transaction, (ii) the industry (i.e., an industry in a highly regulated space would oftentimes require more due diligence), (iii) level of risk tolerance of the parties, and (iv) structure of the transaction (i.e., asset deal or equity deal).

While there is no uniform scope of the due diligence investigation across transactions, there are certain "core" areas of due diligence that are analyzed in each transaction. These common areas of due diligence include the review of (i) the corporate structure and governance of the target company, (ii) material contracts (including leases, customer / supplier agreements, and loan agreements), (iii) litigation related documents, and (iv) documentation related to employment matters and employee benefits.

[3] Access to Due Diligence Materials

For the due diligence investigation to begin, the target company needs to provide access to the requested due diligence materials which is typically provided in the form of a data room which will be discussed in more detail below. If there any antitrust concerns in connection with the transaction, the parties may want to consider limiting the other party's access to competitively sensitive information.[1] Limiting access to competitively sensitive information at the outset is important because typically once the requested due diligence materials are provided in a data room anyone who has access to the data room will have access to such due diligence materials (unless there are certain viewing restrictions applied to the data room). A party's access to competitively sensitive information can be limited by:[2]

- Redacting such information from materials provided to the other party;
- Only providing such information to representatives or employees of the other party that have a legitimate reason for requesting and viewing the information and are not in a position to use such information to compete in the relevant markets; or
- Only providing such information to third party consultants that the other party engages to evaluate the information.

---

[1] *LexisNexis M&A Practice Guide, Ch. 6* Due Diligence by Alissa Babitz.

[2] *LexisNexis M&A Practice Guide, Ch. 6* Due Diligence by Alissa Babitz.

Additionally, one method to limit the risk that competitively sensitive information is shared inappropriately or inadvertently is to only allow access to such information through a “clean” data room that only a small number of authorized individuals may access.[3]

[4] Working Group Lists

The working group list is a single document that identifies the core deal team and practice area specialists involved in the transaction. It is typically prepared at the outset of the transaction by counsel on both sides and shared among the internal deal team, the client, and eventually the broader working group. However, the working group list may be updated throughout the transaction as new individuals become involved in the transaction (i.e., a new practice area specialist becomes involved in the transaction who was not originally involved at the outset of the transaction). The working group list includes the names, roles, and contact information of everyone involved in the transaction, such as lawyers, business teams, bankers, accountants, and other specialists or experts. Having this information centralized ensures that when specific individuals need to be contacted, all necessary details are readily available in one document for ease of access. The importance of maintaining a working group list lies in the ability to streamline communication and coordination among the various parties involved in the transaction as there are various parties involved. This centralized approach not only saves time but also enhances the efficiency of the due diligence process, contributing to a more organized and effective transaction. Further, this list is essential for allocating responsibilities and establishing clear lines of communication in complex transactions involving multiple parties.

The working group list serves as a logistical tool to ensure that all relevant parties are coordinated and that responsibilities are clearly defined. From an organizational perspective, a working group list can be used to make sure that the scope of due diligence is being adequately covered. For example, if a corporate lawyer coordinating the working group list and running the due diligence process knows that the transaction requires for there to be privacy due diligence conducted, but there is no privacy specialist on the working group list, then the corporate lawyer running the due diligence process knows that a privacy specialist needs to be added to the working group list or else that area of diligence (in this case privacy due diligence) is likely not currently being covered.

[3] *LexisNexis M&A Practice Guide, Ch. 6* Due Diligence by Alissa Babitz.

§ 3.03 Due Diligence Request Lists

[1] Overview

The due diligence request list is a critical tool used in corporate transactions to gather and review information about a target company's business. It serves as an organizational aid for both buyers and sellers to track the progress of the due diligence process and the documents exchanged. The list is typically tailored to the specific transaction and the nature of the target company, ensuring that all relevant areas of concern are addressed. The due diligence request list will encompass the scope of due diligence, as the documents that are requested and the questions that are asked of the target company will correspond to the areas of interest of the buyer.

The due diligence process typically begins with the buyer's legal counsel sending the due diligence request list to the seller's counsel. The initial due diligence request list is broad and may be supplemented with more specific requests as the due diligence process progresses and areas of interest or concern are identified. Upon receiving the initial due diligence request list, the seller's legal counsel will review and compile the requested documents, often in consultation with internal specialists and external advisors who are part of the deal team. Given the volume and sensitivity of the information, the seller may provide the requested materials in phases, accompanied by written responses addressing each item on the due diligence request list. This methodical approach helps maintain organization, ensures that all requested information is accounted for, and reduces the risk of inadvertently disclosing privileged or confidential information. Additionally, the seller may include explanations or clarifications to contextualize the provided documents, thereby aiding the buyer's understanding and analysis and helping progress the due diligence process in an efficient manner. The exchange of the due diligence request list is not a one-time event but rather an ongoing process that happens multiple times. As the buyer reviews the provided due diligence materials, additional questions or requests for further information arise. This iterative process allows the buyer to delve deeper into specific areas of concern, ensuring a thorough evaluation of the target company. Effective communication and timely responses from both parties are essential to maintain momentum in the transaction and to address any issues or discrepancies that may emerge during the due diligence phase.

Below is a sample initial due diligence request list that can be used as a starting point.[4] As indicated above, a due diligence request list is tailored based on the scope of the diligence (i.e., the industry of the target / depth of diligence being conducted) and as such each due diligence request list will vary slightly from transaction to transaction.

[2] Sample Diligence Request List

Please provide the following documents and information for [TARGET COMPANY] (the "Company"):

Item Number	Diligence Request
1.00	**Corporate Organization and Capitalization**
1.01	A description of the history of the Company, including any predecessor companies and any changes in structure.
1.02	Has the Company ever had any subsidiaries?
1.03	Certificate of incorporation, bylaws and any other governing documents for the Company,

[4] The sample due diligence request list provided is drafted on the assumption that the target company is a corporation. Certain diligence requests will need to be revised accordingly if the target company is of a different entity type (i.e., limited liability company, etc.).

	including any amendments.
1.04	List of any jurisdictions in which the Company is qualified to do business, has applied for qualification to do business, has an office or employees, or is otherwise operating.
1.05	Schedule listing all current and former (for the past 3 years) officers and directors of the Company, including their dates of service, and in the case of officers, their positions.
1.06	List of all shareholders, including number of shares held, date acquired and percentage ownership.
1.07	Stock ledger, stock transfer books (from the inception of the Company), and copies of all outstanding or cancelled stock certificates.
1.08	Minutes of meetings (and consent resolutions) of (a) the Board of Directors and (b) the shareholders of the Company for the last 3 years.
1.09	Has the Company ever had any stock option plans and forms of option agreements that have been used? If so, please provide copies of the plan and all option grants (whether or not any option was ever vested or exercised). Has the Company ever promised any employee an ownership stake, or a stock option? If so, please provide copies of such promise, if in writing, or a description, if oral.
1.10	All agreements made between the Company and any of its officers, directors, shareholders, any of their immediate families or any entity controlled by an officer, director or shareholder.
2.00	**Real Estate and Tangible Personal Property**
2.01	Does the Company own any real property?
2.02	Does the Company lease any real property? If so, provide copies of the leases.
2.03	List of tangible assets (including machinery, equipment, and other personal property owned or leased by the Company), together, if applicable, with a copy of the lease agreement therefor.
2.04	Agreements relating to pledges or other instruments granting a security interest in any Company property.
3.00	**Intellectual Property**
3.01	List of all patents, trade secrets, know-how, trademarks, service marks, copyrights, trade names, fictitious names, website domain names, logotypes and designs used by the Company.
3.02	List and description of completed or pending IP disputes, including informal claims asserting that the Company infringes a third party's IP, or that a third party infringes the Company's IP.
3.03	All agreements pursuant to which the Company has granted or has been granted a license with respect to any software, patents, trade secrets, know-how, technology, trademarks or other proprietary rights.
4.00	**Contracts**
4.01	All contracts with clients, and/or a written description of any oral arrangements with any client, within the last 3 years (even if the contract has now expired).
4.02	List of current and prospective clients.
4.03	All contracts between the Company and any third party entered into within the last 3 years, or currently still in effect, including (but not limited to): ▪ joint venture, teaming, strategic alliance, joint marketing or partnership agreements; ▪ purchase or lease agreements for machinery, equipment or other personal property; ▪ professional services agreements (including cleaning, maintenance, support, advertising, website hosting or development or other services); ▪ contracts that contain any non-compete or non-solicit; ▪ non-disclosure or confidentiality agreements; ▪ contracts that contain any negative covenants/restrictions or exclusivity provisions; ▪ contracts that may restrict the Company's activities in any manner; or ▪ contracts entered into outside the ordinary course of business.
4.04	Written summaries of any oral agreements.
4.05	Any notices of breach or notices of intent to terminate received by any counterparty to any contract.
5.00	**Insurance and Risk Management**
5.01	Copies of each insurance policy relating to the Company.
5.02	Summary of insurance claims and recoveries for the last 3 years (including pending claims).
6.00	**Employees, Employee Relations, and Employee Benefits**

§ 3.03 Due Diligence Request Lists

6.01	Schedule, for the last 3 years, listing the start/end dates for each employee, the functional role of each such employee and the reason for termination.
6.02	Summary of pending and/or threatened employment-related lawsuits or factual circumstances that may give rise to employment-related lawsuits.
6.03	Summary of unemployment claims for the last 3 years.
6.04	Schedule of current employees (including shareholders who are employees), including compensation, perquisites and other material benefits.
6.05	Copies of any agreements relating to the indemnification by the Company of any current or former officer or director of the Company.
6.06	Copies of all employee benefit plans, including all pension and welfare benefits plans.
6.07	All agreements within the last 3 years, with any employee (including shareholders who are employees), officer, director, consultant or independent contractor, including (but not limited to), all: ▪ employment, consulting or independent contractor agreements; ▪ offer letters; ▪ bonus or incentive payment agreements; ▪ non-compete, non-solicit or non-disclosure agreements; ▪ loan agreements; ▪ severance agreements; or ▪ invention assignment agreements.
7.00	**Financial and Accounting**
7.01	Financial statements (audited, if available) for the past three years, including income statements, cash flow statements and balance sheets and explanations of significant year-to-year changes.
7.02	Schedule of current and aged accounts receivable and accounts payable as of the end of January 2009.
7.03	Any loan or debt agreements to which Company is a party, including (but not limited to): ▪ term or revolving loan agreement; ▪ line of credit; ▪ letters of credit; ▪ corporate credit card agreements; ▪ installment loans; ▪ property or equipment leases; and ▪ all guarantees by or on behalf of the Company.
7.04	Schedule of all outstanding debt of the Company.
7.05	Schedule of bank accounts.
8.00	**Taxes**
8.01	Copies of all federal, foreign, state, and local tax returns for the past 5 years (including all schedules).
8.02	Documentation regarding employee federal income tax and FICA withholding, information returns and deposits of amounts withheld for the past 5 years.
8.03	Tax elections made by or with respect to the Company or its shareholders, including any confirmations from the applicable tax authority for such elections.
8.04	Copies of any IRS determination letters from the Company's inception.
8.05	List of distributions (dividends) to the Company's shareholders since the effective date of the S corporation election.
8.06	For personal and real property taxes, a schedule setting forth, for each location in which such payments were made, the most recent period for which such a tax payment was made and the date on which such payment is due and payable this year.
8.07	Summary of any IRS or other tax proceedings, deficiencies assessed or audits commenced in the last 3 years.
9.00	**Litigation and Regulatory**
9.01	Summary of all pending and threatened litigation, claims, audits, governmental actions or investigations.
9.02	List and description of all settled or concluded litigation, claims or proceedings in the past 3 years, along with copies of any related consent decrees, judgments, orders, settlement agreements or injunctions.
9.03	List of all client, employee, independent contractor or other third party complaints or demands received within the last 12 months with respect to the Company or its services.

9.04	List and description of any ethical complaints or violations filed against the Company, any shareholder, officer, director or any former employee or independent contractor, including any complaints filed with the Federal Election Commission, the Department of Justice (Office of Public Integrity) or any state or local agencies that regulate political or non-profit fundraising.
9.05	Copies of any governmental licenses and permits required for the Company's business as currently conducted or planned.
9.06	Copies of all internal compliance and training manuals, including ethics policies and manuals.
9.07	Information regarding any bankruptcy or similar proceedings with respect to the Company or any of its officers or directors.
10.00	**Environmental, Health and Safety**
10.01	List of all environmental and workers health and safety legislation, regulations and orders to which the Company is subject.
10.02	Copies of all demands, notices or requests for information given to or received from any governmental entity or private party regarding any environmentally damaging or hazardous materials or wastes or disposal of same.
10.03	Copies of all environmental assessments, surveys, and reports previously conducted and obtained with respect to the real property (e.g., Phase I and Phase II Environmental Site Assessments, soil, water or asbestos sampling), or other written documents or materials regarding environmental matters.
11.00	**Other**
11.01	Any other document not otherwise provided above that is material to the Company's business, prospects, assets, results of operations or condition (financial or otherwise).

§ 3.04 Due Diligence Considerations for Specific Industries

[1] Aerospace, Defense, and Government Services Industries

[a] Introduction

With respect to M&A transactions involving companies doing business with the United States Federal Government in the aerospace, defense, and government services (including, as one example, information technology) industries – what we'll generically call "government contracting" – the due diligence investigation of the target's assets, liabilities and business operations, as well as the "reverse" diligence of the buyer and its business, in most respects mirrors the type of investigation that would be undertaken with respect to businesses engaging entirely within the commercial marketplace. Nevertheless, there are a few important distinctions, which are discussed below.

[b] Diligence of the Target Company's Business, Generally

Regardless of the nature of the target's business, buyer counsel may be asked to review the target's contract mix to determine its compatibility with that of the buyer. In particular, for government contractors, that review might include, among other things, a summary of whether a particular contract was a "prime" contract (i.e., where the target is in direct privity with a US government entity) or a "subcontract" (i.e., where the counterparty is another contractor, with the US government as the ultimate customer), its dollar value, its "period of performance," and whether performance of the contract requires an approved facility security clearance (FCL) and/or cleared personnel, permitted access to classified materials. The buy-side due diligence investigation should also determine whether the target enjoys preferential bidder status under any of the various programs of the US Small Business Administration (SBA) that are administered for the benefit of certain groups of contractors, including small businesses, service-disabled veteran-owned small businesses (SDVO-SB), woman-owned small businesses, businesses located in historically underutilized business (HUB) zones, and participants in the SBA's 8(a) program (which are majority-owned by socially and economically disadvantaged individuals). When the answer is "yes," counsel should then ascertain whether the target will remain eligible – after its affiliation with the buyer following the sale – to continue to perform its existing "set-aside" contracts, as well as to enjoy the exercise of option periods under existing contracts, and to compete for and receive new contract awards and grants of task orders and purchase orders under existing contract vehicles. See, e.g., *13 CFR §124.515* (regarding the automatic termination for convenience of 8(a) contracts upon a participant change of control, and the circumstances under which the participant may seek a waiver of such termination); see also *13 CFR §125.12* (regarding eligibility following a contractor change of control under other SBA set-aside programs). Further, the timing of the consummation of a transaction, or even the reaching of an agreement in principle, can also impact the target's ability to remain eligible with respect to certain pending bids. See *13 CFR §125.12(e)(2)(i)* (stating that when events triggering a disqualifying recertification occur within 180 days after the date of an offer but prior to the award, the concern is ineligible to receive the pending small business set-aside or reserved award.).

Finally, a review of the target's contracts should determine whether, when considered together with the buyer's contract mix, such contracts might create an "organizational conflict of interest" (OCI). An OCI is said to exist when a contractor may be unable to render impartial advice or assistance to the government or

to objectively perform its contract work, or when it would otherwise possess an unfair competitive advantage. (A classic example of an OCI would exist when one contractor was assisting its government customer in creating the specifications and prerequisites for a particular procurement, while its affiliate would be competing for such opportunity.) See 48 CFR Subpart 9.5. The identification of OCI risk then requires mitigation, satisfactory to the government customer, before the proposed M&A transaction can move forward. Mitigation might include something as simple as having the relevant government customer approve the use of firewalls between different contractor teams, or as significant as requiring the divestiture of certain contracts and related assets as a condition to approval of the deal.

[c] Required Third-Party Notices and Approvals

[i] Non-Governmental

As it relates to non-government contract counterparties, the diligence review of the target's contracts, for the purpose of identifying necessary third-party notices and consents, is largely similar to that performed with respect to the contracts of commercial businesses. The goal, as always, is to determine which counterparties may be owed notice, and which may need to grant consent, depending on how the deal is structured and exactly what the terms of the underlying contract actually provide. Government contractors often form "teams" to most efficiently and advantageously pursue particular procurement opportunities, and to perform any resulting contracts awarded following successful bids. Such teams will often include a prime contractor, who is directly awarded the resulting federal contract, as well as one or more subcontractors who are engaged to perform some of the prime contractor's obligations to the ultimate government customer. The form of subcontract used between a lower-tier subcontractor and a higher-tier entity (either the prime contractor itself or, sometimes, a higher-tier subcontractor) is typically dictated by the latter, with the result that its approval is usually necessary both for the direct assignment of the contract (as would occur in an asset sale by the lower-tier subcontractor) and for any change of control experienced by the lower-tier contractor (occurring in an equity sale). Government contractors sometimes form joint ventures (JVs) to bid for and to perform prime contracts and subcontracts. These JVs include those resulting from a written joint venture agreement (that may create, sometimes inadvertently, a general partnership under state law), as well as arrangements in which a separate legal entity, such as a limited liability company, is chartered under state law. The language of such JV agreements (including the operating agreement when an LLC is created) should be carefully reviewed to determine whether the approval of other joint venture partners (including other LLC members) may be required when one of the joint venturers undergoes an ownership change in an equity sale.

[ii] Governmental

Asset Sales. For asset sale transactions, where the target's prime government contracts will be transferred to a third-party buyer, approval of the government customer will be required under the formal contract "novation" process set out in the Federal Acquisition Regulations (FAR). See *48 CFR §42.1204*. This process entails submission of detailed documentation to the customer sufficient to assure it (1) that the buyer would otherwise be eligible to receive an award of such prime contract directly, and (2) that the buyer will be receiving in the transaction all or substantially all of the assets used in performing the contracted work. In such situations, in addition to assembling and submitting the appropriate novation package required by the FAR (including legal opinions from counsel to both the transferor and the transferee), counsel may be called upon to assist in such de novo evaluation of the transferee's eligibility. Novations carry with them a certain amount of risk, as the government is under no particular deadline to act upon a novation request, and its approval is purely discretionary. As a result, asset sales are often avoided in the context of government contracting M&A, precisely to avoid the novation requirement. However, should an asset sale be necessary, it will be important to factor in frequent engagement with the relevant contracting officers (COs) to attempt to streamline and expedite the novation request and review.

Equity Sales. With the exception of 8(a) contracts, where approval of the SBA Administrator is required (under the waiver process described above) in order to avoid termination of the contract upon a change of control, no FAR novation approval of prime government contracts is necessary when the target's ownership changes in an equity sale. However, with respect to other, non-8(a) set-aside contracts, the applicable government customers must nevertheless be notified, within 30 days after the sale transaction, as to whether the target – following its affiliation with the buyer – continues to qualify within its particular preferred bidder category. Such certifications will determine the target's eligibility for future set-aside contract awards, as well as for option exercises and grants of task and purchase orders under existing contracts. See *13 CFR §125.12*. For the sale of "non-small" (i.e., non-set-aside) entities, notice of a change in control may still be required depending upon whether certain FAR clauses have been incorporated by reference within the impacted contracts. See *FAR 52.215-19*.

Foreign Buyers and CFIUS. The scope of diligence investigations involving government contractors in M&A transactions is not limited to the target and its assets and particular business activities. If the buyer is foreign, and if the US-based target engages in activities involving national security, critical technology or infrastructure, or sensitive personal data, care should be taken to determine whether approval of the transaction by the Committee on Foreign Investment in the United States (CFIUS) is necessary or advisable. See *50 U.S.C. §4565*.

FCLs and FOCI. Government contractors performing classified contracts are required to maintain approved facility security clearances (FCLs), allowing them appropriately to access classified materials. Regardless of the identity of the buyer, under the National Industrial Security Program Operating Manual (NISPOM), target contractors which possess FCLs will need to coordinate with their "cognizant security office," usually the Defense Counterintelligence and Security Agency (DCSA), to ensure that their FCLs remain valid through a change of control. See 32 CFR Part 117. Where the transaction would result in foreign ownership, control or influence (FOCI) of an FCL(s), because it affords a foreign interest the power to direct or decide matters affecting the management or operations of the contractor, such FOCI must be satisfactorily mitigated before the transaction may go forward. Approved mitigation measures may include anything from simple board resolutions to special security agreements (SSAs) or proxy board arrangements.

[d] Compliance-Related Due Diligence

[i] Generally

While diligence of a government contractor target will be similar to that undertaken with respect to targets in the commercial context as it relates to understanding compliance with contractual obligations, there are several areas that are unique to government contracting.

First, because of the public nature of government contracting, a great deal of information regarding a target can be gleaned from public sources or through open-source searches. For example, public databases such as the System for Award Management[5], USAspending[6], and the Federal Procurement Data System[7] all have publicly available information on government contractors, including their size status and history and certain other corporate information, as well as contract/funding profile and information. Much can be learned from reviewing these websites and comparing them with the target's responses to diligence questions and its preparation of draft purchase agreement disclosure schedules.

Second, the government maintains a formal past performance evaluation process known as the "Contractor Performance Assessment Reporting System" (CPARS). See FAR §42.15. This system sets forth requirements for the federal government in reporting the past performance of a federal contractor.

---

[5] *https://sam.gov/*.

[6] *https://www.usaspending.gov/*.

[7] *https://www.fpds.gov/fpdsng_cms/index.php/en/*.

CPAR reports are key to understanding how a contractor has performed and should be requested and reviewed in any diligence effort. Similarly, the government frequently audits and monitors government contractors. Buyers should be certain to request and review all audits and assessments of a government contractor target, as these reports will identify deficiencies or non-compliances noted by the government. Buyers should also inquire into the corrective action and resolution of any such identified problems, as lingering issues can sometimes take years to fully resolve.

[ii] Intellectual Property

The potential intellectual property rights of the government are another special area of government contracting M&A due diligence. A standard government contract provides that intellectual property developed at public expense will remain the property of the contractor, but with the government retaining an unlimited license. See *FAR §52.227-14*. However, contracts may include special or non-standard intellectual *property clauses* that may encumber the intellectual property, or affix conditions on ownership and use. See, e.g., §52.227-17. These contract provisions should be carefully reviewed prior to consummating any transaction where intellectual property is a key asset of the target.

[iii] Disclosure of Non-compliance

Another unique feature of the government contracting landscape is that known contract non-compliances are required to be disclosed in a timely manner. See *FAR §52.203-13*. It is not uncommon, in the course of diligence, for questions regarding non-compliance to arise, raised either by the target (or its counsel) as it prepares materials for diligence review or begins to prepare disclosure schedules, or by the buyer (or its counsel) as it reviews diligence materials and disclosure schedules. When such questions are raised, the parties and their counsel should discuss whether the matter appropriately triggers a disclosure obligation and whether, how, and to what extent a disclosure should be made. Disclosing a matter to the U.S. government – under this rule that is typically the Office of Inspector General for the cognizant agency – only begins a process that can sometimes take months to resolve. As a result, the parties should be certain to discuss an agreed-upon plan for the transaction pending review and any responsive action by the government.

[2] Telecommunications Industry

[a] Overview

The primary role of a telecommunications regulatory diligence is to fully understand what is being purchased. Many of the most important assets involved in a telecommunications transaction are either directly regulated or heavily impacted by regulation. A properly conducted regulatory diligence will describe the regulatory status of those items in detail so that the buyer will understand what is being purchased and what obligations/faults come along with the purchased assets. The diligence will uncover non-obvious issues that erode the value of the assets, including undisclosed liabilities, governmental investigations, missed payments, unintentional non-compliance and value-impacting contractual triggers. Through this process, discrepancies between the seller's disclosure schedules and the results of the buyer's diligence will be reconciled. All of this information informs what price should be offered for the assets to be acquired, and whether post-signing, regulatory discrepancies can be rectified and/or lead to adjustment to the purchase price or other contractual changes to reflect those concerns.

The second role of the regulatory diligence is to inform the parties as to what regulatory steps if any need to be taken to get to a successful closing. Many assets involved in a telecommunications transaction require either governmental or third party consents prior to closing, and many have precise timeframes and sequences in which to request and obtain such consents. Failure to properly request consents can cause the transaction to fail or cause an increase in costs on the parties. The diligence clarifies exactly what governmental and third party consent approvals are required prior to closing, anticipates difficulties in obtaining those approvals, and informs strategies for efficiently obtaining those approvals.

The reasons a telecommunications transaction requires government approvals are several folds. The Communications Act of 1934 (the "Act") generally requires a licensee to obtain approval from the Federal Communications Commission ("FCC") before it assigns or transfers any FCC license or authorization (e.g., a television station or wireless license) or acquires a Seller that holds an FCC license or authorization. This requirement is triggered by a whole host of different FCC depending on the business involved. Depending on what type of assets are involved and how they are operated, parties may also be required to obtain license transfer or assignment consent from the FCC, or state authorization consents from state public utility commissions and municipalities/local franchise authorities. The timing of obtaining any of these consents all depends on the mix of licenses and authorizations involved, and also the extent to which the agency decides to take a closer public interest look at the transaction.

Consents will also be required from non-governmental third-parties that control regulated assets and contracts. For example, contracts with certain programmers, customers, vendors and utilities will require that the buyer obtains the counter-party's consent prior to allowing transfer or assignment of the contract. Some contractual transfer provisions will trigger a change in the underlying economics of the contracts, and those changes need to be understood and dealt with. Failure to obtain such consent prior to closing can also lead to the termination of essential third-party contracts, which is obviously less than ideal. The initial diligence will identify which third-party consents are needed, whether there are any economic consequences to the proposed transfer, what mechanically needs to be done to obtain each consent, and the expected timelines for resolution.

The buyer must conduct its initial regulatory diligence prior to executing a purchase agreement (or even letter of intent). Because regulatory issues in the telecommunications space can significantly reduce the value of what is being purchased, the buyer should have a thorough understanding of what regulatory land mines exist prior to making its offer. And the concern goes beyond purchase price. The buyer must also be sure in the purchase agreement negotiation stage to review and clarify materiality qualifier language to ensure that significant regulatory issues are fully disclosed and not excluded or discounted from the scheduling.

A proper regulatory diligence will also facilitate debt financing. Lenders do not like regulatory surprises when making loans. But more than that, lenders are concerned that should the buyer default on the proposed loan, they will end up post foreclosure with tainted regulated assets. A typical lender in this space will not only review the buyer's regulatory diligence, but it will also conduct its own side diligence (at the buyer's expense, of course) and then conduct a joint review of the seller's schedules to clear up any discrepancies. After any discrepancies have been resolved, the lender will then ask for an opinion of the buyer's outside regulatory counsel that the diligence has not turned up undisclosed, materially significant issues. A buyer's thorough diligence at the early stage will go a long way towards ensuring that the financing will clear underwriting.

Hopefully, as the deal approaches close, everything in the regulatory consent schedule matches up. Unfortunately, it is all too common for previously undisclosed or undiscovered regulatory issues to appear at this late stage. This is why the diligence needs to be double checked prior to closing, as it is the last chance for the purchase price to be adjusted based on discovered regulatory issues "material" to the business.

The following is a non-exhaustive list of the most important regulatory items typically reviewed during a regulatory diligence.

[b] Wireline Checklist

- Copies of FCC licenses, authorizations, registrations, orders, and certificates authorizing the Seller to provide voice services, local exchange services, intrastate telecommunications services, interstate telecommunications services, international telecommunications services, or Voice over Internet Protocol ("VoIP") services.
- Information on and copies of any material investigations, letters of inquiry ("LOIs"), notices of apparent liability ("NALs"), subpoenas, complaints, inquiries or proceedings (formal or informal) issued by or

pending before the FCC, any state PUC, Office of Inspector General ("OIG"), any state attorney general, or any other federal, state, or local communications regulatory agency.

- Copies of annual and quarterly filings and any material correspondence with the Universal Service Administrative Seller ("USAC"), including information on any audits, investigations, or inquiries.
- Copies of any documents relating to the Seller's receipt of federal or state universal service funds or broadband grants.
- Copies of FCC annual regulatory fee payments.
- Copies of material vendor contracts supporting the Seller's provision of services, including but not limited to, agreements relating to: interconnection, traffic exchange, intercarrier compensation, resale, billing and collection, wholesale services, bandwidth, transport, and indefeasible rights of use ("IRU") agreements.
- Copies of material customer contracts with other telecommunications providers relating to: interconnection, traffic exchange, intercarrier compensation, resale, billing and collection, wholesale services, bandwidth, transport, and IRUs.
- Copies of all right-of-way, easement, or similar agreements and ordinances giving the Seller authority to occupy a public or private right-of-way for the purpose of providing service.
- Copies of any tariffs, price lists, web-posted documents, or other similar documents providing information on the Seller's rates, terms, and conditions.
- Copies of annual reports, fee remittance reports, and other routine compliance reports.
- Copies of any orders or notices from any state authority regarding any penalties, fines, levies, or other sanctions imposed upon the Seller.
- Copies of all certificates, orders, pending applications or other approvals from any state public utility commission or other state agencies or boards relating to the Seller's authority to provide intrastate telecommunications services in each state in which they provide such services.
- Copies of any formal or informal complaints, investigations, and/or litigation regarding the Seller filed with any state authority or state court by customers, other carriers, or other persons; copies of any responses and correspondence relating to such complaints; and any orders issued by any State Authority or state court in such proceedings.

Copies of all state compliance filings made by the Seller.

[c] Wireless Checklist

- For each licensed transmitter involved in the transaction, the FCC license and/or construction permit for each facility.
- For constructed facilities, the date construction was completed along with the FCC date-stamped copy of notification of completion of construction for all FCC licensed stations, or other evidence of construction.
- For facilities under construction, a copy of construction permit/license and status/estimated date of completion of construction.
- If any application has been filed to extend the construction deadline, Seller should provide an FCC date-stamped copy of same (or other proof of filing, if filed electronically).
- For facilities obtained by transfer or assignment, Seller should also provide evidence of transfer or assignment grant and an FCC date-stamped copy of letter (or proof of electronic filing) notifying FCC of consummation.
- FCC date-stamped copies of any pending renewal applications and/or Public Notice granting renewal.

- FCC date-stamped copies of any pending or granted rule waiver requests or requests for Special Temporary Authorization.
- If any petitions to deny, informal objections or other pleadings have been filed with respect to any application (including petitions for reconsideration of granted applications), Seller should provide a copy of the petition, the opposition, and any reply thereto.
- Any enforcement proceedings in connection with any licensed facility, has any party filed a complaint or a request to institute revocation proceedings or any similar pleading? If so, Seller should provide copies of all pleadings and a statement as to the status of the proceeding.
- Is Seller a defendant in any informal, formal or other complaint proceeding before the FCC or any other regulatory agency, or in any civil action that could materially impact its FCC Licenses? If so, Seller should provide copies of the complaint, Seller's answer, and any other relevant pleadings, including motions to dismiss.
- The FCC, the FAA or any state regulatory agency issues any letter, notice, claim or other form of correspondence, including a notice of liability for a fine or forfeiture in connection with any licensed facility? If so, Seller should provide copies of the agency's letter/notice, Seller's response, and a statement as to the status of the matter.
- Are there any pending FCC Enforcement Bureau matters pending? If so, Seller should provide copies of all related responses, documentation and filings.
- Proof of FCC license auction payments, payment schedule, date of payments, and copies of any requests for extension of same.

[3] Health Care Industry

[a] Introduction

Given the large portion of the economy that the health care industry represents (almost 20% of U.S. GDP) and the market interest in transactions, an understanding of the material risks that an acquirer might face is important to an effective and meaningful acquisition. This discussion of due diligence considerations is focused on a subsector of health care – health care services. Health care services include businesses that provide professional/clinical health care services to patients, bricks and mortar in-patient and out-patient health care providers as well as businesses that provide ancillary health care services. So, these are businesses such as hospitals and health systems, nursing homes, behavioral health providers, physicians and health care professional groups, home health and hospice providers, outpatient clinics, ambulatory surgery centers, out-patient rehabilitation, substance use disorder services, senior housing and services, and continuing care retirement communities.

Most, if not all, health care services businesses face certain material regulatory risks that should be the subject of robust due diligence. These risks fall within certain categories that include licensure, payor issues and reimbursement, fraud and abuse, excluded parties and health care privacy-related issues. A summary discussion of each of these risks follows. There is also a final point about regulatory compliance programs which is often another area of diligence that buyers review.

[b] Licensure

In a highly regulated industry like health care, a buyer can expect that the target company will have one or more licenses or permits to operate their business. In that respect, buyers must focus their diligence on evaluating what licenses the seller has, whether they are the correct licenses, ensuring that the licenses have not been subject to adverse enforcement action and that the seller has complied with the regulatory requirements relating to retention of the identified licenses. Loss of a license or even the threat of such a loss will often be material to the seller's business. To diligence the licenses held by a seller and issues

surrounding those licenses, buyers should make specific requests for diligence documentation that include items such as:

1. All current regulatory permits, licenses, certifications, accreditations, certificates of need and other required approvals that the target may have relating to its business.
2. Documents relating to investigations, audits, surveys, site visits and inquiries by governmental agencies and contractors.
3. Documents relating to corrective action plans imposed on the business or implemented by the business.
4. Documents relating to unpaid civil monetary penalties or administrative penalties and civil settlements.
5. Documents relating to any suspension, termination, or revocation of a license.
6. Documents relating to any refusal to approve a license.

The transfer or change of ownership of applicable licenses is also a factor in the diligence process because it can influence material issues such as the structure of the transaction (stock vs. asset) and whether an executory period between signing and closing is necessary to pursue and receive regulatory approvals. As a result, understanding what licenses the seller holds and the process necessary for the buyer to apply to obtain them is extremely important. Often, even though the buyer may ask the seller to provide it with information relative to the regulatory process, the buyer will engage its own counsel or consultants to review the process once it knows what licenses are necessary for post-closing.

[c] Payor Issues and Reimbursement

The U.S. Federal government is the single largest payor for health care services in the U.S. The dollars it spends on health care services far exceed any other payor, including commercial payors. To participate in Federal health care programs, health care services businesses agree to comply with a significant regulatory framework. On the other hand, the relationship that a health care services business has with commercial payors is solely contractual. Due diligence of Federal government program relationships is therefore different than commercial payor relationships in certain respects.

To diligence reimbursement issues irrespective of the payor involved, buyers should make specific requests for diligence documentation that include items such as:

1. Documents relating to investigations, audits, surveys, site visits and inquiries by a payor or a contractor on behalf of a payor.
2. Documents relating to corrective action plans imposed by a payor on the seller or implemented by the seller.
3. Documents relating to any self-disclosures or voluntary disclosures made to any payor.
4. Documents relating to internal audit reports of billing, coding and reimbursement reviews or audits.
5. Documents relating to any third-party reports and related deliverables from consultants engaged in billing, coding and reimbursement audits or reviews.

Material risks for health care services businesses can come from failures to meet requirements for claims submissions. Such businesses can therefore be subject to fines, penalties, demands for repayment and other types of enforcement, both civil and criminal depending on the severity of and facts surrounding the matter. With Federal health care programs, significant failures may also result in termination of participation in such programs.

In addition to legal diligence on regulatory / billing compliance issues, counsel to buyers in these transactions should ensure that the buyer itself (if it has the capability) or with a competent third-party consultant conducts a meaningful billing and coding review of the seller as part of the due diligence process. The due diligence responses provided by a seller in relation to diligence requests will only go so

far in adequately assessing potential risks relating to reimbursement and a third-party review is essential to performing adequate due diligence.

With respect to commercial payor relationships, there are what may seem like general corporate diligence considerations, however, the issues involved can have significant consequences for the transaction. Commercial payor contracts commonly have unique assignment, change of control and or most favored nation clauses that a buyer must diligence to be aware of the effects a transaction may have on those relationships. Depending on the amount of revenue the seller receives from a particular payor these issues can be significant. Buyers need to understand whether commercial payor contracts can be assigned, in most cases there is an absolute prohibition on assignment. In many agreements there are notice and specific requirements relating to a change of control of the contracting provider (i.e. the seller). Additionally, a fair number of commercial payor contract may include most-favored nation clauses or something similar that essentially provide that if the buyer already has a relationship with the payor and there is a differential between the rates paid to seller and buyer, the payor will on a post-closing basis default to the lower rates between the two.

[d] Fraud and Abuse

Fraud and abuse in the health care system is a serious concern of federal and state regulators. Major fraud and abuse laws include, the Federal Anti-Kickback Statute (the "AKS"), *42 U.S.C. §1320a-7b(b)*, the Physician Self-Referral Prohibition (the "Stark Law") *42 U.S.C. §1395nn*, the Criminal and Civil False Claims Acts, *18 U.S.C. §287* and *31 U.S.C. §3729*. These laws prohibit certain business practices as well as provide for penalties relating to fraudulent claims to government payment programs. Liability can come in many forms and can result in both civil or criminal liability depending on the conduct and issues at hand. More so, such liability is rarely immaterial.[8] Due diligence considerations relating to business relationships that can run afoul of applicable fraud and abuse laws involve different types of inquiry.

To diligence business relationships that may have fraud and abuse implications, buyers should make specific requests for diligence documentation that include items such as:

1. Contracts between the seller and other health care businesses or vendors.
2. Documents or memos analyzing any arrangement the seller determined fit into a safe harbor to the AKS or exception to the Stark Law
3. Business relationships with physicians and other health care professionals whether via ownership or compensation.
4. Business relationships with any individual or entity in a position to refer business paid for by governmental programs to the seller.
5. Marketing activities of the seller.
6. Bonus and compensation plans.
7. Internal complaints or concerns relating to compliance with the AKS or Stark.

In addition to the above requests, buyers and their counsel should pay close attention to any responses to general requests for investigations, audits, reviews, settlements, litigation, etc. that specifically relate to AKS or Stark Law issues or similar state law issues. To ensure that those types of matters don't get overlooked, buyers often ask for such documents and information in separate health regulatory diligence requests even though such requests might overlap with more general due diligence requests relating to litigation and government agency enforcement. In most cases, buyers also ask the seller to confirm that they are not aware of any conduct that may potentially lead to enforcement or that is questionably compliant.

---

[8] Due diligence considerations relating to reimbursement and claims that can result in fraud and abuse liability are discussed in *§§ 3.04[3][c]* and *[d]* above.

[e] Excluded Parties

Generally, excluded parties are persons or entities who have either been excluded from participation in federal health care programs or excluded from participation in federal contracts. Exclusion in federal health care programs means that no payment can be made by a federal health care program for any items or services furnished, ordered, or prescribed by an excluded individual or entity. Individuals and entities that have been excluded from participation in federal contracts are barred from receiving federal contracts or federally approved subcontracts and from certain types of federal financial and nonfinancial assistance and benefits.

A seller that has in the past, or is currently, employing an excluded individual or has had, or has, a contract with an excluded party can have material risks associated with it. There are potential civil penalties that can be assessed in addition to repayment of the dollars associated with the excluded person or entity. Buyers generally expect that health care services companies will have checked the appropriate databases periodically to screen for ineligible individuals and entities and steer clear of them.

To diligence excluded party issues, buyers should make specific requests for diligence documentation that include items such as:

1. Whether the seller has a process in place that screens for excluded parties.
2. Evidence that the seller has checked its employees, contractors, and other relevant parties against the exclusion databases.
3. Whether the company has ever had exposure to an excluded party and how was that exposure handled.

[f] Health Care Privacy Issues

The Health Insurance Portability and Accountability Act (“HIPAA”) establishes national privacy standards to protect individuals’ medical records and other personal health information (“PHI”). It also contains regulatory requirements relating to the physical and electronic security standards for PHI. HIPAA applies to “Covered Entities” which include health care providers, insurers and other stakeholders that may use or disclose PHI. Violations of the law and its associated regulations can result in significant civil or criminal liability depending on the nature and extent of the violation. Due to the serious nature of the penalties involved and the enforcement climate, buyers should focus diligence efforts on compliance processes and any prior or ongoing privacy related investigations.

To diligence HIPAA privacy issues, buyers should make specific requests for diligence documentation that include items such as:

1. The seller’s HIPAA compliance policies and procedures covering at least the last 3 years.
2. HIPAA training materials and information on how personnel received HIPAA training.
3. Business Associate Agreements in place over the last 3 years.
4. Documents relating to HIPAA compliance tracking and assessment.
5. Documents relating to any security breaches or incidents, follow-up response, and disclosure of the breaches/incidents to individuals or third parties.
6. List of complaints or allegations of privacy/security breaches involving the company

Additionally, similar to the discussion above relating to the use of third-party consultants for billing and coding reviews, buyers and their counsel should consider engaging competent third-party consultants for at least a portion of the HIPAA-related diligence, particularly the technical diligence relating to digital security.

[g] Regulatory Compliance Programs

Despite not being a legal or regulatory requirement[9] to have a compliance program, the implementation and ongoing operation of regulatory compliance program has become an expectation for buyers. The purpose of compliance programs is to help health care services providers develop controls for adherence to applicable health care law. Essentially, seller having a program is considered “market” and a well-developed and effective program is the yard stick by which buyers can measure a seller’s “culture of compliance”. Practically every program is designed to meet the U.S. Federal Sentencing Guidelines for Organizations, §8B2.1. Effective Compliance and Ethics Program, requirements. More so, the U.S. Department of Health and Human Services Office of the Inspector General has an ongoing campaign to encourage health care services providers to voluntarily develop and implement programs through its voluntary compliance program guidance.

To diligence a sellers regulatory compliance program, buyers should make specific requests for diligence documentation that include items such as:

1. Whether or not the seller has an established compliance committee and officer.
2. Documents relating to regulatory compliance policies, procedures, and training materials.
3. Documents relating to corporate compliance tracking, assessment, and response.
4. Meeting minutes from the seller’s compliance committee, if applicable.

Uncovering a well-developed and effective program during due diligence can give a buyer comfort with respect to sellers’ overall approach to regulatory compliance.

The areas of due diligence inquiry discussed in this section represent material risk issues for health care services providers and should form the starting point for a robust due diligence process. There will be additional unique issues involved in specific types of health care or life sciences transactions that are beyond the scope of this discussion.

[4] Cannabis Industry

[a] Introduction

The sale of a licensed cannabis company presents unique legal complexities due to the intricate regulatory landscape governing the industry. Given the interplay between state and local regulations, and complexities touching corporate records, intellectual property considerations, supply chain management, tax obligations, and leasing arrangements, thorough due diligence is paramount. Outlined below are key areas of focus during the due diligence process for any such sale, providing legal practitioners with a framework to navigate these multifaceted transactions effectively.

[b] State and Local Regulatory Compliance

Cannabis businesses operate under a dual-layered regulatory framework, where both state and local authorities impose licensing and operational requirements. Notably, local jurisdictions may have more stringent rules than state laws, particularly concerning ownership transfers and changes in control. For instance, in California, while state regulations permit ownership changes, local ordinances may require pre-approval or impose restrictions on the percentage of ownership that can be transferred in a single transaction.

Due diligence must include a comprehensive review of both state and local regulations to ascertain the permissibility and procedural requirements for ownership transfers. This assessment will directly influence the structure of the transaction, whether it proceeds as an asset sale, equity sale, or merger. Early

[9] There are certain discreet jurisdictions and provider types that actually do have legal requirements to maintain regulatory compliance programs, but these are not universal. For example, New York State requires them for Medicaid providers that receive over a certain amount of revenue per year from the program and Skilled Nursing Facilities participating in Medicare are required to have a program as well.

engagement with regulatory authorities and obtaining necessary approvals are critical to ensure compliance and avoid post-closing complications.

[c] Corporate Governance and Ownership Structure

Regulatory frameworks often mandate disclosure and vetting of individuals with ownership interests in cannabis businesses. This includes background checks and qualification assessments for equity holders and key personnel. Buyers must scrutinize the seller's corporate records to identify all stakeholders, ensuring that all required disclosures have been made and that there are no hidden interests that could jeopardize regulatory compliance.

Inaccuracies or omissions in ownership disclosures can lead to license revocation or denial of transfer approvals. Therefore, it is common for buyers to require the seller to undertake corporate cleanup efforts, rectifying any discrepancies in ownership records and ensuring that all regulatory filings are accurate and up to date.

[d] Intellectual Property Considerations

The cannabis industry's unique legal status under federal law presents challenges in securing intellectual property protections. The U.S. Patent and Trademark Office (USPTO) does not grant trademark registrations for cannabis-related products that are illegal under federal law. However, businesses can seek state-level trademark protections and federal trademarks for ancillary products that do not contain cannabis.

Due diligence should assess the target company's intellectual property portfolio, including trademarks, trade secrets, and any proprietary technology. Additionally, compliance with labeling regulations is critical, as mislabeling can lead to enforcement actions. Buyers must ensure that the company's products adhere to all applicable state and local labeling requirements.

[e] Supply Chain Management and Record-Keeping

Cannabis businesses are subject to stringent track-and-trace requirements to prevent diversion into the illicit market. States like California mandate the use of systems such as the California Cannabis Track-and-Trace (CCTT) to monitor the movement of cannabis products from seed to sale While attorneys may not directly audit these systems, they should collaborate with compliance officers to verify that the company maintains accurate and complete records. Any gaps or inconsistencies in tracking data can pose significant risks and may necessitate specific representations, warranties, or indemnities in the transaction documents.

[f] Contracts and Insurance Coverage

Cannabis companies often engage in supply chain and facility management contracts that may not be covered by their insurance policies or may have been executed without proper regulatory oversight. Due diligence should involve a thorough review of all material contracts to identify any that lack appropriate insurance coverage or that may be non-compliant with regulatory requirements. Identifying and addressing these issues pre-closing is essential to mitigate potential liabilities. This may involve renegotiating contract terms, obtaining necessary insurance endorsements, or, in some cases, terminating non-compliant agreements.

[g] Tax Compliance and Section 280E

Under *Internal Revenue Code Section 280E*, businesses trafficking in controlled substances prohibited by federal law, including cannabis, cannot deduct ordinary business expenses, leading to higher effective tax rates. Some companies have challenged the applicability of Section 280E, with varying degrees of success. Due diligence must include a comprehensive review of the target company's tax filings, liabilities, and any ongoing disputes with tax authorities. Given the potential for significant tax exposure, buyers often seek special indemnities or escrow arrangements to protect against unforeseen tax liabilities.

[h] Lease Agreements and Real Property Considerations

Leases for cannabis operations often contain specialized provisions, including clauses requiring compliance with all laws, which may not account for the conflict between state and federal cannabis laws. Such provisions can create vulnerabilities, particularly if federal enforcement priorities shift. Due diligence should involve a careful review of all lease agreements to identify and address any provisions that could pose risks. This may necessitate negotiating lease amendments to include cannabis-specific carve-outs or obtaining landlord consents where required.

The cannabis industry is a dynamic and rapidly evolving sector, presenting both opportunities and challenges for investors and legal practitioners. The complex interplay of state and local regulations, coupled with federal legal constraints, necessitates meticulous due diligence in any transaction involving a licensed cannabis company. By proactively addressing the areas outlined above, parties can structure transactions that are compliant, mitigate potential risks, and position themselves for success in this evolving market.

§ 3.05 Data Rooms

[1] Overview

Data rooms are usually online and are used to electronically store and share the information that is exchanged during due diligence process. Using a data room as the central repository of all information exchanged during due diligence helps keep the various parties to a transaction organized and allows for all of the documents exchanged during diligence to be stored in one place rather than being constantly exchanged back and forth between the parties.

[2] Physical vs. Virtual Data Rooms

The key difference between a physical data room and an online virtual data room (VDR) lies in how and where the information and documents are stored and accessed. For a physical data room, the information and documents are stored in a physical location and must be accessed manually and in-person. On the other hand, for the more common VDR, the information and documents are stored virtually in an electronic format and can be accessed remotely by those individuals who have been granted access to such VDR (i.e., as part of the working group, as explained above).

Cost can play an important factor when choosing between using a physical data room or a VDR. While there may be an upfront cost to use a specific VDR platform, such costs are minor in comparison to the costs that were previously expended for trips to a physical data room to be able to review the due diligence materials in person. With using a VDR there is no limit to the number of people that can review the diligence materials at once, whereas in a physical data room the review of a specific document is limited to the number of copies there are of a specific document in the physical data room unless additional copies are made.

The use of a VDR provides greater control to the parties involved in the due diligence process as a VDR allows the party providing the due diligence information to restrict and monitor the access to, and printing or downloading of, the documents provided during the due diligence process. Such restrictive features of a VDR can help protect the confidentiality of the information provided and may also provide additional insight about which diligence areas are of interest to the reviewing party and how much effort is being expended in connection with the review as these analytics and metrics can be tracked and reviewed.[10]

Physical data rooms were more common prior to the increase in secure technologies. These secure technologies were necessary for parties to feel comfortable that the information and documents that were going to be uploaded to a VDR were going to be secure and protected from being disclosed and accessible by unauthorized individuals. The current landscape of corporate transactions involves the overwhelming use of VDRs rather than physical data rooms.

[3] Selected Data Room Mechanics and Protocols

For any data room to help make the due diligence process more efficient, it must be set up in an organized manner. One way in which a data room can be set up in an organized manner is to have a data room index (or in other words, a table of contents of the data room and the contents included in such data room). Oftentimes, the data room index follows the numbering of the initial due diligence request list of the buyer. This numbering

---

[10] *Id.*

system helps keep all of the information and documents organized and makes the data room easy for users to know where to find certain information.

Typically, seller's counsel or the investment bankers are the ones who set-up and maintain the data room, and generally speaking, the rule of thumb is that the party initiating the transaction is the party that is responsible for setting up and maintaining the data room as such party is ultimately the party providing the information that will ultimately be stored in the data room. Representatives of the seller (i.e., the investment bankers and/or seller's counsel) will upload the documents and information responsive to the questions in the diligence request list to the data room. Additionally, each iterative diligence request list that is exchanged between the parties is typically uploaded to the data room as well.

End of Document

§ 3.06 Due Diligence Documentation

[1] Trackers, Notes, and Work Product

The diligence tracker is a helpful tool that helps track what questions have been answered and what documents have been provided during the diligence process and also what questions still need to be answered and what documents still need to be provided during the diligence process. While the diligence tracker will include the items that were requested in the initial diligence request list, the diligence tracker will continually be updated throughout the diligence process. It is important to note that depending on the deal dynamics the diligence tracker will be exchanged back and forth between the buyer and seller teams. However, in other cases the buyer team may have its own internal diligence tracker to track its own review of diligence documents.

Within the diligence tracker, the parties may find it helpful to "tag" the various diligence requests with a level of priority (i.e., high, medium, low) so that the target company and seller's counsel understand which requests are of most importance to the buyer. Additionally, within the diligence tracker there are typically columns left for annotations so that notes and follow-up questions can be left between the parties as information is continually being exchanged. Diligence is a fluid process and as information and documents are provided, follow-up questions may arise. Such follow-up questions can be tracked within the diligence tracker.

It is important to keep track of all documents and information that have been reviewed during due diligence. There is no one right way to keep track of the information that a lawyer has reviewed during due diligence. One way that lawyers keep track of due diligence review is to make diligence charts to chart the various types of documents that have been reviewed. Before reviewing any documents, it is important to understand what the purpose of the diligence review is. A common scope of the diligence review is to look for "red flags". A chart presents a clear and succinct way to present information and can be shared with the client if the client requests a diligence work product.

[2] Due Diligence Memoranda

The due diligence memorandum is a document that summarizes the findings of the due diligence process. Oftentimes, the due diligence memorandum will be presented to the governing body of the buyer and used as a resource for when decisions are to be made about whether to proceed with the transaction. Typically, each specialist who reviewed documents in connection with the due diligence process will be responsible for summarizing such findings in a memorandum format. When drafting the due diligence memorandum, it will be critical to include a list of assumption and limitations as this will limit the liability and clarify the scope of the due diligence memorandum. An example of an assumption / limitation is: "This due diligence memorandum is based solely on the due diligence documents provided as of [DATE]." Including this assumption / limitation protects against liability if a critical due diligence document was provided after the due diligence memorandum was drafted. One key focus of the memorandum is to address any "red flags" that were discovered during due diligence and how such red flags should be addressed. A "red flag" refers to any issue, risk, or potential problem that is identified during the due diligence process that could pose a significant concern to the transaction. It is important to identify such red flags in the due diligence memorandum, as it may impact the purchase price of even whether the buyer may wish to proceed with the transaction.

End of Document

1 Due Diligence in Corporate Transactions Chapter 4.syn

Chapter 4 Organizational Legal Due Diligence

§ 4.01 Introduction

Organizational legal due diligence is a core component of every corporate transaction. Lawyers must review the target company's organizational documents to confirm valid formation under applicable law and verify that the entity possesses the authority to execute the proposed transaction. If lawyers overlook deficiencies at this stage, they may expose the client to risks such as unenforceable agreements, undisclosed liabilities, or improper approvals.

Lawyers must conduct this review with precision and apply legal judgment to assess both the completeness and legal sufficiency of the entity's governance documents. These materials establish the framework for corporate authority and shape how the entity approves actions throughout the transaction process.

The entity type determines the applicable requirements. Corporations, limited liability companies, and partnerships each follow distinct statutory rules governing formation, governance, and authorization. Lawyers must understand these frameworks and confirm that the target company has properly adopted, maintained, and followed its governing documents. They must also determine whether the target company documented required approvals, such as board or member consents, and whether any gaps exist between formal requirements and actual practices.

Organizational diligence supports broader transaction execution by identifying missing approvals, unauthorized actions, or compliance failures that may affect closing or require remediation. Lawyers must resolve these issues before signing or advise clients to include appropriate conditions for closing. Corrective measures may involve ratifications, supplemental approvals, or enhanced contractual protections.

Organizational records also inform due diligence related to the capitalization of the target company. Governance documents often define share rights, conversion mechanics, and equity incentive terms. Lawyers must review these documents to verify that the target company accurately describes its capital structure and that there are no defects affecting ownership or voting rights. Lawyers should address inconsistencies through disclosure, documentation, or adjustment to deal terms.

Lawyers must avoid treating this process as routine. In transactions involving multiple equity classes, historical restructurings, or incomplete records, organizational issues can create material risks. A disciplined and complete review allows lawyers to identify these issues early and recommend measures to mitigate their impact on the transaction.

The following sections outline a structured approach to organizational due diligence. They begin with general principles for reviewing governance documents and proceed through entity-specific considerations. Additional sections address capitalization records and the review of board and shareholder actions that authorize corporate activity.

§ 4.02 Organizational Document Review

[1] Organizational Records Checklist[1]

Lawyers must begin organizational due diligence with a systematic review of the entity's core formation and governance documents. A structured checklist promotes consistency and ensures a complete review across different entity types and transactions. While lawyers must tailor each checklist to the specific entity and deal context, a baseline organizational records checklist should include the following:

1. Certificate or Articles of Incorporation for corporations, or Certificate of Formation or Articles of Organization for limited liability companies
2. Bylaws for corporations, or Operating Agreement for limited liability companies ("LLCs")
3. Partnership Agreement for partnerships
4. All amendments to any organizational documents
5. Certificates of good standing from the entity's home jurisdiction and from all jurisdictions in which the entity qualifies to do business
6. Stock ledger or membership interest register
7. Shareholder, member, or partner consents
8. Resolutions adopted by the board of directors, members, managers, or partners
9. Minutes of board and committee meetings
10. Equity incentive plans, including stock option plans, restricted stock plans, and similar arrangements
11. Issued stock certificates, if applicable, and any related stock transfer agreements
12. Foreign qualification filings
13. "Doing Business As" (DBA) filings
14. Organizational charts, if available

At the outset of the diligence process, lawyers must request and review each of these documents. Lawyers must analyze the contents of each document to confirm legal sufficiency and internal consistency. They must not rely on the existence of documents alone but must verify that the terms align with applicable law, the target company's internal governance practices, and the requirements of the transaction.

[2] Corporation Organizational Records Review

[a] Certificate of Incorporation and Amendments

Lawyers should begin their review with the corporation's certificate of incorporation. This document establishes the legal existence of the corporation and defines its fundamental characteristics, including its name, share structure, and any special provisions. Lawyers must confirm that the certificate has been properly filed with the appropriate Secretary of State (or similar office) and reflects the current corporate

[1] See the Appendix for detailed checklists for corporations, LLCs, and partnerships.

name. They must verify that the certificate specifies the total number of authorized shares, identifies each class of stock, and states the par value or lack thereof for each class. Lawyers must also examine each amendment to the certificate to ensure proper adoption and filing. A history of frequent or inconsistent amendments may signal internal governance issues or prior structural instability that warrants further inquiry.

[b] Bylaws

Lawyers must next review the corporation's bylaws. The bylaws govern the corporation's internal management, including procedures for electing directors and officers, conducting shareholder meetings, determining quorum, and granting indemnification rights. Lawyers must confirm that the bylaws exist in the final form, include effective dates, and reflect all properly documented amendments. They must ensure consistency between the bylaws, the certificate of incorporation, and applicable corporate statutes. Outdated bylaws or those lacking provisions for electronic communication or modern governance practices often require immediate attention and possible amendment.

[c] Board and Shareholder Consents and Resolutions

When reviewing board and shareholder consents and resolutions, lawyers must verify that the corporation has properly authorized all major corporate actions. Board minutes or written consents must support actions such as equity issuances, mergers, asset sales, and entry into material contracts. When the organization's bylaws, operating agreement, or partnership agreement require board or shareholder approval, or when such approval is required by statute, lawyers must confirm the existence of executed and dated shareholder consents or meeting minutes. Missing or incomplete documentation for significant actions—such as the adoption of a stock option plan or the issuance of preferred equity—may necessitate ratifying resolutions before closing. Buyers often condition closing on the remediation of such gaps to ensure the enforceability of prior actions.

[d] Good Standing Certificates

Lawyers must also obtain good standing certificates from the corporation's jurisdiction of formation and from each jurisdiction in which the corporation has registered to conduct business. If the corporation has allowed any qualification to lapse, lawyers must evaluate whether the lapse exposes the corporation to penalties or impairs its contractual enforceability in those jurisdictions.

[e] Stock Ledger

Lawyers must review the stock ledger, which serves as the corporation's official record of equity ownership. The ledger must reflect all historical stock issuances, accurately record share transfers, and include notations of any transfer restrictions or legends. Lawyers must compare the ledger against the capitalization table and disclosure schedules to identify discrepancies. Inconsistencies in these records raise material concerns regarding ownership rights and may indicate that the corporation failed to properly document equity transactions.

[f] Organizational Chart

Finally, lawyers should request a current organizational chart that accurately depicts the corporation's equity ownership and control structure. In transactions involving multiple stock classes, historical financings, or holding companies, the organizational chart provides a critical reference point for confirming ownership percentages, voting rights, and control relationships among shareholders. Lawyers must compare the organizational chart to the stock ledger, capitalization table, and charter documents to ensure consistency. Any misalignment among these materials may indicate undocumented issuances, errors in ownership records, or unauthorized transfers. Lawyers must identify and resolve these discrepancies before closing to ensure that the buyer receives a clear and accurate understanding of the corporation's equity structure and governance authority.

[3] LLC Organizational Records Review

[a] Certificate of Formation

Lawyers must begin by reviewing the LLC's certificate of formation or articles of organization, which establishes the entity's legal existence. This document, sometimes referred to as the articles of organization, must include the proper filing and date-stamp from the Secretary of State. Lawyers must confirm that the name listed in the certificate matches the name used in the operating agreement and all other formation documents. If the LLC has filed amendments to the certificate, lawyers must ensure that those amendments align with other organizational records. Because the certificate of formation typically contains limited substantive information, lawyers must place particular emphasis on the operating agreement during the diligence process.

[b] Operating Agreement

The operating agreement serves as the LLC's primary governance document. Lawyers must confirm that the operating agreement exists in fully executed form and includes clear provisions addressing the membership structure, initial and subsequent capital contributions, and the management framework—whether member-managed or manager-managed. The agreement must define the procedures for voting, authorize or restrict specific actions, and outline the rules governing the transfer of membership interests. Lawyers must determine whether the agreement imposes unanimity requirements for significant transactions, as these provisions may affect both the timing and feasibility of the deal. Lawyers should identify any inconsistencies in authority, any unsigned or outdated agreements, and any conflicting terms that create ambiguity around who holds decision-making power.

[c] Member and Manager Consents and Resolutions

Lawyers must also review member and manager consents and resolutions to confirm proper authorization for significant corporate actions. Where managers act on behalf of the LLC, lawyers must verify that those individuals held authority to approve the transactions in question. For member-managed LLCs, lawyers must ensure that all actions requiring member approval have received properly documented and dated consent. Where the LLC failed to secure appropriate approval for prior actions—such as admitting new members, approving equity issuances, or entering into material contracts—lawyers must recommend corrective measures, including ratifications or supplemental approvals. In transactions that require unanimous member consent, any dissent or ambiguity may delay or prevent closing.

[d] Good Standing Certificates

As with corporations, lawyers must obtain good standing certificates from the LLC's state of formation and from each jurisdiction where the LLC has registered to do business. Any lapse in registration or failure to maintain good standing may trigger penalties or impair the LLC's ability to enforce contracts.

[e] Membership Interests Register

Beyond these core documents, lawyers must also review the LLC's membership interest register, if maintained, to verify the identity of current members, the status of any transfers, and the consistency of ownership with the operating agreement. Where the LLC has issued certificates to evidence membership interests, lawyers must examine those certificates and any related transfer agreements.

[f] DBA Filings

If the LLC operates under a fictitious or trade name, lawyers must confirm that all "Doing Business As" (DBA) filings have been completed and are current.

[g] Organizational Chart

Finally, lawyers should request a current organizational chart that accurately reflects the ownership and control structure of the LLC. Where the entity has multiple classes of membership interests, tiered ownership through holding companies, or one or more subsidiaries, the organizational chart helps identify direct and indirect ownership percentages, control rights, and potential voting blocks. Lawyers must confirm that the chart aligns with the operating agreement, the membership register, and any disclosure schedules provided in the transaction. Discrepancies may signal undocumented transfers, unapproved admissions of new members, or inconsistencies in governance authority. Where lawyers identify such issues, they must address them before closing to ensure clarity of ownership and to prevent post-transaction disputes.

[4] Partnership Organizational Records Review

[a] Partnership Agreement

Lawyers must begin by reviewing the partnership agreement, which governs the rights, duties, and authority of the partners. In the context of limited partnerships (LPs) and limited liability partnerships (LLPs), the agreement defines key provisions concerning profit and loss allocation, management rights, voting thresholds, and partner admission and withdrawal procedures. Lawyers must confirm that the partnership agreement exists in a fully executed and dated form. They must verify that the agreement clearly outlines how the partnership admits new partners, allocates profits and losses, and designates management authority. The agreement must also specify the process for approving major transactions and the voting thresholds required to authorize them. Lawyers must examine dissolution and liquidation provisions to ensure they address the proper winding up of the partnership's affairs. Older agreements often fail to establish clear authority for significant actions, which can lead to ambiguity or disputes in connection with partner consent rights. Lawyers must identify and address such gaps to ensure that the partnership can properly authorize the transaction at hand.

[b] Amendments and Consents

Lawyers must then review all amendments to the partnership agreement and confirm that each amendment appears properly executed and consistent with the original agreement. In reviewing consents and approvals, lawyers must confirm that the partnership obtained the requisite number or percentage of partner approvals for all major decisions. Where the transaction involves a disposition of partnership interests or assets, lawyers must determine whether the selling partners possess authority under the agreement to approve the transaction without violating internal governance provisions. If partner consent thresholds are unclear or unmet, lawyers must advise clients to obtain ratifications or supplemental consents before proceeding.

[c] Good Standing Certificates and Registrations

In addition to governance documents, lawyers must obtain good standing certificates for any registered limited partnerships or LLPs. They must confirm that the partnership maintains active registration in its jurisdiction of formation and in each foreign jurisdiction where it conducts business. Failure to maintain good standing or active registration may restrict the partnership's ability to enforce contracts or conduct business lawfully.

[d] Partnership Interests

Where the partnership maintains a schedule of partners or a register of interests, lawyers must review those records to confirm the identity of current partners, their respective ownership interests, and any recorded restrictions on transfer or assignment. Lawyers should compare these records with the partnership agreement and disclosure schedules to ensure consistency and to identify any undocumented changes in ownership. Inaccuracies in these records may require correction before closing to ensure that all parties clearly understand the partnership's ownership and governance structure.

End of Document

§ 4.03 Capitalization Records

[1] Overview of Capitalization Records Due Diligence

Lawyers must conduct a thorough review of capitalization records in every corporate transaction, regardless of whether the target company is a corporation, limited liability company, or partnership. Capitalization diligence allows lawyers to confirm that the ownership structure is accurate, that equity and profit interests were issued with proper authority, and that no undisclosed rights exist that could impair the transaction. If capitalization records contain deficiencies, the client may face litigation, dilution claims, or post-closing indemnification demands.

To complete this review, lawyers must analyze the equity or membership interest register, capitalization table, and all governing documents and authorizations that support every issuance of stock, membership interests, partnership interests, options, warrants, and convertible instruments. Lawyers must confirm that the entity issued each security in accordance with applicable law, its governing documents, and the requisite approvals of its owners or governing body.

[2] Ownership Records and Issuance Review

[a] Equity or Interest Registers and Capitalization Tables

Lawyers must obtain the entity's official register of equity ownership—whether a stock ledger, membership interest register, or partnership interest schedule—and review it alongside the capitalization table maintained by management. For each recorded issuance, lawyers must confirm that the entity obtained proper approvals and documented any transfers or restrictions. Lawyers must ensure that the register and capitalization table are consistent. Discrepancies require immediate reconciliation and supporting documentation, such as purchase agreements, subscription agreements, or assignment instruments. Because buyers often require certification of capitalization at closing, lawyers must validate the records early to avoid delay or liability.

[b] Approvals for Equity or Interest Issuances

Lawyers must confirm that the entity obtained all required approvals for each issuance of equity or profit interests. In corporations, this includes board and, where necessary, stockholder approvals. In LLCs and partnerships, this includes approvals from members, managers, general partners, or limited partners, depending on the governance structure. Lawyers must determine whether the governing documents impose special voting thresholds or unanimity requirements and must verify that the entity followed the proper procedures. If any approval is missing or defective, lawyers must recommend corrective actions, such as ratifying resolutions, written consents, or waivers. Improper or undocumented issuances create significant risk and may require remediation before closing.

[c] Valid Issuance Under Governing Law

Lawyers must verify that each issuance complies with the legal requirements applicable to the entity's form and jurisdiction. This includes confirming the receipt of valid consideration, the proper recording of the issuance in the entity's records, and compliance with securities law exemptions or filings, if applicable. Failure to satisfy these requirements may render the issuance invalid and expose the entity's owners or

governing body to liability. Lawyers must identify these issues during diligence and ensure that corrective steps are implemented before execution or closing.

[3] Equity Incentive Plans and Option Issuances

[a] Review of Incentive Plans

A target company may have adopted equity incentive plans that authorize the issuance of options, profits interests, or similar instruments. Lawyers must obtain and review each governing plan and any amendments. They must confirm that the entity secured all required approvals—whether from the board, members, partners, or stockholders—and verify the number of interests reserved for issuance. Lawyers must determine whether the entity exceeded its authorized pool and, if so, identify the over-issuance and recommend appropriate corrective action. Buyers commonly require option plan cleanup, including amendments, cancellations, or consents, as a precondition to closing.

[b] Review of Option or Interest Grants

For each grant under an incentive plan, lawyers must review the governing approvals, executed grant agreements, vesting schedules, and valuation or pricing terms. Where applicable, lawyers must confirm that the entity granted options at or above fair market value to avoid adverse tax consequences under rules such as *Internal Revenue Code Section 409A* relating to deferred compensation. Lawyers must also identify any acceleration provisions triggered by a change in control and evaluate the effect of such provisions on the transaction structure or post-closing capitalization.

[4] Convertible Securities, Warrants, and SAFEs

[a] Convertible Instruments

Entities may have issued convertible notes, Simple Agreements for Future Equity (SAFEs), or similar instruments that entitle the holder to equity upon specified future events. Lawyers must obtain and review the full text of each instrument and analyze the conversion mechanics, including triggering events and conversion calculations. Lawyers must determine the timing of conversion relative to the transaction and confirm that the transaction documents clearly address the treatment of each instrument. Failure to address these rights properly may result in unintended dilution or disputes over ownership.

[b] Warrants

Where the entity has issued warrants, lawyers must review each warrant agreement to assess the exercise rights, anti-dilution terms, and expiration dates. They must verify that the entity reserved sufficient equity to cover warrant exercises and that all such warrants appear accurately reflected in the capitalization records. Lawyers must resolve any inconsistencies or deficiencies before closing to ensure that the buyer understands the full scope of post-closing equity rights.

[5] Common Issues and Strategic Best Practices

Lawyers will often encounter missing or incomplete equity registers, unauthorized or undocumented issuances, over-allocation under incentive plans, convertible securities issued without proper approvals, or interests issued without following corporate or contractual procedures. Each of these issues may expose the client to material risk and must be addressed during due diligence.

To mitigate these risks, corporate lawyers should collect and review all governing body and owner approvals for equity-related actions, reconcile ownership records with capitalization tables and plan documents, and identify and correct any deficiencies. When the circumstances require, lawyers must recommend remedial actions, including ratifying resolutions, amended agreements, or targeted consents. Buyers should negotiate detailed

capitalization representations and warranties and require indemnification protection and pre-closing corrective measures to address known issues and protect against undisclosed risks.

End of Document

§ 4.04 Meeting Minutes, Written Consents, and Resolutions

[1] Meeting Minutes

Meeting minutes serve as a contemporaneous record of discussions, deliberations, and formal actions taken by an entity's governing bodies, including boards of directors, members, managers, and partners. Lawyers must review these records to confirm that the entity complied with governance requirements and fulfilled procedural obligations at each meeting.

Lawyers must verify that the minutes document the date, time, and location of each meeting and identify those present. The record must reflect that the meeting satisfied applicable quorum requirements under the entity's governing documents or controlling law. Minutes must also summarize the topics presented, identify the materials reviewed, and state the outcome of each action taken. Where directors, managers, or partners faced potential conflicts of interest, the minutes must reflect full disclosure and document any recusal or abstention from voting.

Well-prepared minutes demonstrate that the entity's decision-makers understood the issues presented, satisfied their fiduciary duties, and reached informed decisions. When lawyers encounter vague, incomplete, or inconsistent minutes, they must determine whether those deficiencies create material risk. Lawyers should recommend corrective action where necessary, including the preparation of supplemental minutes or ratifications to document prior decisions with clarity and precision.

Lawyers must also confirm that the entity consistently maintains minutes for all governing body meetings and, where applicable, committee meetings. Incomplete records may raise enforceability concerns relating to the target company's agreements or cast doubt on the validity of other actions taken. In transactions involving regulatory scrutiny or potential disputes, meeting minutes may become critical evidence. Accordingly, lawyers must evaluate minutes not only for procedural compliance but also for substantive integrity.

[2] Written Consents

Written consents serve as a formal mechanism by which an entity's governing body or ownership group can authorize actions without holding an in-person or telephonic meeting. Corporations, LLCs, and partnerships often rely on written consents to approve routine and extraordinary actions efficiently, provided that the governing documents and applicable law permit such use.

Lawyers must confirm that each consent complies with applicable statutory requirements and internal governance procedures. This includes verifying that the consent reflects unanimous or majority approval, as required; that it identifies the approving parties by name and capacity; and that each signatory executed the consent as of a clearly dated signature page. Lawyers must ensure that the consent describes the approved action with sufficient specificity to support enforceability and post-closing reliance.

In multi-member LLCs and partnerships, lawyers must examine whether the consent meets applicable ownership thresholds for approval and whether the governing documents impose unanimity requirements for particular actions. Where a transaction requires third-party approvals or affects preferential rights, lawyers must determine whether the consent includes appropriate references to those provisions and satisfies notice or waiver obligations.

Lawyers must collect all executed consents and confirm that the records include all pages and exhibits referenced. Inconsistent or incomplete consents may undermine the validity of the approval or raise questions regarding authority. Where the entity failed to secure proper consent, lawyers must recommend supplemental execution or remedial ratification before closing.

[3] Resolutions

Resolutions formalize the approval of corporate, member, or partner actions and serve as critical evidence that the entity acted in accordance with its governing authority. Lawyers must review each resolution to confirm that the approving body properly adopted the resolution, that the resolution clearly states the action authorized, and that it names the individuals empowered to carry out the approved transaction.

Lawyers must confirm that each resolution aligns with the entity's certificate of incorporation, certificate of formation, partnership agreement, bylaws, operating agreement, and statutory requirements. They must evaluate whether the resolution contains sufficient detail, including references to relevant agreements, approval thresholds, and appointed signatories. Where the resolution authorizes equity issuances, mergers, debt financing, or significant asset transfers, the record must support the transaction with clear and complete authority.

When lawyers encounter missing, unsigned, undated, or overly vague resolutions, they must assess whether those deficiencies create enforceability concerns. Defective resolutions often require remedial action, such as ratifying resolutions or supplemental consents, before closing. However, lawyers must determine whether ratified approval suffices under the governing law or whether the original approval required formal action that cannot be replicated after the fact.

Lawyers must also review the resolutions of standing or special committees. For example, in transactions involving audit committees or special M&A committees, lawyers must confirm that the board properly constituted the committee, delegated appropriate authority, and documented its deliberations and approvals. Committee resolutions must identify the basis for their actions and confirm that the members satisfied independence and fiduciary obligations, particularly in conflict or related-party transactions.

Appendix A: Sample Organizational Document Review Checklists

1 Due Diligence in Corporate Transactions Chapter 5.syn

Chapter 5 Environmental Due Diligence

End of Document

§ 5.01 Introduction

Environmental due diligence is a critical component of any due diligence exercise. Environmental due diligence raises many issues, including litigation risks, financial liability, and operational risks. Environmental due diligence also requires an understanding of a target company's regulatory, litigation, and transactional activities. This Chapter provides an overview of what the due diligence team should look for during environmental due diligence; how to organize their environmental diligence; and the special considerations for environmental due diligence in property transactions.

Due Diligence in Corporate Transactions

§ 5.02 Overview of Potential Environmental Liabilities and Risks

[1] Regulatory Requirements

[a] Introduction

Determining whether a target company has complied and is complying with its environmental regulatory obligations requires a basic understanding of federal, state, and local environmental law and regulations. Determining which laws regulate a target company's operations requires a basic understanding of the operations of the target facilities and use of the target properties. Each deal will raise its own environmental regulatory and compliance issues, but experience with prior similar deals is often a useful starting point for identifying the potential permits, approvals, and associated requirements that should be in place.

This Section describes the types of environmental regulatory requirements that may arise during a deal. The discussion focuses primarily on federal environmental obligations, but it is important to remember that states and local governments may have their own parallel permitting and approval processes in place.

[b] Licenses and Permits for Use, Release, Generation, Release, Discharge, Disposal, or Transportation of Hazardous or Regulated Materials

[i] Introduction

Almost every commercial transaction will involve issues related to environmental permitting. Knowing which permits the target should have and what they require forms the backbone of any environmental diligence strategy because of the risks associated with permit violations or the failure to have a required permit altogether.

[ii] Air Pollution Control

The federal Clean Air Act regulates air pollution and emissions from stationary and mobile sources. It establishes a complex permitting system for different types of stationary sources, based primarily on how much they emit and whether or not they are located in areas that have met the National Ambient Air Quality Standards (NAAQS) for certain "criteria pollutants."[1] The Act delegates significant responsibility for implementing and enforcing its requirements to the states, which develop State Implementation Plans for approval by the U.S. Environmental Protection Agency (EPA). Because states can establish more stringent air quality rules than the Clean Air Act, sources that would not require a permit under federal law may nonetheless require a state permit.

Many transactions involving agricultural, manufacturing, or industrial operations will require consideration of federal and state air pollution control laws. The size and location of sources will dictate the type of permits potentially required. The specific type of processes involved will dictate the technical requirements imposed by those permits. Common types of air pollution control permits include:

- ***State permits to operate.*** Most states require facilities, regardless of how much they emit, and subject to certain exemptions, to obtain state permits to operate. State law dictates how long

[1] These criteria pollutants include particulate matter (PM_{10} and $PM_{2.5}$), ozone, nitrous oxides, sulfur oxides, lead, and carbon monoxide.

these permits last; some states may require annual permit renewals, while other states may require renewal every few years. States may also require air permits to construct in order to build a new emitting facility or modify an existing one.

- ***Title V permits.*** Under the federal Clean Air Act, "major sources"—those that emit 100 tons per year or more any air pollutant, 10 tons per year or more any "hazardous air pollutant" (defined in Section 112 of the Clean Air Act), or 25 tons per year or more any combination of hazardous air pollutants—must obtain so-called "Title V permits." These permits ensure that all the requirements applicable to the facility are contained in a single document and include recordkeeping and monitoring requirements. States issue Title V permits under various names, such as "Major Facility Review" permits within the Bay Area Air Quality Management District in California or "Part 70 permits" in Maryland. These permits often last five years. A major source that chooses to implement air pollution controls to avoid exceeding the major source thresholds may receive a "Synthetic Minor Permit" in lieu of a Title V permit.
- ***New Source Review and Prevention of Significant Deterioration permits.*** Sources undergoing construction or modification may also require permits to ensure they do not contribute to exceedances of the NAAQS. Major sources in areas that exceed NAAQS may require New Source Review permits, while major sources in areas that are in attainment with the NAAQS may require Prevention of Significant Deterioration permits. Minor sources may also require these permits. These permits require facilities to evaluate and implement emission limits or air pollution control technology to control emissions. Facilities may also have to acquire emissions offsets in exchange for emitting certain levels of criteria pollutants.

Each air quality permit will impose unique conditions on the source while also containing standard requirements like recordkeeping and monitoring. Outside the real property context, the default assumption should be that a facility or business is subject to air permitting requirements and should have a permit in place. Along with the permit documents themselves, facilities will also likely have annual air emissions data. Some facilities may also have reports demonstrating compliance with technical requirements or emission limits, such as National Emission Standards for Hazardous Air Pollutants and New Source Performance Standards.

Transactions involving the acquisition of vehicle fleets will also likely implicate air pollution control issues. Federal and state law impose fuel efficiency and other performance requirements on different types of vehicles, including cars, buses, trucks, and locomotive engines. Due diligence of these assets should include a review of potentially applicable standards and certifications and information related to compliance with those requirements.

Air pollution control may also implicate issues related to participation in cap-and-trade and renewable energy credit programs. The federal Clean Air Act established a cap-and-trade program for sulfur oxides and nitrous oxides (the major contributors to acid rain) that set a cap on the total amount large sources could emit and established a market-based system for emitters to buy and sell credits representing a set quantity of emissions. This allowed emitters making large reductions to sell their excess emissions to emitters making slower progress so that they could emit more while working to reduce those emissions. States, including California and the New England and Mid-Atlantic states that participate in the Regional Greenhouse Gas Initiative, have their own cap-and-trade programs. In addition to cap-and-trade programs, many states allow businesses to buy and sell renewable energy credits (also referred to sometimes as zero emission energy credits, solar renewable energy credits in the context of solar power, and offshore renewable energy credits in the context of offshore wind); under these programs, the energy generated by solar, wind, and other renewables generates "credits" that energy producers can sell to the grid or to other businesses as a means of offsetting emissions from dirtier sources.

Transactions involving the purchase and sale of energy assets, such as residential and commercial solar facilities or offshore wind farms, will often require consideration of these types of tradable emissions assets. Energy installations will likely have in place agreements with local utilities, energy brokers, or buyers governing the sale of renewable energy credits. Because commercial-scale energy

projects ordinarily require approval from a state public utility or public service commission, the order or tariff approving the project often includes conditions imposed by the state related to energy credits. These conditions may include, for example, minimum output guarantees, a floor or ceiling on the number of credits the system can generate, the price per kilowatt hour of energy produced, and recordkeeping and reporting requirements related to the transfer of credits. Some states also include such requirements in state law and regulations. Due diligence of deals that include energy assets should include review of the underlying laws, regulations, and orders/tariffs governing renewable energy credits as well as the underlying agreements with buyers.

Outside the energy context, due diligence should also involve review of a company's participation in any cap-and-trade program and a review of the underlying laws and regulations, which may include registration, recordkeeping, and reporting requirements.

[iii] Water Pollution Control

The federal Clean Water Act prohibits the discharge of a pollutant from a point source to a navigable water without a permit. In addition to its permitting requirement, the Act imposes requirements related to oil pollution control and technical requirements on certain categories of dischargers. As with the Clean Air Act, the Clean Water Act delegates permitting authority to the states. And as with air pollution control, water pollution control laws at the state level may require their own permits and approvals for discharges to states waters.

Any transaction involving a property that discharges to water will require consideration of water pollution control requirements. Many facilities and operations will require a National Pollutant Discharge Elimination System (NPDES) permit or a state equivalent. Among other things, these individual permits authorize discharges from certain outfalls, set limits on pollutant concentrations, and impose requirements to monitor for certain water quality conditions.

While industrial properties often hold individual NPDES permits, they will also frequently have a so-called "general permit." A general permit is an EPA- or state-issued permit that covers certain types of discharges from a variety of sectors and establishes common conditions and requirements for all covered entities. One common type of general permit held by many industrial facilities is a general permit for industrial stormwater discharges, which may be referred to as a multi-sector general permit, an industrial stormwater general permit, or other similar titles. Common among all such industrial stormwater general permits is the requirement to prepare a so-called Stormwater Pollution Prevention Plan (SWPPP), a document that contains information about a facility and the measures it takes to control stormwater discharges. If a facility has a general stormwater discharge permit, it almost certainly also has a SWPPP.

Other types of documents that facilities with water discharge permits may have in place include Spill Pollution, Control, and Countermeasure (SPCC) plans and Facility Response Plans (FRPs). SPCC plans are required for facilities that store large quantities of oil, and FRPs are plans for responding to "worst-case" discharges of oil or other pollutants. Facilities will also likely have discharge monitoring reports (DMRs) containing water quality monitoring data.

Facilities may also have permits for community or individual drinking wells on their properties. These permits are issued by states. Facilities including publicly owned treatment works (POTWs) may have monitoring data that they are required to collect under the federal Safe Drinking Water Act. States may also issue permits under authority delegated by the Safe Drinking Water Act regulating underground injection of fluids. These types of permits often come up in the context of oil and gas drilling and hydraulic fracturing.

[iv] Solid and Hazardous Waste Management

Federal laws governing the handling, transport, storage, and disposal of solid and hazardous waste include the Resource Conservation and Recovery Act (RCRA) and Solid Waste Disposal Act (SWDA). RCRA and its related statutes provide for the "cradle-to-grave" regulation of solid and hazardous waste. Under RCRA, facilities classified as treatment, storage, and disposal facilities require permits. Facilities

that generate hazardous waste are subject to statutory and regulatory requirements, depending on how much waste they store or generate onsite, such as recordkeeping requirements and limits on the amount of time they can store waste above certain quantities. Landfill facilities also need to meet regulatory criteria to avoid being considered prohibited open dumps.

In addition to any necessary permit, common documentation demonstrating RCRA compliance includes hazardous waste manifests and documents tracking the quantity of waste stored onsite.

State laws may also regulate or limit the amount of solid or hazardous waste a facility can store or generate onsite. These laws may have broader definitions of what constitutes hazardous waste. In the case of emerging contaminants like per- and polyfluoroalkyl substances (PFAS), for example, federal law does not classify PFAS as a hazardous waste, but some state laws do. As a practical matter, this means that hazardous waste requirements may still apply to these substances under state law even if RCRA's hazardous waste provisions do not apply.

Other federal laws beyond RCRA regulate the use and disposal of chemicals. The Toxic Substances Control Act (TSCA) establishes certification requirements for the import of chemicals and establishes a framework for EPA to limit how certain chemicals are used. The Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) also imposes regulatory requirements and in some cases permits that govern the application, use, and disposal of pesticides. And the Hazardous Materials Transportation Act (HMTA) imposes requirements on transporters of hazardous materials. The requirements of these statutes do not come up as frequently as those of RCRA, but in transactions involving processes or operations that may use or generate the substances regulated by these laws, the due diligence team should expect to receive permitting documents, manifests, and other documentation demonstrating compliance.

[v] Potential Risks Associated with Environmental Permitting

Failure to hold necessary permits or comply with existing permits and requirements represent the most common risks associated with environmental permitting. A facility that operates without an air permit, discharges pollutants to water without authorization, or fails to comply with waste management requirements could face agency enforcement actions resulting in civil penalties and fines. These monetary penalties can be substantial; often, each day that an unpermitted activity occurs constitutes a separate violation, and penalties are often calculated on a per-day per-violation basis. Certain minor violations, such as recordkeeping issues or minor exceedances of permit limits, may potentially be addressed without significant fines.

Documents that the target is required to keep or prepare by permit or law can indicate whether a facility has failed to satisfy permit requirements; air emissions data, for example, can demonstrate whether a facility has exceeded permitting thresholds or has become a major source of emissions subject to more stringent requirements. DMRs can similarly indicate whether a facility has persistent issues maintaining water quality levels set out in its NPDES permit. Conversely, a facility's failure to maintain documents can indicate noncompliance with permitting requirements or the legal requirement to even have a permit. Whether a facility is preparing the necessary documents and what those documents say about facility operations are good risk indicators.

The due diligence team can also assess the risk associated with environmental permitting noncompliance by reviewing agency-prepared inspection reports or consultant-prepared compliance reviews. These reports ordinarily identify issues with facility operations that the due diligence team can then follow up on by asking whether the issues are resolved or what steps the target has taken to resolve them. Agency notices of violation or other enforcement documents also provide evidence of noncompliance and can be used to evaluate risk.

Beyond agency enforcement, permit violations can also be subject to so-called "citizen suits." The major federal environmental laws contain provisions that allow nongovernmental organizations or individuals to sue an entity alleged to be in violation of the law or a permit. These types of suits require plaintiffs to provide notice before filing, making it important to not only consider whether a case has

been filed against the target company but whether the target company has received such a notice letter.

The statute of limitations, if applicable, for each type of permit or requirement involved in a deal often serves as the "lookback period" for evaluating risk associated with environmental permitting and approvals. From a deal perspective, a violation that occurred and was resolved outside the statute of limitations period presents a lower risk, whereas a recent violation that remains unresolved with the regulator requires a closer look to determine the likelihood of settlement versus litigation, the potential penalties involved, and the type of corrective action that may be required.

[c] Wetlands, Endangered Species, and Other Considerations

[i] Introduction

Another type of environmental issue that may arise during due diligence concerns considerations related to natural resources, such as wetlands, wildlife, and coastal resources. These issues are more likely to arise in deals that involve resource extraction, energy generation, or infrastructure development, or deals where a project or permit remains pending with respect to a project or activity.

[ii] Wetlands

The federal Clean Water Act protects wetlands that meet the definition of navigable waters by requiring permits (so-called Section 404 permits) to discharge or fill such wetlands. These permits are issued by either the EPA or U.S. Army Corps of Engineers. Other federal permitting requirements related to wetlands may be found in the Rivers and Harbors Act, which prohibits the discharge, fill, or obstruction of certain waters. State laws may impose similar permitting and other protections for state wetlands. A project or activity that will, for example, involve dredging or dumping sediment most likely has or is required to have either a federal or state wetlands permit, or both. Local laws may also be applicable in certain jurisdictions.

At the federal level, the issue of what wetlands constitute "navigable waters" has been the subject of recent litigation and substantial change in scope. The consequences of dredging or filling a wetland without a permit can have significant consequences not only under the Clean Water Act but potentially under other laws that protect habitat, such as the Endangered Species Act. For this reason, it is important not only to have permit documentation but, if a permit has not been obtained, documentation as to the decision-making that went into proceeding without one.

[iii] Endangered Species

The federal Endangered Species Act prohibits the unauthorized take of threatened or endangered species. The U.S. Fish and Wildlife Service or National Marine Fisheries Service may issue permits for the "incidental take" of protected species that prescribe terms and conditions for minimizing harm to the species. Other federal wildlife protection laws such as the Migratory Bird Treaty Act (MBTA) and Marine Mammal Protection Act (MMPA) also prohibit harm to protected species and require permits for activities that may result in harm. The MMPA in particular may be relevant in activities occurring offshore, such as boating and outer continental shelf development. States may maintain their own lists of threatened or endangered species and impose similar prohibitions for those species.

Not all activities subject to the Endangered Species Act will have a permit. Any activity occurring in an area where threatened or endangered species are present will have associated with it a Biological Assessment and/or a Biological Opinion, depending on the amount of interagency consultation required between the federal agency approving the action and the U.S. Fish and Wildlife Service / National Marine Fisheries Service. As with determinations of Section 404 applicability, documentation related to Endangered Species Act compliance and consultation is important. In addition to the Biological Assessment and/or Biological Opinion, these documents may include internal memoranda, species

surveys (such as Information for Planning and Construction (IPaC) reports), and correspondences with federal agencies.

[iv] Coastal Resources

The federal Coastal Zone Management Act (CZMA) mandates that activities that require federal permits or receive federal funding are consistent with state coastal protection policies. The CZMA itself does not require permits. State laws, however, may require permits for coastal development. California, for example, requires a Coastal Development Permit for activities within the California coastal zone. New Jersey also requires permits and approvals for different types of coastal development. Coastal development permitting and related coordination issues may appear in the context of offshore and onshore development and resource extraction activities.

In addition to state permits, documentation pertinent to transactions involving coastal or offshore assets may include a Consistency Certification or Consistency Determination. States issue these types of documents to indicate concurrence with a federal agency's decision to take or authorize action in the coastal zone. These documents along with any applications for state concurrence and related materials are important in evaluating potential risks associated with CZMA compliance.

[v] Other Natural Resource Considerations

Other federal permitting requirements that may be implicated in a deal include permits related to mining operations (*e.g.*, Surface Mining Control and Reclamation Act), outer continental shelf development (*e.g.*, Outer Continental Shelf Lands Act), and timber harvesting, among other authorizations. At minimum, due diligence would typically involve review of the permitting documents, but often other documents, such as permit applications and monitoring reports, should also be evaluated.

[vi] Potential Risks Associated with Natural Resource Considerations

As with environmental permitting related to pollution control, natural resource permitting also raises the risk of agency enforcement for failure to obtain a permit or comply with permit conditions. Recordkeeping requirements contained in these types of permits and licenses can help verify whether a target company has complied with the law.

Some natural resource statutes impose requirements on agencies, rather than private parties, which can become the subject of litigation or agency appeals. In these cases, the agency's action rather than the target's are at issue. These types of challenges, however, still may pose a substantial risk to the target's operations, as they can delay the issuance of permits and approvals or invalidate existing permits or approvals altogether, in turn delaying or stalling ongoing projects or operations.

[d] NEPA and State Counterparts

[i] Introduction

In addition to substantive permitting requirements, federal and state law impose procedural obligations to ensure that governmental or certain private activity will not significantly affect environmental quality or protected environmental resources. A transaction that involves ongoing infrastructure or property development, for example, may implicate considerations of compliance with procedural environmental requirements.

At the federal level, the two primary environmental procedural statutes are the National Environmental Policy Act (NEPA), which requires federal agencies to assess the environmental impacts of major federal actions such as the issuance of federal permits or a grant of federal funding; and Section 7 of the Endangered Species Act, which requires interagency consultation on addressing risk of harm to threatened or endangered species or their critical habitat. Other potentially relevant federal environmental procedural statutes include Section 4(f) of the Department of Transportation Act, which requires transportation projects to avoid the use of or evaluate alternatives to using public parks,

refuges, and historic resources; Section 106 of the National Historic Preservation Act, which requires consideration of how to avoid or minimize harm to historic resources; and Section 6(f) of the Land and Water Conservation Act, which prohibits the conversion of land acquired with Land and Water Conservation Fund monies from recreational to non-recreational use unless other comparable land is made available.

States may also have their own versions of NEPA. While also procedural, some states may impose substantive requirements (*i.e.*, selection of the least harmful alternative) on project applicants.

In general, the risks posed by potential lack of compliance with these statutes involve consideration of whether the agencies and target company have followed the required procedures and prepared the appropriate documents. At least at the federal level, the procedural requirements of these statutes ordinarily fall to the agencies, and it is thus the agencies who would be sued for not following proper procedure. However, because litigation against the agency could invalidate an approval or decision necessary for private action to commence or continue, understanding whether a target company's development has complied with applicable requirements is important for evaluating the risk that a project could be delayed or prevented from moving forward.

[ii] Disclosure, Labeling, Warning, and Notification Requirements

Many federal and state environmental laws impose requirements to notify the public that products contain certain types of chemicals, report to federal or state agencies the type and amount of chemicals used at facilities and prepare plans for notifying the public of an emergency. Examples of such requirements include:

- Labeling requirements under FIFRA and TSCA;
- Risk Management Plans under Section 112(r) of the Clean Air Act;
- Requirements under the Emergency Planning and Community Right-to-know Act related to emergency planning, annual Toxics Release Inventory reporting, and annual Tier II reporting;
- Requirements under Section 103 of the Comprehensive Environmental Response, Compensation and Liability Act (CERCLA) to report releases of hazardous substances in amounts above their reportable quantities to the National Response Center; and
- California Proposition 65 labeling requirements.

In many cases, these requirements come up in the context of transactions involving manufacturing, industrial, and agricultural assets, although foods, apparel, consumer products and other types of products and services can be implicated as well. Often, compliance with these requirements can be discerned through a review of annual reports submitted to EPA or a state agency. These reports are useful not only for evaluating legal compliance but also for learning more about the operations of the assets under consideration. A Toxics Release Inventory or Tier II report, for example, discloses what chemicals are used at particular facilities, in what quantities, and for what purposes. These reports are also useful in identifying additional issues. Documentation of a release reported to the National Response Center could, for example, spur questions of whether the regulator ever followed up with enforcement. As with the other environmental statutes, failure to report, label, or notify under these and similar laws can result in agency enforcement and, in some cases, citizen suits.

Evidence that a facility has consistently submitted reports required under these and similar laws can also have relevance outside the environmental due diligence context. Consistent recordkeeping, or the failure to do so when required, can be an indicator of the target company's recordkeeping practices, environmental practices, and sophistication. This in turn can inform us of the broader approach to the deal.

[iii] Claims-Based Requirements and Risks

Claims-based requirements and risks arise out of administrative, civil, and criminal environmental litigation. As discussed above, major federal and state environmental statutes empower federal and

state agencies to pursue administrative, civil, and criminal penalties for violations. Many also give private parties the right to bring civil suits to either recover damages or force action to comply with the law and remediate the effects of past violations. Environmental litigation can, however, encompass other types of lawsuits. A class action or mass tort claim related to chemical exposure, for example, is an indicator of environmental risk. Trespass, nuisance, negligence, and strict liability claims may also arise out of environmental issues, such as a discrete pollution event from an explosion or malfunction.

Environmental claims may also give rise to requirements that a facility must meet as part of its broader environmental compliance. A company may, for example, enter into judicial consent decrees or administrative orders under CERCLA that require the company to undertake remedial action at a contaminated site. A facility may also enter such settlements with federal and state agencies to resolve violations of air and water pollution control laws, which may require the facility to apply for a permit, install pollution abatement technology, or undertake supplemental environmental projects. These settlements often prescribe detailed schedules for undertaking certain actions, and failure to comply with a settlement can often lead to further legal consequences. It is therefore important to understand whether a target company has complied with any settlements it has entered into, and the steps required for the target to satisfy all its obligations.

[2] Personal Injury/Tort Liability Considerations

At first glance, pending, threatened, or ongoing litigation may appear to fall outside the environmental ambit. But often, litigation gives rise to environmental considerations that require the expertise of the environmental lawyer or consultant. A nuisance or trespass claim arising out of a pollution event, for example, may require review of a facility's environmental practices, permits, and regulatory compliance history. Mass tort claims arising out of exposure to a dangerous chemical similarly may require review of hazardous waste manifests, RCRA permits, or TSCA or FIFRA disclosures. A full understanding of the target company's environmental practices and compliance can provide insight into the risk of an adverse judgment or damages award, which in turn can inform risk allocation decisions or even whether the deal moves forward at all.

[3] CERCLA/Cleanup Liability Considerations

Central to almost any deal is the issue of CERCLA liability. Enacted in 1980 in response to several high-profile pollution events, CERCLA establishes a framework for cleaning up contaminated sites and shifting cleanup costs to responsible parties. CERCLA liability is (subject to certain defenses) generally strict, joint and several, and retroactive. A party can be liable even if they were not directly responsible for contamination and even if they were not negligent. A single party can be liable for the entire cost of cleaning up a contaminated site even if others are also responsible. And a party may be liable regardless of how long ago the contamination occurred.

CERCLA imposes liability on four categories of "potentially responsible parties" (PRPs):

1. The current owner or operator of a facility where a release of a hazardous substance into the environment has occurred;
2. The owners or operator of a facility at the time of disposal of a hazardous substance;
3. Anybody who arranged for the disposal or treatment of a hazardous substance; and
4. Anybody who transported a hazardous substance to a facility where a release occurred.

Any or all PRPs associated with a facility where a release of hazardous substances has occurred can be held liable under CERCLA for the cost of removing a hazardous substance, responding to a release, and remediating a site where a release has occurred. The federal government or a state can either require one or more PRPs to conduct removal, response, and remedial actions, or the government can conduct removal, response, and remedial actions on its own and then sue the PRPs to recover the costs. PRPs can in turn bring cost recovery claims against other PRPs in order to allocate costs among all parties. PRPs that settle claims with the government are generally protected from contribution claims by other PRPs.

CERCLA cleanups can be complicated, costly, and time-consuming. It may often take years just to allocate responsibility among the PRPs let alone conduct the response, removal, and remedial action. And cleanups can be incredibly expensive. For this reason, taking steps during the due diligence process to ensure that a buyer is not on the hook for a seller's potential CERCLA liability is critical.

CERCLA offers limited exceptions to liability that buyers can take advantage of. One category of protections are the landowner liability protections (LLPs), which include protections for contiguous landowners (*i.e.*, landowners contiguous to a property where a release of a hazardous substance has occurred) and bona fide prospective purchasers (BFPPs) of real property. The BFPP protections most often come up in real property transactions. Another type of protection is the secured creditor exemption, which exempts from liability a lender that does not actively participate in the management of a facility and takes steps to protect their investment. This exemption comes up in transactions involving lending or underwriting decisions.

The BFPP protection is the LLP most commonly sought during a transaction and requires that a buyer of real property take specific steps before acquiring the property to establish eligibility. Essentially, the buyer must establish that they conducted "all appropriate inquiry." (There are also post-acquisition requirements that a buyer must follow to establish eligibility, including cooperating with government agencies with respect to any release of a hazardous substance, taking steps to stop an ongoing release, and not taking action that could worsen or exacerbate the release.) CERCLA Section 101, *42 U.S.C. § 9601(40)(B)(ii)(II)*, specifies the following criteria for undertaking all appropriate inquiry at a property:

- "The results of an inquiry by an environmental professional."
- "Interviews with past and present owners, operators, and occupants of the facility for the purpose of gathering information regarding the potential for contamination at the facility."
- "Reviews of historical sources, such as chain of title documents, aerial photographs, building department records, and land use records, to determine previous uses and occupancies of the real property since the property was first developed."
- "Searches for recorded environmental cleanup liens against the facility that are filed under Federal, State, or local law."
- "Reviews of Federal, State, and local government records, waste disposal records, underground storage tank records, and hazardous waste handling, generation, treatment, disposal, and spill records, concerning contamination at or near the facility."
- "Visual inspections of the facility and of adjoining properties."
- "Specialized knowledge or experience on the part of the defendant."
- "The relationship of the purchase price to the value of the property, if the property was not contaminated."
- "Commonly known or reasonably ascertainable information about the property."
- "The degree of obviousness of the presence or likely presence of contamination at the property, and the ability to detect the contamination by appropriate investigation."

These criteria form the basis of ASTM E1527 Standard Practice for Environmental Site Assessments: Phase I Environmental Site Assessment Process, discussed in Section 4 below.

Because of the importance of establishing the BFPP protections by conducting all appropriate inquiry before acquiring property, this aspect of diligence is discussed separately in Section 4 below.

[4] Deal-Specific Issues

Every deal has the potential to give rise to its own unique set of environmental issues. As noted at the start of the chapter, understanding the specifics of the assets under consideration—the location and use of property and the processes and operations involved at a facility—can help the due diligence team identify unique or special issues that warrant consideration. Deal-specific issues may include but are not limited to environmental covenants and easements that limit the use of a property; requirements set forth in agency or judicial consent orders; agreements related to the sale of renewable energy credits; power purchase agreements; activities by

others, whether ongoing or historic, in the vicinity; past on- or offsite disposal practices; contractual indemnities imposing liability for the actions of others; prior stock acquisitions; divested properties; and renewable energy leases (such as commercial solar leases).

End of Document

§ 5.03 General Environmental Due Diligence Process

[1] Overview

This section provides an overview of the general environmental due diligence process.

The environmental due diligence process is iterative. It often starts with broad requests for information, and as more information about the target's operations and compliance come in, it becomes narrower and more focused. The environmental due diligence process may be based on review of records, site assessments, or both. Because of the volume of records that often accompany environmental due diligence review, thorough and careful tracking of all documents obtained and outstanding is critical.

[2] Information Needs

The starting point for environmental due diligence is a basic understanding of the target and its operations. Depending on the nature of the deal, the initial tranche of documents may include a prospectus or presentation identifying the target's operations and assets. Knowing the number of properties or facilities involved in a deal; the operations conducted at all deal-associated facilities; and the nature of the operations themselves helps the environmental due diligence team craft requests, issue spot as documents come in, and evaluate risks.

In the absence of information or preexisting knowledge about a target's operations, the environmental due diligence team may need to conduct independent research to understand the basics of the target's operations. Research may include, but is not limited to, a review of the chemicals and substances associated with the target's operations; the types of machinery and equipment that may be used; and the wastes produced by the target's operations. Background research into the target itself may yield information about ongoing or recent environmental issues that in turn can provide a sense of the risks and issues the environmental due diligence team should be aware of. This type of research has the added value of verifying that the target is providing all necessary information and crafting follow-up requests to obtain information that the target has either not provided or held back.

One valuable source of information that can provide a starting point for review is EPA's ECHO database. The ECHO database provides environmental permitting, compliance, and reporting information for individual permitted facilities. The ECHO database identifies facility identification numbers; permits currently or previously held by a facility; and instances of noncompliance with permits. Because the ECHO database is a record of permits issued under federal law, it will not capture the full universe of potential permitting and approvals potentially held or needed by a facility.

ECHO database may be supplemented by state database reviews. While states may also have their own databases of environmental records, the availability and thoroughness of information may vary from state to state. California, for example, provides large quantities of information about facilities; the Envirostor database hosted by the state's Department of Toxic Substances Control provides detailed information about facilities' hazardous waste permits and compliance.

Another source of information that can guide the due diligence team is information about a facility's solid or hazardous waste releases and liability and associated cleanup obligations or enrollment in state cleanup programs. The National Priorities List (NPL) established pursuant to CERCLA and available on EPA's website comprises all sites listed or proposed for listing under CERCLA because of releases of hazardous substances. Sites listed on the NPL typically have their own individual webpages with information on the PRPs associated with the site, the nature of the contamination at the site, and the remediation and response status. EPA's

brownfields database also provides information on contaminated sites and can be used to determine whether any currently or formerly owned or leased properties are contaminated.

States typically have their own state hazardous waste and brownfield databases that can be used to assess the cleanup status of properties enrolled in state cleanup programs or subject to state hazardous or solid waste liability. This includes sites enrolled in voluntary cleanup programs. Information in these databases can be used similarly to the NPL and federal brownfields database to evaluate the nature of contamination and status of cleanup at target-owned or -leased facilities. As with permitting and compliance information, the amount and quality of information available may vary by state.

The information obtained through independent research and environmental database review is ultimately meant to be the starting point for the due diligence team. The goal of this type of review is to begin collecting information to watch for as documents come in. This information must be checked against the records or responses produced by the target.

The types of documents associated with the various components of environmental due diligence are discussed throughout Sections 2 and 4 and summarized below.

- Permits and licenses and documents required thereunder
    - State and federal air quality permits and air emissions data
    - State and federal water discharge permits, DMRs, SWPPPs, SPCCs, and FRPs
    - State and federal solid and hazardous waste permits and manifests
    - Wetlands permits for dredging or filling activities
    - Permits authorizing the take of endangered or threatened species and associated species monitoring reports
- Prior site assessments and compliance reviews at the target's facilities
    - Phase I Environmental Site Assessment reports
    - Phase II testing and other sampling data
    - Limited Environmental Compliance Reviews
    - Internal or external environmental audits
- Agency inspection documents and documentation of corrective action taken to address any issues identified in the documents
- Agency compliance documents, such as notices of violation, orders on consent, agreed orders, or consent decrees
- Judicial orders or consent decrees
- Litigation documents, such as notices of intent to sue by citizen groups, complaints filed by regulators, or indictments associated with criminal charges
- Conservation easements, environmental covenants, activity and use limitations, environmental deed restrictions, and environmental indemnities
- Documents associated with the purchase and sale of renewable energy credits; the generation or purchase of renewable energy; power purchase agreements; solar leases; and similar types of documents
- Documents associated with agency review of permits and approvals from federal and state agencies, such as:
    - NEPA and state-equivalent documents (environmental impact statements, environmental assessments, environmental impact reports, etc.)

- Endangered Species Act documents (biological opinions, biological assessments, species surveys, and agency correspondences)
- National Historic Preservation Act and Section 4(f) documentation, such as historic and cultural resource assessments and consultation documents with agencies

- Records associated with releases of hazardous substances, such as reports made to the National Response Center and reports submitted to agencies in connection with spill events
- Documentation related to facilities' CERCLA liabilities
- Underground storage tank and aboveground storage tank documents, including internal and external inspection reports
- Environmental insurance policies and claims

While not comprehensive, the list above can be used as a starting point for determining the potential universe of documents associated with a particular transaction. Often, review of these documents will allow the due diligence team to identify additional documents or ask for additional responses to queries necessary to assess compliance and risk.

[3] Data Review and Analysis

Once obtained, documents should be categorized both by type and, if multiple facilities are part of the deal, by property. To the extent possible, documents should also be reviewed or categorized in chronological order, as tracking environmental issues and compliance requires understanding of the "story" at a particular facility.

If the target provides Phase I reports or similar documents, these should be reviewed first. As discussed in *§ 5.04* below, Phase I Environmental Site Assessment reports provide comprehensive overviews of facilities' history and permitting. By starting with these types of documents, the due diligence team can determine historic uses of the property that pre-date the target and the target's prior and current uses of the property. This information, in conjunction with review of the background research sources discussed above, allows the due diligence team to review the remaining documents critically.

After review of any available Environmental Site Assessment reports or similar documents, the due diligence team should turn to the facility's permits and approvals. Environmental licenses typically include an issuance and expiration date. Permits will also identify the equipment and operations covered, which may provide more detail on individual facilities' operations. While the due diligence team should be familiar with a permit's substantive requirements, the most important information at the outset usually concerns any documents or records the permit requires a facility to prepare or submit to regulators. This allows the due diligence team to review the remaining documents for compliance with recordkeeping and reporting obligations. Note, however, that some recordkeeping and reporting requirements are imposed by statute or regulation, so permits should not be used to definitively determine compliance with such requirements.

Review of records and reports mandated by permit or law should be the next step in the review and analysis process. These documents need not be reviewed in detail, at least initially. They may, however, contain additional information about facility operations and equipment. Documents such as SPCC plans and FRPs may include helpful information about the number of tanks and chemicals stored onsite and can be used to determine if all materials related to chemical and waste storage have been provided.

Once permitting and compliance document review is complete, the due diligence team should consider reviewing any agency and court documents associated with the facility. These documents may provide additional detail on facility operations and history not captured in a site assessment (or that can be used to learn about facility operations in the absence of such assessments). They will also provide information on penalty amounts and additional compliance obligations, which in turn can guide review and if necessary supplemental requests related to the payment of such penalties and implementation of mandated corrective action.

Emails, communications, memoranda, and documents prepared in connection with agency review may overlap with review of permits and licenses to the extent the permits and licenses held by the target were issued after such review occurred. These documents may also provide information on pending permits and approvals,

allowing the due diligence team to evaluate the outstanding steps necessary to obtain approval or the likelihood of a permit challenge. These documents may also provide additional color to information contained in permitting and compliance documents.

As this discussion demonstrates, the permitting and compliance review will often be both the starting point and central to the due diligence review. The presence or absence of permits; permit validity; and compliance with reporting and recordkeeping obligations are often the easiest issues to identify and resolve during the due diligence review. Compliance with and resolution of agency or judicial orders are also relatively easy to identify and resolve. Complications can arise, however, if the target has not provided adequate information about its operations and facilities to allow the due diligence team to confirm the universe of documents the target should have.

Components of due diligence review that require more thorough and critical analysis include review of documents prepared in connection with agency review and consultation of a facilities' operations, such as Environmental Impact Statements prepared pursuant to NEPA. Evaluating the risk associated with such review requires familiarity with the review process itself and knowledge of the status of the review under consideration.

As noted above, the environmental due diligence process is iterative. Each tranche of environmental documents should be reviewed in full and with reference to each other to generate supplemental or additional requests for information from the target. Multiple rounds of requests will likely be required.

[4] Environmental Insurance Considerations

Environmental insurance considerations involve both review of the target's environmental insurance policies (and other insurance, as certain non-environmental policies may cover environmental liabilities) as well as consideration of whether the client should obtain environmental insurance. Modern commercial liability insurance ordinarily excludes pollution from coverage, but how pollution is defined is relevant to determining the scope of the exclusion. Older general liability insurance policies may not have this exclusion. Environmental coverage may be available under a separate policy.

Insurance may also cover risks associated with cleanup at a facility. If ongoing remediation or response actions are occurring at the target's facilities and the buyer is willing to take over responsibility for such actions, this type of insurance can offer protection to the buyer.

[5] Environmental Consultants and Other Non-Legal Support

Because of the complex and technical nature of environmental diligence, the due diligence team may require non-legal assistance. As discussed in the next section, environmental consultants may be retained to conduct Phase I Environmental Site Assessment reports and Phase II testing in the context of real property transactions, as well as Limited Environmental Compliance Reviews. Consultants may also be retained to review the documents obtained during the due diligence process to offer opinions on the target's compliance. This type of assistance may be warranted in particularly complex transactions or in situations where compliance with a permit's technical requirements are relevant to the deal.

Other non-legal support that may accompany environmental due diligence may include the environmental, health, and safety teams of both the buyer and seller. Individuals associated with these teams will often be best positioned to provide additional context and, in the case of a buyer, clarify what the legal team should be looking out for in order to satisfy particular concerns.

§ 5.04 Environmental Due Diligence Related to Real Property

[1] Phase I Environmental Site Assessment

As discussed in Section 2 above with respect to CERCLA, due diligence associated with real property raises special concerns related to liability for historic hazardous substance releases. Environmental due diligence of real property is ordinarily focused on identifying and minimizing CERCLA liability risks. Because bona fide prospective purchasers may take advantage of CERCLA liability protections, provided they meet all pre- and post-acquisition requirements, real property due diligence is often structured around satisfying CERCLA's BFPP protection criteria.

A bona fide prospective purchaser satisfies its pre-acquisition obligations for landowner liability protections by conducting all appropriate inquiry into the property it intends to acquire. The criteria for establishing all appropriate inquiry are listed in Section 2 above.

EPA's "all appropriate inquiry" rule (40 C.F.R. Part 312) clarifies how a bona fide prospective purchaser may satisfy the standard. Under the rule, a purchaser may follow the regulatory criteria themselves, but in almost all cases, the purchaser will satisfy the criteria by conducting a Phase I Environmental Site Assessment that complies with the ASTM E1527 standard. This standard and compliance therewith are incorporated into EPA's all appropriate inquiry rule.

An ASTM E1527 Phase I Environmental Site Assessment looks at the historic and current uses of property to determine if a release or potential release of hazardous substances or petroleum products has occurred, is occurring, or threatens to occur. (Note that, while CERCLA excludes some petroleum products from the definition of hazardous substances, such substances are within the scope of an ASTM E1527 Phase I Environmental Site Assessment.) A Phase I Environmental Site Assessment is conducted by a certified environmental professional and includes consideration of the following information to determine if a release or potential release exists:

1. Physical setting and resources of the property
2. Review of government records
3. Review of historic records
4. Site reconnaissance
5. Information provided by the purchaser
6. Interviews with the property's current or former owners or occupants
7. Interviews with government officials
8. Evaluation and report

The findings generated by this information are compiled in a so-called "Phase I report." A Phase I report that complies with the ASTM standard will include all criteria listed above and comply with the specific elements of each criteria outlined in the ASTM standard itself. The report will identify the presence or potential presence of hazardous substances by indicating whether or not a so-called "recognized environmental condition" is present. A recognized environmental condition (REC) is any condition that indicates a past, present, or threatened release of hazardous substances. One type of REC is a so-called controlled recognized environmental condition (CREC), which is a condition that indicates a past, present, or threatened release of hazardous substances but with contamination allowed to remain in place subject to engineering or institutional controls.

Such controls may, for example, include physical barriers or caps to prevent exposure to contaminated material or deed restrictions that prevent certain uses of a property.

A Phase I report may also identify historic recognized environmental conditions (HRECs). HRECs are releases or threatened releases that have been resolved to the satisfaction of a government authority with no controls necessary; in other words, the use of the property is not restricted in any way due to the release or threatened release. An HREC is not a REC but is nonetheless relevant to understanding historic uses and issues at a site.

A Phase I report may also identify so-called de minimis conditions, which are conditions that represent a release but would not likely require attention or response from a regulator. Such conditions may, for example, include minor oil staining associated with trucks or vehicles.

A Phase I report may also identify business environmental risks. These are risks associated with environmental considerations at a property that do not necessarily indicate that a release or threatened release has occurred. The presence of underground storage tanks that are otherwise in good condition may represent a business environmental risk.

Phase I reports may also include other considerations that are not ordinarily within the scope of the ASTM standard but are requested by the report's user. Such considerations may include inspection for asbestos-containing material or lead-based paint; mold or microbial growth evaluation; radon risks; and wetlands inventories. Often, these non-scope considerations may be identified as business environmental risks.

As stated above, a Phase I report must be conducted by a certified environmental professional. The first step in all appropriate inquiry therefore requires identification of an environmental professional and putting together a scope of work. Once retained, the environmental professional will typically order an environmental database search; issue records requests from federal, state, and local agencies; and conduct title and public record searches. The environmental professional will also conduct site reconnaissance by visiting the property and looking for conditions that may indicate a REC. (The ASTM standard identifies specific conditions an environmental professional should look for and requires that the environmental professional document whether or not each condition was observed.) Site reconnaissance also includes observations of adjoining properties to determine if releases or threatened releases may exist at those sites that could impact the target property. Site reconnaissance may also include interviews with the current owners and occupants.

Because a Phase I Environmental Site Assessment requires access to the property, a buyer should ensure that it has full access to the target's property during the diligence period. This may require prior negotiation with the seller, who may impose conditions on when or under what circumstances the environmental professional may enter the site. Ideally, the environmental professional will have full access to the entire site; any access limitations that cannot be accommodated must be noted in the Phase I report.

[2] Phase II Testing Considerations and Related Access and Reporting Issues

Ideally, a Phase I Environmental Site Assessment will come back "clean" or show that any releases or threatened releases have been resolved. If, however, the assessment identifies the presence or likely presence of a release, the buyer must consider whether to conduct further evaluation to determine the nature and scope of any potential releases. This further testing is often referred to as "Phase II testing."

During Phase II testing, an environmental professional will conduct sampling of soil, groundwater, or air (depending on the nature of the contamination or potential contamination identified in the Phase I report). Based on the testing results, the environmental professional may make further recommendations to address the contamination.

Phase II testing raises several issues. First, there is the issue of property access. Phase II testing may require the installation of temporary monitoring wells or the disturbance of soil or groundwater in order to conduct sampling. Sellers may not be willing to provide access for such testing. Second is the issue of timing. The time period for conducting diligence may not accommodate the time necessary to conduct Phase II testing. A pre-negotiated diligence period should account for the possibility of Phase II testing. Third, there is the issue of what to do with sampling results. Detection of contamination above regulatory thresholds may require reporting to federal or state authorities. Because of the risk of reporting, sellers may be unwilling to allow Phase II testing because it may require them to report contamination and open them up to agency enforcement action or

cleanup liability. From the buyer's perspective, however, Phase II testing can be important not only for delineating environmental impacts but also for determining if a deal should go forward at all.

[3] Addressing Subsurface Contamination and Vapor Intrusion Concerns

Phase II testing may require remedial action to address ongoing contamination. Responsibility for undertaking such action will raise issues of allocation of responsibility and risk during contract negotiations. Issues that may arise include:

- Whether remedial action is even required.
- The nature of the remedial action.
- Who should conduct remedial action – In some cases, buyers may want sellers to take responsibility for conducting the remedial action; but in other cases, buyers may want to take on the responsibility themselves to have control over the remedy and may seek indemnification of the remedial costs from the seller.
- Whether any necessary remedial action before closing, or if after closing, the conditions under which a seller responsible for conducting the remediation can access the property.
- Who should cover the costs of remedial action.
- Whether a seller should indemnify a buyer for any liability arising out of the contamination and remedial action.

[4] Leases and Other Relevant Contract Documents

Leases and other contracts may dictate responsibility for environmental contamination and remediation or for other environmental liabilities, risks, or responsibilities. Review of existing leases and other contracts—including activity and use limitations, indemnities or agreements to defend, releases, assumptions, covenants, easements, and other private agreements—is just as important as review of government documents. The target entity, for example, may have agreed with a prior owner to indemnify that prior owner for future costs or claims associated with contamination. Whether or not the indemnity remains valid could be a critically important issue. The seller as a current owner may also have agreed to conduct remedial action related to a prior owner's contamination. This requires the due diligence team to determine if the seller has performed on its obligations and, if applicable, whether future work may also be required and the likely value thereof. Standard commercial contracts may also include indemnities related to environmental concerns; the due diligence team should be aware of these indemnity provisions and their potential impact on buyer.

Limitations on property use are also relevant for evaluating both risk to the buyer and whether and how acquisition of a property advances the buyer's goals. A buyer that wants to redevelop property for residential housing, for example, must be aware of any environmental covenants or easements restricting land uses to industrial and commercial or requiring the preservation of certain areas for habitat, conservation use, or public access.

1 Due Diligence in Corporate Transactions Appendix A:.syn

Due Diligence in Corporate Transactions > Chapter 5 Environmental Due Diligence > Appendix A: Sample Environmental Due Diligence Checklists

Appendix A: Sample Environmental Due Diligence Checklists

Synopsis

Appendix A:Sample Environmental Due Diligence Checklists

End of Document

No Title in Original

This section provides an example of due diligence checklists that teams can use to track diligence requests. The sample checklists provided below are not exhaustive and do not cover every possible situation or transaction. They can, however, serve as a starting point for building a checklist that meets the needs of the individual transaction.

Sample Environmental Compliance and Permitting Due Diligence Checklist

Site	Air Permits	Water Permits	SWPPPs	SPCCs	FRPs	Waste	EPCRA	USTs or ASTs	Boilers
[SITE 1]									
[SITE 2]									
[SITE 3]									

Sample Phase I Environmental Site Assessment Report Checklist

Site	Current Uses	Site history	RECs, CRECs, HRECs	BERs	Tanks	Wells	Septic systems	Located within wetlands?	Phase II recommended?	Other recommendations
[SITE 1]										
[SITE 2]										
[SITE 3]										

1 Due Diligence in Corporate Transactions Appendix B:.syn

Due Diligence in Corporate Transactions > Chapter 5 Environmental Due Diligence > Appendix B: Sample Environmental Due Diligence Requests

Appendix B: Sample Environmental Due Diligence Requests

Synopsis

Appendix B:Sample Environmental Due Diligence Requests

Scope

End of Document

No Title in Original

This section provides an example of due diligence requests. The sample requests provided below are not exhaustive nor intended to cover every possible situation or transaction. They can, however, serve as a starting point for requesting information.

Environmental Diligence Requests	**Current as of**	**Information Provided**	**Comments / Follow-up Requests**
A list of all properties currently owned, leased, or operated by the Company or for which the Company has retained or assumed liabilities, categorized by type of operations conducted at such properties.			
A list of all properties formerly owned, leased, or operated by the Company or for which the Company has retained or assumed liabilities, categorized by type of operations conducted at such properties.			
Copies of all documents and contracts describing the extent to which the Company may have assumed, acknowledged, confirmed, retained or acquired environmental liabilities, including for remediation.			
Descriptions of all threatened or pending federal, state, provincial or local administrative or judicial proceedings, complaints, citations, arbitrations, mediations, information requests or subpoenas, notice of potential liability or notices of violation under environmental laws or regulations, the Occupational Safety and Health Act, and contract, tort, or common law.			
Environmental agency or other environmental inspection reports for the last [five] years.			
All environmental reports and the results of investigations conducted on your Company's behalf by any environmental consultants, including, but not limited to, any Phase I environmental site assessment reports, health and safety compliance audits, environmental compliance audits, internal environmental, health and safety audits, and Phase II (or Phase III or more) reports.			
Any correspondence to or from federal, state, provincial, or local environmental agencies or authorities related to alleged non-compliance with, violations, or potential or actual liability under environmental laws, the Occupational Safety and Health Act, or contract, common law or tort law.			

Scope

A description of any threatened or actual environmental claims made by or against the Company or otherwise concerning the Company or any real property on which it currently operates or formerly operated.			
A list and description of any insurance policies covering the Company or its assets or facilities which may cover environmental claims or losses, whether first party or third party.			
A description of (i) whether any of the Company's assets or facilities have ever been used for the storage, generation, production, treatment or disposal of any hazardous substances, solid wastes, toxic wastes, hazardous wastes, petroleum products, asbestos, lead, PCBs, PFAS, or other materials regulated under applicable environmental or health laws and (ii) any practice by the Company of storing, generating, producing, treating or disposing of any hazardous substances, solid wastes, toxic wastes, hazardous wastes, petroleum products, asbestos, lead, PCBs, PFAS, or other materials regulated under applicable environmental or health law off-site of the Company's assets or facilities.			
A brief description of all penalties, fines or remedial action incurred or sought at each property under any environmental, health or safety laws.			
A description of all current and former operations conducted by the Company at its facilities and whether any hazardous substances, solid wastes, toxic wastes, hazardous wastes, petroleum products, asbestos, lead, PCBs, PFAS, or other materials regulated under applicable environmental or health law have been or are being used, generated, disposed of, or stored in any manner, at any volume, and at any time.			
All current (and for the prior [five] year period) permits, licenses, authorizations, or approvals held by or pertaining to the Company or its operations.			
A list of environmental permits that are required but either have not been obtained or have expired.			
Letters from attorneys for the Company to the Company's independent public accountants concerning litigation and other legal proceedings relating to environmental laws (i.e., "audit letters").			
Any notice letters, requests for information and other communications received by the Company from a governmental authority alleging the Company is a potentially responsible party, including communications related to state or federal Superfund sites at which the Company or any of its subsidiaries is alleged to have contributed to a release of hazardous substances under CERCLA or any			

Scope

other environmental law.			
Has the Company ever conducted any assembly or manufacturing operations at customer locations or any other off-site properties? If so, in what time period(s) were such operations conducted?			
Confirm that Company has no pending NOVs and no outstanding fines or penalties related to environmental issues resulting from Company operations or properties.			
Copies of all civil and/or administrative consent decrees, administrative orders, orders on consent or any similar document entered into by the Company relating in any way to environmental issues associated with Company operations.			
Copies of all testing, sampling and/or monitoring results relating to any environmental issue and/or condition of Company operation or at Company properties, including but not limited to those required under environmental permits, laws or regulations.			
A description of the source of water for each of the company properties identifying which properties are serviced by well water and which are serviced by public water supply systems including the results of any test results of such water source.			
Copies of all Underground Storage Tank or Above Ground Storage Tank registrations and/or documentation regarding any USTs or ASTs in operation at Company properties and/or operations including, but not limited to any documentation regarding the removal of USTs or ASTs and/or investigations conducting involving any UST or AST leak incident and/or removal.			
A list of any current or former above ground and underground storage tanks, including what materials were stored in the tanks, and the current disposition of such tanks (e.g., in use, closed, abandoned, unknown, etc.).			

End of Document

Chapter 6 Real Estate Due Diligence

Synopsis to Chapter 6 : Real Estate Due Diligence

Synopsis to Chapter 6 : Real Estate Due Diligence

Scope

Appendix B: Sample Real Property Due Diligence Request

Scope

End of Document

§ 6.01 Overview

[1] Real Property vs. Personal Property

Prior to beginning the due diligence review of a target company's property, a threshold matter, is to determine what type of property the target company owns. Property is commonly divided into two broad categories: real property and personal property. Understanding the legal and practical distinction between the two types of property is critical to conducting effective and efficient due diligence. Accurately identifying, classifying, and evaluating a target company's property is essential for assessing value, liabilities, and risks associated with acquiring the target company.

Real property in its simplest terms, is immovable property that typically includes the land itself and all things permanently attached to it, including buildings, other improvements, and natural resources. **Personal property**, by contrast, includes all movable property. It is divided into *tangible* personal property—such as machinery, inventory, vehicles, and equipment—and *intangible* personal property, such as intellectual property rights, licenses, contracts, accounts receivable, and securities.

Understanding the difference between real and personal property in a corporate setting allows legal and financial professionals to better evaluate risk, allocate liabilities, and ensure that all relevant property interests are properly accounted for and transferred. It also enables more accurate drafting of transactional documents and mitigates the risk of post-closing disputes. As such, this distinction forms a foundational element of effective due diligence in corporate transactions.

[2] Tailored Scope of Review

[a] Introduction

In the context of a corporate transaction the scope of real property due diligence must be tailored to the character of the assets involved, the structure of the deal, and the buyer's intended use of the property post-closing. A one-size-fits-all approach is rarely appropriate. The nature of the property—whether it is real property or personal property, held in fee simple, co-tenancy, or leasehold—requires a nuanced review to identify risks, uncover latent liabilities, and ensure the property supports the client's objectives.

[b] Real Property and Personal Property

[i] Introduction

Although there are differences between real property and personal property, some of the due diligence review does apply to both types of property. Below we consider several common areas of due diligence that apply to both real property and personal property.

[ii] Character of the Property

A critical component of due diligence is verifying the seller's authority and legal right to transfer the property. This includes identifying the type of interest held:

- **Fee simple ownership** (or its equivalent for personal property) represents the broadest ownership interest, free of reversionary interests.

- **Co-tenancy interests** may limit unilateral rights to transfer and require scrutiny of co-owner agreements and shared-use rights.
- **Leasehold interests** necessitate detailed lease review to evaluate certain terms of the lease including, but not limited to each party's obligations, use limitations, the lease term, rents, termination requirements, and any consents required with respect to the transfer of a direct or indirect interest in the subject property.

[iii] Obligations Associated with Seller's Rights

A seller's right to convey property is not only limited by the type of interest it has in the property, but may also be accompanied by other specific obligations or limitations, including, but not limited to:

- **Compliance with laws**: Verification that the property is operated in accordance with applicable zoning laws, land-use restrictions, environmental regulations, and building codes is essential. Non-compliance may lead to significant post-closing liabilities.
- **Taxes**: Outstanding or misclassified property taxes can burden the buyer. Tax histories should be reviewed to confirm that payments are current and that there are no pending assessments or disputes.

[iv] Third-Party Consents

Many interests, particularly leaseholds or co-owned property, may require third-party consents prior to transfer. Due diligence must include identification of such requirements and a realistic assessment of whether consents can be obtained timely.

[v] Buyer's Intended Use of the Property

The property's suitability for the buyer's post-transaction plans is a material concern. For real property, this may require review of zoning and environmental restrictions. For personal property, considerations may include compatibility with the buyer's operations or technology stack, intellectual property rights, or maintenance requirements.

[vi] Ownership History

Understanding the chain of title or ownership history provides context and identifies potential defects, encumbrances, or claims. A clean history enhances marketability and transferability, whereas gaps or irregularities may require curative action.

[vii] Title Documents

Review of title documents is central to confirming ownership and identifying encumbrances such as easements, covenants, and restrictions. For real property, this typically includes a title commitment and survey; for personal property, documents evidencing ownership and registration (e.g., UCC filings, certificates of title) are reviewed.

[viii] Insurance

Evaluation of current insurance policies and claims history may uncover past issues (e.g., flood, fire, environmental damage) and reveal gaps in coverage. The buyer should assess whether the existing policies can be assigned or if new coverage is needed post-closing.

[ix] Valuation and Appraisals

A reliable appraisal ensures the buyer is paying fair market value and informs financing, tax planning, and purchase price allocation. For real property, this typically includes income-based, market, and cost approaches. For personal property, valuation depends on use, condition, and depreciation.

[x] Maintenance and Operating Costs

Operating cost data, including utilities, repairs, and routine maintenance, help the buyer assess ongoing expenses. For income-producing real estate (i.e., those which have tenants), this may also include rent rolls and common area maintenance (CAM) charges.

[xi] Liens

A search for liens—including tax liens, mechanic's and materialmen's' liens, and UCC filings—is vital to ensure that the property is not encumbered in a way that would impair transfer or use. Liens may need to be satisfied or released as a condition of closing.

[xii] Property Inspection Reports

Physical inspections can reveal issues that are not visible from document review alone. For real property, this may include structural problems, code violations, or deferred maintenance. For personal property, condition assessments and functional testing may be appropriate.

[c] Real Property: Specific Types of Due Diligence

[i] Introduction

When real property is involved in a corporate transaction, the nature of the seller's interest—fee simple, co-tenancy, or leasehold—dictates the specific focus of the due diligence effort.

[ii] Fee Simple and Co-Tenancy Interests

Where the seller owns real property outright (in fee simple) or holds a co-tenancy interest, the following categories of due diligence apply:

- **Title Commitment and Survey**: A title commitment and ALTA/NSPS land survey confirm legal ownership, boundary lines, access rights, and reveal encumbrances such as easements or covenants.
- **Zoning and Land Use Compliance**: Ensuring that the property is zoned appropriately for the buyer's intended use can prevent costly post-closing disputes.
- **Permits and Approvals**: Verification of operating permits, occupancy certificates, and environmental approvals is critical to uninterrupted use.
- **Leases and Occupancy Agreements**: If tenants are in place, lease agreements must be reviewed to understand rights, obligations, term structures, and rent rolls.
- **Environmental Reports**: Phase I and (if necessary) Phase II environmental site assessments identify potential contamination risks that may impact value or require remediation.

[iii] Leasehold Interests

Where the seller holds only a **leasehold interest**, diligence focuses on the lease and its enforceability:

- **Review of Lease Agreement**: Key provisions include term, renewal options, rent figures, assignability and subletting rights, maintenance obligations, termination provisions, and rights of first offer or refusal.

- **Consents**: Transfer of leasehold interests may require landlord and lender approval, which can delay closing or introduce negotiation risk.
- **Condition of Premises**: The buyer should confirm whether leasehold improvements are included and assess their condition and value.

This tailored approach to property due diligence aligns with the broader goals of a corporate transaction: risk identification, legal compliance, and value preservation. By customizing the scope of review based on the nature of the property interest and the buyer's strategic objectives, parties can minimize surprises, confirm a target company will positively impact their business, and enhance the certainty of closing.

§ 6.02 Real Property Due Diligence

[1] Survey Due Diligence

[a] Purpose of a Survey

A survey serves to confirm physical boundaries and the legal description of the property; identify encroachments, easements, and improvements; and ensure the property has legal access and adequate space for its intended use. It also allows the reviewer to verify setbacks and compliance with zoning regulations; identify any restrictions that may impact construction or the intended operation of the property; and confirm conformance with the legal description of the property provided in the title documents.

[b] Types of Surveys

[i] ALTA/NSPS Land Title Survey (most common in commercial deals)

An ALTA survey is a specialized, highly detailed land survey used in commercial real estate transactions to provide comprehensive information about a property's boundaries, improvements, and easements. It adheres to standards set by the American Land Title Association (ALTA) and the National Society of Professional Surveyors (NSPS). This type of survey is the industry standard for commercial transactions.

[ii] Boundary Survey

A Boundary Survey is a type of survey used to determine the actual property lines against the metes and bounds described in the deed. The Boundary Survey is typically used for residential transactions or transactions in which the purchaser does not intend to make any significant changes to the layout of the existing structures after closing and should not be used if the purchaser intends to do any development or any major renovations to the existing structures.

[iii] Topographic Survey

A Topographic Survey is a two-dimensional type of survey representing the actual layout of the land, used to determine the elevation points and contour lines of the property.

[c] Contents of an ALTA Survey

An ALTA survey includes the property boundaries (based on the legal description); improvements (such as buildings, fences, driveways, etc.); easements and encroachments; rights-of-way and public access; utilities (either visible or marked underground); zoning setbacks and building height info (if requested); flood zone designation; and a legal description of the property cross-checked against title documents. The client and surveyor can agree to include additional optional elements, such as topographic info, parking spaces, zoning classification, utility contracts, and more, as "Table A Items."

[d] Key Elements of Review

When reviewing a survey, the key elements to review will include the legal description of the property; the lot dimensions and boundary lines; the existing structures and improvements; the rights-of-way, easements, and encroachments; access points and curb cuts; utilities and setbacks; and flood zone and wetlands designations (if applicable). The reviewer will want to ensure that this information matches across relevant documents and does not negatively impact the intended use or operation of the property.

[e] Coordination with Title Insurance

The survey is reviewed alongside the Title Commitment, and the survey exceptions in the title commitment or pro forma title policy can be removed or limited with a clean survey.

[2] Title Insurance

[a] What is Title Insurance?

Title insurance protects against losses resulting from issues with a property's title that were unknown at the time of closing but existed before the transaction. Unlike other types of insurance that protect against future events, title insurance covers past events that may affect ownership rights.

[b] Purpose of Title Insurance

Title Insurance protects against loss due to title defects or claims and helps ensure clear ownership and transferability of title.

[c] Types of Title Insurance

[i] Owner's Title Insurance

Owner's Title Insurance protects the purchaser (owner) of the property. It covers legal fees and financial losses due to title defects such as forged documents, unknown heirs, errors in public records, and undisclosed easements or liens.

[ii] Lender's (Loan) Title Insurance

Lender's Title Insurance protects the lender's interest in the property until the loan is paid off. This is required by most commercial lenders and is usually paid for by the borrower.

[d] Title Insurance Process

[i] Initiation of the Title Order

The buyer, buyer's attorney, or lender will open a title order with a title company or national underwriter. They will need information including the Purchase and Sale Agreement, property details (including the address, legal description, and parcel number), and legal entity documentation, including type of entity (i.e., LLC, Corporation, Limited Partnership, etc.) and relevant organizational documents.

[ii] Title Search and Commitment

The title company will conduct a comprehensive title search in public records. The purpose of this search is to identify the ownership chain (chain of title) along with any breaks in the chain of ownership; any mortgages, liens, judgments, or unpaid taxes; and any easements, encroachments, or restrictions on the property.

The title company will then issue a title commitment comprised of three key parts: Schedule A, Schedule B-I, and Schedule B-II. Schedule A will identify the proposed insured and the insurance amount, and will include basic facts about the transaction, such as the buyer, seller, and legal

description of the property. Schedule B-I will provide the requirements for the title company to issue a final policy, including payoffs, mortgage releases, corporate authority documents, and the recording deed. Schedule B-II will provide exceptions to the coverage, such as existing recorded easements, encumbrances, and restrictions that will not be covered by the final policy to be provided.

[iii] Risk Assessment and Issue Resolution

The buyer and counsel will review the title commitment and try to clear title issues and negotiate acceptable exceptions. They will work to satisfy all requirements listed in the title commitment, remove or address any problematic exceptions, and coordinate with surveyors, zoning experts, and environmental consultants as needed. The process may involve obtaining affirmative coverage for certain exceptions, negotiating or obtaining certain title endorsements, and working with sellers, title agents, and/or municipalities.

Any title issues must be resolved before closing (e.g., removing liens and/or curing defects). In the event any title issues cannot be resolved prior to closing, they become exceptions to the title policy.

[iv] Policy Issuance at Closing

The premium for the title policy is paid at closing and is a one-time, rather than ongoing, cost. After closing, the title company will record all necessary documents. Once the insurable instrument (i.e., the deed or mortgage) is recorded, the title company then issues the final title policy.

[v] Post-Closing Protection

If a covered title issue later arises (for example, a third party claims an ownership interest in the subject property), the policyholder is protected for legal defense costs, loss of property value, and the cost of settlement or damages.

[e] Key Title Documents

Key Title Documents include the Preliminary Title Commitment (including Schedules A, B-I, and B-II); Title Report; Pro Forma Title Policy; Final Title Policy issued to the buyer or lender; and any Deeds, Easements, and/or Restrictions of the property.

[f] Title Endorsements

Title endorsements provide add-on coverage to tailor the policy to specific risks. These are common in commercial deals to address issues such as zoning compliance, access rights, contiguity for adjacent parcels, and subdivision compliance. These endorsements may vary by jurisdiction and can be negotiated terms.

[g] Common Title Issues

Some of the most common title issues involve the existence of unreleased liens or mortgages, easements that affect development, gaps in the chain of title, and unrecorded interests or claims on the property.

[h] Curing Title Issues

Curing title issues often requires obtaining releases or subordination agreements, procuring and implementing affidavits or indemnity agreements, or directly amending the title commitment.

[i] Interrelationship of Survey and Title Review

Reviewing the survey helps to verify or challenge title exceptions, and a clean survey can allow for the deletion of the general survey exception. It can also ensure the policy covers all necessary items, as an initial title commitment may exclude matters that are visible in the survey.

[j] Best Practices

As title and survey review is often a longer lead-time item on deals, it is best practice to order the title commitment and survey early in the due diligence period of any transaction. The ordering party should provide the surveyor with the title commitment for proper coordination; work with legal counsel to review and resolve title issues; negotiate title coverage and endorsements with the insurer; and update or recertify the survey as needed before closing.

[3] Site Visits

[a] Introduction

Site visits and Property Condition Reports (PCRs) are essential components of real estate due diligence. They provide direct, on-the-ground insights into a property's physical condition, operational context, and compliance with applicable laws, verifying and supplementing findings from title, legal, and documentary reviews.

[i] Purpose of Site Visits and PCRs

These tools help validate the seller's representations, uncover latent defects, and identify risks that may not be evident from documents alone. A properly conducted site visit paired with a comprehensive PCR supports informed decision-making, pricing adjustments, and proper risk allocation in the transaction documents.

The primary objectives of site visits and PCRs include assessing the physical condition and functionality of the property, confirming that the property's use aligns with seller representations and complies with zoning, land use, and environmental regulations, and identifying deferred maintenance, code violations, and other potential liabilities. They also provide an opportunity to evaluate site infrastructure such as ingress and egress, utility systems, and drainage, as well as to observe tenant activity and operational dynamics in income-producing or multi-tenant properties.

[ii] Timing and Key Participants

Site visits should be scheduled early in the due diligence period to allow sufficient time to resolve issues, renegotiate terms, or plan for corrective actions. Key participants in the process typically include the buyer's legal counsel, third-party engineers or architects, environmental consultants, insurance assessors, lenders, and insurance representatives. Property or asset managers often assist in coordinating site access and logistics.

[b] Preparing for a Site Visit

Proper preparation is essential to ensure that the site visit is productive, compliant with legal requirements, and yields actionable information. Before visiting the site, the due diligence team should review several preliminary documents including the title commitment and existing survey, zoning reports and certificates of occupancy, active leases, service and vendor contracts, and any property disclosures provided by the seller. These materials help identify focus areas for the inspection and guide follow-up inquiries.

Logistics should be coordinated in advance with the seller and the property's onsite manager. This includes establishing the scope of access, identifying areas that require special permissions (such as tenant suites or rooftop mechanical spaces), and ensuring that the site will be accessible during the agreed timeframe. Especially in multi-tenant or restricted-access properties, communication and cooperation with the property manager are essential to avoid delays or incomplete inspections.

From a legal standpoint, entry onto the property should be authorized through a formal license to enter agreement. Buyers and their consultants may also be required to sign non-disclosure agreements (NDAs)

to protect confidential business or tenant information. In many cases, the seller will require evidence of insurance coverage and indemnification for any damage or injury caused during the inspection process.

[c] Key Components of the Site Visit

[i] Introduction

A comprehensive site visit includes a physical inspection of the building's systems, common areas, tenant spaces, and site infrastructure.

[ii] Structural and Mechanical Systems

Inspectors should assess all major structural and mechanical systems. This includes the roof, heating and cooling systems, plumbing and electrical infrastructure, and the building envelope to evaluate overall integrity. Critical systems such as elevators, fire suppression, and emergency power should also be reviewed to ensure functionality and compliance with applicable codes.

[iii] Site Improvements

Parking lots, sidewalks, exterior lighting, landscaping, signage, and stormwater drainage systems must be evaluated for safety, compliance, and long-term maintenance obligations. Particular attention should be paid to grading and surface conditions, which may affect stormwater flow and liability exposure.

[iv] Code Compliance

Inspectors should check for adherence to fire safety standards, emergency egress requirements, and the Americans with Disabilities Act (ADA). Any visible evidence of code violations or unpermitted alterations should be flagged for further review.

[v] Environmental Indicators

Observations of stained pavement, chemical storage, underground tanks, or unusual odors may signal environmental risks requiring additional investigation. The location of the property in relation to wetlands, flood zones, or other environmentally sensitive areas should also be verified.

[vi] Tenant Spaces

In properties with tenants, the condition of leased spaces should be assessed. This involves confirming whether tenant improvements comply with lease terms and identifying any unauthorized modifications or damage. Reviewing how tenants use the space also helps assess potential conflicts with zoning or other regulations.

[d] Property Condition Reports (PCRs)

[i] Introduction

The PCR is a detailed written assessment of a property's physical condition, typically prepared by third-party engineers, architects, or building consultants. Most PCRs follow the ASTM E2018-24 standard, which provides a uniform methodology for inspection and reporting.

[ii] Key Components of a PCR

A typical PCR includes an executive summary that highlights the property's general condition and immediate repair needs. The report then presents detailed evaluations of each system and component, such as the roof, electrical and HVAC systems, and structural elements. It differentiates between short-term capital needs—typically those required within the next one to three years—and longer-term

expenditures. The report also identifies any regulatory or code violations, safety hazards, and deferred maintenance concerns. Visual documentation, including photographs and field notes, is usually included to support the findings.

[iii] Use of PCRs

PCRs play a significant role in commercial real estate transactions. Buyers and their counsel use the report to support pricing negotiations, request purchase price adjustments, or justify escrow holdbacks to fund necessary repairs. Lenders often require a PCR as part of their underwriting process, and insurers may rely on its findings to evaluate risk exposure. Additionally, PCRs provide internal stakeholders with data necessary for investment approval or operational planning.

[e] Due Diligence Objectives

The following are the primary objectives sought to be accomplished during the Site Visit and PCR stage of the due diligence process:

- Inspect the property to confirm the property's actual use aligns with the seller's representations and complies with local zoning and land use regulations and permitted activities.
- Ensure that the property complies with applicable laws (such as the ADA).
- Observe site operations:
    - For operational or income-producing properties, teams evaluate occupancy, tenant activities, and how the site integrates into the seller's overall business.
- Assess Infrastructure:
    - The team examines ingress and egress, utility connections, drainage systems, and environmental characteristics such as wetlands or floodplain exposure.
- Coordinate Access:
    - Work with site managers and property owners to arrange access, particularly in multi-tenant or restricted facilities.
- Document Thoroughly:
    - Record all observations and findings to support follow-up questions, reports, and decision-making.
- Follow Up on Issues:
    - If the team identifies physical defects or regulatory concerns, engage additional consultants, seek repair estimates, or renegotiate transaction terms as needed.

[f] Legal and Risk Considerations

[i] Integration of Findings into Transaction Documents

The findings from site visits and PCRs should be carefully integrated into the legal documentation governing the transaction. This integration may include incorporating specific representations and warranties relating to the condition of the property or the absence of known defects, establishing conditions precedent to closing based on satisfactory inspection results, or requiring post-closing repair covenants.

Indemnity provisions may be used to allocate responsibility for known or discovered issues, and sellers may be asked to certify the accuracy of disclosures related to the physical condition of the property.

[ii] Impact on Financing

From a financing perspective, lenders may impose conditions based on PCR findings. These could include requiring that certain repairs be completed before funding or that reserves be set aside in escrow to cover anticipated capital expenditures. Insurance underwriters may also adjust terms or premiums based on identified risks.

[iii] Reliance on Third-Party Reports

One legal risk in relying on third-party reports is the limitation of liability provisions often found in consultant contracts. Buyers should review these carefully to ensure the report provides sufficient protection and recourse in the event of errors or omissions. If the PCR will be shared with lenders, investors, or other stakeholders, buyers should secure reliance letters or ensure that the report is properly assignable.

[g] Best Practices and Common Pitfalls

To ensure effective due diligence, buyers should engage qualified consultants who are licensed and experienced in the inspection of commercial properties. It is important to clearly define the scope of the site visit and/or PCR engagements and avoid inspections that are limited in scope or based solely on visual observation without testing. Comprehensive inspections provide a much stronger foundation for assessing risks and negotiating protections.

Findings should be well-documented. Photos, annotated plans, and detailed field notes serve as valuable references for future inspections or legal discussions. Buyers should avoid assuming that a property's cosmetic appearance correlates with sound condition; many critical defects may be hidden from plain sight.

Care must be taken not to overlook issues that arise due to access limitations. If sellers restrict inspection of certain areas, this should be flagged and addressed. Buyers should also take a proactive approach to negotiating based on the findings of their site visit and PCR rather than waiting until closing or relying on post-closing remedies.

[h] Conclusion

The site visit and Property Condition Report are foundational tools in the real estate due diligence process. When conducted thoroughly, they reveal important information about a property's compliance, functionality, and risk exposure that cannot be gleaned from documents alone.

A coordinated approach—bringing together legal counsel, technical consultants, business stakeholders, and lender representatives—ensures the most accurate assessment of the property. Ultimately, robust site inspections and properly scoped PCRs help buyers make informed decisions, allocate risk appropriately, and avoid costly surprises after closing.

[4] Local Counsel

[a] What Is Local Counsel and Why Are They Beneficial?

In any real estate transaction, especially those involving unfamiliar geographies, local counsel serves as the buyer's legal eyes and ears on the ground. While national or lead transaction counsel may drive the broader negotiation and documentation, local counsel brings crucial local knowledge, covering regional quirks in zoning, permitting, title, taxation, and regulatory compliance. Their insight is not just supplemental—it is often essential to identifying risks that could materially affect the transaction's outcome.

For example, in California, zoning regulations can differ not only from county to county but from one neighborhood block to another. In New York City, air rights, landmark preservation laws, and rent regulation may impact development value and feasibility. Local counsel ensures that these jurisdiction-specific issues are addressed early, thoroughly, and efficiently.

[b] Due Diligence Objectives

[i] Coordinate With Lead Transaction Counsel

The role of local counsel should not be siloed. Instead, it must be carefully integrated into the broader legal strategy. From the beginning of the transaction, local and lead counsel should coordinate to avoid duplication of effort or missed jurisdictional nuances.

Example: Lead counsel may oversee title insurance procurement, while local counsel verifies that recorded easements or access agreements comply with state recording statutes or prescriptive easement doctrines.

[ii] Define Scope Clearly

Engagement letters or initial instructions to local counsel should include a clearly defined scope of work. Common assignments include:

- Zoning and land use review
- Permitting status
- Local tax assessments or abatements
- Title review for region-specific issues
- Review of utility agreements, historical land use, or environmental filings
- Compliance with local building codes or coastal commission approvals

A narrowly tailored scope prevents cost overruns and ensures focus on the areas of greatest risk.

[iii] Request Written Summaries

Local counsel should provide their findings in written form—often as legal memos or summary charts—that can be folded into the buyer's master due diligence report. This written record provides a defensible paper trail and simplifies internal communication with investment, asset management, and legal teams.

Example: A zoning compliance memo might summarize the property's zoning designation, whether the current use is permitted as-of-right, and whether any variances or conditional use permits are required to continue or expand operations.

[iv] Use Local Counsel to Accelerate Approvals

Post-closing obligations may include filing property transfer affidavits, renewing business licenses, or recording assignments. Local counsel can fast-track these actions through their familiarity with local agencies and officials.

Example: In transactions involving change of use, local counsel can help schedule hearings with the zoning board, prepare staff reports, or facilitate required notifications to neighboring property owners.

[v] When Local Counsel Becomes Critical

Some scenarios demand particularly close local legal review:

- Historic or landmarked properties subject to design restrictions
- Retail leases in states with restrictive franchising or disclosure laws
- Industrial or special-use properties subject to state-level environmental regulation
- Coastal, floodplain, or wildfire-risk areas with layered jurisdictional oversight

[5] Appraisals

[a] What Are Appraisals?

Appraisals are formal valuations of real estate properties conducted by independent, third-party professionals. These evaluations are typically performed by licensed or certified appraisers who estimate a property's market value as of a specific date. The appraisal process involves analyzing various aspects of the property, including its physical attributes, location, and condition, in order to reach a supported value conclusion. Appraisals are typically required in transactions involving acquisition, financing, or internal audits.

[b] Why Appraisals Matter in Due Diligence

Appraisals serve as a critical checkpoint for valuation risk during real estate transactions. They provide independent confirmation that a property is worth what the buyer is paying, or the lender is underwriting. Core uses of an appraisal include:

- Validate Purchase Price: Ensure the agreed price aligns with market value.
- Support Debt Financing: Lenders require appraisals to confirm collateral adequacy.
- Cross-Check Internal Underwriting: Compare key assumptions (rent comps, cap rates, vacancy) against a third-party source.
- Comply with Institutional Guidelines: Appraisals must meet internal policies or regulatory requirements for investors and lenders.

[c] Due Diligence Objectives

[i] Engage a Qualified Appraiser

It is critical to retain an appraiser who is both licensed and experienced with the asset type and local market. Institutional deals may require appraisers who meet specific approval lists or have experience with similar property types (e.g., industrial vs. office), ensuring the appraisal is both credible and compliant.

[ii] Verify Alignment with Valuation Assumptions

The appraisal's value conclusion should be compared to the purchase price and internal underwriting to identify any material differences. Discrepancies in cap rates, market rent assumptions, or vacancy projections can impact loan sizing and return expectations and require investigation.

[iii] Understand Drivers of Value

A thorough review of the report should reveal what's behind the appraised value—tenant profile, physical condition, deferred maintenance, comps, and market trends. This context helps determine whether the valuation reflects real, sustainable value or overlooks key risks.

[iv] Ensure Regulatory Compliance

For lender-involved transactions, the appraisal must comply with FIRREA and any institutional or investor-specific standards. This often includes ensuring the lender (not the borrower) ordered the report and that the appraisal meets format and content requirements for closing and audit purposes.

[6] Entitlements and Zoning

[a] What Are Entitlements and Zoning?

Entitlements refer to the collection of rights, approvals, and permits that authorize a property's development or specific use. These may include site plans, building permits, and development agreements,

among others. **Zoning** encompasses the local government regulations that govern how land can be used, including restrictions on use, building height, density, setbacks, and parking. Together, these determine what can legally be built or operated on a given parcel.

[b] Why Entitlements and Zoning Matter in Due Diligence

Zoning and entitlements directly impact the **feasibility, timing, and risk** profile of any real estate development or acquisition. If the current or intended use is not compliant with existing zoning, or if critical entitlements are missing or expiring, the project may be delayed or rendered infeasible. Buyers must confirm that the property's development rights are **valid, transferable, and aligned with their business plan**. Municipal plans or pending zoning changes can also affect value and should be closely monitored.

[c] Due Diligence Objectives

[i] Verify Zoning Compliance

Confirm the property's current zoning designation and assess whether the existing or proposed use is permitted under current regulations. This should include obtaining **official zoning maps** and, where appropriate, **zoning verification letters** from the local planning department. Understanding any **pending zoning changes** or proposed amendments in the area is also critical to evaluating future risk.

[ii] Identify and Evaluate Entitlements

All existing entitlements should be reviewed to ensure they are **valid, active, and transferable**. They must not be subject to unmet conditions, approaching expiration, or administrative disputes. Key documents to examine include **conditional use permits, site development plans, building permits, environmental impact reports,** and any **development agreements** entered into with local jurisdictions.

[iii] Watch for Red Flags

Several issues may signal entitlement or zoning risk. These include **unpermitted structures or nonconforming uses, entitlements nearing expiration**, or evidence of **community or political opposition** to the current or planned use. Be particularly cautious if the project depends on **a future zoning change**, especially when the approval process is discretionary or politically sensitive.

§ 6.03 Leased Real Property Due Diligence

[1] What are Lease Abstracts?

A lease abstract is a summarized version of a lease agreement, designed to capture key financial, legal, and operational terms in a standardized, accessible format. Rather than reading a 50-page lease for each tenant, a properly prepared abstract allows stakeholders to quickly understand the lease's critical elements and identify any risks or obligations.

Lease abstracts are indispensable in transactions involving multi-tenant assets like office buildings, shopping centers, or industrial parks. Lease abstracts are also vital in corporate M&A transactions, where real estate is one of many due diligence categories.

[2] Why Lease Abstracts Matter in Due Diligence

The performance and stability of a property's cash flow often hinge on the quality and structure of its leases. Abstracts allow buyers, lenders, and underwriters to evaluate:

- Rent roll stability and rollover risk
- Tenant creditworthiness
- Unusual or one-sided clauses (e.g., caps on pass-throughs, termination rights)
- Required consents or compliance hurdles (e.g., exclusivity violations, co-tenancy triggers)

[3] Due Diligence Objectives

[a] Assess Portfolio Stability

Abstracts reveal how much of a building is leased, when leases expire, and how concentrated the revenue stream is among top tenants. If 60% of income comes from one tenant with a lease expiring in 12 months, that is a material risk requiring deeper analysis.

[b] Support Valuation and Underwriting

Leases are the backbone of net operating income. Appraisers and credit officers rely on accurate abstracts to model property value and underwrite debt service coverage.
Example: A lease with a below-market renewal option may limit rental upside, impacting valuation despite strong current income.

[c] Inform Post-Closing Planning

Certain leases may contain assignment or change-of-control clauses, requiring tenant approval before the lease can be transferred. Others may offer purchase options, termination rights, or exclusive-use rights that constrain future redevelopment.

[d] Flag Consent or Estoppel Requirements

As part of closing conditions, landlords often must deliver tenant estoppel certificates—signed confirmations that the lease is in good standing, with no outstanding disputes or defaults. Abstracts help identify which leases require these, and what disclosures or waivers may be needed.

[4] Key Provisions to Capture

Every lease abstract should include:

- Basic Lease Information
  - Tenant legal name and any guarantors
  - Premises description (suite number, square footage)
  - Lease execution and commencement dates
  - Expiration and option dates
- Financial Terms
  - Base rent schedule and escalation mechanics
  - Additional rent components (CAM, taxes, insurance)
  - Rent abatements or free rent periods
  - Security deposits or letters of credit
- Operational Rights and Obligations
  - Maintenance and repair duties
  - Utilities metering and responsibilities
  - Parking allocation and signage rights
  - Insurance obligations
- Transfer and Termination
  - Assignment and subletting rights
  - Termination options and early-out clauses
  - Default definitions and notice periods
- Special Clauses
  - Rights of first refusal or first offer
  - Exclusive-use rights or use restrictions
  - Co-tenancy or anchor-tenant dependency clauses
  - Relocation rights or expansion options
  - Tenant improvement (TI) obligations and allowances

[5] Common Pitfalls to Avoid

- Relying on Seller-Provided Abstracts Without Review: Always verify abstracts against the original leases.
- Inconsistent Abstracting Format: Use a standardized template to enable portfolio-wide comparison.
- Overlooking Renewal Options or Kicked-In Clauses: Many critical rights only activate at renewal, expansion, or in default scenarios.

Appendix A: Sample Real Property Due Diligence Checklist

Appendix B: Sample Real Property Due Diligence Request

1 Due Diligence in Corporate Transactions Chapter 7.syn

Chapter 7 Employee Benefits and Labor and Employment Due Diligence

---

End of Document

§ 7.01 Employee Benefits Due Diligence

[1] Introduction

The target company presumably has employees and benefit plans covering those employees. Depending on the structure of the transaction, the employees and benefit plans will transfer or merge into the buyer's operations. Accordingly, the due diligence team must scrutinize any potential liabilities arising from the target company's employee benefit plans and employees.

This section provides an overview of due diligence concerning a target company's employee benefit plans and executive compensation agreements. First, it examines issues relevant to the target company's retirement plans. Second, it identifies matters affecting the target company's welfare plans. Finally, it reviews due diligence considerations for executive compensation arrangements.

[2] Retirement Plan Due Diligence

[a] Overview

A transaction's target company often has at least one retirement plan covering its employees. A retirement plan is an employer program that provides retirement income to employees or defers employee income to periods after employment.[1] Retirement plans are regulated by the Internal Revenue Code (the "Code") and the Employee Retirement Income Security Act of 1974 ("ERISA").[2] ERISA requires that these plans be governed by a written instrument, such as a plan document, trust agreement, and summary plan description.[3] These plan documents detail the plan's characteristics and identify the plan's fiduciaries who administer the plan.[4] The retirement plan's fiduciaries, which include any individual or entity that exercises any discretionary authority over the plan or that renders investment advice to the plan for a fee, must diligently and prudently administer the plan in the best interest of plan participants and their beneficiaries,[5] which generally consist of employees. The plan must also be properly funded either through a trust or other arrangement.[6]

The due diligence team must analyze the retirement plan's structure, administration, finances, and governing documents to ensure it complies with the Code and ERISA. This analysis enables the due diligence team to advise on whether to transfer or terminate the retirement plan through the transaction.

---

[1] *See s*ection 3(2)(A) of Employee Retirement Income Security Act of 1974, as amended ("ERISA"), 29 U.S.C. § 1002(2)(A).

[2] *Id.*; *see also, e.g.*, ***26 U.S.C. § 401***.

[3] *ERISA § 402(a)(1)*, 29 U.S.C. § 1102(a)(1).

[4] *ERISA § 402(a)*-(c), 29 U.S.C. § 1102(a)-(c).

[5] *ERISA § 404*, 29 U.S.C. § 1104(a).

[6] *See e.g.*, *ERISA § 302*, *29 U.S.C. § 1082*.

This subsection identifies the types of retirement plans, due diligence issues for retirement plans, including "qualified" status, funding obligations, and litigation risk, and options for addressing the target company's retirement plans in the transaction, such as terminating said plan or integrating it into buyer's employee benefit plans.

[b] Types of Retirement Plans

[i] Introduction

There are two general types of retirement plans: defined contribution plans and defined benefit plans. The following subsections provide a general overview of these retirement plans and describe the variations of each type.

[ii] Defined Contribution Plan

Defined contribution plans are financed with contributions from employees and employers as set forth in the documents governing the plan. Generally, there are two types of employee contributions, elective deferrals and "Roth" contributions. The former are pre-tax deferrals of the employee's income; the latter reflects after-tax contributions eligible for tax-free withdrawals during retirement. Employer contributions to defined contributions plans are not required by law. However, employers may opt to remit matching contributions[7] or qualified nonelective contributions[8] to employee accounts. While defined contribution plans specify the plan's required contributions, they do not guarantee any retirement benefit for the participants (added word contributions). Instead, the retirement benefit for defined contribution plans is variable, based on the amount of contributions remitted to the plan for an employee and the investment earnings thereon. Accordingly, in defined contribution plans, the plan participant bears the plan's investment risk, as the investment performance of plan assets determines the participant's retirement benefit.

Defined contribution plans are organized under several provisions of the Code. These provisions include sections 401(a), 401(k), 403(b), and 457(b) of the Code. Generally, for-profit entities are eligible for defined contribution plans organized under sections 401(a) and 401(k) of the Code, while nonprofit organizations are eligible for plans organized under sections 403(b) and 457(b) of the Code.

Section 401(a) of the Code provides for the establishment of profit-sharing plans. Profit-sharing plans permit an employer to allocate a share of its profits, pursuant to a predetermined formula, to individual retirement accounts of employees participating in the plan.[9] For-profit and nonprofit entities may avail themselves of defined contribution plans authorized by section 401(a).

Section 401(k) of the Code provides for cash-or-deferred-arrangements ("CODAs"), which allow the employee to "have the employer make payments as contributions to a trust under the plan on behalf of the employee, or to the employee directly in cash."[10] The former option is also known as employee "elective deferrals." [11] Elective deferrals, and investment earnings thereon, are not subject to income taxation until the year of their distribution to the employee or employee's beneficiary,[12] provided employee has attained either attained age 59 ½, died, become disabled, or otherwise separated

---

[7] ***26 U.S.C. § 401(m)(4)(A)*** (defining "matching contribution" as an employer contribution prompted by employee contribution or elective deferral).

[8] ***26 U.S.C. § 401(m)(4)(C)*** (defining "qualified nonelective contribution" as any employer contribution, other than a matching contribution, that cannot be paid in cash to employee).

[9] 26 U.S.C. § 401(a)(27).

[10] 26 U.S.C. § 401(k)(2)(A).

[11] *See* 26 U.S.C. § 401(m)(4)(B).

[12] 26 U.S.C. § 402(e)(3), (4).

service with employer,[13] lest the distribution be subject to a 10% penalty tax.[14] Retirement plans organized pursuant to section 401(k) of the Code ("401(k) Plans") may also provide for employer contributions, including matching contributions,[15] qualified nonelective contributions from employer,[16] profit-sharing contributions,[17] catch-up contributions for employees age 50,[18] and rollover contributions.[19] The Code imposes limitations on contributions to 401(k) plans, such as an annual limit on elective deferrals of $23,500,[20] annual limit on total contributions (except rollover, catch-up, and deemed IRA contributions) of $70,000.[21]

Section 403(b) of the Code permits nonprofit and other tax-exempt organizations, such as those organized under section 501(c)(3) of the Code or public schools, to offer retirement plans that operate like 401(k) Plans with elective deferrals and employer contributions.[22] Retirement plans organized under section 403(b) ("403(b) Plans"), however, cannot offer the same investments to participants as 401(k) Plans. Specifically, 403(b) Plans may only offer investment in annuity contracts or custodial accounts invested in mutual funds.[23]

Retirement plans organized under section 457(b) of the Code ("457(b) Plans) may only be offered by tax-exempt organizations, state governments, and local governments.[24] This provision of the Code provides non-exempt organizations or governmental entities the ability to offer employees a deferred compensation plan similar to that of 401(k) Plans.[25]

[iii] Defined Benefit Plans

Retirement plans that "provide systematically for the payment of definitely determinable benefits to [] employees of a period of years, usually for life, after retirement" are known as defined benefit plans.[26] The benefits of these plans are determined based on a formula set forth in the defined benefit plan's governing documents.[27] The formula is generally based on the participant's age, compensation, and years of service for the employer sponsoring the plan.[28] Defined benefit plans are generally funded by

---

[13] 26 U.S.C. § 402(e)(3), (4).

[14] 26 U.S.C. § 72(t).

[15] 26 U.S.C. § 401(m)(4)(A).

[16] 26 U.S.C. § 401(m)(4)(C).

[17] *See* ***26 U.S.C. § 401(a)***; *26 C.F.R. § 1.401-1(b)(ii)*.

[18] *26 U.S.C. § 414(v)*.

[19] 26 U.S.C. § 402(c)(4).

[20] 26 U.S.C. § 402(g)(1)(B) (subject to cost-of-living adjustments).

[21] 26 U.S.C. § 415(c)(1)(A) (subject to cost-of-living adjustments).

[22] ***26 U.S.C. § 403(b)***.

[23] 26 U.S.C. § 403(b)(1), (7). Notably, SECURE 2.0 Act of 2022, (Div. T of ***Pub. L. No. 117-328***), permitted custodial accounts to invest in collective investment trusts (CITs), however, federal securities laws effectively prevent such investment at this time. *see* Securities Act of 1933 § 3(a)(2), 15 U.S.SC. § 77c (requiring 403(b) Plans to register CITs pursuant to the Securities Act but exempting 401(k) Plans from such registration requirement).

[24] ***26 U.S.C. § 457(e)(1)***.

[25] *See* 26 U.S.C. § 457(b).

[26] *Treasury Reg., § 1.401-1(b)(1)(i)*; *see also* *26 U.S.C. § 414(j)*.

[27] *Treasury Reg., § 1.401-1(b)(1)(i)*; *see also* *26 U.S.C. § 414(j)*.

employer contributions only.[29] Accordingly, the employer is generally the sole source of funds necessary to satisfy the minimum funding standards applicable to the defined benefit plan under the Code and ERISA.[30] Moreover, the employer bears the defined benefit plan's entire investment risk, as the employees receive their defined benefit from the employer regardless of the plan's investment performance. Defined benefit plans must also insure their benefits with the Pension Benefit Guaranty Corporation.[31]

There are generally three types of defined benefit plans: (1) single-employer plans; (2) multiemployer plans; and (3) multiple employer plans and pooled employer plans. Single employer plans are defined benefit plans sponsored by one employer.[32] A multiemployer plan is a plan to which more than one employer is required to contribute and which is maintained pursuant to at least one collective bargaining agreement between at least one employee organization and at least two employers.[33] A multiple employer plan and are pooled employer plan are plans maintained by more than one employer that the Code and ERISA treat as if maintained by a single employer.[34] Each of these types of plans have different rules concerning benefit accrual, funding, discrimination, and deductions.

[c] Retirement Plan Diligence

[i] Introduction

The due diligence team should verify that that target company's retirement plans qualify for tax-advantaged status, satisfy funding requirements, and have no pending litigation liability.

[ii] Qualified Plan Assessment

Section 401(a) of the Code establishes the requirements for "qualified" plan status.[35] Qualified plans are eligible for tax-advantaged treatment, such as tax-deferment on contributions to the plan. To be a qualified plan, the plan, in general, must be:[36]

1. created by an employer;
2. established and maintained pursuant to a written document;
3. communicated to employees;
4. funded through a domestic trust;

---

[28] *26 U.S.C. § 411(b)(1)*; *Treasury Reg., § 1.401-1(b)(1)(i)*.

[29] *See* 26 U.S.C. § 411(c)(2) (demonstrating complicating impact of mandatory employee contributions on benefit calculation); 26 U.S.C. § 411(d)(5) (stating that voluntary employee contributions to defined benefit plan are treated as contributions to defined contribution plan); *Treasury Reg., § 1.411(c)-1(a)*-(c) (demonstrating complicating impact of employee contributions on defined benefit calculation).

[30] 26 U.S.C. § 412; *29 U.S.C. §§ 1082-84*.

[31] 29 U.S.C. §§ 1321-23.

[32] *See* 29 U.S.C. §§ 1002(16)(B)(i), 1083, 1322.

[33] 29 U.S.C. § 1002(37).

[34] 26 U.S.C. § 413(c) (multiple employer plans); 26 U.S.C. § 413(e) (pooled employer plans); Labor Reg., § 2530.210(c).

[35] 26 U.S.C. § 401(a) (stating that a plan or "trust created or organized in the United States and forming part of a stock bonus, pension, or profit-sharing plan of an employer for the exclusive benefit of his employees or their beneficiaries shall constitute a qualified trust" provided it fulfills the requirement of this section).

[36] 26 U.S.C. § 401(a) (identifying criteria for qualified plans); *Treasury Reg., § 1.401-1* (same).

5. administered for the exclusive benefit of participants;

6. structured to cover the minimum percentage of employees identified in the Code;[37]

7. aligned with the minimum vesting standards identified in the Code;[38]

8. monitored to avoid discrimination in favor of highly compensated employees ("HCEs");[39]

9. adherent to the Code's contribution limits; and

10. compliant with the Code's minimum distribution requirements.[40]

As Congress enacts legislation and government agencies, including the Internal Revenue Service ("IRS") and the United States Department of Labor ("DOL"), promulgate regulations, the requirements for qualified status under section 401(a) of the Code become more numerous. For example, in 2019 Congress enacted the Setting Every Community Up for Retirement Enhancement ("SECURE") Act[41] and, in 2022, enacted SECURE 2.0 Act[42] (collectively, the "SECURE Acts"). The SECURE Acts imposed additional criteria for qualified plan status under section 401(a) of the Code. For example, section 107 of SECURE 2.0 Act amends section 401(a)(9) of the Code to increase the age at which the plan must make required minimum distributions to participants from 72 to 73.

To maintain qualified plan status, plan sponsors must amend their plan documents to reflect updated laws and regulations lest they fail to fulfill the requirements of section 401(a) of the Code, risking disqualification from tax-advantaged status. To assist plan sponsors with this compliance, the IRS publishes a Required Amendments List, which identifies the changes in law that require plan amendments, which plans may adopt during a Remedial Amendment Period, a grace period between the effective date of the new law and the deadline for the sponsor to amend its plan to incorporate that new law in the plan.[43] However, in anticipation of a plan termination (which often occurs in connection with transactions), a the target company must amend its plan prior to the plan's termination to reflect all laws and regulations effective as of the termination date, regardless of any applicable Remedial Amendment Period.[44] Absent such amendment, the plan risks the loss of qualified status.[45]

The consequences of disqualification are significant. Specifically, if a plan violates one of the conditions for qualified plan status identified in section 401(a) of the Code, then the plan's trust loses its tax-exempt status, rendering the trust taxable under section 402(b) of the Code.[46] Consequently, the earnings on plan assets become taxable to the trust,[47] the plan sponsor's tax deduction for plan

---

[37] *26 U.S.C. § 410(b)* (articulating minimum coverage standards for qualified retirement plans).

[38] *26 U.S.C. § 411* (articulating minimum vesting standards for retirement plans).

[39] ***26 U.S.C. § 401(a)(4)*** (detailing nondiscrimination rules).

[40] ***26 U.S.C. § 401(a)(9)*** (identifying required distribution rules for retirement plans).

[41] Consolidated Appropriations Act of 2020, Div. O of ***Pub. Law 116-94***.

[42] Consolidated Appropriations Act of 2023, Div. T of ***Pub. L. No. 117-328***.

[43] IRS Website: Required Amendment List - *https://www.irs.gov/retirement-plans/required-amendments-list*. [Seen Aug. 2025].

[44] *Rev. Proc. 2025-4*, §15.05 (updated annually) ("A plan that terminates after the effective date of a change in law, but prior to the date that amendments related to the change in law are otherwise required, must be amended to comply with the applicable provisions of law from the date on which such provisions become effective with respect to the plan.").

[45] *Id*.

[46] 26 U.S.C. § 402(b) (identifying tax consequences of failure to stratify requirement of 401(a) and other relevant Code provisions).

contributions are deferred until the contribution is vested and includible in participant's gross income,[48] HCEs in the plan are taxed on their entire vested account balances,[49] and distributions from the plan are no longer eligible for favorable tax treatment, rendering such distributions, including rollovers to another retirement plan or individual retirement account (IRA), subject to taxation at the time of the distribution and potential 6% excise tax.[50] These consequences could be borne by the buyer if buyer integrates the target company's plan into its employee benefit plans or is otherwise responsible as a successor of the target company. Accordingly, the due diligence team should ensure that the target company's plan complies with section 401(a) of the Code to avoid any adverse tax consequences impacting the transaction.

The due diligence team's inquiry into a target company's retirement plan's qualified status is easier when the IRS has issued a Favorable Determination Letter. The IRS issues such a letter in response to a plan sponsor's request for a determination that the plan is qualified for tax-advantaged status under section 401(a) of the Code and that the plan's trust is tax-exempt under section 501(a) of the Code, provided the plan, indeed, satisfies the requirements for those determinations. The due diligence team may rely on the IRS's Favorable Determination Letter issued to the target company's retirement plan to conclude the plan is qualified though the date of said letter. The due diligence team will have to review the plan to ensure it has incorporated all changes in the law since the issuance of the Favorable Determination Letter.

Many employers adopt pre-approved, prototype plan documents from third-party administrators to govern their retirement plans, as opposed to individual designed plan documents. The third-party administrators routinely obtain Favorable Determination Letters from the IRS for their pre-approved, prototype plans. Moreover, the third-party administrators often provide protype amendments to these prototype plan documents when there are updates to the relevant laws and regulations. Accordingly, to increase the efficiency of retirement plan due diligence, the due diligence team should work with the target company's third-party administrator to determine if a Favorable Determination Letter applies to the relevant plan and whether the third-party administrator has pre-drafted amendments to update the plan.

The following plan failures are common reasons for a target company's retirement plan disqualification from Code § 401(a) qualified status:

1. Failure to satisfy the minimum coverage requirement of Code § 410(b).

    a. Retirement plans must either (i) benefit at least 70% of the target company's non-HCEs (percentage test);[51] (ii) result in a ratio of at least 70% when the percentage of non-HCEs benefiting from the plan is divided by the percentage of HCEs benefiting from the plan (ratio percentage test);[52] or (iii) provide an "average benefits percentage" for non-HCEs that is at least 70% of the "average benefit percentage" for HCEs.[53]

---

[47] *26 U.S.C. § 501(a)* (stating that only organizations organized under § 501(c), (d) and trusts compliant with §401(a) shall be exempt from taxation).

[48] 26 U.S.C. §§ 402(a), (b)(1)-(3), 501(a); *IRS Rev. Ruling 74-299*.

[49] 26 U.S.C. § 402(b)(4); *IRS Rev. Ruling 2007-48*.

[50] 26 U.S.C. § 4973 (providing 6% excise tax on excess rollovers); *Baetens v. Comm'r, 777 F.2d 1160 (6th Cir. 1985)* (holding that rollover distributions are ineligible for preferential tax treatment unless they are from qualified plans); *Benbow v. Comm'r, 774 F.2d 740, (7th Cir. 1985)* (same); *Woodson v. Comm'r, 651 F.2d 1094 (5th Cir. 1981)* (same); *Meyers v. Comm'r, T.C. Memo. 1994-598 (1994)* (same).

[51] 26 U.S.C. § 410(b)(1)(A); *Treasury Reg., § 1.410(b)-2(b)(2)*.

[52] *26 U.S.C. § 410(b)(1)(B)*; *Treasury Reg., § 1.410(b)-2(b)(2)*.

2. Failure to satisfy the nondiscrimination requirements of Code § 401(a)(4).

a. Retirement plans must not provide contributions, benefits, features, or other rights that disproportionately favor HCEs.[54] There are several tests for determining whether a plan disproportionately discriminates in favor of HCEs.[55] The due diligence team may enlist a service provider to perform nondiscrimination testing.

3. Failure to update plan document for operational compliance.

a. Frequently, target companies overlook the need to update their plan documents to reflect changes in relevant laws and regulations, relying on an old Favorable Determination Letter or an outdated prototype plan document. These plan amendment failures result in plan disqualification even when the amendment is irrelevant to plan operations.[56]

In analyzing the target company's plan's qualified status, the due diligence team should also review the retirement plans of the target company's controlled group, as defined in section 1563 of the Code, especially for determining whether minimum coverage and nondiscrimination requirements are satisfied, as the IRS treats the controlled group as a single employer qualified status determinations.[57] However, the Code allows certain employees to be excluded from qualified status analysis, including employees covered by collective bargaining agreements and employees that fail to satisfy the age and service eligibility criteria for plan participation.[58]

To facilitate its qualified plan assessment, the due diligence team should request the plan document, trust agreement, summary plan description, all plan amendments, Form 5500s with audited financial statements, trust account statements, participant account statements, nondiscrimination testing reports, record of plan assets, and plan investment policies of all target company's retirement plans. The diligence team should also review the employee census and payroll register to determine whether the plan satisfies the nondiscrimination and minimum coverage requirements of section 401(a) of the Code.

[iii] Funding Obligation Assessment

The due diligence team's analysis of the target company's retirement plan's financial obligations depends on whether the plan is a defined contribution plan or a defined benefit plan. Defined contribution plan funding obligations are primarily governed by the plan documents and the plan sponsor's fiduciary duties. Defined contribution plan sponsors bear no obligation under the Code or ERISA to satisfy minimum funding standards. Accordingly, in assessing the funding status of a defined contribution plan, the due diligence team that contributions have been remitted, invested, and allocated in accordance with the plan documents. To the extent that the due diligence team identifies operational errors in the target company's defined contribution plan, such as the untimely remittance of contributions to participant accounts, the due diligence team should request the target company to correct the issue through self-correction, if applicable, Employee Plan Compliance Resolution System of the IRS, or the Voluntary Fiduciary Correction Program of the DOL. Alternatively, the due diligence

---

[53] *26 U.S.C. § 410(b)(2)*. The "average benefit percentage" is the average of the employer-provided contribution or benefit provided to a particular benefit classification of a retirement plan. *26 U.S.C. § 410(b)(2)(B)-(C)*. *See also* *Treasury Reg., § 1.410(b)-2(b)(3)*.

[54] ***26 U.S.C. § 401(a)(4)***; *Treasury Reg., § 1.401(a)(4)-1(b)(2)(i)*.

[55] *See* *Treasury Reg., § 1.401(a)(4)-1*.

[56] *Christy & Swan Profit Sharing Plan v. Comm'r, T.C. Memo. 2011-62 (Mar. 15, 2011)* (disqualification for failure to amend to include all required amendments prior to formal termination of the plan).

[57] *26 U.S.C. § 414(b)(1)*.

[58] 26 U.S.C. § 410(b)(3)-(4).

team could recommend covenants or indemnification provisions in the transaction document to ensure that the target company would be monetarily responsible for the plan error.

Defined benefit plans, such as pensions, have more burdensome funding obligations than those of defined contribution plans because defined benefit plans are subject to the minimum funding standards of section 412 of the Code.[59] Under this Code provision, the sponsor of a defined benefit plan must remit an annual contribution to the plan to ensure the plan is able to satisfy all its benefit obligations for its employees upon their retirement.[60] Although plan sponsors may invest the contributions remitted to the defined benefit plan in securities, real estate, and other assets,[61] if those investments devalue, whether for general macroeconomic reasons or for reasons particular to the investment, the plan sponsor is obligated to deposit addition contributions in the defined benefit plan's trust sufficient to satisfy the plan's minimum funding obligations, which would be larger than normal in this scenario due to the devaluation of plan assets.

As a result, the due diligence team must analyze the amount that the target plan regularly remits to the defined benefit plan to satisfy the minimum funding standards of the Code and ERISA. Additionally, the due diligence team should review the investments of the target company's defined benefit to determine the risk of a plan asset devaluation that would require additional contributions from the buyer, beyond that which the target company has normally remitted to said plan.

The due diligence team must also determine whether the target company has a contribution obligation to any multiemployer pension plans, as such defined benefit plans may have a significant financial impact on the transaction. As stated above, a multiemployer plan is a plan to which more than one employer is required to contribute and which is maintained pursuant to at least one collective bargaining agreement between at least one labor organization and at least two employers.[62] They are managed by an equal number of employer trustees and union trustees pursuant to a written instrument, such as a collective bargaining agreement, plan document, or trust agreement, that requires the remittance of contributions to a trust established for the "sole and exclusive benefit of employees" and their beneficiaries.[63]

Multiemployer pension plans ("MEPPs") pose unique issues for corporate transactions because they can impose ERISA withdrawal liability on the transaction's parties. ERISA withdrawal liability is a withdrawing employer's proportional share of liability for the unfunded vested benefits of a multiemployer pension plan ("MEPP") based on the withdrawing employer's contributions fractional share of the MEPP's overall employer contributions.[64] For example, if an employer regularly contributes $1 million per year to a MEPP, with overall employer contributions to said MEPP regularly amounting to $10 million per year, and if the MEPP had unfunded vested liabilities of $100 million, then, when that employer withdraws from the MEPP due to an asset sale, the MEPP would assess withdrawal liability on the withdrawing employer of $10 million, reflecting ten percent of unfunded vested benefits based on its ten percent of employer contributions to the MEPP.[65] This example illustrates a complete withdrawal,

---

[59] *26 U.S.C. § 412(a)(2)*.

[60] *See* *26 U.S.C. § 430* (detailing computation of minimum funding obligation for single-employer plans); *id*., §§ 431-432 (detailing computation of minimum funding obligation for multiemployer plans).

[61] *See* *29 U.S.C. § 1104(a)(1)* (requiring plan sponsors and fiduciaries to act "with the care, skill, prudence, and diligence" of a "prudent man" to administer the plan for the "exclusive purpose of providing benefits to participants and their beneficiaries").

[62] 29 U.S.C. § 1002(37). *See also* *29 U.S.C. 1301(a)(3)*.

[63] Labor Management Relations Act § 302(c)(5), 29 U.S.C. § 186(c)(5).

[64] *ERISA § 4201*, *29 U.S.C. § 1381*.

where the employer either permanently ceases to have a contribution obligation under the MEPP or permanently ceases all covered operations under the MEPP.[66] However, a MEPP may also impose partial withdrawal liability on transacting parties.

A MEPP may impose partial withdrawal liability under three circumstances: (1) the employer's contributions to the MEPP during each of the three most recent three years ("Testing Period") declined by 70%[67] or more when compared to the average of the two years with the employer's highest contributions (not necessarily consecutive) during the five-year period preceding the Testing Period ("70% Decline Partial Withdrawal");[68] (2) the employer terminates one of several collective bargaining agreements that obligate employer to contribute to the MEPP while continuing to perform work covered by the terminated collective bargaining agreement or transferring such work to another location or to an entity owned or controlled by the employer ("Bargaining Unit Take Out Partial Withdrawal");[69] (3) the employer terminates its contribution obligation to the MEPP at one of its facilities but continues to perform work at that facility that would otherwise require contributions to the MEPP ("Facility Take Out Partial Withdrawal").[70] Under these circumstances, the MEPP determines the amount of partial withdrawal liability by calculating the employer's complete withdrawal liability and multiplying that sum by the fraction of employer's contributions for the plan year subsequent to the partial withdrawal over the employer average contributions during five years before the partial withdrawal.[71]

In either a partial or complete withdrawal, ERISA requires that the resulting withdrawal liability be paid in installment payments, based on a calculation set forth in ERISA, over a period not to exceed 20 years.[72] Generally, the employer can negotiate with the MEPP to pay the withdrawal liability as a lump-sum, potentially at the net present value based on a negotiated discount rate.[73]

The parties can structure their transaction to avoid ERISA withdrawal liability, even if the target company contributes to a MEPP. Specifically, transactions that involve a "change of identity, form or place of organization,"[74] "liquidation into a parent corporation,"[75] or a "merger consolidation, or division,"[76] do not prompt the assessment of withdrawal liability, even if the contributing employer ceases to exist because of the transaction, provided the transaction "causes no interruption in employer

---

[65] This example is for illustrative purposes and represents a basic articulation of ERISA withdrawal liability calculation. ERISA provides several methods of calculating withdrawal liability. *See* *ERISA § 4211*, *29 U.S.C. 1391*. Moreover, the MEPP's plan documents can also impact the calculation of withdrawal liability.

[66] ERISA § 4203(a), 29 U.S.C. § 1383.

[67] For employers in the retail food industry, a 35% decline, as opposed to a 70% decline, prompts partial withdrawal liability. *ERISA § 4205(c)(1)*, *29 U.S.C. § 1385(c)(1)*.

[68] *ERISA § 4205(a)(1)*, *(b)(1)*, *29 U.S.C. § 1385(a)(1)*, *(b)(1)*.

[69] *ERISA § 4205(a)(2)*, *(b)(2)(A)(i)*, *29 U.S.C. § 1385(a)(2)*, *(b)(2)(A)(i)*.

[70] *ERISA § 4205(a)(2)*, *(b)(2)(A)(ii)*, *29 U.S.C. § 1385(a)(2)*, *(b)(2)(A)(ii)*.

[71] *ERISA § 4206(a)*, *29 U.S.C. § 1386(a)*.

[72] *ERISA § 4219(c)*, *29 U.S.C. § 1399(c)*.

[73] *See* *ERISA § 4219(c)(4)*, *29 U.S.C. § 1399(c)(4)* (permitting prepayment without penalty).

[74] ERISA § 4069(b)(1), 29 U.S.C. § 1369(b)(1); *see also* *ERISA § 4218(1)(B)*, *29 U.S.C. 1398(1)(B)*.

[75] ERISA § 4069(b)(2), 29 U.S.C. § 1369(b)(2).

[76] ERISA § 4069(b)(3), 29 U.S.C. § 1369(b)(3).

contributions or obligations to contribute" to the MEPP.[77] Based on these provisions of ERISA, a stock sale, by itself, will not engender ERISA withdrawal liability.

Sales of assets, however, where seller contributes to a MEPP, usually result in the MEPP assessing withdrawal liability against the seller because, generally, neither the seller nor the purchaser has an obligation to remit contributions to the MEPP after the transaction. However, the parties to an asset-purchase agreement can avoid this withdrawal liability by drafting the transaction document to conform with *section 4204 of ERISA*,[78] which provides parties to an asset-purchase agreement with a safe harbor from withdrawal liability. To avail themselves of this withdrawal liability safe harbor, the transacting parties must satisfy the following conditions: (i) the sale must be a bona-fide, arm's-length transaction to an unrelated party; (ii) the buyer must have an obligation to contribute to the MEPP at substantially the same level as the "Seller"; (iii) the buyer must, for five years, provide the MEPP with a bond or escrow deposit in an amount equal to the greater of seller's contributions for the plan year preceding the sale or seller's average annual contributions for the three preceding plan years; and (iv) the purchase agreement must provide that the seller is secondarily liable for any withdrawal liability of the buyer to the plan for a period of five plan years following the plan year in which the sale occurred.[79] Under certain circumstances, the Pension Benefit Guaranty Corporation ("PBGC") or the MEPP, upon application, may exempt the parties from the bond or escrow deposit requirement of *section 4204 of ERISA*.[80]

Even if the parties cannot design the transaction to avoid withdrawal liability from the MEPP, ERISA provides several statutory exemptions and defenses. For example, building and construction industry employers and entertainment industry employers that operate on a temporary, project-by-project basis are exempt from withdrawal liability, provided those employers refrain from performing work covered by the relevant collective bargaining agreement or MEPP for five years following their withdrawal.[81] Additionally, employers may dispute the actuarial assumptions underlying the withdrawal liability assessment,[82] demand the application of the 20-year cap on withdrawal liability installment payments,[83] and request the payment of withdrawal liability at the net present value of the 20-year statutory payout period.[84]

Generally, if the target company, or any member of its controlled group as defined in section 1563 of the Code, incurs withdrawal liability prior to the transaction's closing or because of the transaction, then the buyer could be liable for the target company's withdrawal liability as a successor pursuant to federal common law emanating from ERISA.[85]

---

[77] *ERISA § 4218(1)*, *29 U.S.C. 1398(1)*.

[78] *29 U.S.C. § 1384*.

[79] *29 U.S.C. § 1384(a)*.

[80] *29 U.S.C. §1384(c)*; *29 C.F.R. §§ 4204.11-4204.13*.

[81] *ERISA § 4203(b)(2)*, *(c)*, *29 USC § 1383(b)(2)*, *(c)*.

[82] The MEPP's actuaries are required to apply assumptions that reflect the actuary's "best estimate of anticipated experience under the plan." *ERISA §§ 304(c)(3)*, *4213(a)*; *29 U.S.C. § 1084(c)(3)(B)*, *1393(a)(1)*.

[83] *ERISA § 4219(c)(1)(B)*, *29 U.S.C. § 1399(c)(1)(B)*.

[84] *See* *ERISA § 4219(c)(4)*, *29 U.S.C. § 1399(c)(4)* (permitting prepayment without penalty).

[85] *New York State v. C&S Wholesale Grocers, Inc., 24 F.4th 163, 178-181 (2d Cir. 2022)* (holding that successor liability for ERISA withdrawal liability can apply to buyer of assets); *Tsareff v. ManWeb Servs., Inc., 794 F.3d 841, 845-47 (7th Cir. 2015)*

In sum, the due diligence team must ensure that defined contribution and defined benefit plans have fulfilled their funding obligations and avoided financial penalties such as those imposed by the IRS for operational plan failures in defined contribution plans and by MEPPs in the event of an employer withdrawal.

To facilitate its funding obligation assessment, the due diligence team should request the plan document, trust agreement, summary plan description, all plan amendments, Form 5500s with audited financial statements, trust account statements, participant account statements, record of plan assets, and plan investment policies of all target company's retirement plans. The diligence team should also review any collective bargaining agreements of the target company to determine whether the target company has a contribution obligation to a MEPP.

[iv] Litigation and Agency Enforcement Assessment

The due diligence teams should assess the target company's exposure to liability from ERISA litigation and government agency enforcement actions pursuant to ERISA and the Code, including investigations and audits by the DOL, the IRS, and the PBGC, by reviewing any demand letters or complaints from civil plaintiffs and any correspondence, inquiries, or notices from government agencies.[86] For example, the DOL might have issued a Notice of Rejection of the Target Company's Form 5500 for failure to attached financial statements, which can result in civil penalties.[87] Additionally, the due diligence team should review any recently conducted regulatory audits of the target company's retirement plans and request information on any potential regulatory audits of those plans. The due diligence team should ensure that, to the extent the target company is exposed to litigation or agency enforcement, the transaction documents properly address those liability risks.

[v] Integration Analysis

Based on the due diligence of the target company's retirement plans, the due diligence team can advise the parties on how the transaction should address the target company's retirement plans.

For defined contribution plans, the due diligence team may consider the following actions for addressing the target company's retirement plans in connection with the transaction:[88]

- terminate the target company's defined contribution plan before the closing;
- freeze the target company's defined contribution plan as of the closing;
- continue the target company's defined contribution plan after the closing;
- transfer assets from the target company's defined contribution after the closing;
- merge or spin off the target company's defined contribution to the buyer's defined contribution plan after the closing; or
- accept participant elective transfers into the buyer's defined contribution from the target company's defined contribution plan.

A termination of the defined contribution plan requires the target company's board of directors to amend the plan to comply with all laws and regulations in effect at the time of termination to avoid tax

---

(same); *Resilient Floor Covering Pension Trust Fund Bd. of Trs. v. Michael's Floor Covering, Inc., 801 F.3d 1079, 1093 (9th Cir. 2015)* (same).

[86] *See* ERISA §§ 104(a)(5), 502(a), (c), 29 U.S.C. § 1024(a)(5) (statutory authority for DOL investigations and penalties); 29 C.F.R. §§ 2560.502c-2-.502c-8, 2560.502i-1 (regulatory authority for DOL investigations and penalties).

[87] ERISA § 104(a)(5), 29 U.S.C. § 1024(a)(5); 29 C.F.R. §§ 2560.502c-2(g).

[88] *See* Deidre C. Thomas, et al., EBIA: 401(K) PLANS, "Seller's 401(k) Plan: Choices Available to the Seller and the Buyer," § XXXVIII.G. (Thomson Reuters 2025).

penalties for plan disqualification.[89] Once the plan is updated, then the target company's board of directors must adopt a resolution terminating the plan. For 401(k) Plans, the target company's board of directors must adopt this terminating resolution prior to closing of the transaction, otherwise the plan will not be able to distribute benefits to transferred participants for 12 months.[90] Additionally, the distribution of plan assets upon termination must occur "as soon as administratively feasible," which generally requires distribution within one year of termination.[91] According to the IRS, a plan is not fully terminated until it has distributed all its assets.[92]

A frozen defined contribution plan results in the full vesting of participant benefits and a cessation of further contributions.[93] The frozen plan's benefits are not distributed to a participant until the participant's employment is terminated. After the transaction, the seller may retain the frozen plan or transfer it to the buyer. If so transferred, the buyer may maintain the frozen plan separate from its other retirement plans.

The continuation of the target company's defined contribution plan, which occurs automatically by law in stock purchases,[94] requires the buyer to incorporate the plan into buyer's employee benefit plan governance structure. The buyer may maintain the plan as is or modify it through amendment. Although this option is the default option for stock purchase agreements, the parties to stock sales may insert covenants into the purchase agreement whereby seller retains certain assets or liabilities of the plan.

If the buyer prefers to only transfer assets of the target company's defined contribution plan, then the parties may pursue either (i) a trust-to-trust transfer, which involves the withdrawal of target company's assets from its qualified trust and depositing said assets in buyer's qualified trust, (ii) a rollover transfer, which is similar to a trust-to-trust transfer but with no option to distribute assets to participants, or (iii) a merger/spin-off of target company's plan assets to buyer's plan.[95] To the extent the parties intend to pursue a merger or spin-off of the target company's plan into buyer's plan, the parties might have to file a Form 5310-A, Notice of Plan Merger or Consolidation, Spin-Off, or Transfer of Plan Assets or Liabilities.[96] This filing requirement has several exceptions, including exceptions for direct rollovers.[97]

Defined benefit plans generally have the same options as defined contribution plans for disposition as of the transactions closing. However, defined benefit plans have stricter rules than defined contribution plans for termination. Specifically, the defined benefit plan generally must issue a notice of intent to terminate the plan to all affected participant, a notice of plan benefits, file a standard termination notice with the PBGC, and distribute plan assets pursuant to PBGC regulations.[98] Additionally, the plan sponsor, or any member of the plan's controlled group, must make a commitment, in writing, to

---

[89] *Rev. Proc. 2025-4, 2025-1 I.R.B. 158*, §15.05; *see also* Section 1[a][ii][A] of this Chapter, *supra*.

[90] 26 U.S.C. § 410(k)(10); *Treasury Reg., § 1.401(k)-1(d)(4)*.

[91] *IRS Rev. Ruling 89-87*.

[92] *IRS Rev. Ruling 89-87*.

[93] *26 U.S.C. § 411(d)(3)*.

[94] *CenTra, Inc. v. Central States Se. and Sw. Areas Pension Fund, 578 F.3d 592 (7th Cir 2009)* (holding that a "successor corporation in a merger or stock sale inherits the predecessor's [ERISA obligations] just as it assumes contractual liabilities.").

[95] *Treasury Reg., § 1.414(l)-1* (detailing rules for effecting a merger of plans and transfers of plan assets).

[96] *See* Instructions to Form 5310-A.

[97] *See* Instructions to Form 5310-A.

[98] *29 C.F.R. § 4041.21(a)*.

contribute any additional sums necessary to enable the terminating defined benefit plan to satisfy plan benefits.[99] Finally, if the defined benefit plan is a multiemployer pension plan, with the meaning of *section 3(37) of ERISA*, then termination of the target company's obligation to contribute to the multiemployer pension plan could result in the assessment of withdrawal liability on the target company and, potentially the buyer, as a successor of the target company.[100]

Thus, based on the due diligence, the due diligence team has a range of options to consider when determining how the transaction should address the target company's retirement plans.

[3] Welfare Plan Due Diligence

[a] Introduction

A transaction's target company often provides its employees with a variety of welfare plans. A welfare plan is a plan, fund, or program maintained by an employer to provide participants or their beneficiaries medical, surgical, or hospital care benefits, or benefits in the event of sickness, accident, disability, death or unemployment.[101] The due diligence team must review each welfare plan's governing documents to understand the plan's funding status, administration, and compliance with statutory and regulatory guidance. This enables the due diligence team to advise on whether to assume or terminate the welfare plans in connection with the transaction. This subsection discusses (i) the types of welfare plan funding, (ii) welfare plans that are eligible for tax-favorable treatment, and (iii) various legal and reporting requirements applicable to welfare plans.

[b] Plan Funding

An employer may sponsor a welfare plan that is either self-funded or fully-insured. An employer with a self-funded welfare plan pays medical claims from its general assets, a trust, or both. An employer with a self-funded welfare plan assumes the risk that medical claims for a given year will be different than projected. The sponsors of self-funded plans generally hire an actuarial expert to predict the expected medical claims year-to-year and may self-administer claims or outsource claims administration to a third party.

With a self-funded plan, the employer commits to pay claims that are not covered by employee contributions or cost sharing. Through an actuarial expert, the employer generally estimates its monthly contribution toward the cost of coverage. The employer may actually pay more or less toward the estimated cost of coverage depending on the actual claims experience for the year. Once the actual claims experience for the year has been determined, the employer will factor the claims experience into its estimated cost for coverage in the next year.

Often the employer sponsoring a self-funded plan will purchase stop-loss insurance to cover large or unexpected claims. In this case, the employer pays a premium to the stop-loss carrier for stop-loss insurance. The stop-loss insurance begins to cover claims once they reach the relevant attachment point (i.e., the dollar amount after which the policy reimburses the health plan or the employer for covered claims).

A stop-loss policy with a "specific" attachment point protects the employer from claims incurred by a single individual. For example, if the stop-loss policy provides for a specific attachment point of $100,000 per individual per year, the stop-loss insurance will begin paying for an individual's health claims once they exceed $100,000 in a given year. A stop-loss policy with an "aggregate" attachment point protects the employer from total claims for all plan participants and beneficiaries. For example, if the stop-loss policy

---

[99] 29 C.F.R. § 404.21(b).

[100] *See* *ERISA §§ 4201*-4225, *29 U.S.C. §§ 1383-1405*. *See also* Section 1[a][ii][B] of this *Chapter, below.*

[101] ERISA, § 3(1). A welfare plan may also provide vacation benefits, apprenticeship or other training programs, day care centers, scholarship funds, or prepaid legal services.

provides for an aggregate attachment point of $15,000,000, the stop-loss insurance will begin paying for claims once the plan's claims exceed $15,000,000 for all participants and beneficiaries in a given year.

An employer with a fully-insured welfare plan contracts with an insurance carrier that pays claims from the insurance policy. The employer pays the insurance company the policy premiums to maintain plan coverage and may share the cost of the premiums with employees. An insurance company sets the policy premiums based on an evaluation of the employer's expected claims and may decline to issue a quote depending on the projected claim payments.

Unlike an employer with a self-funded plan, an employer with a fully-insured plan assumes no risk for claims and can predict the cost of its health plan coverage in a given year.

[c] Tax-Advantaged Plans

[i] Introduction

Employers may structure their welfare plans such that employees receive welfare plan benefits on a tax-free basis. This section examines these tax-advantaged welfare plan structures.

[ii] Accident or Health Plans

Employees must include in their taxable income any benefits received from an employer unless the Code provides for an exemption. Code Section 105 specifically excludes from income amounts paid by an employer through an accident or health insurance plan to reimburse an employee for medical care expenses.[102] Generally, medical care expenses include those for (i) the diagnosis, cure, mitigation, treatment, or prevention of a disease (and associated transportation), (ii) qualified long-term care services, and (iii) insurance.[103] Code Section 106 excludes from income premiums or contributions paid by an employer for health and accident coverage for its employees.[104] The exclusion applies to employer premium contributions for an insured policy covering one or more employees as well as contributions to a self-funded health plan.[105]

[iii] Cafeteria Plans

Code Section 125 specifically excludes from income amounts an employee contributes to benefits pursuant to a "cafeteria plan."[106] A cafeteria plan is a written plan that permits participants to choose among two or more benefits consisting of cash and certain qualified expenses, such as medical care expenses or dependent care expenses.[107] Under a cafeteria plan, employees may use pre-tax dollars to pay premiums for employer-sponsored medical and other qualified benefits and may make pre-tax contributions to flexible spending accounts and health savings accounts. For highly compensated individuals[108] to enjoy the same tax-favored treatment, the cafeteria plan must provide benefits in a

---

[102] *26 U.S.C. § 105(a)*, *(b)*.

[103] *26 U.S.C. § 213(d)(1)*.

[104] *26 U.S.C. § 106(a)*.

[105] *26 C.F.R. § 1.106-1(a)*; Priv. Ltr. Rul 84-11-064 (Dec. 13, 1983).

[106] *26 U.S.C. § 125(a)*.

[107] *26 U.S.C. §§ 125(d)(1)*, *125(f)(1)*.

[108] The Code contains separate definitions for "highly compensated individuals", "highly compensated employees", and "highly compensated participants." This subsection uses the term "highly compensated individuals" generically with no specific reference to any of the three defined terms.

manner that does not treat highly compensated individuals more favorably than individuals who are not highly compensated.[109]

[iv] Others

The Code contains various other sections providing favorable tax treatment for certain types of welfare plans that are not discussed in this chapter (e.g., Dependent Care Plans (Code Section 129), Educational Assistance Programs (Code Section 127), Group-Term Life Insurance (Code Section 79), and Fringe Benefit Plans (Code Section 132)).

[d] Relevant Laws

Welfare plans are highly regulated. This section provides an overview of the most relevant laws for welfare plan due diligence.

[i] The Patient Protection and Affordable Care Act

Congress enacted the Patient Protection and Affordable Care Act (the "ACA") in 2010 to comprehensively reform health care law in the United States. Certain provisions of the ACA will apply to the target company depending on whether it is an Applicable Large Employer ("ALE") by virtue of employing a sufficient number of full-time employees. An ALE for a calendar year is an employer who employed (along with members of its controlled group) an average of at least 50 "full-time" employees on business days during the preceding calendar year.[110] Any employee working at least 120 hours in a month counts as a "full-time" employee for that month.[111] An employer must convert part-time employees into "full-time equivalents" by dividing the aggregate hours worked by part-time employees by 120.[112]

In general, under the ACA, an ALE may be subject to an Employer Shared Responsibility Payment ("ESRP") penalty if the ALE fails to offer minimum essential coverage to at least 95% of its full-time employees and their dependents.[113] Also, an ALE may be subject to an ESRP penalty if the ALE fails to offer coverage that is affordable or that satisfies the minimum value standard.[114] The ESRP penalties will be assessed only if at least one full-time employee receives a premium tax credit through a marketplace exchange during the relevant year.[115] The IRS may assess ESRP penalties up to six years after the time in which the ALE is required to file information reports with the IRS.[116]

The due diligence team should request that the target provide an employee census or other information to determine whether the target company is an ALE. Additionally, the due diligence team should request copies of Forms 1094-C (discussed below), summaries of benefits and coverage, and other documents to determine whether the target company may be subject to exposure for potential ESRP penalties for failing to offer minimum essential coverage to at least 95% of its full-time employees or

---

[109] *26 U.S.C. § 125(b)(1)*.

[110] *26 U.S.C. § 4980H(c)(2)(A)*.

[111] ABA Joint Committee on Employee Benefits, meeting with IRS and Treasury officials, Q/A-24 (May 9, 2014) (as visited Aug. 14, 2025).

[112] *26 U.S.C. § 4980H(c)(2)(E)*.

[113] *26 U.S.C. § 4980H(a)*.

[114] *26 U.S.C. § 4980H(b)*.

[115] *26 U.S.C. §§ 4980H(a)*, *4980H(b)*.

[116] *26 U.S.C. § 6051(n)*.

failing to provide coverage that is affordable or meets the minimum value standard. If the buyer assumes the target company's health plan or otherwise continues the target company's operations, it may be subject to the IRS's six-year lookback into the assessment of ESRP penalties.

[ii] Consolidated Omnibus Budget Reconciliation Act

Congress enacted the Consolidated Omnibus Budget Reconciliation Act ("COBRA") to provide employees and beneficiaries with the opportunity to continue their health plan coverage when they lose it under certain circumstances (e.g., termination from employment). Coverage generally continues for eighteen months after the event which caused the employee or beneficiary to lose coverage.[117]

An employer must comply with COBRA if it sponsors a health plan and employed at least twenty employees in the prior year.[118] COBRA requires employers to provide employees and beneficiaries notices regarding their rights to elect COBRA.[119]

The due diligence team should request that the target company provide copies of its COBRA notices and a list of individuals that are currently receiving or are eligible to receive COBRA continuations coverage, with the date when COBRA continuation began or will begin, if elected. Once the due diligence team receives this information it can assess any potential exposure for noncompliance with COBRA in general, as well as noncompliance with the notification requirements. Furthermore, in the case of a target company with a self-funded health plan, the due diligence team may assess potential future claims exposure if it continues the target company's health plan.

[iii] Health Insurance Portability and Accountability Act

Congress enacted the Health Insurance Portability and Accountability Act ("HIPAA") to protect patient health information. HIPPA contains privacy laws which prevent health plans from using or sharing protected health information unless authorized to do so by the patient or HIPAA.[120] Employers with fully-insured health plans rely on the health insurance carrier to comply with HIPAA. Employers with self-funded health plans must ensure their plan complies with HIPAA by incorporating a HIPAA compliance program. A HIPAA compliance program involves distributing a HIPAA notice of privacy practices, conducting HIPAA training, and adopting HIPAA policies and procedures.[121]

Additionally, HIPAA generally prohibits group health plans from using health factors to discriminate among individuals as to eligibility for benefits, premiums, or contributions.[122] The term "health factor" means any of the following: health status, medical condition, claims experience, receipt of health care, medical history, genetic information, evidence of insurability, or disability.[123] Under HIPAA, a health plan cannot impose different coinsurance, deductible, copayment, or employee contribution requirements based on the presence or absence of a health factor. For example, requiring an individual with diabetes to pay a higher deductible than an individual without diabetes.

---

[117] *26 U.S.C. § 4980B(f)(2)(B)(i)*.

[118] *26 U.S.C. § 4980B(d)(1)*. Many states (e.g., California and New York) have their own "mini-COBRA" laws that require employers with less than twenty employees to offer continuation coverage. These "mini-COBRA" laws are beyond the scope of this chapter.

[119] *26 U.S.C. § 4980B(f)(6)*.

[120] Title 45 C.F.R. Parts 160 and 164.

[121] *45 C.F.R. §§ 164.520*, *164.530(b)*, *164.530(i)*.

[122] *29 U.S.C. § 1182*.

[123] *29 C.F.R. § 2590.702(a)(1)*.

The due diligence team should request that the target company provide copies of its health plan documents, including policies, summaries of benefits and coverage, evidences of coverage, and summary plan descriptions. As part of its due diligence, the due diligence team should review the documents to determine whether the target company's health plans are discriminatory. The DOL or IRS may assess penalties for HIPAA noncompliance.[124]

[iv] Mental Health Parity and Addiction Equity Act

Congress enacted the Mental Health Parity and Addiction Equity Act ("MHPAEA") to prevent group health plans from providing mental health benefits in a manner that is less favorable than other benefits. Specifically, health plans must have parity between their mental health and substance use disorder benefits and their medical/surgical benefits with respect to two types of treatment limitations – quantitative treatment limitations (*e.g.*, the number of office visits covered by the plan) and nonquantitative treatment limitations (*e.g.*, pre-authorization requirements).[125]

In 2020, Congress amended MHPAEA, requiring plans to conduct a comparative analysis of their nonquantitative treatment limitations.[126] Employers with fully-insured health plans rely on the health insurance carrier to conduct the comparative analysis and comply with MHPAEA. Employers with self-funded health plans must engage a vendor to conduct the comparative analysis and evaluate compliance with MHPAEA.

If the target maintains a self-funded health plan, the due diligence team should request that the target company provide a copy of its comparative analysis to assess compliance with MHPAEA.

[e] Common Issues Arising from Target Company Welfare Plans

[i] Introduction

This section examines issues that frequently arise during the due diligence review of a target company's welfare plans and identifies strategies to address them.

[ii] Plan Funding

The due diligence team should request that the target company provide a list of welfare plans that are self-funded. Generally, the target company will be paying benefit claims for its self-funded welfare benefits from its general assets and assuming the risk that claims for a given year will be higher or lower than projected. The due diligence team should request a copy of the stop-loss policy, third-party administrative services agreement, and financial information about the self-funded plan, such as actual versus budgeted claims history and a report of the plan's incurred but not reported (IBNR) claims. IBNR claims are estimated claims that have occurred but have not been disclosed to the plan. The IBNR analysis provides crucial information about expected future claims costs.

The due diligence team should review these documents to assess the potential financial exposure for claims in the event it assumes the target company's self-funded welfare plan.

[iii] Code 105(h) Compliance

If the target company maintains a self-funded health plan, it must ensure that the plan provides benefits in a manner that does not treat highly compensated individuals more favorably than individuals who are not highly compensated.[127] The Code prohibits discrimination in favor of highly compensated

---

[124] *26 U.S.C. § 4980D*.

[125] *29 C.F.R. § 2590.712(c)*.

[126] Consolidated Appropriations Act, 2021 (CAA, 2021), ***Pub. L. No. 116-260***, Div. BB, §203 (2020).

individuals both as to eligibility and as to the benefits that are provided.[128] If the IRS discovers upon audit that the target company's self-funded health plan fails to comply with Code Section 105(h), it may determine that reimbursements to highly compensated individuals under the health plan must be included in the individual's taxable income and may do so for the maximum statute-of-limitations period (generally three years).[129]

The due diligence team should request a copy of the target company's 105(h) nondiscrimination testing results for any of its self-funded health plans. If the IRS ultimately reclassifies reimbursements to highly compensated employees as taxable income after the buyer assumes the target company's self-funded health plan, the buyer must issue corrected W-2s for all affected employees and may be subject to withholding and payroll tax payments on the reclassified income.

[iv] Code Section 125 Compliance

The target company must maintain a signed, written cafeteria plan document if it allows employees to make pre-tax contributions toward their benefit plans.[130] If the IRS discovers upon audit that the target company has failed to maintain a written plan document, the IRS may reclassify all employees' pre-tax contributions as taxable compensation and may do so for the maximum statute-of-limitations period (generally three years).[131] Furthermore, the target company must conduct annual compliance testing to ensure that the plan complies with Code Section 125 nondiscrimination requirements.[132] If the IRS found the cafeteria plan to be discriminatory, highly compensated individuals would lose the favorable tax treatment of their contributions.

The due diligence team should request a copy of the target company's cafeteria plan document and cafeteria plan nondiscrimination testing results. If the IRS reclassifies employees' pre-tax contributions as taxable income after the buyer assumes the target company's cafeteria plan, the buyer must issue corrected W-2s for all affected employees and may be subject to withholding and payroll tax payments on the reclassified income.

[v] ACA Reporting

Under the ACA, every ALE (or a member of an aggregated group that is determined to be an ALE) must provide full-time employees a written statement by January 31 following the calendar year to which the statement relates.[133] The ALE is automatically granted a thirty-day extension.[134] Additionally, the ALE must file with the IRS an information return and a transmittal by February 28 (March 31 if filed

---

[127] *26 U.S.C. § 105(h)*.

[128] *26 U.S.C. § 105(h)(3)*, *(4)*. The nondiscrimination tests are complicated. However, even without testing, the due diligence team may be able to discover an inherent discrimination issue if, for example, the self-funded health plan is available only to the executives of the target company.

[129] *26 U.S. C. § 6501*.

[130] *26 U.S.C. § 125(a)*.

[131] *26 U.S. C. § 6501*.

[132] *26 U.S.C. § 125(b)(1)*.

[133] *26 C.F.R. § 301.6056-1(g)*.

[134] *26 C.F.R. § 301.6056-1(g)*.

electronically) of the year following the calendar year to which it relates.[135] All employers use Form 1094-C and Form 1095-C to satisfy these reporting requirements.

An employer with a health plan that provides minimum essential coverage to an individual during a calendar year is required to provide a written statement to the responsible individual identified on the return by January 31 following the calendar year that coverage was provided.[136] The employer is automatically granted a thirty-day extension.[137] Additionally, the employer must file with the IRS an information return and a transmittal by February 28 (March 31 if filed electronically) following the calendar year that coverage was provided.[138] If the employer is an ALE that offers self-funded health coverage, the employer uses Form 1094-C and Form 1095-C, Part III to satisfy these reporting requirements. If the employer is an ALE that offers fully-insured health coverage, the employer uses Form 1094-B and Form 1095-C.

The Code imposes a penalty for failing to timely provide ACA forms to individuals[139] or failing to file ACA forms with the IRS.[140] The IRS may also assess penalties if the ACA forms contain errors.[141]

The due diligence team should request that the target company provide copies of the ACA forms provided to individuals and filed with the IRS to confirm that the target company has satisfied its ACA reporting obligations, if applicable. If the buyer assumes the target company's health plan or otherwise continues the target company's operations, it may be subject to an assessment of IRS penalties for the failure to furnish or file ACA forms.

[vi] Annual Reporting

Generally, all welfare benefit plans subject to ERISA that cover at least 100 participants must file an annual report called a Form 5500 with the DOL and IRS.[142] The Form 5500 reports information about the plan including the type of plan and plan features, plan funding, the number of participants as well as financial information such as the amount of fees, premiums and compensation paid to brokers, third-party administrators, and insurance carriers.

The plan must file the Form 5500 within 210 days after the end of the plan year unless it requests a two-and-a-half-month extension by filing Form 5558.[143] The DOL and IRS may assess penalties for failing to file the Form 5500 or for filing the Form 5500 with incorrect or incomplete information.

The due diligence team should request that the target company provide the Forms 5500 filed for its health and welfare plans to review the target company's compliance obligations for annual reporting.

[f] Welfare Plan Diligence Impact on Transaction

---

[135] *Id.* at § 301.6056-1(e).

[136] *26 C.F.R. § 1.6055-1(g)(4)*.

[137] *26 C.F.R. § 1.6055-1(g)(4)*.

[138] *26 C.F.R § 1.6055-1(f)*.

[139] *26 U.S.C. §§ 6722*, ***6724(d)***.

[140] *26 U.S.C. §§ 6721*, ***6724(d)***.

[141] *26 U.S.C. § 6721(a)(2)(B)*.

[142] *See* DOL, 2024 Instructions for Form 5500, p. 3, *available at*, *>https://www.dol.gov/sites/dolgov/files/ebsa/employers-and-advisers/plan-administration-and-compliance/reporting-and-filing/form-5500/2024-instructions.pdf* (last accessed Aug. 13, 2025).

[143] *29 U.S. C. § 1024(a)(1)*; *26 C.F.R. § 1.6081.11(a)*.

From a business perspective, the due diligence team should analyze any of the target company's self-funded welfare plans to determine financial exposure from future benefits claims. Additionally, the due diligence team should evaluate the impact resulting from either continuing the target company's welfare plans after closing or making the buyer's welfare plans available to the target company's employees. Often, the buyer's internal human resources and benefits team will be involved in the business aspect of evaluating the target company's welfare plans.

The due diligence team should analyze the target company's welfare plans to determine whether the target company and buyer may have exposure resulting from statutory and regulatory noncompliance. Primarily, welfare plans provide employees with a variety of benefits that are meant to provide tax advantages to the employees. Much of the risk arising from welfare plan noncompliance results in reclassification of benefit payments as taxable income to employees and impacts the buyer from an employee-relations context.

Another risk arising from welfare plan noncompliance comes from potential penalty assessments by governmental agencies. An agency will discover a noncompliance issue either from an investigation or from self-reporting by the employer which makes penalty assessment risk highly speculative. Often, if a noncompliance issue is discovered in the due diligence process, the buyer will require the target company to correct the issue prior to closing, if possible. When the issue cannot be corrected, the buyer should evaluate terminating the welfare plan and transitioning the target company's employees onto its own welfare plans.

[4] Executive Compensation Diligence

[a] Introduction

This section identifies various executive compensation arrangements that require scrutiny during the due diligence process. This section examines equity awards, nonqualified deferred compensation, and golden parachute payments.

[b] Equity Award Considerations

[i] Introduction

Equity incentive awards are a key component of executive and employee compensation in most public and privately held companies. The types of awards that may be issued by a target company may consist of stock options, restricted stock, restricted stock units, SARs, phantom equity, and/or profits interests. Buyers will want to conduct due diligence of a target company's equity incentive compensation program to identify potential liabilities, to ensure the desired treatment of the awards in the transaction is consistent with the contractual requirements of the award, to ensure legal and tax compliance, and to address post-acquisition incentive and retention strategies.

[ii] Equity Plan Documentation

Equity incentive awards are contractual arrangements between the target company and its employees or other service providers. As such, their terms and conditions govern the rights, obligations, and potential outcomes for award holders in connection with a transaction. Terms governing an equity incentive award are typically set forth in the applicable equity incentive plan and corresponding award agreement. However, other arrangements – such as employment agreements, retention agreements, severance plans or change-in-control programs – may contain provisions that override or supplement those terms.

Typically, the equity plan documentation includes provisions addressing how the equity award will or may be treated in the event of a change control. The definition of a "change in control" must be carefully reviewed to ensure the consummation of the anticipated transaction will fit within the definition.

[iii] Treatment Alternatives

There are various ways in which equity incentive awards may be treated in connection with an M&A transaction. The following are the most common:

- Assumption: Buyer assumes the equity incentive awards and the awards are converted into awards of the buyer. Terms and conditions of the award, including vesting and payment dates, generally remain unchanged.
- Substitution: Buyer substitutes the target company's equity incentive awards for awards granted under the buyer's equity compensation program. The terms and conditions of the award are often modified, but are generally intended to be economically equivalent to the original award.
- Cash-Out: Equity incentive awards are cancelled in exchange for a cash payment based on the deal consideration. For example, stock options that are "in-the-money," or have an exercise price below the deal consideration, would receive cash in respect of each option equal to the difference between the per-share deal consideration and exercise price.
- Acceleration: Vesting of outstanding and unvested awards are accelerated either upon the occurrence of the change-in-control event or upon a qualifying termination of employment following the occurrence of a change-in-control.
- Cancellation: In some cases, outstanding equity awards may be cancelled for no consideration. This is most likely to occur for stock options (or other similar appreciation awards) that are "out-of-the-money" (e.g., an award with an exercise price above the consideration received by shareholders).

[iv] Tax and Legal Compliance

Equity incentive awards are subject to various tax and legal requirements, which should be reviewed in connection with the transaction. Equity incentive awards must be reviewed in connection with the transaction to ensure they either comply with or are exempt from the requirements of *Section 409A of the Internal Revenue Code* ("Section 409A"), and that the intended treatment of such awards in the transaction is consistent with the Section 409A requirements.[144] How the equity incentive awards are treated in the transaction can have an impact on whether the so-called "golden parachute rules" of *Section 280 of the Internal Revenue Code* ("Section 280G") are triggered.[145] As part of due diligence, equity incentive awards must be reviewed to determine whether they have been properly registered under the Securities Act of 1933 or qualify for an applicable exemption from registration.

[v] Retention

The treatment of outstanding equity awards in the transaction can have a significant impact on the go-forward retention of senior management. First, assumed or substituted awards could provide significant retentive value during the period in which the awards are unvested. However, since these awards were originally designed by the target company they may not fully align with the buyer's desired incentive or retention strategy. Second, certain executives whose awards are cashed-out or have accelerated vesting may experience a considerable windfall in connection with the transaction. These executives may have less of an incentive to remain with the business unless a thoughtfully designed executive compensation program is implemented.

[c] Nonqualified Deferred Compensation Plans

---

144 Section 409A is discussed in more detail in Section [1][c][ii][C], below.

145 Section 280G is discussed in more detail in Section [1][c][iii], below.

[i] Introduction

Nonqualified deferred compensation (NQDC) plans are contractual entitlements that allow employees, directors, or independent contractors to defer compensation to a future date, which could include a fixed date, separation from service, or a change in control. These plans are typically unfunded and exempt from many of the requirements of qualified retirement plans, but they must be carefully reviewed to ensure compliance with Section 409A. Identifying and addressing potential 409A violations is critical to avoid potentially significant adverse tax consequences for affected employees or service providers and mitigate risks for the buyer.

[ii] Types of Nonqualified Deferred Compensation Plans

There are several types of NQDC plans. A sample list of plan types of is as follows:

- Elective Deferral Plans: A type of plan whereby eligible employees voluntarily defer a portion of their salary, bonus, or other compensation to a later date.
- Excess Benefit Plans: A type of plan intended to provide benefits to employees relating limits on qualified plans under *Internal Revenue Code Sections 415* and *401(a)(17)*.
- Phantom Stock Plans: A type of equity-based plan that provides employees with the right to receive a cash payment equal to the value of the company's stock, without granting actual equity.

[iii] Unfunded in Nature

Nonqualified deferred compensation is not subject to income tax until it is paid to the participant, provided that the arrangement is unfunded and the participant's rights are subject to the claims of the target company's general creditors.[146] Similarly, a NQDC plan will not be subject to Title I of ERISA, including the nondiscrimination and vesting requirements, unless it is an unfunded plan for the benefit of a select group of management or highly compensated employees.[147] Often times, nonqualified benefits are not set aside in any manner. When the payments become due, they will be paid from the target company's general assets.

Sometimes, so-called "rabbi trusts" are used to pay nonqualified deferred compensation benefits. Funds placed in a rabbi trust remain subject to the claims of the target company's general creditors to preserve the plan's unfunded status for tax and ERISA purposes. However, the funds placed into a rabbi trust cannot be used for the general operations of the target company. By formally setting aside assets in a trust to pay plan benefits, a rabbi trust provides a strong level of assurance for participants that their nonqualified deferred compensation will be paid as promised.

Since NQDC arrangements are unfunded, the buyer should review all such arrangements as part of due diligence to understand the potential liabilities and ensure they are appropriately taken into account in the purchase price or any related purchase price adjustments. Furthermore, a buyer will want to review any funding obligations to a rabbi-trust, particularly those that may be triggered or accelerated in connection with a change in control, to assess potential liabilities, cash flow impacts and compliance with applicable tax and ERISA requirements.

[iv] Section 409A of the Internal Revenue Code

Section 409A of the Internal Revenue Code governs the taxation of nonqualified deferred compensation plans. Nonqualified deferred compensation is defined very broadly, and unless a specific exemption applies, is generally defined to include any deferral of compensation from the year in which the related services are performed to a subsequent year.[148] The term "plan" is also broadly defined to

---

[146] Sproull v. Commissioner, 416 T.C. 244 (1951), aff'd, ***194 F.2d 541 (6th Cir. 1952)***; *Rev. Rul. 60-31*.

[147] *ERISA §§ 201(2)*, *301(3)*, and *401(a)(1)*.

include any agreement, arrangement, plan or program with a single employee, independent contractor or other service provider.[149] Accordingly, the types of compensation arrangements which may constitute a "nonqualified deferred compensation plan" subject to Section 409A is expansive, and may include employment agreements, retention and change in control agreements, equity awards, and traditional deferred compensation plans.

Section 409A regulates nonqualified deferred compensation plans by imposing strict rules on how the plan must be structured. Section 409A includes rules relating to the following:[150]

- Initial deferral elections – must generally be made before the start of the year in which services are performed (with limited exceptions for new hires, performance-based compensation and certain short-term deferrals).[151]
- Timing of payments – payments can only be made upon certain permissible payment events, such as a separation from service, specified time or schedule, change in control, death, disability or an unforeseen emergency.[152]
- Subsequent deferrals – the ability to subsequently defer compensation once a payment date or schedule is set is limited. Any subsequent deferral generally must be elected at least 12-months before the original payment date and be delayed by at least five years from the original date.[153]
- Prohibition on acceleration – the ability to accelerate compensation after the initial deferral election is generally prohibited.[154] However, there may be an opportunity for plan termination and benefit distributions in connection with a "change in control" that would not otherwise be available.[155]
- Six-month delay for specified employees – for public companies, payments on separation from service to "specified employees" must be delayed at least six months.[156]

Section 409A requires both documentary and operational compliance. In the event of a 409A violation, generally, the employee or service provider will be immediately taxed on the value of their outstanding deferred compensation once the benefit is no longer subject to a substantial risk of forfeiture. Additionally, the participant will incur a 20% excise tax on the amount that is required to be included in his or her income, as well as an interest penalty.[157] The interest penalty is calculated at the federal unemployment rate plus one percent, to the extent that the amount being taxed currently would have been taxable in the year first deferred or, if later, when the substantial risk of forfeiture expired.[158] While

---

[148] *Treas. Reg. §1.409A-1(b)(1)*.

[149] *Treas. Reg. §1.409A-1(c)(1)*.

[150] The requirements of Section 409A are expansive and technical and beyond the scope of this book.

[151] *Treas. Reg. §1.409A-2(a)(3)*.

[152] *Treas. Reg. §1.409A-3(a)*.

[153] *Treas. Reg. §1.409A-2(b)*.

[154] *Treas. Reg. §1.409A-3(j)*.

[155] *Treas. Reg. §1.409A-3(j)(4)(ix)(B)*.

[156] *Treas. Reg. §1.409A-1(c)(3)(v)*.

[157] *IRC § 409A(a)(1)(B)(i)*.

the failure to comply with Section 409A generally results in significant adverse tax consequences to the participant, the employer may be subject to withholding and reporting obligations.

Due diligence should include identifying all nonqualified deferred compensation plans – including employment agreements, severance plans, equity awards, and bonus plans – to confirm the definitions, payment triggers, and election provisions are compliant with or exempt from the requirements of Section 409A, and identifying any documentary and operational failures that may require correction.[159] For any nonqualified deferred compensation plans that have a "change in control" as a payment trigger, particular attention should be paid to whether the definition in the plan satisfies the requirements of Section 409A. Finally, the buyer will likely want to understand its rights to amend or terminate a nonqualified deferred compensation plan following the closing of the transaction.

[d] Golden Parachute Payments

[i] Introduction

Sections 280G and *4999 of the Internal Revenue Code* (the "Golden Parachute Rules") disallow a corporate tax deduction for "excess parachute payments" made to certain officers, highly compensated individuals and greater than 1% shareholders in connection with a change in control of a corporation.[160] The Golden Parachute Rules impose a 20% excise tax on the recipient.[161] These provisions can result in an increase of transaction costs and, if not addressed pre-closing, may create unexpected liabilities for both the target company and the buyer.

[ii] Key Concepts

The following are key concepts of the Golden Parachute Rules:

- Disqualified Individuals: Any employee, independent contractor, or other service provider who is an officer, highly compensated individual, or 1% shareholder of the corporation, determined on a controlled group basis.[162]
- Parachute Payments: Compensatory payments made to a disqualified individual that is contingent on the change in control with an aggregate present value equal to or exceeding three times the individuals "base amount" (described below).[163]
- Excess Parachute Payments: The amount by which parachute payments exceed one times the disqualified individual's base amount.[164]
- Change in Control: A change in "ownership"[165] or "effective control"[166] of a corporation, or a change in the ownership of a "substantial portion"[167] of the assets of corporation.

---

[158] *IRC § 409A(a)(1)(B)(ii)*.

[159] Correction may be available under *IRS Notice 2010-6* for 409A documentary errors and under *IRS Notice 2008-113* for 409A operational errors.

[160] *IRC § 280G(a)*.

[161] *IRC § 4999(a)*.

[162] *IRC § 280G(c)*, *Treas. Reg. §1.280G-1 Q&A 15*.

[163] *IRC § 280G(b)(2)*; *Treas. Reg. §1.280G-1 Q&A 2*.

[164] *IRC § 280G(b)(1)*; *Treas. Reg. §1.280G-1 Q&A 2*.

[165] *Treas. Reg. §1.280G-1 Q&A 27*.

[iii] Payments Continent on a Change in Control

The only compensatory payments that are considered for purposes of the Golden Parachute Rules are those that are contingent on a change in control.[168] In general, a payment is treated as continent on a change in control if the payment would not, in fact, have been made had no change in control occurred, even if the payment is also conditioned on the occurrence of another event.[169] Payments that become vested or accelerated in connection with a change in control are considered contingent on the change in control.[170] A payment also is considered contingent on the change in control if (i) the payment is contingent on an event that is closely associated with a change in control, (ii) a change in control actually occurs, and (iii) the event is materially related to the change in control.[171] The termination of a disqualified individual's employment is one of the examples included in the regulations as an event closely associated with a change in control.[172] There is a rebuttable presumption that an event is considered materially related to the change in control if occurs during the period beginning one-year prior and ending one year after the date of the change in control.[173]

In connection with due diligence, the buyer will need to carefully examine the target company's compensation program to identify payments or benefits that may be made to disqualified individuals which could implicate the Golden Parachute Rules.

Examples of compensatory payments that are commonly taken into account for purposes of the Golden Parachute Rules include:

- Severance payments;
- Change-in-control bonus payments made in connection with the transaction;
- The value associated with the acceleration of stock options, restricted stock awards, and other equity-based awards in connection the transaction; and
- Retention bonuses, post-closing equity awards, new compensation and other arrangements entered into in connection with the transaction.

If the present value of compensatory payments that are contingent on a change in control exceed three-times the disqualified individual's base amount, then such payments are referred to as parachute payments. The disqualified individual's base amount is generally the individual's average annual compensation from the corporation for the most recent five taxable years preceding the taxable year in which the change in control occurs. The individual's parachute payments that exceed one-times the individual's base amount is an excess parachute payment and subject to the 20% excise tax and loss of deduction.

[iv] Mitigation Strategies

Private companies may avoid the impact of the Golden Parachute Rules with a shareholder vote to approve compensatory payments and benefits. If shareholders representing more than 75% of the

---

[166] *Treas. Reg. §1.280G-1 Q&A 28*.

[167] *Treas. Reg. §1.280G-1 Q&A 29*.

[168] Treas. Reg. §1.280G–1 Q&A 2.

[169] Treas. Reg. §1.280G–1 Q&A 22.

[170] Treas. Reg. §1.280G–1 Q&A 22(a), (c).

[171] Treas. Reg. §1.280G–1 Q&A 22(b)(1).

[172] Treas. Reg. §1.280G–1 Q&A 22(b)(2).

[173] Treas. Reg. §1.280G–1 Q&A 22(b)(3).

voting power of all outstanding stock of the corporation immediately prior to the transaction approve the compensation and benefits submitted to the vote and such shareholders were provided with adequate disclosure of the payments, such payments will not be considered parachute payments for purposes of the Golden Parachute Rules. Adequate disclosure requires disclosure of the material facts concerning all material payments which would be parachute payments with respect to the disqualified individual. Material facts include, but are not limited to, the event triggering the payment or payments, the total amount of the payments that would be parachute payments if the shareholder approval requirements are not met, and a brief description of each payment. The shareholder vote must determine the disqualified individual's right to receive or retain the payment.

The Golden Parachute Rules provide other opportunities to avoid or reduce the amount of potential excess parachute payments. For example, payments characterized as reasonable compensation for services to be rendered on or after the change in control are not considered parachute payments. The buyer and target company are often aligned in mitigating potential exposure to Section 280G and planning, particularly for public companies, often occurs well in advance of the date of the transaction.

§ 7.02 Labor and Employment Due Diligence

[1] Employment Practices Due Diligence

[a] Overview

A thorough review of the target company's employment practices is a critical component of due diligence. This chapter outlines key aspects of the target company's employment practices, including those concerning health and safety matters, that the due diligence team should evaluate to identify potential risks, liabilities, and integration challenges related to a target company's workforce.

In order to effectively conduct due diligence related to labor and employment matters, the due diligence team must first gain an understanding of the composition of the target company's workforce and its employment practices related thereto. Although there are some compliance issues relevant to generally all workforces, which are outlined in this section, the composition of the target company's workforce will drive some of the specific employment practices that the due diligence team needs to explore in greater detail relevant to a particular transaction. Accordingly, a key first step for the due diligence team is to obtain information on the makeup of the target company's workforce and to determine what employment practices are implicated directly as a result. For instance, the due diligence team should gain an understanding of where the target company has employees,[174] its use of third-party labor, and its obligations to any unions or under any federal grants or contracts.[175] The due diligence team can accomplish this through its initial requests for information to the target company and should request employee and independent contractor censuses early on to assist with these initial efforts.

Many employers also use professional employer organizations ("PEOs"), to handle various Human Resources, payroll, and benefits functions. Learning whether the target company uses a PEO, and obtaining and reviewing a copy of the target company's agreement with its PEO can help with the due diligence team's assessment. While use of a PEO alone is not determinative of a target company's compliance with applicable employment laws, it suggests that the target company has taken steps to engage external support in managing its workforce-related obligations. The presence of a PEO can provide an additional layer of infrastructure to assist the target company in navigating the complex landscape of federal, state, and local employment laws.

[b] Union Employees & Collective Bargaining Agreements

---

[174] The work location of the target company's employees directly implicates the state and local laws that the due diligence team must consider in its analysis of the target company's employment practices. This chapter generally discusses different issues that may arise under applicable state and local laws and includes illustrative examples from specific jurisdictions. These examples are not intended to be exhaustive, and similar issues may exist in many other states or localities.

[175] Federal contractors have additional obligations under applicable federal laws, regulations, and Executive Orders, some of which are briefly identified in this chapter. *See, e.g.,* U.S. Dep't of Lab., *Federal Contractor Requirements*, *https://www.employer.gov/federal-contractor-requirements/* (last accessed August 29, 2025). If the due diligence team learns that the target company is a federal contractor, it should incorporate an assessment of additional obligations applicable to federal contractors into its review of each of the below areas, including, without limitation, those related to diversity, equity, and inclusion; paid sick leave; and the use of E-Verify.

First, this subsection of the chapter briefly reviews considerations for the due diligence team in the event that the target company has union employees or is subject to a collective bargaining agreement. As noted above, the due diligence team should tailor its initial requests for information to gain an understanding of the composition of the target company's workforce. This includes whether the target company has union employees or is a party to any collective bargaining agreement ("CBA") to determine if labor-related matters will be a larger part of the due diligence for the particular transaction. Depending in part on the complexity of the labor issues involved, a labor specialist may offer further advice and counsel as well.

However, even if the target company does not currently have unionized workers, the due diligence team should seek a more fulsome picture of the target company's history in relation to unionized labor and labor matters. For instance, the due diligence team should inquire about any efforts by the workforce to unionize. Such information may suggest that the workforce may seek to unionize in the future. It may also signal that the due diligence team must conduct further due diligence to understand the efforts made to unionize and what transpired as a result. The due diligence team should also confirm whether the target company has experienced any actual or threatened unfair labor practice charges. Nonunionized employees can file unfair labor practice charges with the National Labor Relations Board ("NLRB").[176] Accordingly, simply confirming that a target company does not currently have unionized employees fails to provide a complete picture in terms of potential issues and liabilities that the target company may have experienced or could experience in relation to labor matters. With these efforts, the due diligence team is seeking to rule out any matters that may require further review.

When conducting due diligence on a target company with union employees or that is subject to a CBA, it is critical to evaluate all labor-related obligations to which the target company is subject. The due diligence team should obtain a list of unionized workers. For those workers, the terms of the CBA will likely govern other areas of employment-related due diligence, such as concerning wage and hour compliance and employment policies discussed below.[177] In other words, rather than just assessing compliance with certain federal, state, or local laws as to those workers, the due diligence team may assess compliance with the terms of the CBA. The due diligence team should also therefore obtain a copy of and review all CBAs to which the target company is subject, including key provisions, such as their expiration dates, wage and benefit provisions, grievance procedures, and any clauses related to successorship or obligations upon change of ownership. The due diligence team should also look for any atypical or nonstandard provisions included in the CBAs. Such provisions may present compliance concerns for after consummation of the transaction.

Beyond analyzing the CBAs, the due diligence team must also assess any grievances or charges threatened or filed against the target company. Accordingly, the due diligence team should once again request and examine documentation related to arbitration or grievance proceedings and any complaints filed with applicable agencies, such as the NLRB. Depending on the information obtained and uncovered as a result of reviewing any operative CBAs and other information supplied by the target company on labor matters, the due diligence team may need to conduct further due diligence on issues unique to the target company's workforce.

[c] Wage and Hour Due Diligence

[i] Overview of Applicable Law

Second, this subsection of the chapter discusses the due diligence team's assessment of the target company's compliance with applicable federal, state, and local wage and hour laws as part of the due diligence process.

---

[176] *See* 29 U.S.C. §§158, 160.

[177] *See, e.g.,* 29 C.F.R. § 541.4.

The Fair Labor Standards Act ("FLSA") is a United States federal law that requires employers to provide to covered employees a minimum wage and overtime compensation.[178] The federal minimum wage for covered nonexempt employees under the FLSA is currently $7.25 per hour.[179] The overtime pay requirement for covered nonexempt employees under the FLSA is one and one half times the employee's regular rate of pay for all hours worked in excess of 40 hours in a workweek.[180] Multiple states and some localities in the United States also have their own wage and hour laws that impose similar or additional requirements to the FLSA. For instance, some states and localities have adopted their own minimum wages that are higher than that required under the FLSA,[181] and some states and localities have adopted additional overtime pay requirements from those imposed by the FLSA, such as daily overtime pay.[182]

All employee positions are classified as either "exempt" or "nonexempt" from these requirements imposed by the FLSA and applicable wage and hour laws. Common exemptions recognized under the FLSA are for executive, administrative, professional, computer, and outside sales employees.[183] To qualify for one of these exemptions under the FLSA, an employee position must typically satisfy both a salary test and a duties test. [184] To satisfy the salary test, the employee position must generally receive compensation on a salary basis at a rate of not less than $684 per week or $35,568 per year.[185] However, there are some exceptions to this general salary basis requirement for particular exemptions. For instance, the computer employee exemption allows for positions compensated either on a salary or hourly basis to qualify.[186]

To satisfy the duties test, the position's "primary duty" must involve the performance of certain work defined specifically for each exemption. For instance, to qualify for the executive employee exemption (1) the position's primary duty must include managing the enterprise, or managing a customarily recognized department or subdivision of the enterprise; (2) the employee must customarily and regularly direct the work of at least two or more other full-time employees or their equivalent; and (3) the employee must have the authority to hire or fire other employees, or the employee's suggestions and recommendations as to the hiring, firing, advancement, promotion or any other change of status of other employees must be given particular weight.[187] To qualify for the administrative employee exemption (1) the employee's primary duty must be the performance of office or non-manual work

---

[178] *See* *29 U.S.C. § 201 et seq.*

[179] *29 U.S.C. § 206*.

[180] *29 U.S.C. § 207*.

[181] Approximately 30 states, D.C., Guam, Puerto Rico, and the Virgin Islands impose higher minimum wages than the FLSA. *See* U.S. Dep't of Lab., *Consolidated Minimum Wage Table*, *https://www.dol.gov/agencies/whd/mw-consolidated* (rev. Jan. 1, 2025).

[182] *See, e.g., Cal Lab. Code § 510*.

[183] *See* *29 U.S.C. § 213*.

[184] *See* U.S. Dep't of Lab., *Fact Sheet #17A: Exemption for Executive, Administrative, Professional, Computer & Outside Sales Employees Under the Fair Labor Standards Act (FLSA)*, *https://www.dol.gov/agencies/whd/fact-sheets/17a-overtime* (rev. Sept. 2019).

[185] In April 2024, the U.S. Department of Labor issued a final rule increasing the salary threshold required to satisfy the salary basis test and qualify for an exemption under the FLSA; however, the U.S. District Court for the Eastern District of Texas vacated this rule. Some state and local wage and hour laws impose greater salary thresholds for an employee position to qualify for an exemption under their laws.

[186] *See* *29 C.F.R. § 541.400*.

[187] *See* *29 C.F.R. § 541.100*.

directly related to the management or general business operations of the employer or the employer's customers; and (2) the employee's primary duty includes the exercise of discretion and independent judgment with respect to matters of significance.[188]

The FLSA also recognizes an exemption for highly compensated employees, under which the employee position must satisfy a heightened salary test but then is subject to a less stringent duties test. For instance, the position must receive compensation on a salary basis of not less than $107,432, the position's primary duty must include performing office or non-manual work, and the employee must customarily and regularly perform at least one of the exempt duties of the exempt executive, administrative, or professional employee.[189] Please note that not all state and local wage and hour laws recognize the same exemptions as those recognized under the FLSA, and, even those that do, may impose different requirements for a position to qualify for an exemption, such as the salary threshold involved to satisfy the applicable salary test or the primary duties required to satisfy the duties test. Accordingly, for an employer to classify a position as exempt under the FLSA, state, and local wage and hour laws, the position must satisfy all of the requirements to qualify for an exemption under each set of applicable laws.

Failure to comply with the FLSA and applicable state and local wage and hour laws may result in liabilities for unpaid wages, liquidated damages, and attorneys' fees and costs, as well as civil and criminal penalties, depending on the nature of the violation.[190]

[ii] Employee Classification Issues

The due diligence team must analyze the target company's classification of its employees as either exempt or nonexempt under the FLSA and applicable state wage and hour laws, and, for those nonexempt employees, assess whether the target company has acted in compliance with applicable minimum wage and overtime pay requirements thereunder. If a target company is not acting in compliance with applicable wage and hours, liability for unpaid wages, including unpaid overtime compensation, may rise to a material issue.

To conduct this analysis, the due diligence team must first obtain information on how the target company classifies each employee position. Typically, the due diligence team will want to request classification information on any employee census provided by the target company, along with other details of each employee's employment that will aid the due diligence process, including the employee's name or unique identifier, job title, department, date of birth or age, hire date, work location (city and state), annual base compensation or rate of pay, and incentive compensation. Individual offer letters or employment agreements also often disclose job classification information. In addition to learning the classification of employee positions, it is often helpful for the due diligence team to gain an understanding as to how the target company determined that classification. For instance, the due diligence team may ask whether the target company consults with legal counsel when classifying employee positions or if it did so with respect to any particular positions, though that information is not necessarily dispositive that position classifications are proper.

Once the due diligence team knows how the target company classifies each employee position, it should review the base rate of pay or hourly compensation for each non-exempt position to ensure that it complies with the FLSA's minimum wage requirement as well as the minimum wage requirement of the state/locality where each employee is located. As noted above, many states and localities have adopted higher minimum wage rate requirements than that set under the FLSA.[191] Thus, for instance,

---

[188] *See* 29 C.F.R. § 541.200.

[189] *See* U.S. Dep't of Lab., *Fact Sheet #17H: Highly-Compensated Employees and the Part 541 Exemption Under the Fair Labor Standards Act (FLSA)*, https://www.dol.gov/agencies/whd/fact-sheets/17h-overtime-highly-compensated (rev. Aug. 2024).

[190] *See* 29 U.S.C. § 216.

the target company may pay a non-exempt employee above the $7.25 federal minimum wage but fail to pay the employee the heightened minimum wage required under the state law where that employee works, meaning the target company is out of compliance with applicable state law and could face liability. The due diligence team should also assess the target company's timekeeping practices with respect to nonexempt employees (*i.e.,* by requesting information regarding when and how these employees are expected to track their time) as well as other pay practices, including with respect to overtime pay and breaks. The target company may have specific policies, either in its employee handbook or as standalone documents, setting forth this information, or the due diligence team may need to request additional information in these areas.

When reviewing the target company's overtime pay practices, the due diligence team should check for compliance with the FLSA as well as any additional requirements imposed by the state or locality where each nonexempt employee works. The due diligence team should also determine whether any nonexempt employees are entitled to incentive compensation, such as bonuses. If they are, the due diligence team may need to engage in further follow up with the target company to ensure that it is in technical compliance with overtime pay requirements. For example, the due diligence team may need to obtain greater detail on how the target company calculates the employee's regular rate of pay in connection with the overtime calculation to understand how the incentive pay factors into that calculation (if at all).[192] Similarly, while the FLSA does not require nonexempt employees to receive any particular meal or rest breaks, many state and local laws do. Accordingly, the due diligence team should cross-reference the target company's meal and rest break practices with respect to its nonexempt employees against any requirements imposed by the states and localities where nonexempt employees are located. States and localities may require certain employees to receive meal or rest breaks (*e.g.,* those employees working more than five hours in a day) and/or a particular amount of a meal or rest break (*e.g.,* an uninterrupted meal period of thirty minutes).[193] Accordingly, the due diligence team must assess all details surrounding any meal or rest breaks offered by the target company for compliance with applicable law.

For those exempt positions, the due diligence team must analyze whether it appears the target company has properly classified the positions as exempt under the FLSA and applicable state and local wage and hour laws, or whether it appears the employee positions are actually non-exempt and entitled to minimum wage and overtime pay. First, the due diligence team should check whether each exempt position receives compensation paid on a salary basis sufficient to meet the threshold to pass the salary test under the FLSA and applicable state or local law, unless an exception to the ordinary salary test applies. An employee is paid on a "salary basis" if they regularly receive a predetermined amount of compensation each pay period, and there is no reduction in the employee's salary due to the quantity or quality of their work.[194] The amount of the employee's salary must also then be equal to or greater than the minimum threshold to qualify for an exemption outlined above. If any employee position does not meet the salary test where it applies, the analysis stops there, as the position is misclassified.

Next, the due diligence team should review employee job titles, reporting lines, and job descriptions as an initial step to determine if the position's primary duty satisfies a duties test and qualifies for an exemption.[195] In some cases, the due diligence team may need to pose targeted questions related to

---

[191] U.S. Dep't of Lab., *supra* note 8.

[192] *29 U.S.C. §§ 207(e)(1)*, *(3)*.

[193] *See, e.g.*, *Cal. Lab. Code §§ 226.2*, *510*.

[194] *29 C.F.R. § 541.602*.

[195] Please note that while job titles are helpful for this assessment, they are not dispositive. In applicable regulations and related guidance, the Department of Labor has made clear that job titles alone are not sufficient to demonstrate satisfaction of a duties

particular employee positions to better understand the responsibilities that actually comprise their primary duties. For instance, the due diligence team may ask for a percentage breakdown of how much of an employee's day is generally spent on various job duties identified in the employee's job description to obtain a better sense of what the employee actually does in practice. The due diligence team may also ask questions related to the employee's independence over certain areas of authority identified in or suggested by their job descriptions and oversight over other employees noted on organization charts.

Take, for example, a Senior Graphic Designer position. The due diligence team should first look at how the employee is paid and how much they are paid to determine whether the salary test is satisfied. If it is, the due diligence team should then review the position's job description and ask further follow up questions regarding the scope of the position's responsibilities in practice, such as whether the employee has authority over design strategy and development or predominantly executes on directives. Depending on the position's primary duties, the position may satisfy the administrative or professional employee exemptions.

See below for a visual representation of this analysis.

If the due diligence team determines that there is a risk that the target company has misclassified employee positions, it can request additional information in an effort to determine potential liability to the extent such information is available. For instance, if the target company has exempt employees track their time and can confirm that no potentially misclassified employees have worked overtime hours, that mitigates potential liability for the misclassification. Following the transaction, the classification of employee positions may require review and reclassification, which legal counsel can help to effectuate.

[iii] Other Wage and Hour Compliance Issues[196]

In addition to analyzing compliance with minimum wage and overtime pay requirements under applicable wage and hour laws, there are other wage and hour compliance areas that the due diligence team should assess, which may be more or less relevant depending on the industry of the target company and the type of transaction. For instance, federal, state, and local laws impose restrictions on the working hours of minors, with many states placing caps on the total hours minors of different ages may work and restrictions on the days of the week they can work.[197] Thus, the due diligence team should confirm whether the target company employs any minor employees and may need to audit the schedules of those employees to determine compliance with applicable laws governing the working hours of minors. Some state and localities also require employers to post certain notices in the workplace or meet other notice requirements in relation to the employment of minor employees. If the target company uses a PEO, the PEO may also have controls in place to ensure that the target company is acting in compliance with applicable laws relating to minor employees.

The due diligence team may also need to analyze compliance with certain pay regulations specific to other industries, such as those governing tipped employees, service charges, and tip pooling.[198] Industries such as hospitality, food service, and retail often have heightened risks in these areas due to state and local regulations. Thus, there are some wage and hour issues pivotal to employment due diligence in all transactions and others driven to a greater degree by a specific target company's industry and workforce.

---

test and establish exempt status of an employee. *See* *29 C.F.R. § 541.2*. Thus, the due diligence team should not rely on job titles of employee positions and must seek additional information aimed at a greater understanding of the actual day-to-day responsibilities of the employee position.

[196] Please note that this subsection is not intended to provide a complete accounting of all potential wage and hour compliance issues that might arise in connection with any given transaction but highlights other common wage and hour issues.

[197] *See, e.g.,* *43 Pa. Stat. § 40.1 et seq.*

[198] *See, e.g.,* *N.Y. Labor Law § 196-d*.

[d] Employment Contract Due Diligence

[i] Introduction

Third, this subsection of the chapter addresses the due diligence review of key agreements that employers commonly execute with their employees. This includes not only employee offer letters and employment agreements but also certain incentive compensation plans and various forms of restrictive covenant agreements, such as nondisclosure, non-competition, and non-solicitation agreements. The due diligence team should assess these documents for compliance with applicable federal, state, and local laws, as well as alignment with general best practices and the target company's broader employment policies. Oftentimes, in connection with this part of due diligence of employment-related matters, the due diligence team may advise on new agreements to issue to employees or amendments to make to existing agreements to minimize potential risk and promote better alignment with the buyer's practices following the transaction.

[ii] Employment Agreements and Offer Letters

[A] Introduction

While neither federal law nor any state's laws require employees to receive offer letters or employment agreements upon hire, documentation of the terms and conditions of employment is an advisable best practice that employers often use. Additionally, some state laws require employers to provide certain information to employees in writing at the time of hire, which employers can accomplish through this documentation. Information included in offer letters and employment agreements may also flag other issues that the due diligence team will need to review. In the event that the due diligence team finds employee offer letters or employment agreements noncompliant with applicable law or lacking from a best practices perspective in any way, it may recommend that any employees transferring as part of the transaction execute new letters or agreements following the transaction to the extent the buyer did not already plan to take that action.

The due diligence team should request and examine copies of all executed offer letters and employment agreements with current employees. However, the target company may push back on this request. Target companies with larger workforces or many legacy employees may claim that it is infeasible or impractical to provide that many letters/agreements early on during the due diligence process. If such a situation arises, the due diligence team can request the target company to provide any template offer letters or agreements used by the target company to allow for an initial review and return to executed copies thereafter. As an added measure, the due diligence team may also ask the target company to identify any employees who have executed letters or agreements with nonstandard terms, such as those entitling the employee to severance rights. This step helps to uncover inconsistencies and potential risks related to the target company's obligations under its contracts. Although the due diligence team should uncover this information with its own review of the executed copies, having the added representations on the matter from the target company is helpful as additional support.

[B] Offer Letters

If the target company uses offer letters, the due diligence team should assess whether the laws of the state where the employee works requires disclosure of any information upon hire and whether the letter reflects compliance therewith, or if the target company has accomplished compliance

through other means, such as through notices in the target company's employee handbook.[199] For instance, notice requirements under state laws range from basic information that employers easily incorporate into employee offer letters, like the frequency and method of payment, to more specific, detailed information regarding state-specific entitlements that employers may elect to provide through other means.[200] If the due diligence team finds that the target company has not complied with applicable notice requirements either through its offer letters or by using other means, the target company may face liability for noncompliance, though it is likely low risk depending on the notices involved. Regardless, the due diligence team should recommend remediating the issue following the consummation of the transaction.

The due diligence team must also confirm whether the target company's offer letters include an at-will employment disclaimer or proscribe a term of employment, which may limit the ability to terminate the employee absent notice or some other condition. At-will employment is a doctrine currently recognized federally and in all states, except Montana.[201] At-will employment means either the employer or the employee may terminate the employment relationship at any time, with or without cause or notice, as long as the reason for termination is lawful. If the target company intended to create an at-will employment relationship with all employees where it is allowable under applicable law, a statement regarding that relationship should appear in all employee offer letters. Failure to provide notice of the at-will employment relationship in employee offer letters increases the risk of potential complications in connection with employee separations and even possible tort or contract claims by aggrieved employees. That said, the target company may incorporate disclaimers regarding the at-will employment relationship in other employment documents to mitigate that potential risk.

However, if the target company employs individuals in Montana, the due diligence team should carefully review offer letters executed with those employees to ensure that they do not include an at-will employment disclaimer. If they do, the due diligence team should send further requests for information to the target company surrounding any employees in Montana who have separated from employment in the past three years, including the actions taken by the target company in connection with those separations and any documentation related thereto. Despite the offending at-will employment disclaimer in offer letters, the target company may have complied with Montana law in practice when separating with employees, mitigating any potential liability. Nevertheless, the due diligence team should flag the target company's use of the at-will employment disclaimer and present remediation options after consummation of the transaction.

Aside from the at-will employment disclaimer, additional terms in employee offer letters for the due diligence team to review include those setting forth the terms of the employee's engagement with the target company (*e.g.,* the employee's job title, exempt/nonexempt classification, overtime eligibility, base salary, bonus or incentive compensation, *etc.*) and any contingencies on the offer of employment, such as the employee furnishing proof of their ability to work lawfully in the United State and/or the employee's successful completion of a background check. Contingencies in offer letters may help to demonstrate compliance with other laws or raise additional issues that become a part of due diligence. For instance, a contingency on the employee furnishing work authorization documentation supports that the target Company intends to comply with the Immigration Reform Control Act of 1986, an issue discussed below. A contingency on the employee successfully passing a background check should trigger the due diligence team to conduct further review of the

---

[199] Please note that employers are also required to post certain workplace posters separate and apart from other notice requirements, which the due diligence team may assess separately. *See, e.g.,* U.S. Dep't of Lab., *Workplace Posters*, https://www.dol.gov/agencies/whd/posters (last accessed Aug. 29, 2025).

[200] *See, e.g.,* N.Y. Lab. Law § 195(1)(a); Mass. Gen. Laws ch. 175M, § 4(a).

[201] *See* Mont. Code An.. § 39-3-904 (requiring discharge "for good cause" if an employee has completed their probationary period and prohibiting terminations in other contexts).

target company's use of background checks. For instance, this language signals that the due diligence team should request additional information regarding background check procedures if it has not already done so, including the target company's use of a third-party vendor to assist with compliance with federal and state fair credit reporting laws. Restrictive covenants (*e.g.,* nondisclosure, non-competition, and non-solicitation provisions) may appear in offer letters but are more commonly found in employment agreements or other standalone agreements, as discussed below. If such covenants are contained in the offer letters, the due diligence team should also assess their enforceability.

Finally, beyond the content of offer letters, the due diligence team should consider their use across the workforce. For instance, if the target company lacks consistent use of offer letters or has a wide range of formats in use, the due diligence team may also suggest remediating post-closing for standardization. When a buyer issues new offer letters in connection with a transaction, the general terms and conditions of an employee's employment should not change in a substantial fashion. Though likely low risk, if the buyer were to significantly change the terms of the employment relationship, an employee may allege constructive discharge.[202]

[C] Employment Agreements

If the target company uses employment agreements, the due diligence team should generally conduct a thorough review of the clauses covering the same terms and conditions of the employee's engagement with the target company identified with respect to offer letters above. However, in the context of employment agreements, the due diligence team should also pay particular attention to any provisions governing termination. Although employment agreements may provide for at-will employment, they are more likely than offer letters to place restrictions on terminating an employee's employment. For instance, employment agreements may simply impose notice requirements, obligating one or both parties to the agreement to provide advance written notice before terminating the employment relationship. Alternatively, employment agreements may incorporate more complex termination clauses, including those under which the target company may be obliged to offer the employee severance. The due diligence team must identify these provisions and evaluate whether the transaction may trigger them.

A typical employment agreement may contain multiple types of termination clauses, including termination due to death or disability, termination for cause, termination without cause, and termination for good reason. While the agreement itself dictates exact definitions of these terms, the due diligence team should understand how each functions in practice.

At a basic level, termination for cause typically refers to a situation in which the employer discharges the employee due to misconduct, such as misappropriation or gross negligence. In these cases, the employer often has no obligation to provide advance notice or severance pay to the employee. However, some agreements require that the employee receive written notice and an opportunity to cure the behavior before termination becomes effective. Termination without cause generally allows the company to terminate the employee for any reason or no reason. However, when this type of clause appears in an employment agreement, it typically comes with the contractual severance obligations noted above. In other words, if the employment agreement includes clauses covering termination for cause and termination without cause, and the employer elects to terminate the employee without cause, the agreement may require the employer to pay the employee a specified number of weeks or months of their base salary, cover the cost of continued health insurance coverage, or provide them with other separation benefits as severance. The due diligence team must flag these obligations, as they will continue to remain in place as long as the agreement remains in effect and could represent a financial liability.

Some employment agreements, particularly those involving executive-level employees, also include a termination for good reason clause. This provision gives the employee the right to

---

[202] *See* U.S. Dep't of Lab., *WARN Advisor,* https://webapps.dol.gov/elaws/eta/warn/faqs.asp (last accessed Aug. 29, 2025).

voluntarily resign, provided that certain triggering conditions occur, and if they do so, affords the employee the right to severance. Although the specific definition of good reason again varies by agreement, it may include relocation of the employee's worksite beyond a certain distance, a material reduction in job duties or responsibilities, a decrease in base salary or benefits, or the consummation of a corporate transaction. Because these definitions can be broad and transaction-sensitive, a merger or acquisition itself may trigger termination for good reason. As such, this clause can create unexpected severance costs and talent retention issues if not carefully reviewed in advance. Thus, it is pivotal for the due diligence team to identify, analyze, and flag all termination-related provisions during their review of employment agreements. These clauses can influence transaction strategy, post-closing integration, and financial forecasting.

In addition to the provisions outlined above, employment agreements often contain other clauses that impose ongoing obligations on employers and restrictions on employees. The due diligence team will want to ensure that it has a full understanding of the scope of these provisions and the possible implications that they have during the due diligence process. Like some of the provisions outlined above, these clauses may drive certain decisions made in connection with the transaction and/or following its consummation.

For example, employment agreements may include restrictive covenants, such as conflicts of interest, nondisclosure, non-competition, and non-solicitation provisions, which govern the conduct of employees both during and after their employment. As part of the due diligence process, the due diligence team should carefully review these provisions to ensure they are enforceable under applicable law and appropriately tailored in scope, as discussed below. Other key provisions, such as change-in-control bonuses and those governing equity compensation, may indicate other obligations that the target company has to the employee. The due diligence team should identify and review the terms of these provisions early on, as the transaction itself may impact the obligations the target company owes to employees. Employment agreements may also include alternative dispute resolution clauses, such as mandatory arbitration provisions, which bind both parties to follow particular processes in the event disputes arise. Finally, the due diligence team must closely examine the governing law provision incorporated in each employment agreement, as it can have a direct impact on the enforceability of these contractual terms. Additionally, if a governing law provision designates a jurisdiction with no meaningful connection to the parties or the work performed, a court may refuse to enforce it and instead apply the law of a more closely related jurisdiction.

A thorough review of offer letters and employment agreement enables the buyer to better anticipate potential risk and liabilities related employment matters. Indeed, as demonstrated throughout this subsection, offer letters and employment agreements may vary, as they are unique to every employment relationship and may be the byproduct of negotiations. Accordingly, a significant part of due diligence concerning employment practices of the target company includes the due diligence team's review of these individual agreements.

[iii] Incentive Compensation Plans

Although offer letters and employment agreements outline compensation terms, some employers maintain standalone short-term incentive compensation plans as well.[203] Eligible employees may individually execute these plans or the target company may retain them within written policies applied more broadly to particular segments of the workforce, such as with sales teams or management. These plans may cover various forms of performance-based compensation, including bonuses and commissions, which the due diligence team must review.

---

[203] Not all employers that offer short-term incentive compensation, including bonuses and commissions, define those benefits in written plans. Even when not memorialized in writing, the issues surrounding bonus and commission awards highlighted in this subsection apply.

The target company's incentive compensation plans set forth the terms and conditions for both eligibility and payment of bonus awards and/or commissions, with varying levels of detail. There are generally two types of performance-based bonus awards–discretionary and nondiscretionary. A discretionary bonus is based on subjective factors and awarded at the employer's sole discretion. By contrast, an employee earns a nondiscretionary bonus when the employee and/or the target company meets specific, objective criteria.[204] For instance, a bonus award premised solely on the target company achieving certain profits is likely nondiscretionary upon achievement of that objective criteria.[205] While the target company may characterize bonuses under its plan in a particular fashion, the target company's characterization of the bonus award is not determinative of its type. Indeed, oftentimes, the target company may include a disclaimer that a bonus award is discretionary. Yet, it is the actual terms of the bonus that controls its characterization. Similarly, the target company's incentive compensation plans may outline commissions that eligible employees may earn. Commissions are generally tied to sales or other business activities, and considered "earned" by the employee upon satisfaction of particular criteria set out in the plan documents. Depending on the level of detail of the applicable incentive compensation plans, they may include other terms governing the payment of bonuses or commissions, such as language regarding the timing of payment, forfeiture of payment, or the target company's right to claw back payment.

Some state and local wage payment laws treat nondiscretionary bonuses and commissions as wages, which means that once an employee earns them, they are due and payable to employees, and the employer cannot forfeit or withhold them.[206] These laws may also impose limitations on the target company's ability to clawback payments previously made. Thus, the due diligence team must request copies of any incentive compensation plan documents or other policies and procedures governing bonuses and commissions to ensure compliance with the restrictions under applicable state and local laws. In conducting this review of the plan documents, the due diligence team should assess any definitions or criteria applicable to employees achieving bonuses to determine whether they are likely discretionary or nondiscretionary and commissions to determine when the employee earns them. If the due diligence team finds that bonuses are likely nondiscretionary, it should scrutinize any conditions placed on their payment. Likewise, the due diligence team should review any forfeiture or clawback provisions related to commissions for compliance with applicable law.

In the event that the target company's incentive compensation plans include terms that do not comply with state or local wage payment laws, there is a risk of claims for unpaid wages. In some cases, the due diligence team may find that the target company's incentive compensation plans are legally compliant, though not well-defined. In such case, the due diligence team may propose issuing new plans or amendments following consummation of the transaction. However, any remediation efforts taken should not apply retroactively or divest employees of any incentive compensation that they earned under the terms of prior plans.

For more information regarding other types of incentive plans, please refer to the Employee Benefits section of this chapter.

[iv] Restrictive Covenant Agreements

---

[204] While the issue as to whether a bonus is discretionary or nondiscretionary is often a matter of interpretation under the relevant jurisdiction's wage payment law, because the discretionary versus nondiscretionary character of bonuses is also relevant to the calculation of overtime under the FLSA, the United States Department of Labor has issued guidance regarding when bonuses are considered discretionary versus nondiscretionary that is helpful to the overall analysis. *See* U.S. Dep't of Lab, *Fact Sheet #56C Bonuses under the Fair Labor Standards Act (FLSA)*, https://www.dol.gov/agencies/whd/fact-sheets/56c-bonuses (Dec. 2019).

[205] *Id.*

[206] *See, e.g.,* Md. Code Ann., Lab. & Empl., § 3-501 et seq.

[A] Introduction

Employers commonly require employees to enter into various types of restrictive covenants as a condition of employment. As noted above, employers may incorporate these restrictive covenants into other employment agreements or use standalone agreements.[207] These agreements can represent valuable assets in a transaction, signaling that the target company has proactively safeguarded its customer relationships and proprietary information. Thus, the existence and enforceability of these agreements are often critical to preserving the value of the target company's business post-closing and an important aspect of employment-related due diligence.

The enforceability of different types of restrictive covenants is a constantly evolving area of employment law, with many states and localities moving toward heavier scrutiny of such agreements.[208] Therefore, the due diligence team should request and review copies of all such agreements executed with the target company's current employees and assess these agreements under the laws of the state referenced in the agreement's governing law provision (as applicable) as well as the laws of state in which each individual employee works as of the date of the agreement's execution.[209] Depending on the type of agreement involved, subject matter experts over other areas of law should also review these agreements as part of the due diligence process to better assess their enforceability and their actual protection of the target company's interests.

[B] Nondisclosure and Inventions Assignment Agreements

First, nondisclosure and inventions assignment agreements are standard agreements that employees routinely execute upon hire.[210] In fact, in many cases, employers condition offers of employment on their execution. However, from the employment law perspective, some state and local laws place restrictions on the use of such agreements and their form. Accordingly, the due diligence team must analyze the form and context within which the target company has its employees execute these agreements. To do so, the due diligence team must take stock of: (1) which employees executed these agreements, (2) where those employees work, (3) any governing law provisions in the agreements themselves, and (4) any limitations that may apply to the agreements as a result of laws in those jurisdictions. If the restrictive covenant agreements do not conform to limitations under applicable laws, there is a risk that they are void or their enforceability is limited. In such cases, the due diligence team should flag their findings and may recommend that employees execute new agreements following the transaction.

As noted above, many states and localities have passed laws limiting the enforceability of such agreements in certain contexts, typically in connection with an employee's separation from employment or resolution of potential claims against an employer. For example, at least twenty states have passed laws in the past few years prohibiting the use of nondisclosure agreements in the context of the settlement of sexual harassment claims.[211] Accordingly, as part of its review, the

---

[207] Some employers do not have employees execute actual agreements but use employment policies to address issues traditionally covered by restrictive covenant agreements, such as confidentiality and non-competition. As a general matter, policies are less likely to give rise to binding commitments. Accordingly, if the due diligence team uncovers that is the employer's practice, it may flag that issue as part of due diligence.

[208] The Federal Trade Commission issued a final rule banning non-competition agreements nationwide, though a district court issued an order enjoining its enforcement on September 4, 2024. *See* Federal Trade Commission, *FTC Announces Rule Banning Noncompetes*, https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-rule-banning-noncompetes (April 23, 2024).

[209] This assessment provides a full picture of potential noncompliance in the event a court disregards the choice of law provision.

[210] Nonemployees, like independent contractors, may also execute these agreements. Accordingly, the due diligence team should review the use of such agreements with nonemployee labor as well.

due diligence team should obtain an understanding of how the target company uses these agreements, particularly if it has executed any agreements outside of the ordinary course of business. Beyond considering the context within which the target company executes these agreements with employees, the due diligence team should also examine their contents, with a particular focus on their scope and any disclaimers regarding their reach. For instance, some states and localities have placed limitations on the duration of the enforceability of nondisclosure agreements, whereas others have required certain disclaimers in inventions assignment agreements.[212]

Aside from this general review for enforceability under employment laws, these are also the sorts of agreements that subject matter experts in the respective areas (*e.g.,* intellectual property) should review as part of the due diligence process.

[C] Non-Competition and Non-Solicitation Agreements

Second, non-competition, customer non-solicitation, and employee non-solicitation agreements are other common forms of restrictive covenant agreements that employers may require employees to execute, often applying both during and after employment.[213] At common law, these types of restrictive covenants are generally enforceable, provided that they are no broader than necessary to protect an employer's legitimate business interests, meaning that they are reasonable in scope, duration, and geographic reach, and do not cause an undue hardship to the employee or harm to the public interest, though the specific application of this reasonableness standard varies across jurisdictions.

However, in recent years, many states and localities enacted statutes that impose additional restrictions or outright prohibitions on the use of these restrictive covenants. As a result, the due diligence team must again conduct a jurisdiction-specific review and analysis of any such restrictive covenant agreements used by the target company.

Overall, the due diligence team should determine which employees of the target company have executed these types of restrictive covenants and when they did so to assess their enforceability under the restrictions imposed by various state and local laws. While some state laws broadly prohibit non-competition agreements,[214] many states and localities that have passed laws limiting their enforceability have taken a more targeted approach. For instance, several states, including Colorado, Illinois, Maine, Maryland, New Hampshire, Oregon, Rhode Island, Virginia, Washington, and the District of Columbia prohibit non-competition agreements executed with employees who earn less than a defined salary threshold.[215] In addition, some states have restricted the use of non-competition agreements in specific industries, such as in the healthcare field, where public interest is a larger concern.[216] Whether these restrictions extend beyond true non-competition agreements to non-solicitation agreements also varies from state to state.

---

[211] *See, e.g.,* *820 Ill. Comp. Stat. 96/1-1 et seq.*; Doreen S. Martin and Keith Olsen, *The List of States Regulating Non-Disclosure Provisions Continues to Grow,* Venable LLP (June 6, 2024), *https://www.venable.com/insights/publications/2024/06/the-list-of-states-regulating-nondisclosure*.

[212] *See, e.g.,* *Cal. Lab. Code § 2870*.

[213] Please note that the enforceability of these types of agreements in the employment context varies from the corporate transaction context. This subsection section focuses on the due diligence team's review of these agreements executed with the target company's employees in the employment context.

[214] *See* *Cal. Bus. & Prof. Code §16600(a)*.

[215] *See, e.g.,* *Va. Code § 40.1-28.7:8*.

[216] *See, e.g.,* *Md. Code Ann., Lab. & Empl., § 3-716*.

The due diligence team must also evaluate the timing and context of each employee's execution of the relevant restrictive covenant.[217] To be enforceable, the employer must support the agreement by adequate consideration. Generally, the commencement of employment or a change to the terms and conditions of employment, such as a raise or promotion, can serve as adequate consideration to support a restrictive covenant. By contrast, state laws vary as to whether continued at-will employment alone is sufficient consideration. Accordingly in jurisdictions where it is not adequate consideration, restrictive covenants signed during employment without some additional support may be void and unenforceable.

Moreover, several states impose procedural requirements with which the employer must comply for an agreement to be valid and enforceable. These may include providing the employee with adequate notice of the agreement prior to the start of employment or the agreement's execution, such as a seven-day review period, or mandating specific disclosures in the agreement, such as language advising the employee to seek the advice of legal counsel.[218] Thus, the due diligence team must determine when during the employment relationship the employee executed the restrictive covenant and other circumstances surrounding its execution to fully assess its enforceability. For instance, the due diligence team should look for any language in the applicable agreement addressing the timing and context, such as the consideration provided to the employee and any review period offered to the employee prior to the execution of the agreement.

The due diligence team must also closely review the actual terms of the restrictive covenants, with a particular focus on their scope, taking into account variations on the general reasonableness analysis for each applicable jurisdiction. This includes the temporal duration, range of activities restricted, and geographic reach of the relevant restrictive covenant. Indeed, some states have statutorily defined presumptions as to the scope of a restrictive covenant that a court will find reasonable or unreasonable.[219]

Finally, if a restrictive covenant is overly broad or otherwise unenforceable under applicable state law, the due diligence team should consider whether the jurisdiction allows for "blue penciling," a doctrine that permits a court to modify an overbroad provision to make it enforceable. Some states permit courts to revise overbroad terms, while others prohibit judicial modification. Thus, as a final step to the analysis, the due diligence team should assess the likelihood that a court will upheld a restrictive covenant as written or modify it if challenged.

[e] Employment Policy Due Diligence

[i] Introduction

Fourth, employment due diligence should also extend to the target company's written employment policies and procedures, which often serve as the framework for day-to-day workforce management and legal compliance. This subsection examines the due diligence team's overall evaluation of employment policies, which is critical not only for assessing potential legal exposure, but also for understanding the target company's workplace culture, enforcement practices, and readiness for post-closing integration, as applicable. Although the due diligence team will review specific policies and procedures as part of its analysis of other employment practices outlined in this chapter, this subsection considers a general audit that the due diligence team should conduct of the target company's written policies for alignment with applicable federal, state, and local laws and best practices.

---

[217] Aside from the reasons set forth in this paragraph, the timing of when employees executed restrictive covenants agreements is also relevant to the due diligence team's analysis, as many of the statutes referenced above only recently went into effect and many not govern agreements executed prior to their effective date.

[218] *See, e.g.,* *820 Ill. Comp. Stat. 90/1 et seq.*

[219] *See, e.g., Fla. Stat. § 542.335*.

[ii] Policies Covering Federal, State, and Local Entitlements

To begin its analysis of the target company's employment policies, the due diligence team must request a copy of the target company's employee handbook and any other standalone written policies governing employment matters. Although not dispositive of legal compliance, the due diligence team may also request information from the target company regarding when it last updated its employee handbook and whether it engaged employment counsel in connection with that update. Such information helps to demonstrate the target company's efforts to align its policies with applicable law.

As part of the due diligence team's analysis of the employee handbook, it should determine whether the handbook covers all entitlements under applicable federal, state, and local law, particularly where such laws impose notice requirements on employers. This may arise in the context of certain forms of leave afforded to employees, such as family and medical leave and paid sick leave under federal, state, and local law. For instance, if the target company lacks policies covering these entitlements, that may reflect that it failed to provide employees with required benefits under applicable law, which could create potential liability. However, once the due diligence team confirms that the target company has policies covering legal entitlements, the inquiry does not stop there. The due diligence team should then review the policies for compliance with requirements under applicable law. For example, in the context of paid sick leave, the due diligence team should determine whether the policies provide for at least the minimum amount of leave required and address all covered usages of leave under applicable law. Additionally, as part of its review of leave policies, the due diligence team should check to ensure that the policies do not violate any restrictions imposed on the administration of leave by law. For example, if the target company has a vacation or paid time off policy, the due diligence team should review the policy for compliance with any state or local laws limiting the forfeiture of such leave from year-to-year and requiring the payment of such leave upon separation from employment.

Beyond requesting a copy of the target company's employee handbook and standalone employment policies, the due diligence team may need to craft separate requests for information concerning the target company's employment practices that are not set forth in written policies. By way of example, depending on the states in which the target company has employees, applicable law may require the target company to provide employees with anti-discrimination and harassment training.[220] However, employers do not always outline information regarding training in written employment policies. Accordingly, the due diligence team must separately assess the target company's compliance with other obligations imposed by applicable employment laws in addition to those expressly set forth its written policies.

[f] Employee Attrition Due Diligence

[i] Introduction

Fifth, this subsection of the chapter addresses various issues related to employee attrition, which may provide meaningful insight into the stability of the target company's workforce and its potential legal exposure. As part of the due diligence process, a review of attrition-related matters should include turnover data, with particular attention to any reductions in force, and the target company's compliance with the federal Worker Adjustment Retraining and Notification Act of 1988 (the "WARN Act") and state mini-WARN Act requirements. The due diligence team should also consider the target company's use of separation agreements, including whether the target company routinely uses such agreements in the context of involuntary separations, and the agreement's compliance with applicable legal requirements, such as mandatory revocation and review periods for a release of claims under the Age Discrimination in Employment Act ("ADEA"). Finally, the due diligence team should identify any severance obligations that the target company has that may have potential financial or operational impact.

---

[220] *See, e.g.,* N.Y. Lab. Law § 2, 201.

[ii] WARN Act Compliance

To analyze issues related to employee separations, the due diligence team should request attrition data, including a list of all voluntary and involuntary employee separations over the past three years with the date of each separation identified. As an added measure, the due diligence team should also request that the target company identify any reductions in force or plant closings that it conducted in the past three years or plans to conduct prior to the consummation of the transaction, including the date, number of employees impacted, and circumstances surrounding the reductions in force or plant closings. As noted above, such information provides valuable insight to the due diligence team into the stability of the target company's workforce, which may prompt further review of other areas, as well as its compliance with the WARN Act and state mini-WARN Acts.

The WARN Act generally requires employers with 100 or more full-time workers to provide 60 days' written notice in advance of covered "plant closings" or "mas layoffs."[221] Approximately 13 states have passed their own mini-WARN Acts, which also impose notice requirements on employers conducting mass layoffs or plant closings. These laws vary by jurisdiction and often have lower employee thresholds than the federal WARN Act, meaning that they may apply to an action even when the WARN Act does not. While the other triggering events and notice requirements under many mini-WARN Acts mirror the WARN Act, [222] others may also apply in broader circumstances, require longer notice periods, and even impose severance requirements.[223] Some localities have also passed mini-WARN Acts.[224] Accordingly, when analyzing attrition data, the due diligence team should consider compliance with both the WARN Act and any mini-WARN Acts based on the jurisdictions in which former employees performed work at the time of their separation from employment.

Under the WARN Act, a "plant closing "typically includes a permanent or temporary shutdown of a "single site of employment" or one or more operating units within that site that results in an "employment loss" of 50 or more employees.[225] A "mass layoff" typically includes a reduction in force resulting in an employment loss at a "single site of employment" during any 30-day period for (1) at least 33% of the employees at that site, *and* (2) at least 50 employees.[226] A "single site of employment" can refer to either a single location or a group of contiguous locations.[227] For example, separate buildings or areas that are not directly connected or even in immediate proximity can constitute a single site of employment if they are in reasonable geographic proximity, used for the same purpose, and share staff and equipment.[228] With respect to remote workers, U.S. Department of Labor guidance advises that they are generally considered assigned to the site of employment from which their work is assigned.[229] The WARN Act not only looks at employment losses occurring over the 30-day period referenced above but considers losses within a 90-day period.[230] For example, an employer is required

---

[221] *See* *29 U.S.C. § 2101 et seq.*

[222] *See* *Del Code Ann. tit. 19 § 1901 et seq*.

[223] See *N.J. Stat. § 34:2-1 et seq*.

[224] *See, e.g.,* Phila. Code § 9-1500 *et seq*.

[225] *See* 29 C.F.R. § 639.3(b).

[226] *See* 29 C.F.R. § 639.3(c).

[227] *See* 29 C.F.R. § 639.3(i).

[228] *See* U.S. Dep't of Lab., *WARN Advisor*, *https://webapps.dol.gov/elaws/eta/warn/glossary.asp?p=Single%20Site%20of%20Employment* (last accessed Aug. 29, 2025).

[229] *See generally* U.S. Dep't of Lab., Employer's Guide to Advance Notice of Closings and Layoffs, *https://www.dol.gov/sites/dolgov/files/ETA/layoff/pdfs/_EmployerWARN2003.pdf* (last accessed Aug. 29, 2025).

to give advanced notice under WARN if a series of smaller layoffs trigger WARN in the aggregate looking forward or backward 90 days, unless the employer can show that the layoffs are separate, distinct, and not intended to evade the WARN Act.

If an employer is unable to comply with WARN Act notice requirements, Department of Labor guidance acknowledges that "the provision of pay and benefits in place of notice is a possible option."[231] Additionally, there are limited exceptions to the notice requirement under the WARN Act, though the employer carries the burden to prove that an exception applies under the circumstances.[232] Additionally, even if an exception applies to exempt an employer from the 60-day notice requirement, the employer must still give as much advance notice as is practicable under the circumstances. These exceptions include "faltering business" in the context of a plant closing, "unforeseeable business circumstances" in the context of plant closings and mass layoffs, and "natural disasters" in the context of plant closing and mass layoffs. However, not all state mini-WARN Acts recognize the same exceptions that exist under the WARN Act.[233]

An employer who violates the WARN Act is liable to each affected employee for an amount equal to back pay and benefits for the period of the violation, up to 60 days.[234] Wages paid over the notice period and any voluntary and unconditional payment not required by legal obligations (*i.e.,* severance) may offset this liability. The employer may also face a $500 civil penalty for each day of the violation. If there is a lawsuit related to a failure to adhere to the WARN Act, a court can also award reasonable attorney's fees and costs. Mini-WARN Acts may impose additional liabilities beyond those under the WARN Act.

When analyzing compliance with WARN Act and mini-WARN Act obligations, the due diligence team should review any information provided by the target company regarding reductions in force and plant closings. It should also cross-reference that information with the attrition data provided to ensure alignment. Beyond reviewing the reductions in force specifically identified by the target company, the due diligence team should conduct an independent assessment of the attrition data to determine if there are any other dates on which multiple involuntary separations took place, suggesting that additional reductions in force may have occurred beyond those identified by the target company, or whether additional terminations within a 90-day period of a reduction in force identified by the target company could be aggregated with those identified. In connection with any reductions in force identified by the due diligence team, it should determine whether the number of separations met the threshold to trigger the WARN Act or any mini-WARN Act. The due diligence team may require additional information to make this assessment, such as the reporting location of remote employees to determine whether sufficient employment losses occurred at a single site of employment.

Moreover, if the due diligence team determines that there is a risk that a reduction in force may have triggered the WARN Act or a mini-WARN Act, the due diligence team should obtain additional information regarding the target company's efforts to comply or any exceptions to WARN Act obligations the target company believes apply. Concerning these efforts, the due diligence team should review a sample of any notices provided to affected employees and any separation agreements executed with affected employees. The due diligence team may also question whether the target company engaged counsel to assist with administering the reductions in force in question. Depending on the due diligence team's findings, if there is a risk of noncompliance with the WARN Act, the potential liability may warrant a disclosure or an exclusion from the transaction.

---

[230] *See* 29 C.F.R. § 639.5(a).

[231] *See* U.S. Dep't of Lab, *WARN Advisor*, *https://webapps.dol.gov/elaws/eta/warn/faqs.asp* (last accessed Aug. 29, 2025).

[232] *See* 29 CFR § 639.9.

[233] *Md. Code Ann., Lab. & Empl. § 11-301 et seq.*

[234] *See supra* note 56.

[iii] Separation Agreements & Severance Obligations

In addition to attrition data, the due diligence team should also request copies of all separation agreements executed with former employees in the past three years. The number of separation agreements provided should give the due diligence team a sense of the target company's practices surrounding the use separation agreements. For instance, whether the target company requests execution of a separation agreement as a routine practice. However, if the due diligence team requires further clarity, it may ask the target company for additional information regarding its use of separation agreements, including whether the target company has ever offered an employee a separation agreement that the employee declined to execute. Such information may suggest an aggrieved former employee intends to file a claim against the target company and warrants additional follow up by the due diligence team.

When reviewing the target company's separation agreements, the due diligence team should focus on whether the agreements include standard disclaimers regarding wages paid to the employee in connection with work performed prior to the separation date and any non-waivable rights retained by the employee, such as the right to file a complaint with an administrative agency. The due diligence team should also assess other terms and conditions built into the agreement, including the severance provision to determine whether the target company may have outstanding obligations to the employee thereunder; the general release provision to determine whether it is likely sufficient to generally release claims under applicable federal, state, and local law; and any restrictive covenants, like nondisclosure and non-disparagement provisions to determine their reasonableness and enforceability. Finally, the due diligence team should also assess whether the agreement includes review and revocation periods consistent with applicable law.

Specifically, to effectuate a release claims under the ADEA with employees who are ages forty or older, the Older Workers Benefit Protection Act requires the employee to receive 21 days to review and seven days to revoke a release of claims under the ADEA.[235] In the context of reductions in force, the required review period extends to 45 days, and the employee must also receive an exhibit identifying the titles and ages of employees affected by the reduction in force.[236] Some state laws may also require that employees receive certain review or revocation periods, aside from those imposed by the OWBPA. Thus, the due diligence team should check separation agreements to see if they incorporate review and revocation periods and may need to confirm with the target company the ages of those employees who executed the applicable agreement to ensure its compliance with applicable law.

Although separation agreements may provide the due diligence team with some information regarding the target company's practices surrounding the payment of severance upon separation, the due diligence team should specifically request that the target company provide any written severance policies and confirm whether it follows a customary practice with respect to severance pay. Even if an employer does not maintain a written severance policy, there is a risk that a custom or practice could create an implied right to severance and give rise to claims for breach of contract in the event the target company does not payout severance in conformance with that practice. Accordingly, the due diligence team will want to identify whether that risk exists.

[g] Independent Contractor Due Diligence

Sixth, this subsection of the chapter addresses due diligence related to the target company's use of non-employee labor. Chiefly, this includes the target company's use of independent contractors, sometimes referred to as consultants or freelancers. The due diligence team's review in this area generally focuses on

---

[235] *See* *29 C.F.R. § 1625.22*.

[236] *See* *29 C.F.R. § 1625.22*.

two key issues: (1) the classification of these workers as independent contractors, and (2) the terms of their engagement, as set forth in any written agreements that they have executed with the target company.

The Department of Labor has issued regulations addressing how to analyze whether a worker is properly classified as an employee or independent contractor under the FLSA. Under current regulations,[237] the Department of Labor applies an "economic reality" test based on a totality-of-the-circumstances analysis.[238] This test involves an assessment of six non-exhaustive factors that guide the inquiry into whether a worker is economically dependent on an employer or in business for itself. These factors include (1) the opportunity for profit or loss depending on managerial skill; (2) the investments by the worker and the employer; (3) the degree of permanence of the work relationship; (4) the nature and degree of control; (5) the extent to which the work is integral to the business; and (6) the skill and initiative required.[239]

In addition to the test developed to assess the classification of independent contractors under federal law, states and localities have developed alternative tests to assess this classification, which are often more stringent than the economic realities test and may begin with a rebuttable presumption a worker is an employee. For example, some states apply variations of an "ABC test," under which a worker is presumed an employee unless the employer can prove that (A) the worker is free from control and direction in performing the work, (B) the work performed is outside the usual course of the employer's business, and (C) the worker is engaged in an independently established trade, occupation, or business.[240] Misclassification of workers as independent contractors under or state law can result in significant wage and hour liability, tax obligations, benefits entitlements, and other penalties.

First, to assess the target company's classification of independent contractors, the due diligence team should first obtain a list of the target company's independent contractors engaged in the past three years and a general overview of the terms of each independent contractor's engagement, including their dates of engagement, work location, role or services provided, rate of pay, and average hours worked per week. The due diligence team should also obtain copies of any written agreements executed with these independent contractors, as the agreements may provide more details regarding the engagement that aid the analysis. The due diligence team should consider this information light of the non-exhaustive factors used under the federal economic realities test and any tests that may apply in the jurisdiction in which the target company's independent contractors provide services.

For instance, the due diligence team should look to see whether the target company's independent contractors are individuals engaged directly to provide services personally or companies with their own businesses. If the latter, the independent contractors are more likely to be in business for themselves and to satisfy multiple factors under the economic realities test. The due diligence team should also consider the length of the engagement of the target company's independent contractors. If the target company has engaged a particular contractor for many years and plans to continue that engagement, that fact likely weighs in favor of a finding that the contractor is an employee and misclassified. Similarly, the due diligence team should consider the roles held by the target company's independent contractors and their similarity to the roles held by the target company's employees. If a role held by a particular independent contractor is the same as that held by an employee, or the target company previously engaged the independent contractor as an employee in the same capacity, that again weighs toward a finding the independent contractor is an employee and misclassified.

A high-level outline of key information that may aid the due diligence team's analysis is copied below:

---

[237] Please note that, though still in effect at this time, the current Department of Labor regulations are subject to litigation and are likely to change.

[238] See U.S. Dep't of Lab., *Fact Sheet 13: Employee or Independent Contractor Classification Under the Fair Labor Standards Act (FLSA),* https://www.dol.gov/agencies/whd/fact-sheets/13-flsa-employment-relationship (rev. March 2024).

[239] *Id.*

[240] *See* State of Cal. Dep't of Industrial Relations, *Independent Contractor Versus Employee,* https://www.dir.ca.gov/dlse/faq_independentcontractor.htm (rev. March 2025).

Key Signs of Employee/Employer Relationship	Key Signs of Independent Contractor/Contracting Entity Relationship
• Performs work traditionally performed by employees and exclusively for one business	• Performs work as part of an independent business and for multiple clients
• Continuing/indefinite relationship	• Defined or project-based relationship
• Paid on a salary basis	• Paid on a flat fee basis
• Employer supplies tools and equipment	• Supplies own tools and equipment
• Employer directs when and how the work is to be performed	• Sets own schedule; determines how work is to be performed

Second, the due diligence team should also review key provisions of the independent contractor agreements used by the target company to understand the terms governing the engagement of independent contractors and alignment with best practices. For instance, the due diligence team should confirm the agreements include disclaimers regarding the independent contractor relationship and payment of taxes. Although not dispositive of the classification, an employer may use evidence of such disclaimers in support of its classification of workers. The due diligence team should also determine whether such agreements include indemnification provisions and alternative dispute resolutions provisions, such a provision requiring mandatory arbitration, which may benefit the target company in the event disputes arise.

If the due diligence team determines that there is a risk that the target company has misclassified workers as independent contractors, it can request additional information in an effort to determine potential liability to the extent such information is available. For instance, if the target company has independent contractors track their time and can confirm that no potentially misclassified contractors have worked overtime hours, that mitigates potential wage and hour liability for the misclassification; however, potential tax and other liability may remain. Where misclassification risks are identified, the buyer should consider appropriate contractual protections and post-closing remediation.

[h] Employment-Related Litigation Due Diligence

Seventh, the due diligence review of employment matters should include employment-related claims, complaints, grievances, and governmental audits. In addition to formal proceedings, this subsection of the chapter identifies how the due diligence team should tackle concerns raised internally that have not amounted to formal litigation.

At the outset of due diligence, the due diligence team should request copies of all claims, complaints, grievances, and governmental audits concerning employment matters pending, threatened, or filed in at least the past three years.[241] The due diligence team must make clear that this request applies to all employment matters, including discrimination, harassment, and retaliation, and wage and hour issues, which are common areas of employment litigation. If the target company identifies any claims responsive to this request, whether in the form of a charge filed with an administrative agency or formal complaint filed in court, the due diligence team should request any responsive documentation filed by the target company and information concerning the current state of proceedings. If the matter is pending, the due diligence team should assess what defenses the target has raised or may raise and the apparent strength of those defenses as well as whether the target company is covered by insurance in connection with the claim.

Beyond formal claims filed with applicable government agencies or in court, the due diligence team should also request information concerning whether the target company has received any complaints in the past three years regarding discrimination or harassment or illegal conduct pursuant to a whistleblower policy, and what actions the target company took in relation thereto (if any). The due diligence team should also review the Company's anti-discrimination and harassment and whistleblower policies for compliance with applicable law and best practices to identify any shortcomings that may limit defenses in the event that any complaints subsequent to the transaction arise. For instance, such policies should include clear reporting channels and prohibit retaliation. The due diligence team's review of potential and actual employment-

241 Three years is the applicable statute of limitations period for many types of employment-related claims. Thus it is often incorporated as the relevant lookback period for due diligence in this area. However, it may be advisable or appropriate to extend to a longer lookback period, such as five years, particularly if any concerns arise with any written term contracts.

related litigation matters helps provide a more comprehensive view of potential liability faced by the target company.

[i] Immigration Due Diligence

Eighth, this subsection of the chapter is intended to acknowledge the due diligence team's review of the target company's compliance with federal work authorization requirements, including proper completion and retention of Form I-9. Immigration specialists should assist with broader due diligence of immigration issues, such as assessing visa sponsorship practices and compliance with other U.S. Citizenship and Immigration Services requirements ("USCIS").

Under federal law, all U.S. employers are required to verify the identity and employment authorization of each individual hired after November 6, 1986, by completing Form I-9 within three business days of the employee's start date.[242] Form I-9 requires the employee to present original documentation establishing both identity and work authorization, and for the employer to examine and record the information. Employers are also required to retain I-9s for a designated period. The due diligence team should confirm that the target has established appropriate I-9 compliance policies, maintains complete and accurate records, and has procedures in place for reverifying work authorization where required. The due diligence team should pay particular attention to whether the target company has conducted internal I-9 audits, how it handles missing documentation, and whether it has faced any U.S. Immigration and Customs Enforcement ("ICE") inspections.

The due diligence team should also confirm whether the target company uses E-Verify, which helps to reflect overall compliance. E-Verify is a web-based system run by ICE for employers to confirm employee eligibility to work lawfully in the United States. Use of E-Verify is mandatory for all U.S. federal contractors and employers in certain states.[243]

Noncompliance with I-9 requirements can lead to significant civil penalties, and criminal liability in the case of willful violations. Accordingly, identifying and addressing I-9 compliance issues during due diligence is critical to assessing potential risk and determining whether action is warranted prior to or after closing.

[2] Employee Health & Safety Due Diligence

[a] Introduction

Matters concerning the health and safety of a target company's employees is relevant to the due diligence conducted in connection with any transaction. As part of employment-related due diligence, the due diligence team must assess the target company's compliance with applicable workplace health and safety regulations. This includes evaluating whether the target has implemented appropriate safety programs, experienced citations, and maintained required records in accordance with applicable law. The due diligence team should also review any internal policies or practices adopted by the target company to further promote the safety and health of its workforce, even where compliance concerns are not directly implicated, as such policies may reflect the target company's overall approach to risk management.

[b] Occupational Safety and Health Act Compliance

[i] Introduction

Under the Occupational Safety and Health Act of 1970 ("OSH Act"), states and U.S. territories have the option of participating in the federal Occupational Safety and Health Administration program governed by federal OSH Act regulations; adopting their own workplace safety and health programs ("State Plans"); or implementing an industry or worker-specific hybrid approach that incorporates both federal and state regulations.[244] Accordingly, the federal OSH Act covers many private sector employers and

242 See 8 C.F.R. § 274a.2.
243 See 48 C.F. R. § 22.1802.
244 See 29 U.S.C. § 667.

their workers within the 50 states and U.S. territories, though there are currently twenty-two jurisdictions that administer State Plans covering both private sector and state and local government workers.[245] These State Plans are monitored by the Occupational Safety and Health Administration ("OSHA") and must be at least as effective as the federal OSHA program. While many states with State Plans adopt the federal OSHA standards verbatim, others have enacted more stringent standards in some instances.

[ii] The General Duty Clause & Specific Standards

Section 5(a) of the OSH Act establishes the general duty placed upon employers to maintain a safe and healthful workplace.[246] First, employers must comply with the "General Duty Clause" encapsulated by Section 5(a)(1), which requires each employer to furnish to each of its employees a place of employment free from recognized hazards causing or likely to cause death or serious physical harm.[247] OSHA can use this General Duty Clause in its enforcement activities to reach hazards not otherwise addressed by a hazard-specific standard discussed below. For instance, if, during an inspection, an OSHA Compliance Officer ("CO") finds a hazard that could cause serious injury or death that is not covered by an existing OSHA standard, the CO may cite to the General Duty Clause in issuing a citation against an employer. Second, as covered in Section 5(a)(2), each employer must "comply with the occupational safety and health standards promulgated under th[e] Act."[248] These standards identify specific hazards applicable to the general industry or particular industries, such as construction.

Both subsections of Section 5(a) discussed above place a duty on employers to identify and assess hazards in their workplaces. Thus, the due diligence team should request all written safety policies, plans, or processes that the target company has relating to health and safety, including hazard identification and assessment. Beyond obtaining and reviewing written plan documents, the due diligence team may also request information concerning methods used by the target company to inspect all operations, equipment, and areas of the physical workplace, and any recent incident investigations or reports connected to safety issues. Such information helps reflect whether the target company has acted in compliance with OSH Act regulations and whether there is a risk of future safety incidents and/or citations.

In addition to the target company's internal safety records, the due diligence teams should confirm whether OSHA has issued any citations against the target company in the past three years. If the target company has received citations, OSHA may subsequently use those citations as support for a heightened classification if the target company engaged in subsequent violations of the same standards.

[iii] Recording and Reporting Work-Related Injuries and Illnesses

In addition to identifying and assessing hazards in the workplace, employers must also comply with other rules, regulations, and orders issued pursuant to the OSH Act, which include following certain administrative requirements. For instance, the OSH Act requires the display of certain posters and may require employers to conduct certain trainings.[249] Accordingly, to the extent not covered by the written policies requested, the due diligence team may separately information regarding workplace poster and safety training to assess compliance in these areas.

Finally, under the OSH Act and State Plans, employers are subject to certain recordkeeping and reporting obligations. For example, under the OSH Act, employers must keep records of fatalities, injuries, and illnesses that are (1) work-related, (2) a new case, and (3) meet one or more of the general recording criteria in § 1904.8 or a special case reporting criteria in § 1904.8 through 1904.12 of the OSH Act.[250] To record a work-related fatality, injury, or illness that meets this criteria, the employer

245 U.S. Dep't of Lab., State Plans, https://www.osha.gov/stateplans (last accessed Aug. 29, 2025).
246 See 29 U.S.C. § 654(a)(1).
247 See 29 U.S.C. § 654(a)(1).
248 See 29 U.S.C. § 654(a)(2).
249 See, e.g., OSHA, Training Requirements in OSHA Standards, https://www.osha.gov/sites/default/files/publications/osha2254.pdf (last accessed Aug. 29, 2025).

must first fill out an OSHA Form 300. The employer must also fill out an OSHA Form 301, which is an injury and illness report used to record the information on how each injury or illness identified on Form 300 occurred. Finally, at the end of each calendar year, employers must complete and certify an OSHA Form 300A, which includes a summary of all work-related injuries and illnesses. The OSHA Act also requires employers to report the death of any employee that results from a work-related incident directly to OSHA within eight hours of the fatality, and any in-patient hospitalization of one or more employees, or an employee's amputation or loss of an eye that results from a work-related incident to OSHA within 24 hours. [251] As such, the due diligence team should request copies of these records, which help demonstrate safety issues that may exist at the target company's workplace as well as whether the target company maintains required records regarding safety matters.

[c] Other Health & Safety-Related Policies

Besides evaluating compliance with the OSH Act, the due diligence team should review whether the target company has implemented other policies aimed at employee safety and health, including those concerning workplace smoking, a drug and alcohol-free workplace, and workplace violence prevention.

For instance, certain state and local laws require employers to impose restrictions on smoking in the workplace, and companies often adopt internal smoking policies to ensure compliance and promote a healthy work environment. The due diligence team should confirm whether the target has such a policy in place and whether that policy complies with all requirements under applicable state and local laws, such extending workplace smoking restrictions to e-cigarettes. Similarly, applicable law may require the target company to adopt a drug-and alcohol-free workplace policy; yet, even where not required, such policies help promote a safe and productive work environment. The due diligence team should review whether the target company has a written policy that prohibits the use of drugs and alcohol in the workplace and adopts drug testing procedures compliant with applicable state and local laws placing restrictions on such testing. With this review, the due diligence team should also examine how the policy addresses related issues, such as prescription medication use, reasonable accommodations, and procedures for discipline.

Finally, the due diligence team should consider any workplace violence prevention policies, which help demonstrate the target company's approach to risk management. The due diligence team should confirm whether the target company has adopted a policy that defines prohibited conduct, outlines reporting procedures, and establishes a clear protocol for investigating and responding to incidents. In reviewing these policies, the due diligence team should also consider how they are communicated and enforced, whether they are consistently applied, and whether there have been any recent incidents or complaints. Even when not legally required, these policies serve as an indicator of the target company's management of its work environment.

250 29 C.F.R. § 1904.4.
251 29 C.F.R. § 1904.39(a).

Chapter 8 Intellectual Property Due Diligence

Synopsis to Chapter 8 : Intellectual Property Due Diligence

Due Diligence in Corporate Transactions

End of Document

§ 8.01 Overview

As we noted in Chapter 1, intellectual property due diligence has evolved significantly over the past decade or two. In the past, due diligence by intellectual property lawyers was reserved for "IP companies" – technology companies, media companies, companies with strong brand recognition, etc. In today's world, all companies are "IP companies." At a minimum, all companies utilize business software to operate their business, and in many cases one or more elements of business software are critical to the day-to-day operation of the business. Many businesses have turned to custom software applications, either developed internally or by third party contractors, to more efficiently run the business and/or to provide better customer experience. And in connection with the rise in social media, companies are increasingly engaging in sophisticated marketing and media campaigns to improve brand recognition and perhaps find alternative revenue streams. Today due diligence review by intellectual property lawyers is the norm, not the exception.

In this chapter we discuss the different types of intellectual property and key considerations in conducting due diligence. We continue on to explore the different types of intellectual property agreements that the intellectual property may encounter and the important aspects of those agreements. Next, we discuss review of the target company's practices for protection of its owned and licensed intellectual property, followed by brief discussion of intellectual property disputes. We close the chapter with special considerations for the intellectual property lawyer when reviewing the use, deployment, and development of artificial intelligence technologies.

Throughout the due diligence process, it is important for the intellectual property lawyer to keep in mind the nature of the target company's business. Throughout the due diligence process, the intellectual property lawyer should use this information to guide their review. For example, if at the outset of due diligence, it appears that the target company has no reason to own any patents, then the initial patent due diligence request may be to simple request identification of patents or patent applications, without asking for additional details. While the intellectual property due diligence lawyer must be thorough in their due diligence, minimizing off-topic or unnecessarily detailed requests can help build rapport and generate good will.

Similarly, the intellectual property lawyer should understand the structure of the acquisition and how that may impact elements of the due diligence review. This is particularly important in a carve-out transaction where the buyer will likely not be acquiring a fully self-sufficient business. Therefore, the intellectual property lawyer must pay attention to which assets will be transferring in the sale and identify where any licenses between the target company (long term or transitionary), transition services, or replacement licenses or services may be required, and any risks to the buyer post-acquisition due to the loss of access to any non-transferring intellectual property.

Throughout the process, the intellectual property lawyer must keep notes to record what materials have been reviewed, follow up due diligence requests sent to the target company, due diligence findings, and other important information regarding the due diligence process. These notes will aid the intellectual property lawyer to draft any due diligence reports required by the buyer but also serve a more practical purpose. Acquisitions may at time stretch out over long periods of time, and even if parts of the deal team remain continuously active on the acquisition, weeks or even months may pass between the intellectual property lawyer's active involvement in the due diligence process and other aspects of the transaction. When the intellectual property lawyer finally drafts their portion of the due diligence report, they need to be prepared to tailor the report to the buyer's needs. Some buyers will only want red flags and key findings regarding valuable assets, while other buys may want an exhaustive report of the materials reviewed, lower materiality findings and issues, and detailed recommendations for post-acquisition integration.

Due Diligence in Corporate Transactions

End of Document

§ 8.02 Due Diligence for Specific Forms of Intellectual Property

[1] Patents

[a] Background

Patents are a form of intellectual property that provide inventors with exclusive rights to their inventions to encourage invention, investment in technology, and disclosure of inventions. In the U.S., patent rights are established under and governed by federal law. Patents under U.S. fall within three types: utility patents, which protect new and useful processes, machines, manufactures (processes for creating tangible articles or commodities), and compositions of matter;[1] design patents, which protect new, original, and ornamental designs for an article of manufacture;[2] and plant patents, which protect distinct and new varieties of plants.[3] Patent rights are not automatic upon invention, and the inventor (or its assignee), must apply for patent protection within statutorily prescribed time period. Patent inventors must be natural persons, and ownership initially vests with the individual inventor(s), who may freely assign ownership to another person. If an invention meets patentability requirements and a patent is granted, the owner of the patent has time-limited exclusive rights to make, use, sell, offer to sell, and import the patented invention.

[b] Due Diligence Requests

The intellectual property lawyer begins the patent due diligence process by requesting a list of all patents and other invention related applications, filings, and issuances. This list should include issued patents, reexaminations, and reissues, and patent applications, including divisionals, continuations, and continuations-in-part. The request should also include related information for each such item, including:

- Identification of record and beneficial owners;
- The applicable jurisdiction(s);
- The patent number, application serial number, and other similar identifiers;
- The title;
- Filing, priority, and issue dates;
- Classification codes;
- The type of claimed invention; and
- Approaching maintenance and other deadlines (the forward-looking duration will depend on the deal timing).

[c] Independent Search and Verification

---

[1] *35 U.S.C. § 101*.

[2] *35 U.S.C. § 171*.

[3] *35 U.S.C. § 161*.

The intellectual property lawyer must also conduct independent searches to verify the accuracy of the materials provided by the target company, identify any additional patents and related items that were not disclosed, and review additional information in the official office records. The U.S. Patent and Trademark Office (USPTO) and other applicable global patent offices have publicly available online databases. The intellectual property lawyer may also utilize commercial search solutions that access all applicable databases and produce a single consolidated approach. In addition to verifying the information that the target company provided, the intellectual property lawyer should use its independent searches to review:

- Assignments by the individual inventors;
- Chain of title, including any gaps or inconsistencies;
- Recorded security interests and releases;
- Current status of the patent or application, noting in particular any upcoming filing or fee deadlines;
- Office actions; and
- Recorded licenses.

The intellectual property lawyer cannot rely entirely on independent searches for patent due diligence, however. First, there is typically some lag time between filings and actions occurring and being posted to the publicly available databases, which may vary depending on USPTO staffing and other factors. Second, and more importantly, patent applications are generally not published until 18 months after the earliest filing date, and in certain instances publishing may be withheld for a longer period of time.

[d] Substantive Review of High Value Patents

If the target company's intellectual property portfolio includes any patents or applications that are particularly valuable (e.g., cover a large portion of the target company's product line, have a high defensive value for counterclaims to third-party infringement claims, or otherwise are financially or strategically important to the purchases), then the intellectual property lawyer will likely conduct a substantive review of those high value patents. Typically, the intellectual property lawyer will engage a patent prosecution attorney for this review to assess the scope, validity, and enforceability of the patent. As part of this review, the intellectual property lawyer may request that the target company provide copies of any patentability and validity searches or opinions or may conduct its own independent analysis. The intellectual property lawyer may also seek to review the files of the inventors and the patent prosecution attorney, as well as the patent prosecution file history, to identify any potential inequitable conduct issues that could limit enforceability.

[2] Copyrights

[a] Background

Copyrights are a form of intellectual property that provide individuals and businesses with certain exclusive rights to their original literary, artistic, musical, and other statutorily defined works. In the U.S., copyrights are generally established under and governed by federal law, though there are state law copyright protections that may apply to the extent outside of preemption. Copyright protection applies automatically under U.S. law upon creation of a qualifying work. Unlike patents, copyrights are not always initially owned by the individual natural person authors. Through the concept of "work made for hire", works created by employees within the scope of their employment, or works meeting certain criteria are specially ordered or commissioned by party, the employer or party that commissions the work is deemed to be the initial owner.[4] The owner of the copyright has time-limited exclusive rights to reproduce, prepare derivative works, distribute, publicly perform, publicly display, and publicly transmit.

---

[4] See *17 U.S.C. § 101*, *§ 201*.

[b] Due Diligence Requests

Similarly to patents, the intellectual property lawyer begins the copyright due diligence process by requesting a list of all registered copyrights and other copyright related applications and filings, as well as a list of any material unregistered copyrights.[5] The request should also include related information for each such item, including:

- Identification of record and beneficial owners;
- The applicable jurisdiction(s);
- The registration number and other similar identifiers;
- The title; and
- The registration date.

[c] Independent Search and Verification

The intellectual property lawyer must also conduct independent searches to verify the accuracy of the materials provided by the target company, identify any additional copyright registrations and related items that were not disclosed, and review additional information in the official office records. The U.S. Copyright Office and other applicable global copyright offices have publicly available online databases. In addition to verifying the information that the target company provided, the intellectual property lawyer should use its independent searches to review:

- Chain of title, including any gaps or inconsistencies;
- Recorded security interests and releases;
- Current status of the registrations and renewals;
- Recorded licenses; and
- Recorded statutory termination notices.

The U.S. Copyright Office online database only includes information on copyright registrations from 1978 and later, and foreign databases may have similar limitations. Since copyrights have a very long duration, the intellectual property lawyer may need to conduct an in-person review of U.S. Copyright Office records, particularly if the target company is a media company or otherwise holds high-value copyrights pre-dating 1978.[6]

The intellectual property lawyer should also review public marketing and other materials of the target company for material copyrightable works, such as websites and social media. Possible items of interest include advertising and marketing materials, white papers and other literary works, product documentation, and training materials. The intellectual property lawyer should pay particular attention to materials that are only made available to paid customers or from which the target company, directly or indirectly derives financial benefit.

[d] Use of Third-Party Works

As part of its review of the target company's copyrights, the intellectual property lawyer should pay particular attention to any third-party works that have been integrated into the target company's works. This can take many forms, but most commonly as images, video, and audio used in used in marketing and other materials and third-party components (including open source software) used in proprietary software. The use of such third-party works without a license, or not in compliance with the applicable license terms,

[5] Unlike patents, U.S. copyright protection exists immediately upon authorship. Registration of copyrights provides key enforceability benefits, but unregistered copyrights retain value and may later be registered.

[6] The U.S. Copyright Office is currently testing a virtual card catalog for older copyright registrations, but it does not guaranty the accuracy or quality of the online records.

presents a risk of an infringement claim. While many such uses are made without the specific intent to infringe a third-party's works, an infringement claim could lead to significant liability or business disruption for the target company depending on the nature and scope of the use. See further discussion on intellectual property licenses in Section [3][b] below.

[e] Moral Rights

Moral rights can be broadly described as authors' or artists' interests and rights in controlling the use of their creative works. Moral rights are not an element of copyright, but rather a related right tied to work's original creator. U.S. law has very limited moral rights under the Visual Artists Rights Act of 1990 (*17 U.S.C. § 106A*), which are limited to visual works of art. However, many foreign jurisdictions have much stronger moral rights, so it is important that the intellectual property lawyer engage local counsel when conducting due diligence involving works created outside of the U.S.

[3] Trademarks

[a] Background

Trademarks are a form of intellectual property that is used to indicate the source or origin of goods or services and distinguish a person's goods or services from another's.[7] Trademarks may consist of words, names, phrases, symbols, designs, colors, sounds, and other devices, and combinations of the foregoing. Rights in trademarks under U.S. law are established and maintained by commercial use of a mark. Trademark rights in the U.S. arise under both federal and state law, including common law unfair competition principles. Registration of trademarks is not required, but registration confers additional benefits onto the owner. Trademarks do not have a fixed term or duration but can be lost through nonuse and certain other acts or omissions.[8]

[b] Due Diligence Requests

Again, the intellectual property lawyer begins the trademark due diligence process by requesting a list of all trademark registrations, applications for trademark registration and other related applications and filings, as well as a list of any material unregistered trademark rights. The request should also include related information for each such item, including:

- Identification of record and beneficial owners;
- The applicable jurisdiction(s);
- The registration number, application serial number, and other similar identifiers;
- Filing and registration dates;
- Approaching maintenance and other deadlines (the forward-looking duration will depend on the deal timing).

[c] Independent Search and Verification

The intellectual property lawyer must also conduct independent searches to verify the accuracy of the materials provided by the target company, identify any additional copyright registrations and related items that were not disclosed, and review additional information in the official office records. The USPTO and other applicable global trademark offices have publicly available online databases. There are also commercial services that query multiple jurisdictional databases and provide a consolidated result list. In

---

[7] Technically trademarks are for identifying and distinguishing goods, while service marks are for identifying and distinguishing services, but in general usage "trademarks" are broadly used to cover indicia of origin for all goods and services.

[8] U.S. federal trademark registrations are term limited but can be repeatedly renewed so long as certain conditions are met.

addition to verifying the information that the target company provided, the intellectual property lawyer should use its independent searches to review:

- Chain of title, including any gaps or inconsistencies;
- Recorded security interests and releases;
- Current status of the registrations and applications, noting in particular any upcoming filing or fee deadlines;
- The goods and services categories applicable to each trademark;
- Recorded licenses; and
- Recorded statutory termination notices.

[d] Substantive Review of Trademarks

While some trademarks will have little to no value to the buyer post-acquisition, in many acquisitions core brand trademarks are highly valuable and therefore additional substantive review is warranted. As with patents, the intellectual property lawyer should engage a trademark attorney to assist with this substantive review to assess potential issues with the scope, validity, or enforceability of the trademarks. In particular, the intellectual property lawyer should assess whether the trademark registrations cover the key jurisdictions and categories of goods and services that are material to the buyer. This review will typically include assessing whether other parties may hold rights to use the same or similar marks in other jurisdictions, additional goods and services, or additional trade channels. Additional, the intellectual property due diligence lawyer should identify any facts that may lead to loss of trademark rights, including nonuse, licensing without adequate quality controls (commonly referred to as naked licensing), genericization (when the mark becomes primarily known to the public as the good or service itself, rather than the source of origin of the good or service), assignment of marks without their associated goodwill, or assignment of intent-to-use applications separate from substantially all of the business to which the mark pertains.

[e] Domain Names

While domain names are not themselves trademarks, they are often grouped with trademarks for intellectual property due diligence purposes because domain names, like trademarks, uniquely identify companies and/or their products and services, and domain names often use elements or registered or unregistered trademarks. The intellectual property lawyer should request from the target company a list of domain names owned or used by the company, including for each the registrant individual and entity, the registrar and the renewal dates. The intellectual property lawyer should confirm the accuracy of the information provided by searching each such domain name via the WHOIS search available at ICANN and most domain registrars' websites. The intellectual property lawyer will be particularly reliant on the target company's due diligence responses regarding domain names because there are no reliable methods to search for domain names by the registrant entity.[9]

The intellectual property lawyer will likely discover through WHOIS searches that some of the domain names have registered using private registration. How exactly this appears in WHOIS searches will vary based on the service used, but they all serve to mask the identity of the registrant by inserting an intermediary as the registrant of record. The intellectual property lawyer should request that the target company provide evidence of ownership of each privately registered domain name. This most typically is in the form of a screen shot from the registrar's domain management portal showing the domain name and registrant information.

---

[9] While there are some "reverse WHOIS" lookup tools available online, the results from these tools tend to be inconsistent and inaccurate.

It is frequently the case with domain names that some may be registered only in the name of an individual, typically one of the information technology employees of the company, but occasionally a third-party contractor. The intellectual property lawyer should flag this for the corporate lead lawyer and recommend that the registration be updated prior to closing. However, the buyer and the target company should coordinate on the timing of such an update to ensure that this does not interfere with any further transfer of the registration at closing.

[4] Trade Secrets

Trade secrets broadly include any information that is a secret and that gives the owner a competitive economic advantage. Accordingly, trade secrets are distinct from other forms of intellectual property, which are generally public and derive their value from public use. Trade secrets are governed in the U.S. by both federal and state laws, including common law unfair competition principles. The intellectual property lawyer will typically only request a general description of trade secrets and other similarly sensitive information, such as know-how, unpatented technologies, and processes. While many of these items may not qualify as trade secret status under applicable law, the interest from a due diligence perspective is the same because the focus of the review is primarily on the measures that the target company takes to protect the confidentiality of sensitive information The intellectual property lawyer should also request details and copies of policies regarding the protection of trade secrets and other confidential or sensitive information. See Section [4] for further discussion of review of trade secret protection policies.

[5] Proprietary Software

Software is not a separate form of intellectual property, but rather a combination of other types of intellectual property. It qualifies as a copyrightable work of authorship, may frequently contain trade secrets in the form of valuable algorithms and techniques, may practice patentable inventions, and often includes trademarks within its name, design, and packaging. When present, proprietary software is also often a particularly valuable part of the target company's intellectual property portfolio. Proprietary software may be the target company's primary product or a significant component of its services offerings. It may also be a critical element of the target company's backend operations, literally running the company. Therefore, when proprietary software is part of the target company's intellectual property portfolio, the intellectual property lawyer must conduct extensive due diligence to identify potential issues that may impact its value or expose the target company to liability.

In addition to conducting due diligence on the individual intellectual property components discussed above, the intellectual property lawyer should submit due diligence requests regarding the software more comprehensively as a whole. The intellectual property lawyer should inquire about:

- The function of the software and how it is used in the business;
- Whether the software is made available or distributed to customers or other third parties, and if so, in what manner (e.g., installed on third party devices, provided as a hosted software-as-a-service or platform-as-a-service offering, etc.);
- Whether the software was developed by or on behalf of the company or obtained through an acquisition;
- Whether employees, third party contractors, or a combination were and are involved in development and maintenance of the software, and obtain copies of employment, contractor, development, or other agreements related to such work;
- Known defects, bugs, or other issues that may prevent the target company from fulfilling its contractual obligations to customers or from efficiently operating its business; and
- All third-party components used in, combined with, or relied upon to develop and run the software, including open source software components.

The intellectual property lawyer should take particular care to identify any potential issues clouding title and ownership of the software. If the software was acquired in an acquisition of another company, the intellectual property lawyer should review the purchase agreement and disclosure schedules for any abnormal representations or any disclosures that may raise concerns. If the software was developed by or on behalf of

the target company, the intellectual property lawyer should ensure that there are written agreements with all developers that adequately assign ownership of the software to the target company.[10] The intellectual property lawyer should also closely review the applicable license agreements for any third party components to ensure that the target company's use of the third party components is permitted and identify any material restrictions that may impact the buyer's post-acquisition plans for the target company.[11]

End of Document

[10] See Sections [3][d] and [4] below for discussion of employee and third party developer agreements.

[11] See Section [3][b][ii] below for discussion inbound license agreements and subsection [A] for specific discussion of open source software.

§ 8.03 Intellectual Property Agreements

[1] Introduction

The types of intellectual property agreements to which the target company may be a party can vary depending on the target company's business. Accordingly, the intellectual property lawyer should request copies of all agreements relating to intellectual property that is owned, used, or held for use in the business, but the request should also specifically identify a number of types of agreements, including:

- Form customer agreements if the target company's business involves licensing or distributing any intellectual property, along with agreements for key customers;[12]
- Licenses, covenants not to use, or other agreements granting permissions or waiving rights to intellectual property;[13]
- Acquisition, sale, or transfer of intellectual property;
- Development, research, collaboration, strategic partnership, joint venture, and other agreement related to the development or exploitation of intellectual property;
- Indemnification agreements (other than agreements entered into in the ordinary course where indemnification is incidental to the overall agreement);
- Settlement and other agreements related to resolution of intellectual property disputes; and
- Agreements granting any lien or other encumbrance on intellectual property.

[2] Customer Agreements

The intellectual property lawyer's primary concern when reviewing customer agreements is maintaining the target company's ownership of and the right to use its intellectual property. The customer agreements should grant to customers appropriately limited rights[14] and expressly retain for the target company all other rights in and to the target company's intellectual property. The intellectual property lawyer must be particularly mindful of any exclusive or perpetual licenses and will need to conduct further due diligence to assess the impact of any such licenses.

Many customer agreements, particularly those on customer forms or that are heavily negotiated by customers, will include provisions assigning ownership of work product to the customer. The intellectual property lawyer must closely review these provisions to ensure that (i) only the intellectual property that was developed specifically for the customer is assigned to the customer and (ii) the target company retains ownership of all pre-existing or independently developed intellectual property. An overbroad work product assignment provision creates a risk that the target company has assigned to a customer valuable intellectual property and may then be infringing that customer's intellectual property rights by using that intellectual property elsewhere in the

---

[12] Copies of agreements with key customers will typically be requested elsewhere in the due diligence requests, and therefore can be excluded here.

[13] Copies of agreements with key vendors will also typically be requested elsewhere in the due diligence requests. However, the materiality threshold is generally not appropriate for intellectual property agreements, so this intellectual property request will often expressly include all inbound license agreements from vendors.

[14] The scope of appropriate rights will depend on the target company's business.

target company's business. If the intellectual property lawyer discovers any such issues, they will need to conduct further due diligence to determine the nature of the intellectual property that was assigned and explore potential mitigation strategies.

[3] License Agreements

[a] Outbound Licenses

The intellectual property lawyer must closely review all outbound licenses (agreements where the target company grants rights to licensees to use the target company's intellectual property) that are not ordinary course customer agreements. In many instances the target company will not have any outbound licenses other than customer agreements. The intellectual property lawyer must ensure that it understands the business context around each outbound license and will likely need to discuss it directly with the target company's management. In general, key issues to look for are any encumbrances or other restraints on the target company's exploitation of its intellectual property, including exclusivity or non-competition; perpetual licenses; any sublicensing rights and limitations; and non-market representations and warranties or indemnification. If the outbound license involves trademarks of the target company, the intellectual property lawyer should also ensure that the agreement includes adequate quality controls. The intellectual property lawyer will need to coordinate closely with the corporate lead lawyer and buyer decisionmakers to ensure that the buyer understands the impact of the outbound license on the buyer's valuation of the target company.

[b] Inbound Licenses

The target company will always have some inbound license agreements if it is an operating company. In many instances, these will be limited to standard, non-negotiated vendor license agreements for business software and software-as-a-service (SaaS) products. The intellectual property lawyer should coordinate with the corporate lead lawyer to determine what, if any, due diligence review the intellectual property lawyer should conduct for such inbound license agreements. Often due diligence of such agreements is limited to general contract review by the corporate due diligence team in combination with review of the business terms of such agreements by the buyer.

There will, however, be instances where the inbound license agreements are more material and review by the intellectual property lawyer is required. This will typically include any patent or trademark specific license agreement, or a license agreement for software or SaaS that is included in the target company's products or services, which is a critical component of the target company's information technology infrastructure or represents a particular high monetary value. In such cases, the intellectual property lawyer will typically review the license agreement in full detail, similarly to the level of review required when negotiating such an agreement. Key elements of such review will include:

- Scope: Scope includes the subject licensed intellectual property, the extent of the license rights, and the territory. The intellectual property lawyer should closely review what license rights are included or excluded and whether or not the licensed territory covers all key jurisdictions to the buyer. For patent and trademark license agreements, the licensed field is particularly important to closely analyze.
- Term and Termination: The intellectual property lawyer should review the term and termination provisions in consultation with the buyer and together with all other terms of the agreement. The buyer may prefer a long term without easy termination in some cases, and in other cases may want flexibility. The intellectual property lawyer should pay particular attention to the licensor's termination rights and how the license in wound down in the event of a termination.
- Exclusivity: Whether or not the license is exclusive will weigh heavily on the value to the target company and the buyer.

- Expansion Rights: The intellectual property lawyer should assess whether and to what extent the target company has the right to expand the scope of the license, whether by including additional licensor intellectual property in the license, or by expanding the scope of the license, including rights of first refusal or rights of first negotiation. The intellectual property lawyer should identify the conditions attached to any such expansion and whether the target company can unilaterally elect expansion or further negotiation is required.
- Sublicensing: The intellectual property lawyer should review any restrictions on sublicensing and consult with the buyer to determine if this conflicts with the buyer's business plans.
- Fees and Royalties: Intellectual property licenses may have complex revenue or profit based royalty structures. The intellectual property lawyer must understand how fees are determined and confirm that this aligns with the buyer's expectations.
- Maintenance and Enforcement Rights and Responsibilities: The intellectual property lawyer should ensure that the agreement includes appropriate obligations on the licensor to maintain and enforce its intellectual property rights. Alternately, in exclusive license agreements the target company may have rights to take actions to maintain and enforce the intellectual property on its own, and to join the licensor in any action, as necessary.
- Warranties and Indemnification: For all licenses, the intellectual property lawyer will want to pay attention whether to what extent the ownership, validity, enforceability, patentability, and/or registrability of the intellectual property, and whether the licensor will indemnify the target company for any third-party claims of intellectual property infringement. For software and SaaS licenses, the intellectual property should assess any performance warranties or related obligations (such as service level and availability commitments) and indemnification for other issues such as breach of confidentiality or data security obligations.
- Assignment: If the acquisition is structured as an asset sale, the intellectual property lawyer must be careful with assignment provision (or the lack thereof). In contrast to most agreements, license agreements under U.S. law are generally not assignable by the licensee with consent from the licensor unless the agreement expressly states otherwise. There are exceptions, but the intellectual property lawyer will need to carefully review applicable law if not relying on express assignment rights in the agreement.

[c] Open Source Software Licenses

Open source software licenses are a unique subset of inbound license agreements. Open source software is typically made available to the general public online and is "free" to download and use.[15] However, there are license terms that attach to open source software, and some open source licenses that include restrictive terms that may limit the licensee's rights with respect to its own intellectual property or otherwise. These licenses are commonly referred to as "reciprocal" or "copyleft" licenses. The most common such open source licenses are the GNU General Public License (GPL) and the GNU Lesser General Public License (LGPL).

Where the target company uses open source software with its own proprietary software, the intellectual property lawyer must review the applicable open source licenses to assess the potential impacts on the target company. As always, the starting point is a due diligence request identifying all open source software, the applicable license type and version, how the open source software is used and combined with the proprietary software, and whether or not the open source software has been modified by or on behalf of the target company. This request is generally also coupled with a request for production of the target company's policies and procedures regarding the use of open source software. If the target company does

[15] Open source software has various definitions depending on the source, with the Open Source Initiative and Free Software Foundation definitions being the most commonly used. However, there are "free" software licenses that do not meet these definitions but are still commonly grouped together with open source software. For purposes of this discussion, we consider all software that is made available to the general public at no monetary charge to be open source software.

not have robust policies and procedures for the review and documentation of open source software usage or does not adequately audit and enforce compliance with such policies, then the intellectual property lawyer should approach any open source software list produced by the target with healthy skepticism. In this case, the intellectual property lawyer may recommend that the buyer requires the target company to allow a third party open source software audit to ensure adequate due diligence.

A full review of the common open source licenses is out of scope for this book. The intellectual property lawyer must be familiar with the terms of the common open source licenses and carefully review the terms of any applicable licenses with which it is not familiar. The intellectual property lawyer should also confirm with the corporate lead lawyer and the buyer whether the intellectual property lawyer should seek to independently verify that the identified applicable license terms are correct.[16] The intellectual property lawyer should review each open source software component to determine whether any problematic license terms apply and then will likely need to conduct further due diligence through written follow ups and discussions with target company management to determine whether and to what extent there are issues. The most common major open source issue is use of open source software in a manner that requires the target company to license portions of its proprietary software in source code form under the same open source license terms as the open source software component. The intellectual property lawyer should also be attentive to attribution, license pass through, and other similar requirements that do not directly threaten the target company's proprietary software but still create a risk of enforcement or license revocation. The intellectual property lawyer must also pay attention to open source licenses that are incompatible – that is, for the target company to fully comply with one open source license it cannot fully comply with another open source license.

[d] Acquisition, Sale, or Transfer Agreements

The intellectual property lawyer will need to review any agreements to acquire or dispose of material intellectual property to determine the exact intellectual property involved and whether any unperformed obligations by any party remain. For an acquisition of intellectual property by the target company, the intellectual property lawyer should pay particular attention to any reversion other type right that could cause the target company to lose ownership of the applicable intellectual property.

[e] Development and Exploitation Agreements

Development and exploitation agreements can take on many forms. Basic development agreements where a third party developed intellectual property for the target company are the most basic.[17] The intellectual property lawyer will need to review the agreement to confirm that the developer is bound by appropriate confidentiality obligations and that target company acquired all rights to the intellectual property developed for the target company ("work product") by way of a present assignment.[18] Typically the third party developer will retain ownership of certain pre-existing or independently developed intellectual property that may be included with or relied upon the work product, in which case the intellectual property must ensure that the target company has adequate license rights to such retained intellectual property and take note of any material restrictions to such license.

Joint development and joint exploitation agreements tend to be much more complex, and all the possible permutations of ownership and rights issues are beyond the scope of this chapter. The intellectual property lawyer will need to review such agreements to understand in particular what intellectual property of all

---

[16] Open source license terms can often be verified through online open source repositories, such as Github. However, the intellectual property lawyer must exercise caution because the applicable license terms can change and may not be the same as those applicable when the target company received the open source software.

[17] See Section [4] below for a discussion of employee intellectual property assignment agreements.

[18] Reliance on a "work made for hire" provision alone is not adequate because (i) "work made for hire" only applies to copyrights and (ii) the Copyright Act of 1976 (*17 U.S.C. §§ 101 et seq.*) has specific requirements for works made for hire created by non-employees.

parties is involved, how ownership of intellectual property is allocated, what rights and restrictions each party has regarding the exploitation of intellectual property, and what happens upon termination of the agreement. The intellectual property lawyer should be attentive to any imprecise drafting that may lead to disputes over ownership or other rights.

[f] Other Intellectual Property Agreements

The remaining types of intellectual property agreements are less common, and review of such agreements will always be heavily context sensitive. The intellectual property lawyer will need to ask additional questions to the target company to understand the business or legal need for such agreements. As with other intellectual property agreements, the intellectual property lawyer's review of these agreements should focus on potential issues that restrict the target company's rights, grant rights to third parties, require the payment of any amounts, or otherwise materially impact the value of the intellectual property or the viability of the buyer's post-acquisition business plans.

§ 8.04 Protection of Intellectual Property

While elements of the target company's policies and procedures regarding the protection of intellectual property will arise during due diligence of each of the substantive intellectual property topic, the intellectual property lawyer should also seek to understand the target company's general policies and procedures regarding the protection of intellectual property. This will help the intellectual property lawyer identify any systemic gaps or other broad issues that indicate an increased risk of intellectual property issues. The intellectual property lawyer should also recommend post-acquisition actions that the buyer should take to better manage and protect the target company's intellectual property portfolio.

The specific due diligence questions to ask regarding protection of intellectual property will vary greatly depending on the target company's business and intellectual property portfolio. Therefore, while the intellectual property lawyer will include broad requests for documents in the initial due diligence requests, the intellectual property lawyer will likely need to ask focused following up due diligence questions in writing or in discussions with the target company's management.

At a minimum, the intellectual property lawyer will need to review the policies, procedures, and agreements regarding confidentiality and intellectual property assignment obligations of employees and contractors. Ideally, the target company will have standard agreements that all employees and independent contractor sign, which include robust confidentiality obligations and a present assignment of all intellectual property created by the employee on target company time, using target company resources, or that is related to the target company's business. The intellectual property lawyer should work closely with the labor and employment lawyer to ensure that these provisions provide adequate protection for the target company while remaining in compliance with applicable labor laws. The intellectual property lawyer must also be familiar with applicable laws that limit the scope of inventions assignment by employees.[19] Where the target company does not consider itself to be in the business of developing and exploiting intellectual property, these policies may only be memorialized in an employee handbook, in which case the intellectual property lawyer will need to inquire whether employees sign any sort of acknowledgement of the handbook policies and whether this presents any enforceability concerns.

The intellectual property lawyer will also need to review all policies related to the target company's protection of trade secrets and third party intellectual property. In addition to requiring confidentiality obligations of employees, the intellectual property lawyer should inquire about policies limiting access to employees with a need to know and practices when sharing trade secrets and confidential information with third parties. The intellectual property lawyer should also understand the target company's policies and procedures for ensuring its compliance with licenses and other intellectual property agreements with third parties, including whether and how the target company conducts audits.

If the target company's business has high value in particular types of intellectual property, then the intellectual property lawyer will want to inquire about policies tailored to those types on intellectual property. For example, if the target company develops and exploits inventions, then the intellectual property lawyer must inquire about policies

---

[19] Approximately half of the states in the U.S. have some degree of restrictions on mandatory assignments of inventions by employees. The intellectual property lawyer should consult with local counsel as needed to ensure compliance and should pay particular attention to how local laws and courts handle assignments that exceed what is statutorily permitted. In some instances, this may void the assignment entirely, while in others the assignment may simply be limited to that which is statutorily permitted.

regarding inventions disclosures and freedom-to-operate and freedom-to-use analyses. If the target company has high brand recognition with valuable trademarks, then the intellectual property lawyer should identify the target company's policies regarding trademark clearance, registration, usage, and quality control. And for all types of intellectual property, the intellectual property lawyer should understand the target company's policies regarding intellectual property designations and monitoring and enforcement of third-party infringement.

Due Diligence in Corporate Transactions

End of Document

§ 8.05 Intellectual Property Disputes and Litigation

As part of the intellectual property due diligence process, it is important to learn about any past, pending, or threatened disputes or litigation involving intellectual property. The intellectual property lawyer should request that the target company provide details and copies of all related document for any actual or potential dispute or litigation. These requests should include: any allegations that the target company or its products, services or business infringe any third party intellectual property rights; any allegations that any third party is infringing the target company's intellectual property rights; and any challenges by or against the target company challenging the ownership, validity, enforceability, patentability, or registrability of a party's intellectual property. These requests should extend to correspondence short of formal court or administrative actions such as cease-and-desist letters, notices, and offers to license. The intellectual property lawyer should also review litigation searches conducted by the due diligence team (or perform their own litigation searches) to identify any intellectual property related litigation that the target company may not have disclosed.

Review of each intellectual property dispute will depend on the facts and circumstances of such claims. For active or threatened disputes, the intellectual property lawyer should, potentially in conjunction with litigation counsel, collect as much information as possible to make an informed assessment of the potential liability exposure, risk of injunctive or other equitable relief, or other harm that may occur to the target company. For resolved past disputes, the intellectual property lawyer should review all judgements, settlements, and other related agreements to assess any ongoing restrictions on the parties, outstanding performance obligations (such as payments of awards or settlement amounts), and other material impacts on the target company, its business, or its intellectual property.

§ 8.06 Special Considerations for Artificial Intelligence Technologies

With the rapid recent growth of artificial intelligence (AI) technologies in general, and specifically generative AI technologies, the intellectual property lawyer must consider how the use of AI in business and product development influences the due diligence process. The intellectual property lawyer will need to conduct different levels of due diligence review base on the target company's use of technologies, which can roughly be broken up into four major categories: (i) use of third party AI technologies in general business operations; (ii) development AI technologies or training of AI models by the target company itself; (iii) inclusion of AI technologies in the target company's product or service offerings to its customers; and (iv) use of AI technologies in the target company's intellectual property development processes. The intellectual property lawyer will need to coordinate review of AI technologies with other members of the due diligence team because AI issues cross many legal disciplines depending on the manner of use. It is important that some member of the team take responsibility for assessing compliance with the growing number of AI-specific laws, and a key part of the due diligence process is to review the target company's compliance policies and procedures, including compliance with disclosure and anti-bias requirements.

If the target company uses third-party AI technologies for general business operations, then the intellectual property lawyer's AI due diligence will remain mostly the same as described previously in this chapter. When reviewing the relevant license agreements for AI technologies, the intellectual property lawyer should pay careful attention to confidentiality provisions and rights for the licensor to use the target company's data, or derivatives thereof, in any manner outside of the scope of providing services to the target company. The intellectual property lawyer will need to understand what data the target company provides to the AI technology licensor, and if any third party data in involved, assess whether there are any conflicts between the rights granted under the AI license agreement and the rights that the target company has to use such data under its agreements with customers or third party data providers. The intellectual property lawyer should also carefully review indemnification and limitations of liability provisions to understand what potential liabilities may not be covered by the AI technology licensor.

When the target company is developing its own AI technologies or training its own AI models, the intellectual property lawyer will need to conduct significant additional due diligence and will likely need to have discussions with the target company's management and engineering leads. It is important to understand what elements of the AI technologies the target company owns and what elements are licensed from third parties and to identify any significant business risks that may arise from losing rights to use the elements licensed from third parties. The intellectual property lawyer will also need to identify the sources of any third-party data used in developing the AI technologies or training the AI models and review all relevant agreements to ensure that the target company has adequate rights to use such data. If the target company uses any publicly available data without an express license to such data, the intellectual property lawyer should request copies of any fair use analysis that the target company or its lawyers have performed and conduct an independent fair use analysis. However, the intellectual property lawyer should keep in mind, and should advise the corporate lead lawyer and the buyer, that application of fair use AI training is far from settled law, with no U.S. court having made a substantive ruling to date and numerous cases currently working their way through the courts.

If the target company includes AI technologies (whether first party or third party) in its product or service offerings, the intellectual property lawyer should review customer agreements for provisions that adequately the target company from customer claims and other related liabilities. The customer agreements must include provisions providing the target company, and if applicable its licensors, the right to use customer data consistent with the AI technologies process and use data, whether for the customer's benefit or otherwise. The intellectual property lawyer should also assess the indemnification and limitations of liability provisions for any gaps compared to the

corresponding provisions in the applicable third-party AI technology license agreements and otherwise for liability exposure that the target company may have. If the applicable third-party AI technology license agreements include any required pass-through provisions or otherwise have terms that are necessary or advisable to pass-through to the customer to protect the target company, then the intellectual property lawyer should assess and note any discrepancies.

Finally, if the target company uses AI technologies in the process of developing its own intellectual property the intellectual property lawyer will need to engage in a fact intensive review to determine if, and to what extent, the target company's use of AI technologies limits the target company's rights in its intellectual property (and by extension, the value of that intellectual property). Currently under U.S. law, works and inventions that are created entirely by AI are not eligible for copyright or patent protection, respectively.[20] However, the U.S. Copyright Office, USPTO, and the courts all currently allow protection for the human created portions of works and inventions where AI has been used as a tool in the creative or inventive process. The law is currently too undeveloped in the area to draw bright lines, but the intellectual property lawyer will need to carefully review how the target company uses AI in its development processes. The intellectual property lawyer will likely also need to consult with copyright and patent specialists, as applicable, to assess and advise the buyer of the risks. The intellectual property lawyer should also be mindful of the potential for the buyer to inadvertently disclose information about its intellectual property development through the AI technologies and should assess the contractual (and potentially technological) protections in place to limit access and use of any information input to the AI technologies.

[20] See *Thaler v. Perlmutter, 130 F.4th 1039 (D.C. Cir. 2025)*; *Thaler v. Vidal, 43 F.4th 1207 (Fed. Cir. 2022)*.

1 Due Diligence in Corporate Transactions Chapter 9.syn

Chapter 9 Privacy and Data Security Due Diligence

Synopsis to Chapter 9 : Privacy and Data Security Due Diligence

---

End of Document

§ 9.01 Overview

[1] Introduction

Privacy and data security have become increasingly important during due diligence as regulatory frameworks evolve and are vigorously enforced. Acquisition targets across many industries process personal data to run their businesses and conduct their operations. The goal of data privacy and data security due diligence is to identify the privacy and security obligations that apply to the target company and any gaps between these obligations and the target company's practices. These obligations will depend on a variety of factors, including the nature, sensitivity, and volume of the data the target company processes; the purposes for which the data is processed; the industries and jurisdictions in which the target company operates; the customers or consumers the target company serves; the products and services the target company provides; the terms of contracts the target company has signed; and the representations the target company has made in privacy policies or other public statements. In addition to evaluating the target company's data privacy and data security compliance measures and materials, due diligence should include review and evaluation of any privacy or security incidents, complaints, and investigations, which can pose risks to both the target company and the buyer post-closing. In addition, personal data can be a valuable asset that a buyer may wish to acquire as part of a corporate transaction. Due diligence should include a review of whether the desired data can be lawfully transferred to the acquirer, as well as whether the acquirer's intended processing of the acquired data is permissible. Below is an overview of key concepts used in this chapter.

[2] Personal Data

Generally, the concept of "personal data" (and similar terms) as used in privacy laws includes information that relates to an identified or identifiable natural person, though some privacy laws extend this to include information about a household. While the scope and definition of "personal data," and similar terms such as "personal information," and "nonpublic personal information" vary depending on the applicable privacy law, such definitions are broad in many privacy laws, and due diligence processes and questions should be scoped accordingly. One example is the definition of "personal information" in the California Consumer Privacy Act, which "means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." *Cal. Civ. Code § 1798.140(v)(1)*. For consistency, within this chapter we use the term "personal data" as a general term for information regulated under privacy and data security laws.

[3] Data Subject

A "data subject" is a natural person to whom personal data relates. The terms used by privacy laws may vary. In the United States, the following terms are common: "consumer," "customer," or "individual." For consistency we use "data subject" within this chapter to address the concept of the individual (or sometimes household) that is the subject of personal data.

[4] Processing

"Processing" is a broad term for any operation or set of operations performed on data or information, including access, collection, use, analysis, disclosure, modification, deletion, and destruction. Privacy laws generally regulate the processing of personal data by persons and entities. Processing is often interpreted broadly, and

counsel should note that access alone is typically considered “processing” and therefore is subject to privacy law obligations.

[5] Controller

Many privacy laws distinguish between a person or entity that “determines the purposes and means of processing” of personal data and a person or entity that merely “processes” personal data on behalf of another person or entity. The former is often referred to as a “controller,” though similar terms across privacy laws include “business” and “covered entity.” The throughline in these concepts is that the “controller” has the ability to choose why and how personal data is processed and the primary responsibility for complying with privacy requirements. If the target company is a “controller” with respect to personal data, then the privacy due diligence process will typically involve review of additional obligations and documents, including privacy notices and consent flows.

[6] Processor

A “processor” is a party that processes personal data on behalf of a controller or other processor pursuant to a contract to provide services to or on behalf of the controller or other processor. The processor typically does not control or determine the purposes and means, or the “how” or “why,” personal data is processed, and therefore typically has more limited obligations under privacy laws. Similar concepts exist in a range of privacy laws and include “service providers” under the California Consumer Privacy Act and “business associates” under the Health Information Portability and Accountability Act. If the target company is a “processor” with respect to certain personal data, counsel should ensure that the target company’s processing does not exceed the authorization granted to it by the “controller.”

[7] Pseudonymization

Personal data can be obscured, hashed, or encrypted such that it cannot be used to identify an individual without the encryption/hash key or other information. Additionally, certain types of data identify a device but not a specific individual. Such information is generally referred to as “pseudonymous” information, as it is information that can be linked to a data subject with additional information. Unlike anonymized or deidentified information, “pseudonymous” information is typically still regulated as “personal data” by privacy laws, so due diligence should also address such data.

[8] Anonymization/Deidentification

If personal data is rendered anonymous or deidentified such that it cannot be used to identify an individual, then the personal data has been “anonymized” or “deidentified” and it is no longer personal data subject to the applicable privacy laws. Note that privacy laws may have differing requirements for anonymization or deidentification standards, so any due diligence process should take into account regulatory deidentification requirements if deidentified information is key for the target company’s business model or operations.

§ 9.02 Applicable Compliance Regimes

[1] Introduction

A key component of the privacy due diligence process is identifying which of the myriad privacy laws apply to the target company's business, operations, and data processing. To assist with this process, we have provided an illustrative list of privacy laws that commonly arise or pose certain specific risks in corporate transactions. However, given the rapid pace of evolution in privacy laws, we note that the list below of laws and regulations is not comprehensive. We expect that the regulatory privacy and security landscape will continue to change following publication of this chapter and thereafter and encourage counsel to remain aware of developments in this space and consult with knowledgeable privacy counsel as part of the due diligence process.

[2] Section 5 of the Federal Trade Commission Act

[a] Introduction

Section 5 of the Federal Trade Commission Act (*15 U.S.C. § 45*) (Section 5) is one of the most significant and versatile federal laws used to regulate U.S. privacy and data security practices by companies. It empowers the Federal Trade Commission (FTC) to prohibit "unfair or deceptive acts or practices in or affecting commerce." While the statute was enacted in 1914, it has evolved over time into the FTC's principal legal basis for addressing privacy and cybersecurity practices by businesses operating across all sectors of the economy regulated by the FTC. Section 5's broad applicability and scope means that due diligence counsel should be familiar with Section 5 and its applicability to a wide range of target companies.

[b] Applicability

Section 5 applies broadly to any "person, partnership, or corporation" engaged in commerce, with limited exceptions (e.g., certain common carriers and banks, which are typically regulated by other federal agencies). The FTC has used Section 5 to investigate and enforce against companies in a broad range of privacy and security matters, including related to targeted advertising, precise location data, biometric data use, and dark patterns.

[c] Key Privacy and Security Considerations

[i] Introduction

Section 5 prohibits regulated entities from engaging in "deceptive" and "unfair" practices. In this section, we focus on these prohibitions in the privacy and data security contexts, as well as on other guidance and materials promulgated pursuant to the FTC's Section 5 authority.

[ii] Deceptive Practices

A practice is "deceptive" if there is a material representation, omission, or practice that is likely to mislead a consumer acting reasonably under the circumstances. In the privacy context, this often relates to misstatements in privacy policies, terms of service, or user interfaces. The FTC has enforced against companies for misrepresenting their practices with respect to data collection, use, and disclosure, as well as misrepresentations related to the choices available to them. Deceptive practices

can also include inadequate or confusing disclosures, retroactive changes to privacy terms, and failing to honor consumer's choices or privacy settings. As a result, due diligence should include an evaluation of whether a target company clearly, accurately, and conspicuously describes its personal data processing practices in public disclosures, such as in a privacy policy or notice, and honors its stated privacy and security promises contained in such privacy policy or notice.

[iii] Unfair Practices

An unfair practice, by contrast, is one that causes or is likely to cause substantial injury to consumers that is not reasonably avoidable and is not outweighed by countervailing benefits. For example, this standard has been applied to organizations that fail to implement reasonable data security measures, even in the absence of an explicit promise to do so. The FTC has enforced against businesses for failing to encrypt sensitive data in transit, not monitoring network activity, using default or easily guessable passwords, and lacking internal access controls or employee security training. The Commission has made clear through consent orders and enforcement actions that it expects companies to adopt a risk-based, context-specific approach to data security, even in the absence of statutory mandates. As a result, due diligence should include an evaluation of whether a target company implements and maintains reasonable safeguards to protect personal data it processes, taking into account the nature of the personal data the target company processes and the risks posed by the unauthorized disclosure or use of such personal data.

[iv] FTC Privacy and Security Guidance

The FTC has emphasized principles such as data minimization, purpose limitation, and transparency as part of what constitutes reasonable data stewardship in both guidance materials and enforcement actions. Companies that collect excessive amounts of personal data without clear business need, use sensitive data in opaque or unexpected ways, or do not appropriately place data subjects on notice of personal data processing may be at risk of scrutiny.

[d] Enforcement

The FTC enforces Section 5 through administrative proceedings and civil actions in federal court. If the Commission determines that a practice is deceptive or unfair, it may issue a cease and desist order and, in some cases, seek injunctive relief, restitution, disgorgement, or monetary penalties. Privacy and security-related enforcement actions often result in consent orders that require the company to implement comprehensive privacy or information security programs, submit to independent assessments, and report to the FTC on compliance with the consent order for up to 20 years. These consent orders often also include detailed provisions on board-level oversight, data inventorying, employee training, and third-party vendor management. Moreover, the FTC's evolving enforcement priorities, including its recent statements on algorithmic bias, AI model training, and deceptive design (so-called "dark patterns"), underscore that Section 5 will remain a dynamic source of privacy law and risk. Buyers should be attuned not only to what a target company says in its policies, but also to how its products behave in practice, and whether its data practices meet consumer expectations and emerging regulatory norms.

[e] FTC Section 5 Due Diligence

Privacy and security due diligence under FTC Section 5 often includes review of:

- Public or data subject-facing representations regarding privacy and security in privacy policies, blog posts, marketing materials, and other public communications;
- Whether privacy policies or other representations would create risks if, or outright prohibit, the transfer of personal data to and/or its processing by an acquiring entity;
- Personal data processing activities, including any unusual, risky, or unexpected processing activities and comparison against the target company's representations regarding same;

- Safeguards, policies, and procedures to protect personal data, including comparisons against the target company's representations regarding same;
- Data subject complaints, consumer protection complaints, FTC investigations, consent orders, litigation, and enforcement actions relating to privacy and security; and
- Data breaches impacting personal data, including how they were resolved and whether third parties were notified.

[3] European Union General Data Protection Regulation (GDPR)

[a] Introduction

While this chapter is primarily focused on U.S. due diligence, a discussion of the EU General Data Protection Regulation (GDPR) is relevant both because its territorial scope can apply to U.S. target companies and because it provides a useful framework for evaluating obligations under other privacy laws. The GDPR expands the reach of EU privacy regulation extraterritorially. It also provides for significant penalties for noncompliance, with maximum penalties for certain violations set at the greater of €20 million or 4% of an organization's annual global turnover. The GDPR has subsequently influenced legislation in jurisdictions worldwide, including the Brazilian General Personal Data Protection Law (LGPD), the California Consumer Privacy Act and similar U.S. state laws, China's Personal Information Protection Law (PIPL), and the United Kingdom's own version of the GDPR post-Brexit. As a result, many of the key terms and concepts used in other privacy laws have their basis in the GDPR. In addition, the GDPR's extraterritorial reach makes it relevant to even U.S. counsel who represent or conduct due diligence on target companies that have EU operations, EU employees, or offer or sell products or services within the EU.

[b] Applicability

The GDPR's territorial scope is broad and extends outside of the borders of the European Union. It applies not only to organizations established within the EU but also to those *outside* the EU if they process personal data of individuals located in the EU in connection with offering goods or services or monitoring their behavior within the Union. This extraterritorial reach means that any company that collects or processes personal data of persons within the EU may be subject to the regulation. Corporate lawyers conducting due diligence must assess whether the target company, its affiliates, or its service providers fall within this broad scope, particularly in transactions involving international operations or digital platforms with EU users.

[c] Covered Personal Data

The GDPR protects "personal data," which it defines as any information relating to an identified or identifiable natural person. This includes not only clear identifiers such as names, addresses, and identification numbers, but also online identifiers (like IP addresses), location data, and factors specific to a person's physical, physiological, genetic, mental, economic, cultural, or social identity. The GDPR also distinguishes "special categories of personal data," such as data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic information, health information, sexual orientation, sex life, and biometric information used to identify a person, which are subject to stricter processing conditions. Unlike many U.S. laws, the GDPR also does not have any exemptions for nonprofit organizations nor personal data about data subjects in their employment or professional capacities.

[d] Key Requirements

[i] Introduction

The GDPR introduces a comprehensive framework of obligations for both data controllers and processors. Five key provisions relevant in the diligence process are described below.

[ii] Lawful Basis for Processing

Unlike many U.S. laws, the GDPR's default approach is to *prohibit* processing of personal data unless there is a specific, enumerated lawful basis upon which to do so. Under Article 6 of the GDPR, there are six recognized lawful bases for personal data. The most commonly used are the following:

- **Consent of the Data Subject.** Under the GDPR, consent to processing of personal data must be a freely given, specific, informed, and unambiguous indication of the data subject's agreement. Importantly, consent is revocable; a data subject must be able to withdraw their consent to processing at any time, and the controller must cease processing based upon such withdrawn consent. This makes consent a poor choice for many processing operations, and counsel should review target company privacy policies to identify whether material processing activities rely on consent.
- **Contractual Necessity.** A GDPR-regulated organization may process personal data when it is necessary for the performance of a contract with the data subject or to take pre-contractual steps at the data subject's request. Importantly, the contract at issue must be with the data subject; processing to perform under a contract with a third party, such as where a survey provider is collecting personal data pursuant to a contract with its customer, is not itself a sufficient lawful basis.
- **Legal Obligation.** Processing is permitted when it is required for compliance with an EU or EU Member State legal obligation to which the controller is subject.
- **Legitimate Interests.** Finally, the GDPR permits processing of personal data when it is necessary for the legitimate interests of the controller or a third party, except where they are overridden by the interests or fundamental rights and freedoms of the data subject. Organizations relying on legitimate interest as a lawful basis for processing should conduct and document a "legitimate interest analysis," which is a risk analysis that identifies the purpose of the processing (i.e., the legitimate interest for which the personal data will be processed); identifies whether the processing is necessary and proportionate for fulfilling the legitimate interest; and finally balances the processing that is necessary for fulfilling the legitimate interest against the interests and fundamental rights of the data subject, such as by analyzing the nature and sensitivity of the personal data to be processed, the reasonable expectations of the data subject, and the likely impact of the processing on the data subject and any safeguards that can be put in place to mitigate negative impacts. Legitimate interest analyses, if appropriately conducted and documented, can provide counsel with significant insight into a target company's practices and risk profile.

[iii] Transparency/Notice

The GDPR requires that controllers provide data subjects with clear, accessible, and comprehensive privacy notices that provide a range of information about the controller's personal data processing activities. These notices must specify, among other things:

- The identity and contact details of the controller (and, where applicable, its representative and Data Protection Officer)
- The purposes and legal bases for processing (including any legitimate interests)
- Categories of personal data processed
- Recipients or categories of recipients of the data
- Data retention periods

- The existence of and how to exercise data subject rights
- Whether data will be transferred outside the EU and the relevant safeguards
- The right to lodge a complaint with a supervisory authority
- The existence of any automated decision-making or profiling, if any, and the anticipated consequences or impacts thereof

These notice requirements are most commonly met through a public-facing privacy policy or notice posted on the controller's website, which should be reviewed and compared to the target company's actual practices and policies as part of the due diligence process.

[iv] Data Subject Rights

The GDPR provides data subjects with certain legal rights that grant them a level of control with respect to the processing of personal data about them. These rights include:

- **Right of Access.** Data subjects can obtain confirmation of whether personal data about them is being processed and, if so, access to the data and related information.
- **Right to Rectification.** Data subjects can request corrections to inaccurate or incomplete personal data about them.
- **Right to Erasure ("Right to be Forgotten").** Under certain conditions, data subjects can request the deletion of personal data about them.
- **Right to Restrict Processing.** Under certain conditions, individuals can limit the ways in which their data is processed.
- **Right to Data Portability.** Under certain conditions, data subjects can request personal data held by a controller be provided to them in a structured, commonly used, and machine-readable format to enable it to be easily transferred from one controller to another.
- **Right to Object.** Data subjects can object to processing carried out pursuant to the lawful bases of public interest or legitimate interests. Data subjects also have the right to object to the processing of personal data for direct marketing purposes.
- **Rights Related to Automated Decision-Making.** Under certain conditions, data subjects have the right to not be subject to a decision based solely on automated processing that produces legal or similarly significant effects on the data subject.

Organizations must be able to comply with these requests within one month of receipt. Given the complexity and operational burden associated with responding to these rights requests, many organizations implement internal policies and technical systems to address and handle rights requests. Due diligence should assess whether the target company has procedures, tracking mechanisms, and personnel in place to manage such requests, and whether it has a history of complaints or regulatory investigations related to the exercise of these rigs.

[v] International Data Transfers

The GDPR regulates transfers of personal data outside of the European Union with the goal of ensuring that personal data subject to the GDPR remains subject to appropriate protections in other jurisdictions. This includes international transfers between affiliated or related entities. The most common mechanisms for lawful international transfers are:

- **Adequacy Decisions**. Additional safeguards are not required for transfers to jurisdictions that the European Commission (and/or the UK Information Commissioner's Office, if applicable) has designated as having data protection regimes that provide an "adequate" level of protection for personal data. Notably, the United States is not a jurisdiction subject to an "adequacy decision," though the EU-U.S. Data Privacy Framework establishes limited "adequacy" for

organizations that certify compliance with the applicable framework and comply with its requirements.

- **Standard *Contractual Clauses***. The most common method to lawfully conduct transfers of personal data between two parties involves the use of Standard *Contractual Clauses*, which are a non-negotiable set of contract terms that set forth contractual protections with respect to international transfers of personal data. The most recent forms were promulgated in 2021, and allow a range of customization to address transfers between controllers and/or processors in a range of processing scenarios.
- **Binding Corporate Rules.** Less common are Binding Corporate Rules, which are internal policies and procedures adopted by multinational companies to handle intra-company international data transfers. They must be approved by EU supervisory authorities to be effective.
- **Derogations.** The GDPR provides for derogations, which are narrow exceptions that apply in specific and/or one-off situations, such as where a transfer is required to protect the vital interests of an individual.

[vi] Vendors

Article 28 of the GDPR requires that contracts with processors include certain specific processing terms. These include:

- **Subcontracting restrictions.** Processors may not engage a subcontractor with access to personal data without either (i) obtaining the controller's prior consent; or (ii) providing the controller with notice of the engagement and an opportunity to object.
- **Processing restrictions.** Processors must only process personal information pursuant to documented instructions from the controller.
- **Assistance with Compliance.** Processors must assist the controller in the controller's obligation to respond to data subject rights, to notify supervisory authorities and data subjects of security breaches, and to conduct data protection impact assessments and prior consultations with supervisory authorities.
- **Security**. Processors must implement appropriate security measures pursuant to Article 32 of the GDPR, taking into account the nature of the personal data processed and the risks presented by its processing.
- **Return and Deletion.** Processors must, at the termination of the agreement and at the choice of the controller, either delete or return personal data to the controller then delete such personal data.
- **Audit and Inspection.** Processors must submit to audits and inspections by the controller or the controller's designee.

[vii] Enforcement

The GDPR is enforced by independent supervisory authorities in each EU member state, and by the Information Commissioner's Office in the UK. These authorities have wide-ranging powers, including conducting investigations, issuing warnings and reprimands, ordering cessation of processing, and imposing administrative fines. Penalties for non-compliance can be severe: up to €20 million or 4% of a company's total worldwide annual turnover, whichever is higher, for the most serious infringements. Lesser breaches can still result in significant financial penalties and reputational harm. As such, GDPR noncompliance carries significant potential risk.

[viii] GDPR Due Diligence

GDPR due diligence often includes review of:

- Applicability of GDPR to some or all of the target company's business or operations;
- Privacy notices and policies for accuracy, completeness, and compliance with GDPR requirements;
- Personal data processing activities, including any special categories of personal data processed, and data maps, records of processing activities, or similar materials created with respect thereto;
- Lawful bases for processing, including any legitimate interest analyses;
- Data subject rights request handling processes, policies, and procedures;
- International data transfers, including any mechanisms to ensure the lawfulness thereof;
- Processor agreements to ensure all GDPR-required terms are included;
- Complaints, investigations, litigation, or other proceedings brought by data subjects, consumer protection organizations, and/or supervisory authorities; and
- Any personal data breaches, including the resolution, remediation, and notification of data subjects and third parties with respect thereto.

[4] U.S. State Comprehensive Privacy Laws

[a] Overview

Until 2020, the United States did not have a comprehensive privacy law that regulated most processing of personal data. This changed with the passage of the California Consumer Privacy Act (CCPA) in 2018, which became the first comprehensive privacy law passed by a U.S. state. California was closely followed by Colorado, Utah, Virginia, and other states. As of the time of writing, there are currently more than twenty (20) state comprehensive privacy laws that have been passed and/or are effective, with more in consideration in state legislatures nationwide. These comprehensive state privacy laws are in some ways similar to one another, but contain many key distinctions and differences that makes state law compliance challenging. A full discussion of all such laws is outside of the scope of this chapter and would likely be incomplete as of the date of publication; instead, below we summarize a number of common elements across many of these state laws. Acquirers should, however, consult with knowledgeable privacy counsel regarding state privacy law due diligence, as there are many nuances and distinctions between these state laws, and the laws themselves are rapidly evolving as states pass additional legislation and amendments.

[b] Applicability

State privacy laws have varying applicability triggers, often tied to one or more of an entity's revenue, size, volume of personal data processing, and/or volume of data sales. Most of these thresholds are disjunctive; that is, only one of the thresholds must be met in order for the law to apply.

[i] General

Most state privacy laws apply to entities that meet certain thresholds discussed below, are controllers, and do business in or offer products and services to the applicable state, regardless of where the entity has offices or operations. However, note that activity that occurs entirely outside of a given state may be exempted; for example, California's privacy law exempts transactions where all personal data was collected and processed outside of the borders of California.

[ii] Revenue or Size Thresholds

Most state privacy laws apply to entities that exceed revenue or size thresholds. For example, California's law applies to controllers that meet other requirements and exceed $25 million (adjusted over time) in annual revenue in the preceding fiscal year, while Texas's privacy law applies to controllers and processors that are not "small businesses" as defined by the U.S. Small Business Administration.

[iii] Personal Data Volume Thresholds

Most state privacy laws apply to controllers that process personal data about a certain volume of data subjects within the state. For example, Colorado law applies where a controller processes personal data about 100,000 or more data subjects resident in the applicable state. In contrast, application of Texas's privacy law does not depend on the volume of personal data processed.

[iv] Personal Data Sale Thresholds

Many state privacy laws also apply to controllers that derive significant revenue from, or sell a certain volume of, personal data. For example, California law applies where a controller buys, sells, or discloses for targeted advertising purposes the personal data of 100,000 or more California data subjects or derives 50% or more of its annual revenue from selling personal data or disclosing it for targeted advertising purposes, while Colorado's law applies where a controller derives revenue from the sale of personal data and processes the personal data of at least 25,000 Colorado residents.

[v] Nonprofit Status

Many, but not all, of these state privacy laws exempt not-for-profit organizations. For example, laws in California, Connecticut, Florida, Indiana, Iowa, Montana, Tennessee, Texas, Utah, and Virginia provide exemptions for "nonprofit organizations" or "nonprofit corporations," as defined in the applicable state law. Each law's definition of those terms is different, however, so not all nonprofits will be exempt from privacy laws in those states; for example, Virginia's law exempts only 501(c)(3), 501(c)(6), and 501(c)(12) not-for-profit organizations. Similarly, Delaware, Maryland, and Oregon state privacy laws exempt only nonprofits with certain missions, such as those dedicated to addressing insurance crime and fraud, while Colorado and New Jersey's privacy laws do not exempt nonprofit organizations at all.

[vi] Applicability to Processors

While the state omnibus privacy laws focus on obligations by controllers, they require controllers to bind processors to state privacy law compliance obligations indirectly via contract. In addition, some laws include requirements that apply directly to processors, such as obligations to assist controllers with data subject rights requests. As such, processors who might otherwise be exempt from such laws may face state law compliance obligations by virtue of the controllers they serve.

[vii] Sectoral Law Exceptions

Most state privacy laws include certain entity-level or data-level exceptions for other sectoral federal and state privacy laws, commonly including the Health Information Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), and state analogues such as the California Confidentiality of Medical Information Act.

[c] Covered Personal Data

These state comprehensive privacy laws regulate the processing of a broad scope of personal data.

[i] Scope of Personal Data

Perhaps the broadest definition of regulated data is contained in California's law, which regulates information "that identifies, relates to, describes, is reasonably capable of being associated with, or

could reasonably be linked, directly or indirectly, with a particular consumer or household." More typically, Colorado's privacy law governs the processing of any information that is "linked or reasonably linkable to an identified or identifiable individual." While most state laws tend to use a definition closer to that of Colorado, these definitions are nevertheless broad and capture a wide range of information that is or can be associated or linked with an individual.

[ii] Data Subjects

Most state privacy laws apply to the personal data of data subjects in their personal or household context, excluding information about individuals acting in a commercial or employment context. As of the date of this writing, California's law is the only state omnibus privacy law that applies to employee personal data and personal data about business contacts.

[iii] Sensitive Personal Data

Many state laws introduce a new category of "sensitive" personal data, often including Social Security numbers, driver's license or passport numbers, financial account logins, precise geolocation information, racial or ethnic origin, religious beliefs, genetic data, medical information, biometric identifiers, sexual orientation, and information of a known child under the age of 13, among other data elements. These laws impose additional conditions around the processing of sensitive personal data, such as requiring additional notices, opt-in requirements, and/or granting data subjects the right to limit the processing of sensitive personal data. For example, Colorado requires express, opt-in, revocable consent for certain processing of sensitive personal data.

[d] Key Requirements

[i] In General

State privacy laws generally impose both substantive and procedural obligations on regulated controllers. These can include requirements related to transparency, purpose limitations, data minimization, and the provision of specific data subject rights. Among these compliance components are:

[ii] Notices

Each state privacy law imposes specific notice and transparency requirements regarding personal data processing. Controllers must generally provide a clear, understandable, and reasonably accessible privacy notice, which describes the categories of personal data collected, the purposes for collection and use, categories of third-party recipients, methods for exercising consumer rights, and information about targeted advertising or sales. Where applicable, such as in Colorado, notices must also inform consumers of their right to appeal rights requests and how to submit such appeals. Some states impose additional notice and transparency obligations; for example, California's law requires controllers to annually update privacy policies; describe in privacy policies whether certain categories of personal data are sold, disclosed for targeted advertising, or provided to processors; and provide data subjects with a "notice at collection" explaining what personal data is collected, the purposes of collection, whether the information will be sold or shared for targeted advertising purposes, and any financial incentives for the collection or processing of personal data.

[iii] Data Subject Rights

State privacy laws generally provide data subjects with a range of rights regarding personal data about them, including:

- **Right to Know.** Data subjects may request that a controller disclose the categories and specific pieces of personal data processed about them, along with information about sources, purposes of collection, and disclosures to third parties.
- **Right to Delete.** Data subjects may request deletion of personal data collected, subject to certain exceptions (e.g., legal obligations or internal uses).
- **Right to Correct.** Data subjects may request correction of inaccurate personal data about them.
- **Right to Opt Out of Sale and/or Targeted Advertising.** Data subjects can direct controllers not to "sell" personal data about them nor share it with third parties for cross-context behavioral advertising or targeted advertising. The term "sell" is defined broadly under many state omnibus privacy laws to include disclosures in exchange for non-monetary compensation. In general, disclosures to third parties not acting as "processors" are likely to be considered sales.
- **Right to Limit Use of Sensitive Personal Information.** Data subjects may request certain restrictions on the use and disclosure of sensitive personal data, or may revoke consent previously given for such processing.
- **Right to Non-Discrimination.** Many state laws provide that controllers may not retaliate against data subjects for exercising their privacy rights.
- **Right to Appeal.** Most state laws require that controllers provide data subjects with an appeal process if the controller refuses to respond; this appeal process typically must be conspicuously available and similar to the process for submitting a data subject rights request.

Controllers must provide conspicuous means for data subjects to submit rights requests, such as dedicated webforms and toll-free numbers, and must respond to data subject rights requests within specified deadlines, often 45 days (extendable in certain circumstances). Some state privacy laws also permit data subjects to authorize agents to make rights requests on their behalf. Finally, some state privacy laws impose specific requirements regarding the verification of data subject rights requests as well as the contents of any responses thereto.

[iv] Data Protection Assessments

Most state privacy laws require controllers to conduct and document data protection assessments for processing activities that present a "heightened risk of harm" to data subjects. For example, Colorado's law requires these assessments for processing of personal data for targeted advertising; sales of personal data; profiling with substantial, unfair, deceptive, or unlawful effects on data subjects; and processing of sensitive data. These assessments must weigh the benefits of the processing against the potential risks to the data subject, identify safeguards to mitigate or reduce these risks, and must be made available to the Colorado Attorney General upon request. For due diligence purposes, the presence (or absence) of completed data protection assessments for these "heightened risk of harm" activities may be an indicator of maturity in the target company's compliance program.

[v] Universal Opt-Out Mechanism/Global Privacy Controls

Many state laws require controllers to honor a universal opt-out signal (including the Global Privacy Control) indicating a data subject's decision to opt out of sales and processing for targeted advertising. This requirement presents particular diligence concerns for companies involved in digital advertising ecosystems.

[vi] Processor Contracts

Most state privacy laws require that controllers enter into written agreements with any entity acting as a processor on their behalf that contain certain mandatory terms, including:

- **Details of Processing**. Contracts with processors must describe the nature and purpose of the processing of personal data, the type(s) of personal data involved, and the duration of the processing. California specifically states that this information must be specific and cannot be a reference to the service agreement more generally.
- **Processing Restrictions.** California imposes numerous specific contractual requirements, including requiring prohibitions against selling, sharing for cross-context behavioral advertising, or processing personal data outside of the direct business relationship between the processor and the controller, and from combining personal data received from or on behalf of the controller with other personal data the processor obtains from other sources in certain contexts.
- **Compliance.** Among other requirements, California requires that processors must agree to provide the same level of privacy protection for personal data as is required of the controller, and must notify the controller in the event the processor determines it can no longer comply with California law.
- **Assistance with Compliance.** Typically, a processor agreement must require the processor to assist the controller in the controller's obligation to respond to data subject rights, conduct and document required data protection assessments, and provide information necessary to demonstrate compliance with applicable laws.
- **Subcontracting.** Most state privacy laws require that a contract with a processor specify that engagement of subcontractors to process personal data must be subject to a written agreement that meets all processor requirements under state laws. Some state privacy laws, including those in Colorado and Maryland, also require that processors must provide controllers with notice and an opportunity to object prior to engaging the subcontractor.
- **Personnel Confidentiality.** Under most state privacy laws, a contract with a processor must include that a processor must impose a duty of confidentiality with respect to personal data on each person processing personal data for or on behalf of the processor.
- **Security.** State privacy laws typically require that a contract with a processor must require the processor to implement "reasonable" or "appropriate" technical and organizational measures to ensure a level of security appropriate to the risk of processing.
- **Audits.** Most state privacy laws require controllers to impose some kind of controller audit or inspection right and many expressly allow for an independent, third-party assessor as a more processor-friendly alternative option. For example, Colorado's law allows the controller to agree, in lieu of an audit right, to allow the processor to arrange for a qualified and independent auditor to conduct an audit of the processor's policies and technical and organizational measures using an "appropriate and accepted control standard or framework and audit procedure," and provide a report of such audit to the controller upon request.
- **Return/Deletion.** At the choice of the controller, the processor must delete or return all personal data at the end of the provision of services, unless retention of personal data is required by law.

[vii] Controller/Data Sale Contracts

As of the time of writing, California's law is the only U.S. state law that regulates the terms of contracts with all recipients of personal data, including "third parties" (i.e., entities that receive personal data from a business and are not processors to that business. These contracts must include:

- **Processing Restrictions.** The recipient must only process personal data for the limited and specified purposes in the contract.
- **Compliance.** The recipient must comply with California law, including by providing the same level of privacy protection for received personal data as is required of the controller providing the

personal data under California law, and must notify the controller in the event the recipient determines it can no longer comply with California law.

- **Business Rights.** Controllers must have the right to take reasonable and appropriate steps to (i) ensure that the recipient processes personal data obtained from the controller in a manner that complies with California law; and (ii) upon notice thereof, stop and remediate unauthorized processing of personal data obtained from the controller.

Uniquely, California expressly prohibits entities that provide cross-context behavioral advertising services from acting as a "processor." Instead, such vendors must be "third parties" under California law.

[e] Enforcement

[i] Regulatory Enforcement

Most state laws are enforced by enforced by state regulators such as the applicable state attorney general. Some states permit other governmental authorities to enforce state privacy laws as well; for example, Colorado permits district attorneys to enforce violations, and California created a new enforcement authority, the California Privacy Protection Agency (CPPA), which shares enforcement jurisdiction with the California Attorney General. Enforcement bodies are typically empowered to investigate potential violations, impose administrative fines, and bring civil cases in court. Many privacy laws include mandatory notice and cure periods for most violations; however, some of these cure periods were amended out or sunset, meaning enforcement actions may proceed without prior notice or opportunity to remedy.

[ii] Penalties and Fines

State laws diverge significantly on noncompliance penalties and fines, though they often allow penalties or fines to accrue on a per-violation basis that can result in significant liability. For example, in California, penalties for state privacy law noncompliance include fines of up to $2,500 per violation or $7,500 per intentional violation or violations involving minors, while violations of Colorado's privacy law are considered deceptive trade practices under Colorado's Consumer Protection Act and are subject to civil penalties of up to $20,000 per violation (and separate consumers and/or transactions are separate violations).

[iii] Limited California Private Right of Action

California's privacy law also includes a private right of action for data subjects that have had unencrypted or unredacted personal data about them subject to unauthorized access, theft, or disclosure due to a failure to implement reasonable security procedures.

[f] State Privacy Law Due Diligence

U.S. state privacy law due diligence often includes review of the target company's:

- Privacy notices and policies, for completeness, accuracy, and compliance;
- Personal data processing activities, the data elements processed, and whether any sensitive personal data is processed;
- Personal data "sales" and review of compliance around such processing activities;
- Processing of personal data for targeted advertising purposes and review of compliance around such processing activities;
- Financial incentives for processing of personal data, and confirmation that appropriate notices are provided to data subjects with respect thereto;

- Data subject rights webforms, opt-out pages, policies, appeal processes, and other mechanisms for effectuating data subject rights requests;
- Contracts with processors (and, in California, third parties) that receive personal data for compliance with privacy law obligations;
- History of data subject or regulatory complaints, investigations, or enforcement actions; and
- Data breaches, including notifications and remediation measures, for potential private right of action exposure under California law and/or follow-up enforcement actions by state regulators.

[5] United States Sectoral Laws

[a] Overview

The United States does not (as of the time of this writing) have a comprehensive federal privacy law that applies broadly across industries to the processing of personal data. Instead, with the exception of the state privacy laws discussed in the preceding section, the United States typically uses a sectoral approach at the federal level in structuring its privacy laws, targeting regulations to industries, data, or processing activities that regulators have identified as requiring additional protections. For example, some laws regulate certain industries, such as healthcare or financial services; other laws regulate the processing of certain types of data, such as children's data. Other laws regulate specific processing activities or uses of personal data, such as telemarketing (TCPA), creation and use of consumer reports (FCRA), and transfers of U.S. personal data to "countries of concern" (Bulk Data Rule). As a result of this sectoral approach to regulation, when conducting diligence on a target company that operates within the United States, it is particularly important to understand (1) the industry(ies) the target company operates in; (2) the types of personal data the target company processes; (3) the purposes for which the target company processes personal data; and (4) any third parties that receive personal data from the target company and the purposes for which they receive such personal data. A summary discussion of notable sectoral United States privacy laws that often come up in due diligence is below, though we encourage you to consult with knowledgeable privacy counsel as a comprehensive discussion of all such laws is outside of the scope of this chapter.

[b] U.S. Department of Justice Bulk Data Rule ("BDR")

The U.S. Department of Justice's Bulk Data Rule, formally titled *Safeguarding Americans' Sensitive Data from Foreign Adversaries* and issued pursuant to Executive Order 13873 and the International Emergency Economic Powers Act (IEEPA), went into effect on April 15, 2024. This regulation prohibits or restricts the transfer U.S. persons' bulk sensitive personal data and government-related data to "countries of concern"and "covered persons." It aims to mitigate national security risks stemming from the exploitation of personal data of U.S. persons and government-related data. Given its breadth, BDR due diligence is important for any U.S. entity with access to large amounts of personal or government data that engages with international partners, employees, or vendors.

[i] Applicability

The DOJ Bulk Data Rule (BDR) applies to any "U.S. person" – defined to include U.S. citizens, nationals, legal permanent residents; any person in the United States; and entities organized solely under the laws of the United States that engages in a "covered transaction." A covered transaction involving any transfer of bulk U.S. sensitive personal data or government-related data toa "country of concern" or a "covered person." Countries of concern currently include China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela, although others could be added later. A covered person includes, but is not limited to, a resident of a country of concern; an entity that is organized, chartered, or with a principal place of business in a country of concern; is an employee or contractor of such a person or entity; an individual or entity designated by the Attorney General; and any entity that is 50% or more owned, individually or in the aggregate, by one or more countries of

concern or persons or entities or concern. Notably, the rule also captures indirect arrangements such as subcontracting, data hosting, or analytics services where foreign entities may gain access to covered data, even if not directly listed as a transaction party. Due diligence should include a review of the target company's customers, vendors, cloud infrastructure, affiliates, and international data flows. Even a seemingly domestic transaction could fall within scope of the BDR if the target company uses analytics vendors in a country of concern or permits foreign nationals access to U.S. bulk data assets.

[ii] Covered Data

The BDR protects two types of data: "bulk U.S. sensitive personal data" of U "government-related data." "Bulk" data is defined by reference to volume thresholds for certain covered data categories, and includes:

- Human genomic data of >100 U.S. persons (includes genetic tests and genetic sequencing data);
- Human 'omic data of >1,000 U.S. persons (includes epigenomic data, proteomic data, and transcriptomic data but not pathogen-specific data);
- Biometric identifiers of >1,000 U.S. persons (includes physical characteristics or behaviors that are used to recognize or verify the identify of an individual);
- Precise geolocation data of > 1,000 U.S. persons (defined as information that would permit location of an individual within 1,000 meters or 3,200 feet);
- Personal health data of >10,000 U.S. persons (includes basic physical measurements and health attributes (bodily functions, height, weight, vital signs, symptoms, allergies), social, psych, behavioral, and medical diagnostic, intervention, treatment history; test results; logs of exercise habits; immunization data; data on reproductive and sexual health; and data on the use or purchase of prescribed medications);
- Personal financial data of >10,000 U.S. persons (includes information about payment cards and/or bank accounts, including purchases and/or payment history; data in a bank, credit, or financial statement; and data in a credit report or consumer report;
- Covered personal identifiers of >100,000 U.S. persons (includes identifiers in combination with other data that would allow linking to sensitive personal data, subject to certain exclusions); and
- Combined data that contains any of the above categories where any individual data type meets the threshold for the lowest number of persons or devices in that category.

Notably, and unlike most laws discussed in this chapter, such data meets the relevant definition of "bulk U.S. sensitive data" **regardless of whether it is anonymized, pseudonymized, encrypted, de-identified, or otherwise obscured**.

"Government-related data" regulated by the BDR includes precise geolocation data, with no volume threshold, within any area on a list of government locations, including:

- The worksite or duty station of federal government employees in national security positions;
- Military installations;
- Facilities or locations that support federal government national security, defense, intelligence, law enforcement, or foreign policy functions; and
- Sensitive personal data marketed as linked or linkable to current or former employees, contractors, or senior officials of the U.S. government, including its military and intelligence communities.

[iii] Prohibited and Restricted Transactions

The BDR includes a list of "prohibited transactions," which are prohibited, and "restricted transactions," which are permitted if certain mandatory safeguards are in place; without those safeguards, such transactions are also prohibited.

- **Prohibited Transactions**. The rule prohibits the sale, licensing or other commercial transactions involving bulk U.S. sensitive personal data or government-related data with a country of concern or covered person. The rule further prohibits commercial transactions with all other foreign persons (that are **not** a covered person) prohibited unless there is a contractual provision in place prohibiting onward transfer to a country of concern or covered person.
- **Restricted Transactions.** The BDR restricts other transactions—namely those that include vendor, employment, or investment agreements that involve access to bulk U.S. sensitive data or government data to a country of concern or covered person. Restricted transactions are permitted if they comply with the security requirements promulgated by the Cybersecurity and Infrastructure Security Agency (CISA), along with other applicable due diligence, auditing, and reporting obligations. If the requisite CISA security requirements and other requirements are not in place,. That said, transactions involving bulk U.S. 'omic data or biospecimens from which 'omic data can be derived are always prohibited transactions, even if the transaction involves a vendor, employment or investment agreement.
- **Exempt Transactions.** Finally, there is a category of "exempt" transactions that are not subject to the BDR. These include personal communications, information or informational materials, transfer of data normally incident to international travel, financial services, transactions authorized by federal law and international agreements, investment agreements subject to the Committee on Foreign Investment in the United States (CFIUS), and certain corporate group transactions. For instance, the exempts some internal corporate transfers of data (like human resources, payroll, and business-related travel) within the same corporate "family" as generally exempt from the BDR's restrictions, provided they meet certain criteria.

[iv] Contract Requirements

For data brokerage transactions involving access to bulk U.S. sensitive personal data or government-related data by foreign person that is not a covered person or country of concern, contracts must include requirements that the foreign person refrain from engaging in subsequent covered data transactions involving data brokerage of the same data with a country of concern or covered person and must report any known or suspected violations of this contract requirement.

[v] Enforcement

The BDR imposes significant penalties for violations, including a maximum fine of $368,136 or twice the transaction amount, whichever is greater. Willful violations of the BDR could lead to criminal fines of up to $1,000,000 and 20 years' imprisonment. The Department of Justice (DOJ) may also refer violations to other agencies, such as the Department of Homeland Security (DHS) or the Office of Foreign Assets Control (OFAC), if additional national security or sanctions implications are present. Importantly, the DOJ can initiate enforcement actions even if the transaction is domestic, if there is foreign access to regulated data through intermediaries.

[vi] BDR Due Diligence

BDR due diligence includes review of:

- Assessment as to access to and control over any covered bulk U.S. sensitive foreign data or government-related data by the target company, the acquiring entity, and/or any affiliates, third parties, or vendors with access to data regulated by BDR;
- Data transfers that may constitute prohibited or restricted transactions or involve countries of concern or covered persons;

- Dealings with countries of concern or covered persons;
- Contract measures implemented with respect to covered transactions involving foreign persons;
- Security measures for restricted transactions;
- Policies and procedures required for BDR compliance;
- Records that are kept pursuant to BDR requirements; and
- Any history of enforcement, complaints, or investigations pursuant to BDR.

[c] Protecting Americans' Data from Foreign Adversaries Act (PADFAA)

[i] Introduction

PADFAA, which went into effect on June 23, 2024, makes it unlawful for a data broker to sell, license, or otherwise engage in the commercial transfer of personally identifiable sensitive data of a U.S. individual to a foreign adversary country or entity that is controlled by a foreign adversary country. Foreign adversary countries covered by PADFAA include four of the six countries of concern covered by the Bulk Data Rule: China, Iran, North Korea, and Russia.

[ii] Applicability

PADFAA regulates "data brokers," which it defines as any entity that engages in the sale, licensing, renting, trading, releasing, disclosing, providing access to, or otherwise making available personally identifiable sensitive data of a U.S. person that the entity did not collect directly from the data subject to another entity for valuable consideration.

[iii] Covered Personal Data

PADFAA regulates "personally identifiable sensitive data of a U.S. person" and has a different definition than U.S. sensitive personal data covered under the Bulk Data Rule. PADFAA's definition of personally identifiable sensitive data includes, among other things, government-issued identifiers, such as Social Security numbers; health data; financial account information; biometric data; genetic information; geolocation information; private communications; and information about an individual under the age of 17, and "U.S. individual" means any person living in the United States.

[iv] Transfer Restrictions

Unlike the Bulk Data Rule, PADFAA restricts all applicable transfers of such data, irrespective of the number of U.S. individuals affected. The restrictions prohibit the sale or commercial transfer of data to the four foreign adversary countries listed above and to (i) any person living in these four countries; (ii) any entity headquartered in, with a principal place of business in, or organized under the laws of these countries ("adversary foreign entity"); (iii) any entity subject to 20% or more ownership by an adversary foreign entity or a person living in any of the four foreign adversary countries; or (iv) any person subject to the direction or control of any of the above.

[v] Enforcement

Failure to comply with PADFAA is enforced as an "unfair or deceptive act or practice" under the Federal Trade Commission Act and is subject to enforcement by the FTC as described in our analysis of the FTC Act Section 5 above.

[vi] PADFAA Due Diligence

PADFAA due diligence includes review of:

- Whether the target company is a regulated data broker;
- Assessment as to access to and control over any personally identifiable sensitive data of a U.S. person by the target company and/or the acquiring entity;
- Data transfers of personally identifiable sensitive data that involve countries of concern or covered persons;
- Dealings with countries of concern or covered persons;
- Contract measures implemented with respect to covered transactions involving foreign persons
- Security measures for restricted transactions;
- Policies and safeguards implemented to prevent prohibited transfers of personally identifiable sensitive data of a U.S. person; and
- Any history of enforcement, complaints, or investigations pursuant to PADFAA.

[d] Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA), enacted in 1998 and implemented by the Federal Trade Commission (FTC) through its COPPA Rule, regulates the processing of personal information collected online from children under the age of 13. The statute reflects heightened societal concern over the privacy and safety of children in digital environments and imposes stringent obligations on operators of websites, mobile apps, and online services that are directed to children or knowingly collect data from them. COPPA compliance is a notable area of due diligence in transactions involving platforms, games, educational technologies, and digital services that engage with child users.

[i] Applicability

COPPA applies to operators of websites or online services directed to children under 13 or that have actual knowledge they are collecting personal information from children under 13. Whether a website or online service will be considered child-directed will depend on numerous factors, including the service's subject matter, visual content, language, characters, or advertising.

[ii] Covered Personal Data

COPPA governs the collection, use, and disclosure of "personal information," defined as "individually identifiable information about an individual collected online" from children under 13. Covered personal information includes full name, home address, email address, telephone number, and Social Security number, as well as persistent identifiers such as IP addresses, cookies, device identifiers, and geolocation data. The definition also extends to photographs, video or audio files containing a child's image or voice, and any other information that permits physical or online contact with the child. During diligence, counsel should review whether the company collects any such data and whether the data is used for targeted advertising, profiling, or third-party sharing, which significantly increases compliance obligations and risks.

[iii] Key Requirements

COPPA imposes privacy obligations on covered operators, with a focus on securing verifiable (and revocable) parental consent before collecting personal data from children. The core requirements include:

- **Notice and Transparency.** Operators must provide clear and comprehensive privacy notices describing their data collection practices. This includes both an online privacy policy and, in some cases, a direct notice to parents detailing the types of personal data collected, how it is used, whether it is shared, and with whom.

- **Verifiable Parental Consent.** Before collecting personal data from a child, operators must obtain verifiable parental consent using methods reasonably designed to ensure the person giving consent is the child's parent. Acceptable methods include use of credit cards, printed and signed consent forms, video conferencing, or knowledge-based authentication. "Email plus" methods may be used when data is processed for limited internal purposes and not disclosed to third parties.
- **Parental Rights.** Parents have rights with respect to the personal information collected from their children, including to review and delete their child's personal information and to revoke parental consent.
- **Data Security.** Operators are required to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.
- **Restrictions on Data Sharing.** Disclosing children's personal information to third parties requires clear parental consent. Operators must also ensure that service providers or third parties maintain equivalent levels of security and confidentiality.

[iv] Enforcement

COPPA is enforced by the Federal Trade Commission (FTC), which has the authority to investigate violations, impose civil penalties, and seek injunctive relief. Civil penalties for violations can be substantial (up to $53,088 per violation as adjusted for inflation). The FTC has brought enforcement actions against operators of social networks, gaming apps, educational platforms, and connected toys, resulting in multimillion-dollar settlements and mandated compliance programs. State attorneys general also have enforcement authority under COPPA, and violations may give rise to reputational damage, class action risk under state consumer protection laws, and adverse media attention.

[v] COPPA Due Diligence

COPPA due diligence often includes review of:

- Digital properties and apps to determine whether any are child-directed;
- Children's personal data processing activities, including any disclosures of such personal data to third parties and any knowledge that personal data is collected from children under the age of 13;
- Online notices and notices to parents for accuracy and compliance;
- Parental consent processes, verification mechanisms, and consent withdrawal mechanisms;
- Security measures and safeguards to protect children's personal data; and
- Complaints, investigations, enforcement actions, and/or data breaches with respect to children's personal data.

[e] Fair Credit Reporting Act ("FCRA")

[i] Introduction

The Fair Credit Reporting Act (FCRA) is a federal law designed to promote accuracy, fairness, and the privacy of information in the files of consumer reporting agencies (CRAs). The FCRA regulates how personal information is collected, shared, and used by CRAs, users of consumer reports (such as employers, lenders, and landlords), and furnishers of data to CRAs. The FCRA is relevant during due diligence when a transaction involves target companies engaged in credit reporting, background screening (including with respect to employee or personnel background checks), or financial services.

[ii] Applicability

The FCRA applies to any entity that meets the statutory definition of a "consumer reporting agency," as well as any business that uses or furnishes consumer reports. A "consumer reporting agency" is defined broadly to include any entity that regularly assembles or evaluates consumer information to provide reports to third parties for use in determining creditworthiness, insurance eligibility, employment, or other specific permitted purposes. This includes traditional credit bureaus (e.g., Experian, Equifax, TransUnion), tenant screening services, background check companies, and newer data aggregators or analytics firms that meet the definition of a CRA. The FCRA also applies to "users" of consumer reports, such as employers, landlords, financial institutions, and insurers, who rely on such reports to make decisions about consumers. In addition, entities that "furnish" data to CRAs, such as banks, telecom providers, and debt collectors, are subject to specific FCRA obligations concerning accuracy and dispute resolution. In evaluating whether a given target company is subject to the FCRA, it is important to consider whether the target company is creating or using consumer reports, whether such reports are used for FCRA "permitted purposes," and/or whether the target company is furnishing personal data to a CRA.

[iii] Covered Information

The FCRA regulates "consumer reports," which are defined as communications of information by a CRA bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, used or expected to be used for evaluating eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment; housing; or other permissible purposes outlined by the FCRA. Consumer reports can include credit histories, payment records, criminal background information, driving records, and employment verifications. "Investigative" consumer reports—a subset of consumer reports involving information obtained through personal interviews—are subject to heightened disclosure and consent requirements. For diligence purposes, legal counsel should identify whether a target company handles consumer reports or data used for consumer reports, and examine the nature, sources, and flow of such data throughout its systems and partnerships.

[iv] Key Requirements

FCRA requirements vary depending on whether the regulated party is a CRA, user of consumer reports, and/or furnisher of personal data to CRAs. Some critical obligations include limiting data usage to statutorily permitted purposes, obtaining consent when required, maintaining data accuracy, and honoring consumer rights. Counsel should be particularly aware of the FCRA's "permitted purposes." CRAs may only furnish consumer reports, and users of consumer reports obtained from CRAs may only use such reports, for specific permitted purposes identified in Section 604 of the FCRA, which include:

- Decisions relating to credit transactions involving the consumer;
- Employment purposes, including evaluation for employment, promotion, reassignment, or retention as an employee (with the consumer's written authorization);
- Underwriting of insurance;
- Determinations of eligibility for a government license or benefit;
- Evaluations of credit or payment risk for existing accounts;
- Business transactions initiated by the consumer (e.g., rental applications);
- Court orders or subpoenas; and
- Legitimate business needs in connection with a consumer-initiated transaction.

Any furnishing or use of consumer reports outside of these specified purposes is prohibited. Even where a target company is not a CRA or a furnisher, it may be subject to the FCRA when using reports

for background check or employment screening purposes, and it should have processes in place for addressing FCRA requirements such as obtaining consent.For CRAs, the FCRA imposes duties including the following:

- Implementing procedures to ensure accuracy of data;
- Disclosing consumer report data to consumers upon request and facilitating dispute resolution;
- Reinvestigating disputed information promptly and reporting results; and
- Limiting report content to time-bound disclosures (e.g., most negative items cannot be reported after seven years).

For data furnishers, the FCRA requires reporting accurate information to CRAs, investigating disputes referred by CRAs, and correcting inaccuracies.

[v] Enforcement

The FCRA is enforced by multiple entities, including the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and state attorneys general. Each has the authority to bring enforcement actions for violations of the statute and its implementing regulations. The CFPB has published guidance, undertaken rulemaking, and imposed substantial civil penalties, including multimillion-dollar settlements involving major credit reporting agencies and background screening firms. Violations of the FCRA can result in civil liability, both in the form of agency penalties and private litigation. Affected consumers can bring individual or class action lawsuits for willful or negligent noncompliance with certain obligations under the FCRA. Remedies may include actual damages, statutory damages of up to $1,000 per violation (in cases of willful noncompliance), punitive damages, and attorneys' fees. Claims may arise from failures to follow pre-adverse action procedures in employment settings, inaccurate reporting, or the unauthorized use of consumer reports. Due diligence should assess whether the target company has any history of consumer litigation under FCRA, including class actions or arbitration matters. Counsel should also examine the target company's internal audit practices and responsiveness to regulator inquiries, particularly if the company provides data to or relies on data from third-party CRAs.

[vi] FCRA Due Diligence

FCRA due diligence depends on the role of the target company under FCRA. As a result, FCRA due diligence should begin by evaluating whether the target company is a CRA, a user of consumer reports, and/or a furnisher of data to CRAs.

Due diligence on CRAs often includes review of:

- Policies and procedures designed to ensure accuracy of consumer reports and correct inaccurate data;
- Policies and procedures regarding disclosure of personal data to data subjects;
- Policies and procedures regarding disputing inaccuracy of personal data, investigation of inaccuracies, and the resolution of inaccuracies and disputes; and
- Policies regarding the contents of consumer reports and the retention and disclosure of data.

Due diligence on users of consumer reports often includes review of:

- Consumer report usage to confirm it fits within FCRA "permitted purposes" or an exemption thereto; and
- Consent forms, adverse action notices, and dispute resolution mechanisms (particularly in the employment context).

Due diligence on furnishers of information to CRAs often includes review of:

- Policies and procedures designed to ensure accuracy of furnished personal data and correct inaccurate data; and
- Policies and procedures regarding disputed information and resolution of disputes.

[f] Gramm-Leach-Bliley Act ("GLBA")

[i] Introduction

The Gramm-Leach-Bliley Act (GLBA) and its regulations establish a federal regulatory framework governing the privacy and security of consumer information processed by financial institutions. While this section focuses on the GLBA as the overarching federal framework for financial information privacy, counsel should note that many states also have financial data privacy laws that apply alongside the GLBA, including the California Financial Information Privacy Act, that is stricter than the GLBA in certain respects. Such state laws should also be considered in diligence where relevant.

[ii] Applicability

GLBA applies to "financial institutions," including any company engaged in certain financial activities. This includes not only traditional banks and insurance companies, but also securities firms, mortgage brokers, financial counseling services, check-cashing services, payday lenders, personal property appraisers, and many online financial platforms and fintech companies offering financial products or services to individuals for personal, family, or household use. Importantly, the GLBA does not cover financial services provided to business customers. Determining GLBA applicability in the diligence process requires an analysis of whether the target company engages in consumer-facing financial activities that make it a "financial institution" under GLBA.

[iii] Covered Personal Data

GLBA regulates the processing of "nonpublic personal information" or "NPI," which is personally identifiable financial information that (1) is provided by a consumer to a financial institution to obtain a financial product or service; (2) resulting from any transaction with the consumer involving a financial product or service; or (3) otherwise obtained by the financial institution in connection with providing a financial product or service to a consumer.

[iv] Key Requirements

GLBA is implemented through rules issued and enforced by a range of federal financial regulators, most notably Regulation P (the Privacy Rule) and the Safeguards Rule.

- **Regulation P.** This regulation requires financial institutions to provide consumers with clear, conspicuous privacy notices describing their data practices. These notices must be delivered when a customer relationship is established and may also be delivered annually thereafter for continuing relationships. The notices must explain what NPI is collected, how it is used, whether it is shared with nonaffiliated third parties, and how consumers can opt out of certain disclosures. GLBA permits sharing with nonaffiliated third parties for marketing or other purposes only if the consumer has received prior notice and an opportunity to opt out, with certain exceptions such as disclosures required by law or those necessary to process a transaction requested by a consumer. Regulators have promulgated a model privacy notice form that, if completed and provided to consumers in accordance with regulatory requirements, acts as a "safe harbor" for compliance with GLBA privacy notice requirements, and many financial institutions use this form to meet their obligations. GLBA due diligence should include a review of the GLBA privacy notice to ensure it meets regulatory requirements, as well as any policies and procedures relating to consumer opt-outs and sharing of NPI.

- **Safeguards Rule.** The Safeguards Rule requires regulated financial institutions to develop, implement, and maintain a comprehensive written information security program for customer information (any record containing NPI) that is appropriate to the size, complexity, and nature of their activities. This program must include administrative, technical, and physical safeguards to protect customer information. It also mandates the designation of a qualified individual to oversee this program, which must include elements like periodic risk assessments, employee training, monitoring and management of service providers, and continuous program adjustments based on evolving threats.

[v] Vendors

The Safeguards Rule imposes specific obligations on financial institutions to oversee service providers that have access to NPI. Financial institutions must take reasonable steps to ensure that service providers are capable of maintaining, and maintain, appropriate safeguards to protect NPI. This includes contractual obligations requiring service providers to implement security measures consistent with GLBA standards. These contracts must also address data confidentiality, breach notification responsibilities, and, where appropriate, audit rights or other oversight mechanisms. Due diligence should include a review of the target company's vendor management policies and procedures, as well as a sampling of contracts with key service providers to confirm that GLBA-required provisions are included.

[vi] Enforcement

GLBA is enforced by a variety of federal agencies depending on the type of financial institution. These include the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), federal banking regulators (such as the Office of the Comptroller of the Currency and the Federal Reserve), the Securities and Exchange Commission (SEC), and state insurance authorities for entities under their jurisdiction. Violations can result in civil penalties, consent decrees, and reputational damage.

[vii] GLBA Due Diligence

GLBA due diligence typically includes review of:

- Whether the target company is a "financial institution" subject to GLBA obligations;
- NPI processing activities;
- Privacy notices provided to data subjects, including if the model privacy notice is used;
- Mechanisms for offering and effectuating data subject opt-out requests;
- Target company's information security program, including any vendor management policies and procedures; and
- Vendor contracts for vendors with access to NPI to ensure such contracts meet GLBA requirements.

[g] Health Information Portability and Accountability Act of 1996 ("HIPAA")

[i] Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, establishes a federal regulatory framework for the privacy and security of protected health information (PHI). For counsel conducting due diligence, understanding HIPAA's scope, obligations, and enforcement mechanisms is

essential when evaluating transactions involving healthcare providers, health plans, healthcare data vendors, or digital health platforms.

[ii] Applicability

HIPAA applies to "covered entities" and their "business associates." Covered entities include health care providers (e.g., hospitals, physicians, clinics) who transmit health information electronically in connection with standard transactions (electronically billing health plans for medical care), health plans (including health insurers and employer-sponsored plans), and healthcare clearinghouses. Business associates are third parties that perform functions or services involving PHI on behalf of covered entities, such as billing companies, cloud service providers, IT vendors, consultants, and legal or accounting firms with access to health data. In the M&A context, HIPAA applicability turns on whether the target company is a covered entity or business associate; both types of entities are directly regulated by HIPAA and must comply with applicable HIPAA requirements.

[iii] Covered Personal Data

Protected Health Information (PHI) under HIPAA includes individually identifiable health information transmitted or maintained in any form (electronic, paper, oral, etc.) that relates to a person's past, present, or future physical or mental health, the provision of health care to the person, or the payment for health care. In practice, this definition is quite broad, as PHI includes data elements like names, addresses, and email addresses when they are processed by or on behalf of a covered entity, in addition to information about medical diagnoses, medical treatment, and the payment for treatment. Notably, HIPAA excludes from its scope de-identified health information, but imposes strict deidentification criteria for PHI to become de-identified health information under *45 CFR 164.514*. To be considered de-identified, a covered entity or business associate must have no reasonable basis to believe that the data can be used to identify an individual, and must either: (1) obtain an expert determination from a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify the data subject; or (2) remove a list of 18 specific and enumerated identifiers from the PHI.

[iv] Key Requirements

HIPAA's regulations are separated into the Privacy Rule, Security Rule, and Breach Notification Rule.

- **Privacy Rule.** HIPAA's Privacy Rule governs the permissible uses and disclosures of PHI by covered entities and business associates. It mandates that PHI may generally only be used or disclosed for treatment, payment, and health care operations, or with written patient authorization (though exceptions exist). The Privacy Rule also requires covered entities to adopt policies and procedures outlining Privacy Rule compliance, provide patients with a Notice of Privacy Practices, limit access to PHI to the minimum necessary, and afford individuals rights including access to their PHI, amendment, and accounting of disclosures. As such, due diligence processes that involve HIPAA should include a review of HIPAA policies and procedures and any Notice(s) of Privacy Practices provided by the covered entity to data subjects.
- **Security Rule.** Applicable specifically to electronic PHI (ePHI), this rule requires entities to implement appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of ePHI. Administrative safeguards include risk assessments, workforce training, incident response plans, and the policies and procedures the entity implements to comply with Security Rule obligations; physical safeguards involve facility access controls and device security; and technical safeguards include access controls, audit controls, and encryption measures. Security Rule compliance should be documented and

reviewed periodically, and HIPAA risk assessments conducted pursuant to Security Rule requirements should be conducted at least annually. These risk assessments are often a helpful tool for evaluating the HIPAA compliance posture of a target company.

- **Breach Notification Rule.** In the event of a HIPAA "breach," which is an impermissible use or disclosure of unsecured PHI that compromises the privacy or security of PHI, the covered entity or business associate must provide prompt notification to affected individuals, the U.S. Department of Health and Human Services (HHS), and, in some cases, the media, unless a covered entity or business associate conducts and documents a four-factor risk assessment that determines that there is a low probability that the PHI has been compromised. Required notifications must occur without unreasonable delay and no later than 60 days from discovery of the breach. The rule also obligates entities to maintain documentation of breach risk assessments and mitigation steps. Due diligence should evaluate whether the target company has experienced reportable breaches, how they were handled, and whether they triggered regulatory action or litigation.

[v] Vendors

HIPAA requires covered entities and business associates to enter into compliant "business associate agreements" (BAAs) before PHI is made available to a business associate. Compliant BAAs must meet HIPAA requirements set forth in *45 C.F.R. 164.504(e)*, including describing the permitted uses and disclosures of PHI, requiring the business associate to safeguard PHI in accordance with HIPAA standards, requiring the business associate to assist the covered entity in responding to HIPAA individual rights requests, and imposing obligations around breach notification, subcontractor compliance, and PHI return or destruction upon contract termination. From a due diligence perspective, it is important to confirm that all BAAs are in place, up to date, and compliant with regulatory requirements, as absence or insufficiency of BAAs can expose both the covered entity and the business associate to liability. Counsel should also assess whether a target company acts as a business associate itself, and if so, how it manages contractual and regulatory compliance across its client relationships. Counsel should note that while an executed BAA can be evidence that a particular entity is a business associate, as a practical matter many HIPAA covered entities or business associates require all of their vendors to execute BAAs, regardless of whether the vendor actually processes PHI, so additional verification steps may be warranted if an executed BAA is the only evidence that HIPAA applies to a given target company.

[vi] Enforcement

HIPAA compliance is vigorously enforced by the Office of Civil Rights ("OCR") within the Department of Health and Human Services, which has authority to investigate complaints, conduct audits, and impose civil monetary penalties for HIPAA noncompliance. HIPAA noncompliance liability and costs can be substantial, and some HIPAA violations can give rise to criminal liability as well. OCR has enforced HIPAA violations against hospitals, health care providers, insurers, and technology companies that service HIPAA covered entities and business associates. Due diligence should include a review of any past OCR audits, complaints, corrective action plans, or investigations.

[vii] HIPAA Due Diligence

HIPAA due diligence often includes review of:

- Whether the target company is a covered entity and/or business associate;
- HIPAA policies and procedures;
- HIPAA risk assessments and remediation;
- Safeguards in place to protect the privacy and security of PHI;

- Personnel trainings on protection of PHI;
- Contracts with vendors that process PHI to ensure appropriate business associate agreements are in place; and
- History of HIPAA incidents, breaches, complaints, enforcement actions, and the reporting and resolution thereof.

[h] Illinois Biometric Information Privacy Act

[i] Introduction

The Illinois Biometric Information Privacy Act (BIPA), *740 ILCS 14/1 et seq.*, enacted in 2008, is one of the most consequential biometric privacy laws in the United States because of its strict consent requirements and class-action-friendly private right of action with statutory damages. BIPA regulates the processing of biometric identifiers and biometric information by private entities operating in Illinois. Although BIPA received limited attention in its early years, a surge in class action litigation over the past decade has transformed it into a significant legal risk for companies using facial recognition, fingerprint scanning, voiceprints, or other biometric identification technologies. As a result, BIPA compliance has become a critical area of inquiry in the due diligence process, and counsel should evaluate target companies for BIPA compliance when the target company operates in Illinois and/or collects biometric data from Illinois residents.

[ii] Applicability

BIPA applies to all private entities that collect, capture, purchase, receive through trade, or otherwise obtain biometric identifiers or biometric information from individuals in Illinois. The term “private entity” is defined broadly and includes individuals, corporations, LLCs, partnerships, and other legal or commercial organizations. BIPA does not apply to government agencies, courts, or financial institutions subject to the federal Gramm-Leach-Bliley Act. Importantly, courts have construed BIPA to apply extraterritorially to out-of-state companies that collect biometric data from individuals located in Illinois, even if the company has no physical presence there. In due diligence, the key threshold inquiry is whether the target company collects or processes biometric data of Illinois residents, regardless of where the target company is headquartered. Common BIPA risks include timekeeping systems using fingerprint or handprint scans, security surveillance employing facial recognition, authorization or authentication technology using palm or iris scanning, and technology platforms that process biometric inputs for authentication.

[iii] Covered Personal Data

BIPA draws a distinction between biometric identifiers and biometric information. “Biometric identifiers” are defined as retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry. These identifiers are considered inherently sensitive because they are immutable and cannot be changed if compromised. “Biometric information” is defined as any information derived from a biometric identifier that is used to identify an individual. This could include algorithms generated from biometric scans that are used for facial recognition, for example. From a diligence standpoint, counsel should assess whether any biometric technologies are in use within the target company’s workforce, customer base, or product offerings, and whether the associated data meets BIPA’s definitions. Particular attention should be paid to workplace applications (e.g., employee timeclocks), identity verification processes, and customer-facing biometric features (e.g., self-check-in kiosks).

[iv] Key Requirements

BIPA imposes strict informed written consent requirements, processing restrictions, and procedural requirements on regulated entities:

- **Informed Written Consent**. Before collecting or obtaining a biometric identifier or biometric information, a private entity must provide written notice to the data subject (or their legal representative) that informs them that a biometric identifier or biometric information is being collected or stored and describes the specific purpose and length of time for which the biometric data will be collected, stored, and used, and must obtain a written release executed by the data subject or their legal representative. Consent cannot be implied, bundled with other agreements, or obtained through a general privacy policy or Terms of Use. The Illinois General Assembly recently amended BIPA to clarify that a "written release" can be an electronic signature. As a result, companies can obtain valid consent to process a biometric identifier or biometric information through electronic means.
- **Prohibitions on Sale**. Biometric identifiers and biometric information may not be sold, leased, nor traded, nor may any private entity profit from a data subject's biometric identifier or biometric information.
- **Restrictions on Disclosure**. Biometric data may not be disclosed, redisclosed, or disseminated without the data subject's consent, unless required by law, pursuant to a warrant or subpoena, or as part of a lawful financial transaction authorized by the individual.
- **Reasonable Security Measures**. BIPA requires private entities to store, transmit, and protect biometric information and biometric identifiers using a standard of care equivalent to or greater than that used for other confidential and sensitive information.
- **Publicly Available Retention and Destruction Policy**. Private entities must develop and make publicly available a written policy that establishes a retention schedule and guidelines for permanently destroying biometric data when the initial purpose for collection has been satisfied, or within three years of the individual's last interaction with the private entity, whichever comes first.

Due diligence on target companies that are or may be subject to BIPA should include a review of any BIPA consent processes, transfers of BIPA-regulated data, the security measures and safeguards in place to protect BIPA-regulated data, and the retention and destruction policies required by BIPA.

[v] Enforcement

One of the most significant aspects of BIPA is its private right of action, which has made it a magnet for class action litigation. Any data subject "aggrieved" by a violation of the Act may bring a lawsuit and recover statutory damages of $1,000 per negligent violation and $5,000 per intentional or reckless violation, or actual damages, whichever is greater. The statute also permits recovery of attorneys' fees and injunctive relief. Courts have interpreted "per violation" broadly, meaning that each unauthorized scan or failure to comply with statutory requirements can count as a separate offense—leading to significant liability in high-volume use cases. In 2019, the Illinois Supreme Court held in *Rosenbach v. Six Flags Entertainment Corp.* that plaintiffs do not need to allege actual harm or data misuse to pursue a claim; instead, a mere procedural violation is sufficient to establish standing. Subsequent rulings further clarified that BIPA claims are subject to a five-year statute of limitations. In a significant change to the law that reduces potential damages for violations, the Illinois General Assembly amended BIPA in 2024 to clarify that repeated scans of the same data subject's biometric identifier constitute only a single violation, rather than a separate violation for every scan.

[vi] BIPA Due Diligence

In corporate transactions, the potential for large-scale statutory damages poses a serious financial risk. As a result, BIPA due diligence often includes review of the target company's:

- Use of biometric technology and whether it implicates the state of Illinois;
- Written notices and policies regarding biometric identifiers and information to ensure they meet BIPA requirements;

- BIPA consent flow and process;
- Internal security standards with respect to biometric identifiers and information; and
- History of consumer complaints and pending or past litigation under BIPA.

[i] New York Department of Financial Services Cybersecurity Regulation (23 NYCRR Part 500)

[i] Introduction

The New York Department of Financial Services (NYDFS) Cybersecurity Regulation (NYDFS Cybersecurity Regulation), codified at 23 NYCRR Part 500, is one of the most prescriptive cybersecurity frameworks in the United States. First effective in March 2017 and most recently amended in November 2023, the rule establishes minimum cybersecurity standards for entities regulated by NYDFS, including financial institutions, insurance companies, broker dealers, and other regulated organizations. The NYDFS Cybersecurity Regulation is also a useful framework for counsel reviewing the cybersecurity programs of target companies that are not subject to NYDFS regulation, as its requirements closely align to and operationalize cybersecurity best practices.

[ii] Applicability

The NYDFS Cybersecurity Regulation applies to all "covered entities" regulated by the New York Department of Financial Services. This includes banks, mortgage lenders and servicers, insurance companies, money transmitters, licensed virtual currency businesses, and certain investment companies and financial service providers that are licensed, registered, or otherwise authorized under New York banking, insurance, or financial services law. The NYDFS Cybersecurity Regulation also indirectly extends to "third-party service providers" through contractual obligations that covered entities must impose to safeguard sensitive information shared with vendors. Importantly, the regulation applies not only to entities physically located in New York, but also to out-of-state companies that are licensed to operate in New York or that service New York customers under NYDFS jurisdiction. In a transactional context, counsel should confirm whether the target company is directly regulated by NYDFS or indirectly subject to the rule through business relationships with Covered Entities.

[iii] Protected Nonpublic Information

The NYDFS Cybersecurity Regulation protects "nonpublic information," which is defined as business information that is not publicly available and is:

- Business related information of a covered entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the covered entity;
- any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: Social Security number, driver's license number or non-driver identification card number, account number, credit or debit card number, any security code, access code or password that would permit access to an individual's financial account, or biometric records; and/or
- Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to: the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, the provision of health care to any individual, or payment for the provision of health care to any individual.

Note that as the NYDFS Cybersecurity Regulation is a security law, it includes within its scope data that does not constitute personal data but is nevertheless subject to protections.

[iv] Required Components of an Information Security Program

The NYDFS Cybersecurity Regulation mandates that covered entities establish and maintain a comprehensive, risk-based cybersecurity program designed to protect the confidentiality, integrity, and availability of the entity's information systems and nonpublic information. This program must be commensurate with the size and complexity of the organization, the nature of its activities, and the sensitivity of the information it processes, and must address a number of specific requirements, including the following:

- **Governance and Oversight.** Covered entities must appoint a Chief Information Security Officer (CISO) responsible for overseeing the cybersecurity program and reporting at least annually to the board or governing body. Senior leadership is expected to engage in cybersecurity governance, risk evaluation, and policy enforcement.
- **Risk Assessment.** Covered entities must perform periodic risk assessments to identify threats and vulnerabilities, which in turn must inform cybersecurity policies and controls. These assessments must be documented and updated to reflect material changes in business operations or technology.
- **Cybersecurity Policies and Procedures.** Covered entities must adopt written policies approved by senior management or the board of directors. These policies must cover areas including data governance, data classification, data retention, asset inventory and management, access controls, business continuity and disaster recovery, availability, monitoring, secure software development, physical and environmental security controls, customer data privacy, vendor and third-party service provider risk management, customer data privacy, risk assessment, incident response and notification, and vulnerability management.
- **Access Controls and Multi-Factor Authentication (MFA)**. Covered entities must limit access to information systems and sensitive data based on job responsibilities and must implement MFA for remote access to internal systems, external systems from which nonpublic information is accessible, and privileged accounts, provided that the CISO may approve equivalent or more secure compensating controls.
- **Data Encryption**. Nonpublic information must be encrypted both in transit and at rest, or alternative compensating controls must be implemented if encryption is infeasible.
- **Monitoring and Testing.** Covered entities are required to conduct periodic or continuous monitoring, penetration testing, and/or vulnerability assessments, as well as monitor user accounts for unauthorized access to or use of nonpublic information. Logging and security event alerts must be centralized unless the CISO approves equivalent or more secure compensating controls.
- **Incident Response and Breach Notification**. Covered entities must maintain an incident response plan detailing roles, responsibilities, and procedures for managing and reporting cybersecurity events. Under the 2023 amendments, any cybersecurity event must be reported to NYDFS within 72 hours, and extortion payments must be reported within 24 hours with a follow-up report due within 30 days.
- **Employee Training and Awareness**. Covered entities must conduct periodic, but no less often than annual, cybersecurity awareness training that includes social engineering. Such training must be provided to all personnel and be updated to reflect risks identified by the covered entity in its risk assessment.
- **Third-Party Risk Management**. Covered entities must implement third-party service provider risk management policies that include risk assessments, minimum security practices, due diligence, and periodic assessment and monitoring of third-party service providers that access sensitive data or systems. Third-party service providers must be subject to "representations

and warranties addressing the third-party service provider's cybersecurity policies and procedures that relate to the security of the covered entity's information systems or nonpublic information."

- **Annual Certification and Compliance Documentation**. Covered entities must submit an annual certification of compliance to NYDFS by April 15 of each year. The covered entity's CISO must also maintain documentation of the cybersecurity program, including risk assessments, policies, and incident reports, for at least five years.

As noted above, while these obligations are mandatory on covered entities, with the exception of the annual certification requirement, the NYDFS Cybersecurity Regulation's detailed requirements are also a useful checklist or framework for evaluating any target company's cybersecurity program.

[v] Enforcement

NYDFS has broad authority to investigate and enforce compliance with the NYDFS Cybersecurity Regulation. It may initiate investigations, conduct examinations, and issue subpoenas or requests for information. Where violations are identified, NYDFS may pursue administrative penalties, including fines, cease-and-desist orders, and potential license revocation. Violations are subject to penalties under New York Financial Services Law § 408, with monetary fines that may be assessed per violation and compounded by the number of affected consumers or duration of noncompliance. The Department has demonstrated a growing willingness to enforce the rule aggressively, as evidenced by recent enforcement actions against both large and midsize financial institutions for failure to implement timely incident response protocols or adequate risk assessments. Critically, the annual compliance certification is not a mere formality; false certifications can form the basis for enforcement actions. NYDFS has emphasized that companies must maintain adequate records to support their certifications and may face liability if audits reveal discrepancies.

[vi] NYDFS Cybersecurity Regulation Due Diligence

- NYDFS Cybersecurity Regulation due diligence often involves review of:
- Cybersecurity policies, procedures, and governance structures;
- Risk assessments and efforts taken to address or remediate identified risks;
- Safeguards, including use of encryption and MFA;
- Third-party service provider contracts and risk management processes; and
- Contents of any annual certifications provided by a covered entity to NYDFS.

[j] State Data Breach Notification Laws

All 50 U.S. states, plus the District of Columbia, Puerto Rico, Guam, and U.S. Virgin Islands, have statutes that require notification of data breaches involving covered personal data to data subjects and, in many cases, notification to state regulators and/or major consumer reporting agencies. These laws can vary in the scope of regulated data that requires notification, the circumstances that constitute a notifiable data breach, whether a risk of harm is a precondition to required notifications, whether notice is required to regulators and any numerical thresholds for such notice, the contents of data breach notices to individuals and/or regulators, and any exceptions for entities subject to other federal privacy regulatory regimes such as GLBA or HIPAA. While a complete discussion of all 54 state data breach notification laws is beyond the scope of this chapter, we identify notable considerations and trends in these laws that are relevant for due diligence below.

[i] Applicability

These state data breach notification laws generally apply to entities that own, license, store, or otherwise process regulated personal data of a given state's residence. They often distinguish between the "owner" or "licensor" of the personal data, who has the obligation to ensure that any required notices are provided, and a party, such as a vendor, that stores or processes the data but does not own or license it, who has the obligation to notify the owner or licensor. Because data breach notification laws typically turn on the residence of the data subject and not the location of the company processing the data, it is common for one data breach event to trigger multiple state data breach notification laws, or even all of them.

[ii] Covered Personal Data

Most state data breach notification laws are intended to act as identity theft protection laws, and therefore cover a narrower scope of data that can be used to commit identity theft. As such, most state data breach notification laws require notification if a first name or first initial and last name in combination with one or more of the following data elements:

- Social Security number and/or individual taxpayer identification number.
- Federal or state government ID number such as a passport number, driver's license number, military identification numbrer, or other number issued by a government agency; and
- Financial account number, credit/debit card number, in combination with any required security or access code or password that permits access to a data subject's financial account.

However, many state data breach notification laws include additional data elements, such as:

- Information regarding a data subject's medical history, mental or physical condition, medical treatment or diagnosis by a health care professional;
- Health insurance numbers;
- Biometric information used to authenticate a data subject;
- Genetic data;
- Username and password for access to an online account; and
- In some cases, a "catchall" for any information that could be used to permit a person to commit identity theft.

[iii] Key Requirements

State data breach notification laws vary, but in the due diligence context the following key requirements are relevant:

- **Notice Triggers.** State data breach notification requirements can have varying notice triggers, which can include not just confirmed data breaches but also "reasonably suspected" compromises of regulated personal data.
- **Exceptions and Harm Thresholds.** Many, but not all, state laws include exceptions to notice requirements if the regulated entity determines that there is no substantial risk of harm to affected data subjects or if the personal data was encrypted and the encryption key was not compromised.
- **Timing of Data Subject Notice.** Some states require notice to be provided to data subjects within 30 days after discovery of a breach, while others require notice within 45 or 60 days or merely "without unreasonable delay." Most such laws contain exceptions that permit delays in notifications where requested by law enforcement.
- **Contents of Data Subject Notice.** Many state laws require that certain general or state-specific information must be included in notices to data subjects and/or regulators. In addition, some state laws are inconsistent as to the contents of required notices; for example, Massachusetts'

data breach notification law prohibits including a description of the nature of the breach or the number of Massachusetts data subjects affected, while the former is required by every other state data breach notification law and the latter is required by a smaller number of other state data breach notification law.

- **Regulator Notice.** Many states require notification to the attorney general, consumer protection office, or other state functional regulator if a certain number of state resident data subjects are affected. These notices may be required on specific timelines, ranging from 10 days to 30 days or more. Some state regulators require notification through online forms, which can request detailed information about the breach and the notifying organization's safeguards to protect personal data. Other state data breach notification laws require an organization to notify a regulator if the organization determines that notification is not warranted due to a risk of harm exception. Finally, some state regulators will publish copies of data subject breach notices on public, searchable databases, increasing the risk of reputational harm.
- **Consumer Reporting Agency Notices.** Many states include requirements to notify the major consumer reporting agencies of any breach that exceeds a certain numerical threshold.
- **Credit Monitoring Services.** A small but growing number of states require the provision of credit monitoring or identity theft restoration services to data subjects for 12 to 24 months if certain particularly sensitive data elements, such as Social Security numbers, are compromised.

[iv] Enforcement

State data breach notification laws are often enforced by state attorneys general, consumer protection offices, or other functional regulators. Failure to provide notice or comply with a given notification law may constitute an "unfair or deceptive trade practice" under state consumer protections laws, or may be subject to specific civil penalties or other remedies set forth in the state data breach notification laws themselves. In addition, state regulators will often collaborate and share information about large or multistate breaches, which can result in enforcement by regulators in multiple states.

[v] Data Breach Law Due Diligence

State data breach notification law diligence often includes review of:

- Any known or suspected data breaches or compromises of personal data to determine whether they were notifiable, including review of any determinations that notice was or was not required;
- The target company's response to any data breaches, including investigation, remediation, and notification processes;
- The contents of any notices provided to third parties, data subjects, and/or government regulators regarding a data breach;
- Any litigation, complaints, investigations, or enforcement actions relating to data breaches; and
- Law enforcement communications relating to data breach notification, including any requests to delay notification at a law enforcement agency's request.

[k] Telephone Consumer Protection Act

[i] Introduction

The Telephone Consumer Protection Act (TCPA), enacted in 1991 and codified at *47 U.S.C. § 227*, is a federal law that restricts telemarketing, automated calls, and unsolicited communications to protect consumer privacy. Though originally aimed at curbing nuisance calls, the statute has become one of the most litigated consumer protection laws in the United States due to its generous statutory damages

and expansive and class-action friendly private right of action. While recent case law has reduced the scope of federal TCPA claims somewhat, TCPA litigation, and litigation under mini-TCPA state laws such as the Florida Telephone Solicitation Act (FTSA), remain a significant source of risk for target companies that conduct telemarketing, place automatically dialed and/or prerecorded voice calls, or send SMS or text messages to mobile telephone numbers.

[ii] Applicability

The TCPA applies broadly to any person or entity that initiates or facilitates telephone calls or text messages to data subjects in the United States using specified technologies or practices. This includes not only traditional telemarketers but also e-commerce companies, SaaS platforms, debt collectors, and third-party marketing vendors. The TCPA governs calls to wireline phones, mobile phones, fax machines, and VoIP services. The Federal Communications Commission (FCC), which is tasked with implementing and interpreting the TCPA, has interpreted the statute to apply not only to those who place calls but also to parties "on whose behalf" the calls are made. As a result, target companies may be held vicariously liable for TCPA violations committed by their agents or contractors. During due diligence, counsel must therefore consider both direct and indirect exposure particularly where a target company uses outsourced marketing services or acquires telemarketing leads from third-party aggregators.

[iii] Covered Activities

The TCPA prohibits several specific categories of conduct. Chief among them is the use of an automatic telephone dialing system (ATDS) or an artificial or prerecorded voice to call or text a cellular phone number without the prior express consent of the recipient. The definition of ATDS has been the subject of extensive litigation and FCC rulemaking, and while the Supreme Court in *Facebook, Inc. v. Duguid* (2021) narrowed the statutory definition of ATDS, many systems used in modern marketing still fall within its scope. The TCPA also prohibits, among other things:

- Unsolicited prerecorded or artificial voice calls to landlines, unless an exemption applies;
- Telemarketing calls to numbers on the National Do Not Call Registry, unless the caller has an established business relationship with the consumer;
- Certain types of calls made to emergency numbers, hospital rooms, or similar protected lines; and
- Failure to provide certain disclosures, such as caller identification and opt-out instructions during telemarketing calls.

Text messages are treated as "calls" under the TCPA, meaning that SMS marketing must comply with the same consent and disclosure rules. Certain categories of calls, such as those made for emergency purposes or by tax-exempt nonprofit organizations, are exempt from some restrictions. In practice, many of the largest TCPA class actions have stemmed from marketing texts, autodialed promotional calls, and robocalls to consumers who did not provide valid consent, particularly where consent was assumed from online forms, referrals, or ambiguous privacy policies.

[iv] Key Requirements

The cornerstone of TCPA compliance is obtaining the appropriate form of prior consent. For non-marketing calls or texts to wireless numbers using an ATDS or prerecorded voice, prior express consent is sufficient, typically satisfied by the consumer voluntarily providing their phone number in the normal course of business, without conditions, so long as the messages relate to the purpose for which the number was originally provided. For telemarketing or advertising calls to wireless numbers, however, the TCPA requires prior express written consent, which must be written, signed by the person receiving the call or text, and clearly state the consumer's agreement to receive such communications. The consent must be unambiguous, obtained before the call or text is made, and include disclosures that no purchase is required. TCPA rules also impose disclosure, opt-out, and identification obligations

on telemarketers. Telemarketers must provide the name of the entity on whose behalf the call is being made, a valid telephone number or address, and, for prerecorded calls, an automated mechanism to allow recipients to opt out. Additionally, telemarketers must maintain internal do-not-call lists, honor opt-out requests promptly, and train personnel accordingly. Businesses engaging in mass telephone communications should implement robust consent and contact management systems, process do-not-call requests in a timely manner, maintain audit trails, and vet third-party lead sources for compliance. If a company acquires user data or customer contacts through a merger or asset purchase, due diligence should assess whether any TCPA consents originally obtained transfer to the acquiring party.

[v] Enforcement

The TCPA is enforced by both the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC), but its most potent enforcement mechanism is its private right of action, which has made it a frequent basis for class action litigation. Any person who receives a prohibited call or text may bring a lawsuit for statutory damages of $500 per violation (i.e., per call or text), and up to $1,500 per willful or knowing violation. These penalties can scale quickly, especially in mass-marketing scenarios, where thousands or millions of unsolicited messages may be at issue. Courts have certified class actions under the TCPA involving voice calls, SMS campaigns, and fax advertisements, leading to multimillion-dollar settlements. Even inadvertent violations, such as calling a reassigned number or failing to screen against the Do Not Call Registry, may result in liability. The absence of intent is not necessarily a defense, although willfulness may increase the amount of damages. The FCC also has authority to issue fines and enforce compliance through consent decrees and forfeiture orders. In recent years, the agency has aggressively pursued robocallers, lead generators, and companies that disguise caller identity (spoofing).

[vi] TCPA Due Diligence

TCPA due diligence often includes review of the target company's:

- Use of telephone calls, text messages, or similar communications for telemarketing and non-telemarketing purposes;
- Consent collection and recordkeeping practices for telephone calls;
- Evaluation of any use of ATDS or recorded voice;
- Vendor contracts with call centers, telemarketers, and/or lead aggregators;
- Compliance with internal and national Do Not Call requirements;
- History of data subject complaints, prior class actions, or TCPA settlements; and
- Policies and training programs relating to call compliance.

§ 9.03 Review of Privacy Compliance Program

[1] Introduction

Once counsel has identified the laws and obligations applicable to the target company, the next step in conducting privacy due diligence is to review the target company's compliance program and posture to identify gaps between the regulatory requirements and the target company's practices. While an overview of relevant policies, procedures, and requirements is provided above for each of the discussed regulatory schemes, it is helpful to consider the below high-level points as part of due diligence review.

[2] Privacy Notices

The majority of the privacy laws discussed in this chapter require regulated entities to post and comply with public privacy notices that describe how personal data is collected, used, shared, disclosed, and otherwise processed. Because such notices are generally publicly available and enforceable against the target company, a poorly drafted, incomplete, missing, or misleading privacy notice can act as an announcement to regulators that a target company is not in compliance with privacy laws and can also impede an acquirer's ability to obtain or process personal data obtained from a target company. Deficiencies in privacy notices may also indicate broader failures in governance and compliance. In conducting due diligence, privacy notices should be reviewed to ensure that they are compliant, accurate, complete, and clearly and conspicuously provided on target company websites or internal systems.

[3] Privacy Policies and Procedures

Reviewing a target company's privacy policies, practices, and notices is a key part of the due diligence process. Depending on the scope of privacy laws and obligations applicable to the target company, as well as the target company's level of sophistication and compliance posture, a target company may have extensive or minimal internal policies and procedures regarding privacy and the processing of personal data. As noted above, many privacy laws require regulated entities to implement policies and procedures to address compliance, respond to data subject rights requests, and manage third-party and vendor risk, among other things, and these policies and procedures are often the primary evidence of the target company's compliance program. Due diligence review should not be limited to just the paper policies, however, and counsel's review should attempt to confirm that these policies have been implemented in practice.

[4] Consents and Lawful Bases

Many of the privacy laws discussed in this chapter require there be some valid consent or other lawful basis pursuant to which processing of personal data occurs. Where data subject consent is required, due diligence should include a review of consent flows and any consent language to ensure that the proper level of informed consent is obtained and documented. Where processing is based on a lawful basis or permitted only for specific purposes, due diligence should include a review of whether the target company's processing activities are lawful and fit within the scope of the permitted processing.

[5] Data Maps and Privacy Assessments

Some target companies may have conducted data mapping exercises, conducted privacy impact assessments, or created registers of processing activities to assist with their privacy compliance. These are helpful artifacts

for due diligence review as they provide helpful information regarding both the processing activities of the target company as well as the target company's sophistication regarding privacy compliance, and can help identify areas that may warrant further due diligence review.

§ 9.04 Review of Cybersecurity Program

[1] Introduction

The scope of due diligence often includes a review of the safeguards and materials underlying the target company's cybersecurity program. Legal due diligence reviews of cybersecurity programs are generally scoped to identify potential compliance, legal, or regulatory issues, and as such do not typically involve testing of safeguards or controls by counsel. At minimum, most organizations are required to implement reasonable, risk-based security measures to protect personal data against unauthorized processing, access, use, or compromise. However, some target companies may be subject to laws or regulations, such as HIPAA or the NYDFS Cybersecurity Rule, that impose more detailed or specific requirements.

[2] Reasonableness

Where there are no specific regulatory obligations regarding cybersecurity applicable to a target company, counsel may wish to consider using the NYDFS Cybersecurity Rule referenced above as a framework for due diligence review of a target company's cybersecurity program, even for target companies not subject to the rule, as its requirements are often considered best practices for a mature cybersecurity program involving the processing of sensitive personal data. That said, if a target company not subject to the NYDFS Cybersecurity Rule has a cybersecurity program that does not meet the standards set by the NYDFS Cybersecurity Rule, that does not mean that the program is *per se* "unreasonable." Instead, counsel should consider the nature and sensitivity of the information being processed by the target company; the risk of harm posed to the target company, its clients, and/or data subjects if the information is compromised or subject to unauthorized access, loss, or modification; and the safeguards the target company has implemented to protect that information.

[3] Cybersecurity Audits or Assessments

Another useful due diligence artifact that counsel should consider requesting and reviewing are any internal, external, or independent information security audits or assessments conducted by or on behalf of the target company, such as pursuant to AICPA SOC 2 Type II, ISO/IEC 27XXX, NIST Cybersecurity Framework, or similar frameworks or standards. These assessments, when properly scoped, can provide a useful overview of the maturity and sophistication of the target company's cybersecurity practices and are often used by organizations to substantiate their cybersecurity programs to customers and regulators.

§ 9.05 Acquisition of Personal Data as an Asset

As data is a valuable asset, it is increasingly common for acquirers to use corporate transactions as a means to expand or acquire critical datasets for the acquirer's own use and benefit. Where acquisition of data is a key consideration for the acquirer, it is important for due diligence to evaluate both whether the acquirer can lawfully obtain the desired data and whether, once acquired, the acquirer can process the acquired data for its intended purposes. This often involves review of the target company's privacy notices, as a target company's privacy notice should ideally include a disclosure that personal data may be transferred to a third party or acquirer in the event of a sale, bankruptcy, or other corporate transaction, as well as include disclosures that describe the intended processing by the acquirer. Failure to include this language, particularly where the privacy notice includes broad statements that the target company will not sell or disclose personal information to any third party, may limit the ability of the target company to transfer personal data to an acquirer or require remedial steps such as notice and/or choice provided to data subjects. In addition, if the data sought by the acquirer is licensed or obtained from third parties, due diligence should include review of contracts with third-party data providers to evaluate whether any restrictions on transfer, processing, or sublicensing of personal data would interfere with or create risk regarding the acquirer's acquisition of the data or its intended processing activities. Finally, if there are concerns about the acquirer's ability to lawfully process data acquired from a target company, it is helpful to evaluate the potential risks posed to the acquirer and any ways to mitigate or reduce this risk, such as whether an acquirer can "cure" the issue by providing notice to and/or obtain consent from data subjects to process acquired personal data that is subject to a restrictive privacy notice. In situations where the transfer of data in connection with a corporate transaction poses risk that an acquirer is not willing to accept, an acquirer may request pre-closing deletion of unlawfully collected data or data that is not permitted to be transferred to the acquirer.

§ 9.06 Sources of Risk

[1] Introduction

While we discuss statute-specific privacy risks above, below we summarize the primary sources of risk in privacy and security due diligence, identify useful documents and artifacts for review, and briefly discuss how these terms tend to work out in practice in acquisition agreements.

[2] Investigations and Enforcement

One of the most common sources of privacy risk is regulatory noncompliance. The legal landscape governing data privacy and cybersecurity is both broad and rapidly evolving, encompassing numerous overlapping international, state, and local laws. Companies that have failed to implement appropriate governance structures, consent mechanisms, breach notification procedures, or cross-border transfer safeguards may be operating out of compliance, often unknowingly. Due diligence should evaluate whether the target company has been subject to inquiries, investigations, or enforcement actions by regulatory bodies such as the Federal Trade Commission, state attorneys general, supervisory authorities, or industry-specific oversight agencies, as well as whether the target company engages in any processing activities or is within an industry that is commonly subject to regulatory scrutiny. Even closed investigations may signal issues with compliance or continuing obligations under settlement agreements or consent orders, which may have the effect of prohibiting the acquiring entity from processing personal data obtained from the target company in certain ways or at all. Moreover, pending inquiries can pose substantial risk, especially when fines, penalties, or operational mandates could attach post-closing or be transferred with the ownership of the target company. Purchase agreements often include broad compliance with law representations and warranties, and these can be heavily negotiated in the privacy and cybersecurity context because of the risk posed by privacy and cybersecurity enforcement and the challenge of complying with multiple overlapping sets of regulatory obligations.

[3] Litigation

While the majority of privacy laws discussed above are primarily enforced by regulators or government agencies, some of the laws noted above (BIPA, TCPA) are included in our list of key regulatory considerations because they include a private right of action for violations, which significantly increases the risk of noncompliance. Even where there is no private right of action, plaintiffs may allege harms arising from data breaches, unexpected or controversial data processing activities, or unlawful surveillance. The presence of active litigation, and particularly putative class actions, can affect both valuation and risk allocation. Even where claims are meritless or nascent, counsel should consider the costs of defense, potential damages, reputational harm, and impact on customer trust. Due diligence should cover the full scope of threatened, pending, or resolved privacy and security-related litigation, including pre-litigation demand letters, internal complaints, data subject complaints, and arbitration proceedings. Counsel should also review privacy or cybersecurity indemnity provisions, insurance coverage (particularly cyber insurance), and any past settlements that could impact the ongoing business or future conduct of the target company.

[4] Contract, Vendor, and other Third-Party Risks

Target companies frequently rely on complex webs of vendors, affiliates, and service providers to process personal data and conduct business and operations. These third-party relationships may expose companies to liability if third parties experience data breaches or violate applicable laws, as privacy laws, regulators, and

plaintiffs often hold the controller responsible for the noncompliance, security breaches, and/or processing of its processors, vendors, and other third parties with access to personal data. As such, due diligence should include a review of third-party privacy and security risks, including identifying where and to what extent the target company acts as a controller versus a processor in these relationships; identifying processing activities that are higher risk due to the nature, amount or sensitivity of personal data or other confidential information processed by or on behalf of the third parties; reviewing contracts with third parties to identify processing restrictions, security and privacy requirements, and indemnity or other risk allocation provisions; and reviewing any processes the target company has in place regarding conducting due diligence on and contracting with third parties regarding personal data or confidential information.

[5] Privacy Incidents and Security Breaches

Perhaps the most visible and damaging form of privacy and security risk arises from security incidents and data breaches. These events can lead to regulatory investigations, customer attrition, business interruption, and costly remediation efforts. They may also become public knowledge, undermining brand value and raising significant concerns for acquirers about the integrity and sustainability of the target's operations. As part of due diligence, counsel should assess whether the target company has experienced any security breaches, insider threats, ransomware attacks, credential leaks, or loss/theft/unauthorized disclosure of personal data or other sensitive information, and evaluate the target company's response thereto, including any notifications provided to third parties and follow-on investigations, enforcement actions, or litigation. Counsel should also examine the target company's incident response protocols, breach notification history, forensic investigation results, and communications with regulators and affected individuals regarding security breaches. In addition, responsibility for undiscovered security incidents is a significant risk that is often heavily negotiated in the purchase agreement, and it is important to evaluate the target company's security posture to help inform these negotiations, including by providing insight as to the likelihood of a material undiscovered incident that could create risk for both the target company and the acquirer.

1 Due Diligence in Corporate Transactions Appendix A:.syn

Due Diligence in Corporate Transactions > Chapter 9 Privacy and Data Security Due Diligence > Appendix A: Sample Privacy and Data Security Due Diligence Checklist

Appendix A: Sample Privacy and Data Security Due Diligence Checklist

Synopsis

Appendix A:Sample Privacy and Data Security Due Diligence Checklist

Scope

End of Document

No Title in Original

1. Privacy Compliance

(i) Evaluate the target company's privacy governance function, including its structure, staffing, reporting lines, and oversight by executives or board.

(ii) Review the target company's personal data processing activities in connection with:

(A) The target company's products, services, marketing, and operations;

(B) The target company's personnel, employees, and job applicants; and

(C) The target company's marketing activities, including without limitation processing of personal data for direct marketing, telemarketing, email marketing, interest-based advertising, and purchases of personal data for marketing or advertising purposes.

(iii) Identify the categories of personal data processed by the target company and the purposes for which it is processed.

(iv) Identify privacy laws applicable to the target company, including those that apply based on the target company's size, revenue, jurisdictional scope, services, industries, employees, types of personal data processed, volume of personal data processed, and/or data processing activities.

(v) Identify any processing of personal data that is deemed "sensitive" or otherwise subject to heightened or sectoral privacy requirements.

(vi) Evaluate the target company's public-facing privacy notices and disclosures.

(vii) Review the target company's internal privacy policies, procedures, standards, mechanisms for providing privacy notices, obtaining consent, exercising data subject rights, and managing preferences.

(viii) Identify any purchases or sales of personal data by the target company and review any policies, procedures, opt-out mechanisms, contract templates, and/or similar materials associated therewith.

(ix) Review any privacy risk assessments, audits, or similar reviews of the functioning of the privacy compliance program and/or the target company's personal data processing activities.

(x) Review internal privacy training and awareness programs.

(xi) Analyze international transfers of personal data for compliance.

(xii) Assess whether the target company's privacy program addresses all applicable privacy laws and personal data processing legal requirements and/or assess the risks of any noncompliance.

2. Security Program

(i) Evaluate the target company's security governance function, including its structure, staffing, reporting lines, and oversight by executives or board.

(ii) Identify data security laws and obligations applicable to the target company.

(iii) Review the target company's security policies, procedures, and standards, including:

(A) The target company's risk assessment policy;

(B) The target company's incident response plan;

(C) Review the target company's business continuity and/or disaster recovery plans;

(D) Review the target company's vendor management and/or third-party risk management program; and

(E) Review internal security training and awareness programs.

(iv) Review any security risk assessments, audits, penetration tests, vulnerability assessments, or similar reviews of the functioning of the security program and/or the safeguards used by the target company.

(v) Assess whether the target company's security program addresses all applicable laws and legal requirements and/or assess the risks of identified violations.

3. Privacy and Security Contracting

(i) Review process for negotiating privacy and security contract terms with third parties, including customers and vendors.

(ii) Review forms or templates of DPAs or other privacy or security agreements used by the target company.

(iii) Review customer and vendor agreements, including data protection agreements (DPAs) for key customers and vendors to identify processing restrictions, privacy and security compliance obligations, and privacy and security risk allocations.

4. Security Incidents and Data Breaches

(i) Review security incidents or data breaches that affected the target company, including:

(A) The target company's discovery of and response to any security incidents or data breaches;

(B) Communications and/or notices provided to third parties regarding security incidents or data breaches; and

(C) Inquiries, complaints, investigations, litigation, enforcement actions, or other proceedings resulting from a security incident or data breach.

5. Privacy or Security Complaints, Investigations, Enforcement, Litigation

(i) Analyze complaints, investigations, enforcement, and litigation with respect to privacy, cybersecurity, or processing of personal data and review the target company's responses to and resolution of such matters.

(ii) Evaluate risks posed by pending, ongoing, or unresolved complaints, investigations, enforcement, or litigation.

(iii) Identify any privacy, cybersecurity, or personal data processing obligations that apply to the target company as a result of any complaints, investigations, enforcement, litigation, or settlement thereof.

6. Transaction-Specific Concerns

(i) Consider allocation of responsibility for unknown security incidents when negotiating representations and warranties.

(ii) Evaluate whether the target company is subject to any processing or disclosure restrictions (including any arising from contractual, statutory, regulatory, or privacy notice obligations) that would impact the target company's ability to provide personal data to the acquirer for the acquirer's intended processing, including any enforcement actions, consent orders, settlements, or other

provisions that would impact the target company's ability to provide personal data to the acquirer for the acquirer's intended processing.

(iii) Evaluate whether to require the target company to take risk mitigation measures pre-closing, such as by implementing policies or safeguards and/or deleting data that cannot be transferred to the acquirer.

(iv) Review the target company's privacy and cybersecurity insurance coverages, including coverage of privacy and/or security risks discovered post-closing.

End of Document

1 Due Diligence in Corporate Transactions Appendix B:.syn

Due Diligence in Corporate Transactions > Chapter 9 Privacy and Data Security Due Diligence > Appendix B: Privacy and Data Security Due Diligence Requests

Appendix B: Privacy and Data Security Due Diligence Requests

Synopsis

Appendix B:Privacy and Data Security Due Diligence Requests

Scope

End of Document

No Title in Original

1. About the Target Company

a. **Jurisdictional Scope.** In what jurisdictions, including U.S. states and internationally, does the target company have offices, employees, or other operations?

b. **International Entity Structure.**

i. If the target company has international operations or offices, do these operations or offices operate under the same corporate entity as the U.S. operations or do they operate under an affiliated or related entity?

ii. Is the target company owned or controlled by a person located in, or the governments of, China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, or Venezuela?

iii. Is the target company incorporated under only the laws of the United States?

c. **Employees.**

i. How many employees does the target company have?

ii. Does the target company have any employees in California?

iii. Does the target company have any employees outside the U.S.? If so, in which non-U.S. countries?

d. **Annual Revenue.** What was the target company's annual revenue in the preceding fiscal year?

e. **Volume of Personal Data Processed.**

i. Does the target company process (access, use, reference, store, etc.) personal data about more than 25,000, 50,000, or 100,000 individuals in any one U.S. state?

ii. If yes, please identify the U.S. states and an approximate number of consumers in each state (i.e., greater than 25,000, greater than 50,000, greater than 100,000).

f. **Personal Data Sales.**

i. Does the target company "sell" personal data (i.e. make personal data available to another entity for that entity to use for its own benefit)?

ii. If so, is 50% or more of the target company's annual revenue attributable to selling personal data?

iii. If so, please estimate the number of individuals about whom personal data was sold, licensed, or otherwise made available to third parties for the third parties' own use.

g. **Website and App Links.** Please provide links to the target company's website(s) and any applications, services, or similar online properties the target company owns or controls.

h. **Transfer of Data to Acquirer.** Is the target company subject to any obligations that would prohibit or restrict the transfer of personal or confidential data from the target company to the acquirer upon consummation of the proposed transaction, such as commitments to not "sell" data about users to third parties?

i. **Insurance Coverages.** Please provide copies of any target company insurance policies or coverages that cover privacy or cybersecurity claims.

2. Products, Services, and Customers.

a. **Jurisdictional Scope.** Please list the jurisdictions in which the target company offers its products and/or services.

b. **Direct-to-Consumer (D2C) Sales.**

i. Please describe the products and/or services the target company provides to individual or household consumers, if any.

ii. Please describe any personal data processed by or on behalf of the target company in connection with the provision of D2C services, and the purposes for which the personal data is processed.

iii. Please estimate the percentage of annual revenue attributable to D2C sales.

c. **Business-to-Business (B2B) Sales.**

i. Please describe the products and/or services the target company provides to corporate or enterprise customers, if any.

ii. Please describe any personal data processed by or on behalf of the target company in connection with the provision of B2B services, and the purposes for which the personal data is processed.

iii. Please estimate the percentage of annual revenue attributable to B2B sales.

d. **Use of Customer Data.**

i. If the target company receives personal or confidential data from its customers, does the target company use such customer data only for the benefit of the customer?

ii. If no, please describe how the target company uses such customer data.

e. **Customer Agreements and Terms.**

i. Please provide copies of any forms of customer agreements used by the target company, including without limitation purchase agreements, terms of use, clickwrap terms, master services agreements, data protection agreements, information security requirements, business associate agreements, or similar terms.

ii. Please provide copies of any agreements with key or strategic customers of the target company.

iii. If applicable, please describe how the target company negotiates the privacy and security terms of its engagements with customers to ensure that the target company can comply with the requirements therein.

f. **Regulated Sectors.** Does the target company operate, or provide services to customers within, any of the following industries or use cases? If so, please indicate which industries, and whether the target company itself operates within these industries or provides services to customers within these industries:

i. Healthcare

ii. Financial services

iii. Education

iv. Consumer reporting

v. Data of individuals known to be under the age of 18

vi. Location data services

vii. Data brokerage

viii. Adtech, targeted advertising, or behavioral advertising

g. **Marketing.**

i. Does the target company use any of the following to market or advertise to customers?

ii. If so, please provide any policies and procedures regarding compliance with legal obligations with respect to such marketing.

1. Telemarketing, SMS/text message marketing

2. Email

3. Interest-based advertising, online behavioral advertising, retargeting

4. Purchase of leads or contact lists

3. Privacy Compliance

a. **Governance.** Please identify any persons or employees responsible for overseeing the target company's privacy compliance.

b. **Compliance Scope.** Please identify any laws regarding privacy or the processing of personal data that the Company has identified as applying to its business, operations, or services, and describe the steps the Company has taken to comply with such laws.

c. **Data Maps.** Please provide copies of any data maps, records of processing activities, or similar materials that describe the target company's processing of personal data.

d. **Audits and Assessments.** Please provide copies of any privacy compliance audits or assessments, reports, data protection impact assessments, legitimate interests assessments, privacy impact assessments, transfer impact assessments, or other materials designed to document, assess, or verify the target company's privacy compliance.

e. **Privacy Policies and Notices.** Please provide copies of all privacy policies, notices, and disclosures provided or made available by the target company to consumers, customers, employees, job applicants, website visitors, and other individuals.

f. **Privacy Compliance Policies.** Pleas provide copies of any policies, procedures, or other materials designed to address privacy law compliance within the target company's organization.

g. **Data Subject Rights.** Please provide copies of the target company's policies and procedures for handling individual rights requests pursuant to privacy laws, which may include rights of access, correction, deletion, opt-out of processing, and other rights, or if there are no such policies or procedures, please describe the target company's practices with respect thereto.

h. **International Data Transfers.** Please describe any international transfers of personal data conducted by the target company, particularly with respect to:

i. Transfers of personal data from the European Economic Area, United Kingdom, or Switzerland to other jurisdictions; and

ii. Transfers of personal data (even in deidentified or encrypted form) about U.S. persons to recipients in or controlled by China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, or Venezuela.

i. **Background Checks.** Please describe any background checks the target company conducts on its employees and/or job applicants and provide any consent forms, adverse action processes, and similar documents used by the target company with respect thereto.

j. **Trainings.** Please describe any privacy trainings provided to the target company's employees, including the frequency of such trainings, the contents of such trainings, and whether attendance is tracked.

k. **Location Data.** Does the target company collect or process location data or precise location data, such as information that could be used to locate an individual or device within a certain level of precision (e.g., within 3200 feet, within 1,750 feet, or similar)?

i. If so, please describe, including the precision of the location data, the purposes for which the location data is collected, used, and disclosed to third parties, and any consents obtained by the target company with respect thereto.

l. **Biometric Data.** Does the target company collect or process biometric information, such as fingerprints, handprints, voice prints, or scans of hand or face geometry, for the purposes of identifying an individual?

i. If so, please describe, including the purposes for which the biometric information is collected, used, and disclosed to third parties, and any consents obtained by the target company with respect thereto.

ii. If so, does the target company process biometric information about individuals located in Illinois?

4. Security Program

a. **Governance.** Please identify any persons or employees responsible for overseeing the target company's information security program.

b. **Compliance Scope.** Please identify any laws regarding cybersecurity or data protection that the Company has identified as applying to its business, operations, or services, and describe the steps the Company has taken to comply with such laws.

c. **Audits and Assessments.**

i. Please provide copies of any security audits or assessments, risk assessments, penetration test results, or other materials designed to assess or test the target company's security program and/or safeguards.

ii. Has the target company ever had its security program audited, evaluated, or reviewed by a client or other third party? If so, please describe, including any material issues identified and remediation or mitigation thereof.

d. **Penetration and/or Vulnerability Testing.** Please describe the target company's penetration testing and/or vulnerability testing practices and provide copies of the most recent reports thereof.

e. **Information Security Program.** Please provide copies of the target company's information security program, including without limitation any of the following policies and procedures:

i. Risk assessment policy

ii. Incident response policy

iii. Business continuity and/or disaster recovery policy(ies)

iv. Access control policy

v. Data classification policy

vi. Data retention policy

vii. Encryption policy

viii. Employee training policy

ix. Monitoring and logging policy

x. Secure software development policy

xi. Vendor and third-party risk management policy

f. **Trainings.** Please describe any cybersecurity trainings provided to the target company's employees, including the frequency of such trainings, the contents of such trainings, and whether attendance is tracked.

5. Vendors.

a. **Vendors Processing Personal Data.** Please identify any vendors that process personal or confidential data for or on behalf of the target company and describe the services provided, including

i. Vendors that process employee data; and

ii. Vendors that process customer or consumer data.

b. **Vendor Agreements and Terms.** Please provide copies of any forms of vendor agreements used by the target company, including without limitation master services agreements, data protection agreements, information security requirements, business associate agreements, or similar terms.

c. **Vendor Management.** Please describe how the target company conducts due diligence on and/or monitors its vendors with respect to privacy and cybersecurity compliance.

6. Security Incidents and Data Breaches.

a. Has the target company experienced any security incidents, data breaches, or compromises of personal data or confidential data in the past six (6) years? If so, please provide, for each such event:

b. A description of the event, including when and how such event was discovered, how such event was investigated or remediated, the nature or types of data affected, and whether any third parties, individuals, or government bodies were notified;

c. Copies of any reports, such as forensic reports or memoranda, evaluating the nature and scope of the breach and the target company's obligations or response thereto;

d. Copies of any communications or notices provided to individuals, third parties, or government regulators regarding such event; and

e. Any inquiries, complaints, investigations, litigation, enforcement actions, or correspondence with any third party with respect to such event.

7. Privacy or Security Complaints, Investigations, Enforcement, Litigation

a. Has the target company been the subject of any inquiries, complaints, investigations, litigation, or enforcement actions with respect to privacy, cybersecurity, or its processing of personal or confidential information? If so, please provide, for each such event:

b. A description of the event, including the entities involved, when the target company became aware of such event, and copies or descriptions of any such allegations, complaints, or claims;

c. A description of how the matter was resolved, including copies or descriptions of any settlements, judgments, injunctive or equitable relief, fines, penalties, or consent orders against the target company; and;

d. Any ongoing or continuing obligations that apply to the target company with respect thereto.

1 Due Diligence in Corporate Transactions Chapter 10.syn

Due Diligence in Corporate Transactions > Chapter 10 Cross-Border Transactions / Foreign Investment Due Diligence

Chapter 10 Cross-Border Transactions / Foreign Investment Due Diligence

---

End of Document

1 Due Diligence in Corporate Transactions § 10.01

Due Diligence in Corporate Transactions > Chapter 10 Cross-Border Transactions / Foreign Investment Due Diligence

§ 10.01 Overview

Cross-border mergers, acquisitions, and investments have become a defining feature of the twenty-first century global economy. Corporations seek growth, diversification, and access to new technologies and markets by acquiring or partnering with entities abroad. Conversely, sovereign governments, regulators, and international organizations have responded with increasingly complex and overlapping regimes to scrutinize such transactions. The convergence of business imperatives with national security, competition policy, and public interest considerations creates a landscape in which transactional and investment due diligence has become both legally essential and strategically indispensable.

The scrutiny applied to cross-border transactions and investments is not confined to traditional antitrust concerns. This chapter discusses how governments are increasingly invoking national security rationales to review acquisitions and investments in sensitive industries such as defense, telecommunications, semiconductors, data infrastructure, and artificial intelligence. The tension between these two perspectives — capital mobility as an economic good, versus capital mobility as a potential security threat — lies at the heart of the modern regulatory environment for cross-border transactions. Over the last three decades, the pendulum has swung markedly toward heightened scrutiny. Whereas the late twentieth century was characterized by liberalization, deregulation, and the removal of barriers to foreign investment, the twenty-first century has witnessed the resurgence of economic nationalism. Governments across North America, Europe, and Asia now increasingly view foreign acquisitions not through the lens of economic efficiency alone, but through the broader prism of strategic autonomy, technological sovereignty, and resilience of critical supply chains. The United States' Committee on Foreign Investment in the United States (CFIUS), the United Kingdom's National Security and Investment Act (NSIA), and the European Union's Foreign Direct Investment Screening Regulation are emblematic of this trend.

As such, legal professionals and business advisors are now tasked with navigating a dynamic landscape characterized by disparate regulatory regimes, differing standards of corporate governance, ever-evolving compliance requirements, national security concerns, and a rapidly changing geopolitical landscape. Therefore, transactional and investment due diligence must extend beyond financial and commercial analysis. It requires a holistic evaluation of political risk and the target's exposure to extraterritorial regimes. Investors must ask: How do regulatory frameworks apply? Which agencies in which countries have jurisdiction? How does the transaction intersect with evolving notions of national and economic security? The answers to these questions can fundamentally shape deal feasibility and negotiation dynamics.

The consequences of failing to navigate these regimes are profound. Transactions that close without required transactional or investment approvals may be subjected to ex post review and unwinding. Civil and criminal penalties can be severe: CFIUS, for example, may impose fines up to the value of the transaction for failure to file a mandatory declaration.

Beyond formal enforcement, the commercial consequences of non-compliance can be equally damaging. Delayed approvals may erode deal value, trigger contractual penalties, or allow competitors to seize market opportunities. Reputational harm may affect both the buyer and seller, particularly where national media and political actors frame the transaction as a threat to national interests. In the capital markets, uncertainty about regulatory clearance can depress share prices, complicate financing, and invite activist intervention.

Critically, transactional and investment due diligence must be forward-looking. It is insufficient to merely confirm compliance with existing laws; counsel and advisors must also anticipate pending legislative and regulatory reforms. For example, in the United States, debates about outbound investment screening suggest that U.S. investors may soon face regulatory constraints when investing in sensitive technologies abroad. In Europe, discussions about digital sovereignty may lead to new restrictions on data-related transactions. Perhaps the most challenging aspect of modern cross-border due diligence is the interdisciplinary nature of the risks involved. A single transaction may simultaneously implicate the corporate law, tax law, antitrust law, data privacy law, export control regimes, sanctions laws, and national security screening mechanisms of multiple jurisdictions. Layered atop these legal frameworks are political dynamics: parliamentary inquiries, media campaigns, and lobbying efforts may shape the regulatory outcome as much as legal arguments.

For this reason, transactional and investment due diligence in cross-border transactions cannot be reduced to a checklist. It requires a nuanced appreciation of the political economy of host jurisdictions, the enforcement culture of regulators, and the geopolitical context of the transaction. Transactions involving Chinese investors in U.S. technology firms, for example, are scrutinized differently than Europe-to-U.S. acquisitions in traditional manufacturing. The identity of the investor, the nature of the target, and the strategic sector involved all interact in complex ways that must be evaluated holistically.

Due Diligence in Corporate Transactions

§ 10.02 Transactional and Investment Due Diligence Teams

The effectiveness of cross-border transactions depends significantly on the composition and coordination of due diligence teams. An ideal team for international cross-border due diligence must be multidisciplinary, integrating legal, financial, regulatory, and geopolitical expertise. From the buyer's perspective, the objective is to uncover risks and validate value; from the seller's perspective, the priority is disclosure management and liability allocation.

Key roles include: corporate counsel to manage deal structure; regulatory and trade lawyers to identify exposure under sanctions, export controls, anti-bribery, anti-money laundering and foreign investment regimes; tax advisors, competition economists and antitrust lawyers to anticipate merger reviews; and experts to probe environmental, social, and governance (ESG) exposure. Sellers also require internal compliance officers, finance teams, and external consultants to prepare disclosures, manage reputational risks, and facilitate regulator engagement.

In both cases, the effectiveness of due diligence depends not only on technical expertise but also on the coordination between disciplines and the buyer and seller. A siloed approach risks overlooking interdependencies—such as how tax structuring may intersect with investment restrictions, or how data privacy may affect national security reviews in strategic industries.

§ 10.03 Selected Regulatory Considerations

[1] Overview

Foreign investment regulation has become a defining feature of the modern M&A environment. Inbound and outbound deals alike must confront layers of national security, tax, and competition oversight. The U.S. provides particularly salient examples in Committee on Foreign Investment in the United States (CFIUS) and Foreign Investment in Real Property Tax Act (FIRPTA), both of which carry heavy implications for transaction structuring.

A robust diligence process requires familiarity with both substantive obligations (e.g., when a filing is triggered, what approvals are required) and procedural dynamics (e.g., timelines, disclosure obligations, confidentiality protections). Equally important is understanding the overlapping jurisdictional reach, meaning that clearance in one jurisdiction does not immunize a transaction from review elsewhere.

[2] Committee on Foreign Investment in the United States (CFIUS)

[a] CFIUS: Purpose and the FIRRMA Expansion

The Committee on Foreign Investment in the United States ("CFIUS") is U.S. government's interagency committee tasked with reviewing certain transactions involving foreign investment in the United States for national security risks. In 2018, Congress enacted the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) strengthening and modernizing CFIUS to address national security concerns more effectively, including by broadening the authorities of the President and CFIUS related to certain foreign non-controlling investments and real estate transactions that previously fell outside CFIUS's jurisdiction.

[b] Covered CFIUS Transactions

CFIUS jurisdiction is broad, covering both controlling and certain non-controlling investments in U.S. businesses engaged with critical technologies, infrastructure, or sensitive data (referred to as "TID" businesses).

- **Critical Technologies**: These include items controlled under the Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR), and other statutory frameworks and technologies in sectors such as semiconductors, quantum computing, aerospace, AI, and biotechnology which are of particular concern. FIRRMA established a close linkage between sensitive technology, export control classification and CFIUS jurisdiction: if a U.S. business produces, designs, or tests sensitive or export controlled technology, foreign investment may trigger mandatory filing.
- **Critical Infrastructure:** Infrastructure is defined broadly to include telecommunications networks, energy grids, ports, transportation systems, and financial infrastructure. Recent practice indicates heightened sensitivity to telecommunications and digital platforms that underpin economic security.
- **Sensitive Personal Data**: CFIUS has increasingly focused on companies that maintain or collect data on U.S. citizens. This includes health data, financial data, geolocation data, and even consumer usage patterns when collected at scale.

The review process can result in mitigation agreements, presidential blocks, or even post-closing divestitures. “Covered transactions” requiring mandatory filing include:

- **Acquisitions of Control**: Any transaction where a foreign person obtains control over a U.S. business. “Control” is interpreted expansively — not merely majority ownership but also rights that confer significant influence, such as veto rights, access to sensitive information, or the ability to appoint key personnel.
- **Non-Controlling Investments**: FIRRMA extended jurisdiction to minority investments that grant foreign investors access to nonpublic information, board seats, or substantive decision-making in sensitive sectors.
- **Real Estate Transactions**: CFIUS now reviews real estate transactions near airports, seaports, and military installations, even if no U.S. business is acquired.
- **Other Covered Transactions**: Transactions structured through joint ventures, licensing arrangements, or contractual agreements may still be covered if they grant functional control or access.

[c] CFIUS Filing Requirement and Timeline

Filing is mandatory if a transaction meets the definition of a “Covered Transaction” per the mandatory filing rules set forth by CFIUS. However, in certain cases, parties may also decide to make a voluntary filing for transactions that do not necessarily meet the criteria for mandatory filing but implicate national security and are likely to invite government scrutiny. Voluntary filings alleviate the risk that CFIUS independently identifies the transaction post-closing and requests a filing for its review. In such cases, if CFIUS determines that the transaction raises U.S. national security concerns, then CFIUS has the authority to unwind the transaction.

The CFIUS review process unfolds in multiple stages:

- Pre-Filing Stage: Prior to making a formal filing, parties must submit a draft notice to CFIUS for comments and requests for clarification. There is no defined timing for the same and this stage can be multiple rounds.
- Review (45 days): Initial formal assessment to determine whether the transaction raises national security concerns.
- Investigation (45 days, extendable): If concerns are identified or the review is not completed within 45 days, the transaction proceeds to a more in-depth investigation. This may involve engagement with defense, intelligence, and homeland security agencies.
- Presidential Decision (15 days): In rare cases where CFIUS cannot resolve concerns, the matter is referred to the President, who has authority to block the transaction outright.

Transactions that are not cleared outright— *the vast majority are cleared*— are resolved through negotiated mitigation agreements, where the foreign investor agrees to conditions such as limiting data access, appointing U.S.-only security officers, or creating proxy boards.

[d] CFIUS Due Diligence

CFIUS due diligence must assess the target’s industry classification, ownership structure of investors, and data sensitivity. Strategic measures may include voluntary filings, structuring rights to reduce foreign control, and preparing contractual covenants for regulatory cooperation. For buyers and sellers alike, CFIUS diligence requires proactive and strategic planning:

- Buyer’s Obligations: Buyers must map ownership structures, evaluate whether their investors include foreign governments, and anticipate how regulators will perceive the transaction politically as well as legally.

- Seller's Preparations: Sellers in sensitive industries often conduct pre-sale CFIUS assessments to reassure buyers that risks are known and manageable.
- Deal Structuring: Parties may mitigate CFIUS risk by carving out sensitive assets, restricting foreign access to certain data, or creating governance structures that limit control rights.
- Contractual Protections: Buyers often demand covenants obligating cooperation with CFIUS, conditions precedent tied to approval, and "reverse termination fees" if the deal fails due to regulatory blockage.

CFIUS is not simply a legal hurdle; it reflects broader geopolitical dynamics. The U.S. has increasingly linked foreign investment review to strategic competition with China, concerns about technological leadership, and the protection of supply chains. For multinational corporations, this means that regulatory risk is not static but evolves with shifting political priorities. More broadly, CFIUS has become a model emulated globally. The UK's NSIA, the EU Foreign Direct Investment Screening Regulation, and similar regimes in Japan, Canada, and Australia reflect a convergence toward more restrictive scrutiny of foreign investment. Thus, diligence on CFIUS is not merely U.S.-specific and can foreshadow the approach other jurisdictions may take.

[3] Foreign Investment in Real Property Tax Act (FIRPTA)

FIRPTA subjects gains of foreign sellers from U.S. real property interests to federal income taxation. Buyers must withhold and remit a portion of the purchase price to the U.S. Internal Revenue Service (IRS) unless exemptions apply. The diligence process must determine whether the seller is a foreign person, whether the asset qualifies as a U.S. real property interest, and whether exemptions such as domestically controlled Real Estate Investment Trusts (REITs) are available. Buyers bear liability for non-compliance, making FIRPTA a key diligence area in real estate transactions.

[4] United States Direct Investment Abroad

Outbound U.S. investment raises a distinct set of risks. Host jurisdictions may impose restrictions on foreign investment in sensitive sectors (China's Negative List, India's sectoral caps, EU Member State FDI screening), while U.S. law maintains extraterritorial reach. Sanctions, export controls, and the FCPA continue to apply abroad, exposing U.S. investors to liability.

Emerging outbound screening, including the proposed Outbound Investment Security Program (OISP), indicates a shift toward regulating U.S. capital flows into sensitive foreign sectors such as semiconductors, AI, and quantum technologies. Due diligence must therefore include regulatory mapping of host-country regimes, export control implications, sanctions screening, and anti-corruption reviews.

Transactional and investment due diligence considerations include:

- Host country investment screening regimes: e.g., China's Negative List, UK NSIA requirements, and EU Member State FDI laws.
- Emerging U.S. restrictions on outgoing investments.
- Anti-corruption risks: evaluating compliance with the Foreign Corrupt Practices Act (FCPA) in jurisdictions with high perceived corruption.
- Geopolitical risks: ensuring that investments do not create exposure to secondary sanctions or trade embargoes.

U.S. investors should adopt a two-pronged approach: (1) reviewing host country legal frameworks for inbound investment, and (2) mapping extraterritorial application of both current and emerging U.S. laws and regulations, *e.g.*, OISP, sanctions and export controls.

[5] UK and EU Transaction and Investment Notifications

The UK and EU impose transaction and investment notification regimes that can significantly affect deal timing and certainty. For example, the UK's National Security and Investment Act (NSIA) requires mandatory pre-closing notifications for foreign acquisitions in 17 sensitive sectors including advanced materials, advanced robotics, artificial intelligence, communications, computing hardware, data infrastructure, defense, energy, transport and others. In the EU, the EU FDI Screening Regulation sets forth a framework for FDI screening at Member State level and encourages, but does not mandate, implementation.

Due diligence in the UK/EU context requires early jurisdictional triage, coordination of filing strategies between jurisdictions and also buyer and seller, preparation of evidence packages, and anticipation of potential remedies across competition and foreign investment reviews.

§ 10.04 Conclusion

Cross-border transactional and foreign investment due diligence is a strategic exercise, not simply a compliance requirement. The regulatory environment is dynamic, shaped by national security, competition policy, and geopolitical developments. Effective teams anticipate regulatory triggers, coordinate multi-jurisdictional filings, and structure transactions to mitigate risk. By doing so, practitioners protect deal value, facilitate closing, and ensure long-term integration success in an increasingly complex global marketplace.

Chapter 11 Export Rules and National Security and International Trade Regulations Due Diligence

Due Diligence in Corporate Transactions

End of Document

§ 11.01 Overview

In today's interconnected global economy, cross-border transactions are increasingly subject to complex and stringent national security and international trade laws. For acquirers and investors, the stakes are high: failure to identify regulatory exposure related to sanctions, export controls, customs obligations, antiboycott regulations, or anti-corruption regimes can result in significant civil and criminal penalties, reputational damage, disrupted operations, and even deal termination. Conversely, robust diligence in these domains can uncover hidden liabilities, protect against successor liability, and offer valuable insights into integration and risk mitigation post-closing.

The scope of relevant U.S. regulatory regimes is vast. U.S. sanctions laws, enforced by the U.S. Department of Treasury's Office of Foreign Assets Control ("OFAC"), impose restrictions on dealings with designated persons and embargoed countries and carry extraterritorial reach. U.S. export control laws, including the Export Administration Regulations ("EAR") enforced by the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") and the International Traffic in Arms Regulations ("ITAR") enforced by the U.S. Department of State's Directorate of Defense Trade Controls ("DDTC"), govern the export and reexport of sensitive goods, technologies, and software and military items. Customs laws administered by U.S. Customs and Border Protection ("CBP") affect how products are classified, valued, and declared at the border. The Department of Commerce also enforces antiboycott provisions under the Export Administration Act, while the Census Bureau mandates Electronic Export Information ("EEI") filings. And finally, there is the Foreign Corrupt Practices Act ("FCPA"), which criminalizes bribery of foreign officials and imposes strict books and records obligations.

Due diligence in these areas must be structured, strategic, and tailored to the target's industry, geographic footprint, supply chain, and customer base. Counsel should seek to understand both formal compliance mechanisms (*e.g.*, policies, procedures, audit trails) and the real-world behaviors and controls that govern operations. The diligence process should not only focus on current compliance status but also evaluate the robustness of internal control frameworks, past regulatory engagements, and the tone of management.

Representations and warranties in purchase agreements serve as a critical risk allocation tool. Buyers should seek fulsome representations affirming compliance with international trade and national security laws, no past violations, and the accuracy of disclosures provided during diligence. Sellers, in turn, must ensure that representations reflect their actual compliance posture and are not overly expansive, while carefully crafting disclosure schedules to carve out known exceptions. Failure to do so may result in significant post-closing enforcement liability on the Buyers side or may result in indemnification claims on the Sellers' side.

This chapter proceeds by analyzing the legal regimes at play, offering a comprehensive narrative on how to conduct due diligence under each regime, identifying the specific records and documents to request, and explaining their relevance and importance to assessing legal and business risk.

§ 11.02 International Trade Due Diligence

[1] Overview

International trade due diligence forms the backbone of regulatory risk assessment in cross-border M&A and investment transactions. The purpose is to ensure that the target company complies with U.S. and applicable foreign laws governing the cross-border movement of goods, services, technology, and financial transactions. This involves evaluating compliance with laws administered by OFAC, BIS, DDTC, CBP, and the Census Bureau, the Securities and Exchange Commission and the Department of Justice among others.

Effective diligence requires an integrated approach. Rather than reviewing each regulatory regime in a vacuum, the diligence team should develop a risk map of the target's operations. Key risk indicators include complete lack of compliance protocols, sales or shipments to high-risk jurisdictions (*e.g.*, sanctioned countries), involvement in sectors subject to high export control scrutiny (*e.g.*, aerospace, defense, telecommunications), use of third-party intermediaries, operations in high-risk jurisdictions, and import-heavy supply chains. Additional risks arise from merger integration, where the acquiring party inherits the target's compliance culture and practices.

A foundational task is to review the target's trade compliance policies. The presence of a written export compliance manual, sanctions screening procedures, antiboycott compliance guidance, and FCPA training protocols are all indicia of a mature compliance function. Absence or obsolescence of these documents may suggest ad hoc compliance or reliance on informal controls. Equally important is the company's organizational structure. Does it have a dedicated compliance officer and training for personnel? Is senior leadership aware of export or sanctions risks? Is there a mechanism for internal reporting? Responses to these questions shape the diligence team's understanding of the company's internal controls.

From there, diligence expands to include transactional review. Key may documents include but should be tailored to the entity under review:

- **Denied party screening logs**: to assess whether the company systematically screens transactions against the SDN List and other restricted party lists.
- **Product and Customer Lists**: to verify the need for export classifications and country-of-destination controls.
- **Export Classification and Licensing history**: including logs of classifications of exported items per the EAR or ITAR, BIS or DDTC export licenses and OFAC licenses, which help gauge the complexity of the company's export operations.
- **Import/Export Audit reports**: both internal and external audits may highlight past deficiencies or instances of noncompliance.
- **Voluntary disclosures or enforcement history**: any history of prior OFAC, BIS, CBP, anti-corruption investigations or investigations in any other local jurisdiction, or settlements is a red flag that warrants further inquiry.

Each of these documents offers a data point. Together, they enable the diligence team to triangulate whether the target operates within the bounds of applicable laws or is exposed to regulatory liabilities.

[2] U.S. Sanctions Regulations

[a] Overview

The United States maintains a complex and far-reaching sanctions regime intended to further national security, foreign policy, and economic goals. Administered by the Office of Foreign Assets Control ("OFAC") within the U.S. Department of the Treasury, these sanctions prohibit U.S. persons from engaging in transactions with certain embargoed countries, entities, and individuals. Sanctions are generally imposed under statutory authorities such as the International Emergency Economic Powers Act ("IEEPA"), the Trading with the Enemy Act ("TWEA"), and more targeted laws like the Global Magnitsky Human Rights Accountability Act and the Countering America's Adversaries Through Sanctions Act ("CAATSA").

Sanctions programs are divided into two broad categories: comprehensive sanctions— which prohibit virtually all transactions with a country, such as those on Iran, North Korea, Cuba and certain Russian-occupied regions of Ukraine, and list-based or targeted sanctions— which apply to named individuals and entities on lists such as the Specially Designated Nationals and Blocked Persons List or the "SDN List". OFAC may also impose sectoral sanctions, which restrict certain categories of transactions, such as financing or technology transfers, with specific sectors of a foreign economy.

Importantly, U.S. sanctions laws have extraterritorial reach in several contexts. U.S. persons remain subject to U.S. sanctions no matter where they are located, and non-U.S. subsidiaries and affiliates of U.S. companies may also be required to comply with sanctions. OFAC may also exercise jurisdiction over transactions and dealings with a "U.S.-nexus" which is broadly interpreted. Moreover, secondary sanctions allow the U.S. to sanction non-U.S. persons who engage in material dealings with sanctioned entities or countries. This extraterritoriality significantly increases the importance of sanctions compliance for multinational and non-U.S. targets.

Penalties for violations are steep. Civil penalties under IEEPA can reach $377,700 per violation (adjusted for inflation), while criminal penalties include up to $1 million in fines and up to 20 years imprisonment (*50 U.S.C. § 1705*). Importantly, Civil enforcement actions for violations of U.S. sanctions are strict liability, meaning that intent is not required to trigger a penalty.

[b] Due Diligence

Sanctions due diligence important for identifying legal and reputational risks in a proposed transaction. The scope and intensity of the review should be proportional to the target's geographic reach, customer base, and industry profile. A company operating in high-risk jurisdictions or with customers in high-risk jurisdictions may warrant deeper scrutiny due to the higher probability of sanctions exposure.

A due diligence review begins by mapping the company's geographic operations and customer/vendor base. Key diligence steps include:

1. **Request and Review Sanctions Compliance Policies and Procedures**: As an initial step, obtain and evaluate the company's written sanctions compliance policies and procedures. This includes its OFAC compliance manual, internal guidance for employees, risk assessment frameworks, training and incident escalation protocols. The existence and comprehensiveness of these documents are strong indicators of whether the company is managing sanctions risks proactively. A lack of formal policies may suggest inconsistent or nonexistent compliance practices.

2. **Screening Practices and SDN List Checks**: Determine whether the company conducts real-time screening of all customers, vendors, and transactions against the SDN List and other restricted lists (*e.g.*, BIS Entity List, UN Sanctions List). Review automated screening system reports and understand escalation procedures. Gaps in this process are critical; missed matches could result in unauthorized dealings with blocked persons. A lack of screening indicates that sanctions are not on the Company's radar. In which case, the customers and vendors should be screened by the due diligence team.

3. **Dealings in High-Risk Jurisdictions**: Analyze the target's history of dealings with embargoed jurisdictions such as Cuba, Iran, Syria, North Korea, or Crimea. Review customer lists for at least

the past ten (10) years to the extent available, and request information regarding any known dealings. Also review customers in the UAE, Turkey, or Hong Kong as transactions routed through intermediaries in these jurisdictions are subject to sanctions evasion risk.

4. **OFAC Licenses and Interpretive Guidance**: Ask whether the company has sought or obtained any OFAC licenses or guidance letters. A history of licensing may indicate that the company understands its regulatory obligations. Conversely, the absence of licenses in case of activity that likely requires them is a potential indicator of noncompliance. Review issued licenses for expiration, scope, and conditions.

5. **Compliance Program Maturity**: Evaluate the overall sanctions compliance program. In addition to requesting compliance policies, examine training materials, internal audit reports, and organizational charts showing reporting lines for compliance officers. Determine if there is a designated OFAC compliance officer and whether the board receives regular compliance updates. A mature program suggests lower regulatory risk and may also indicate the likelihood of early detection and self-remediation of issues.

6. **Voluntary Self-Disclosures (VSDs) and Regulatory History**: Ask whether the company has submitted any voluntary self-disclosures to OFAC. Review correspondence and outcomes of any enforcement matters, settlement agreements, or cautionary letters. A company that has previously submitted VSDs and enhanced its compliance program afterward may be a lower risk target than a company that remained silent after violations.

7. **Third-Party Risks and Intermediaries**: Evaluate relationships with resellers, distributors, and agents. Request compliance certifications and due diligence files for third parties operating in higher-risk jurisdictions. The absence of third-party due diligence procedures for high-risk jurisdictions is a vulnerability.

8. **Sanctions Compliance Clauses in Agreements**: Evaluate sample customer, vendor, contractor and agent agreements to identify whether these agreements have contractual clauses requiring sanctions compliance. The presence of a sanctions compliance clause shifts some (minimal) burden of compliance to the counterparty and can indicate that the company has some awareness of its sanctions compliance obligations.

Each document serves a different diagnostic function, for example:

- **Compliance policies and procedures** reflect the company's commitment to sanctions controls and the institutionalization of compliance practices.
- **Screening logs** show proactive efforts to prevent violations.
- **Dealings in high-risk jurisdictions** expose red flags.
- **Licenses** demonstrate compliance awareness.
- **Audit reports** reveal the company's interest in identifying and responsiveness to risks.
- **Trainings provided** reflect a culture of compliance.

Findings should be assessed to identify specific and overall sanctions risks. If significant exposure is found, the buyer may need to pursue one or more mitigation strategies: restructuring the deal to exclude high-risk assets, requiring remediation covenants, strong representations and warranties, or conditioning closing on voluntary disclosure to OFAC.

§ 11.03 U.S. Export Controls

[1] Overview

The United States imposes export control laws to regulate the dissemination of sensitive goods, technologies, and software to foreign persons and countries. These laws serve national security, foreign policy, and nonproliferation objectives. The principal regulatory regimes are:

1. **The Export Administration Regulations (EAR)**, administered by the Bureau of Industry and Security ("BIS") at the U.S. Department of Commerce. These regulations apply to dual-use items—those that have both civilian and military or strategic applications. The EAR classifies items using Export Control Classification Numbers ("ECCNs") and may require licensing for exports or reexports depending on the item, destination, end user, and end use. Additionally, the EAR includes specific controls on end uses and end users, including military end-user controls, and mandates screening against the BIS Entity List, Denied Persons List, and Unverified List.
2. **The International Traffic in Arms Regulations (ITAR)**, administered by the Directorate of Defense Trade Controls ("DDTC") at the U.S. Department of State. These rules apply to defense articles, defense services, and related technical data designated on the U.S. Munitions List ("USML"). ITAR is significantly more restrictive than EAR; virtually all exports of ITAR-controlled items require prior authorization, and reexport or transfer to foreign persons (even within the U.S.) is strictly controlled.

U.S. export controls "follow the item" if the item in question is "U.S.-origin," or in some cases incorporates U.S.-origin items or controlled U.S. technology, or is exported or reexported from the U.S. Whether or not items are subject to U.S. jurisdiction depends on whether item is considered "subject to the EAR" per Part 734 of the EAR or if they are defense items on the USML. It is important to note that seemingly innocuous and common items like software incorporating encryption, mobile phones and computers can be "subject to the EAR." These obligations extend not only to the physical shipment of goods but also to the transfer of controlled technology or software online and to foreign nationals within the United States—a concept known as a "deemed export."

The EAR further restricts exports based on the end use and end user. The BIS maintains a Military End-User ("MEU") rule, which prohibits or restricts exports of certain items to military end users or for military end uses in certain countries, including China, Russia, and Venezuela. In addition, the BIS Entity List identifies specific foreign parties that are subject to additional licensing requirements due to national security or foreign policy concerns. U.S. exporters must screen transactions to avoid unauthorized dealings with these restricted parties. Violations can result in severe civil and criminal penalties, including multi-million-dollar fines, debarment from government contracting, and imprisonment. Under the Export Control Reform Act of 2018 (*50 U.S.C. § 4801 et seq.*), civil penalties under the EAR can be $374,474 (inflation adjusted) per violation or twice the value of the transaction. Civil penalties under the ITAR can be up to $1,271,078 (inflation adjusted) per violation or twice the value of the transaction, and criminal penalties for both include fines of up to $1 million and 20 years in prison.

[2] Due Diligence

Due diligence in export controls requires a methodical assessment of the target company's products, technologies, customers, internal compliance infrastructure, and historical export activities. The diligence team should begin with a comprehensive understanding of the target's business model and product lines to identify export-controlled components or activities.

Key diligence steps include:

1. **Determine Jurisdiction and Classification**: Identify whether the target's products, software, or technology fall under EAR or ITAR jurisdiction. Request lists of products and services, *e.g.*, software, hardware and consulting services, classification matrices, prior commodity jurisdiction (CJ) determinations, and export licenses. Confirm whether the company has military contracts. Confirm whether the company has self-classified items or obtained BIS classification rulings or DDTC commodity jurisdiction letters. Improper classifications can lead to unauthorized exports and enforcement exposure.
2. **Request and Review Export Control Compliance Policies and Procedures**: Begin by obtaining and reviewing the company's export control compliance manual, ECCN classification protocols, technology control plans (TCPs), employee training records, and licensing procedures. Evaluate whether the company maintains a current, documented export compliance program and policies. Lack of documentation or reliance on informal controls is a notable risk, especially if the target's products, software, or technology are highly controlled and the target exports to high-risk jurisdictions likely subject to a licensing policy.
3. **Evaluate Licensing History and Practices**: Request and review all BIS export licenses, DDTC licenses, Technical Assistance Agreements ("TAAs"), Manufacturing License Agreements ("MLAs"), and related documentation. Review license conditions, expiration dates, and recordkeeping practices. Investigate whether the company has engaged in any unlicensed exports or has pending applications.
4. **Assess Deemed Export Controls**: Evaluate whether the company employs foreign nationals and whether appropriate controls are in place to prevent unauthorized deemed exports (*i.e.*, release of controlled technology to foreign persons in the U.S.). Review internal controls for access to controlled technical data, including physical and electronic barriers and employee access logs.
5. **Examine Screening Protocols**: Determine whether the company screens all parties (end users, consignees, freight forwarders) against the Consolidated Screening List, which includes the BIS Entity List, Denied Persons List, and the DDTC Debarred List. Review screening logs, results, and escalation records.
6. **Review Past Violations or Disclosures**: Ask whether the company has filed any Voluntary Self-Disclosures (VSDs) with BIS or DDTC. Review any prior enforcement actions, warning letters, or communications with regulators. If issues were identified, assess whether appropriate remedial measures were taken.
7. **Assess Third-Party and Supply Chain Risks**: Review diligence procedures for intermediaries, agents, distributors, and overseas manufacturing partners. Determine whether third parties are contractually required to adhere to U.S. export controls laws and whether compliance audits have been conducted.
8. **Export Controls Compliance Clauses in Agreements**: Evaluate sample customer, vendor, contractor and agent agreements to identify whether these agreements have contractual clauses requiring export controls compliance. The presence of export controls compliance clause shifts some (minimal) burden of compliance to the counterparty and can indicate that the company has some awareness of its export controls compliance obligations.

Each document requested in this process reveals critical dimensions of export risk:

- **Compliance manuals** reflect the organizational framework for adhering to export laws.
- **Classification records** reveal whether the company has appropriately scoped its export obligations.
- **Licensing documents** show the volume and nature of controlled exports.
- **Screening and access controls** indicate whether risks are being mitigated in real time.
- **Audit and training records** reflect operational compliance and employee awareness.

The diligence team should synthesize this information and identify items subject to heightened controls (*e.g.*, encryption software, sensitive technology, military items), countries of concern, end-users of concern and any red flags. Material findings may warrant pre-closing remediation, indemnification, strong representations and warranties, or conditioning closing on voluntary disclosure to BIS or DDTC.

§ 11.04 U.S. Customs Regulations

[1] Overview

U.S. Customs regulations govern the lawful importation of goods into the United States and are enforced by U.S. Customs and Border Protection ("CBP"). These laws encompass a wide range of obligations, including accurate tariff classification, proper valuation of merchandise, determination of country of origin, compliance with marking requirements, and adherence to admissibility restrictions such as those concerning products made with forced labor. In the context of corporate transactions, particularly those involving import-intensive businesses, customs compliance is critical to preventing successor liability, avoiding delays or seizures at the border, and preserving favorable duty treatment under preferential trade programs such as free trade agreements.

Importers of record are legally required to exercise "reasonable care" in ensuring that import entries are accurate and complete, as mandated under *19 U.S.C. § 1484*. Reasonable care extends to the provision of correct Harmonized Tariff Schedule of the United States ("HTSUS") codes, accurate valuation including intercompany transfer pricing between related parties, declarations of country of origin for marking and tariff purposes, and verification that goods are not subject to enforcement actions or exclusions (*e.g.*, antidumping and countervailing duties, Section 301 tariffs, or Uyghur Forced Labor Prevention Act ("UFLPA") restrictions).

Penalties for customs violations can be significant. Under *19 U.S.C. § 1592*, civil penalties for negligence, gross negligence, or fraud in customs filings can range from four times the loss of revenue to the domestic value of the imported goods. Moreover, CBP has intensified its enforcement of UFLPA, which imposes a rebuttable presumption that the importation of any goods, wares, articles, and merchandise mined, produced, or manufactured wholly or in part in the Xinjiang Uyghur Autonomous Region of the People's Republic of China, or produced by certain entities, is prohibited by Section 307 of the Tariff Act of 1930 and that such goods, wares, articles, and merchandise are not entitled to entry to the United States.

[2] Due Diligence

Customs due diligence focuses on ensuring that the target company's import practices comply with all applicable legal and regulatory obligations and that the company has effective procedures to mitigate enforcement risks.

1. **Request and Review Customs Compliance Policies and Procedures**: As an initial step, obtain all written customs compliance manuals, standard operating procedures (SOPs), and internal guidance documents. Key policies should address HTS classification, valuation methodologies, country of origin determinations, recordkeeping, sully chain mapping for forced labor and responses to CBP inquiries. Their existence and scope provide insight into whether the target has institutionalized customs compliance or operates reactively.
2. **Review Import Entry Filings and Supporting Documents**: Request a representative sample of past CBP entry filings, including CBP Form 7501, commercial invoices, packing lists, and bills of lading. These records reveal how the company classifies and values imports, which countries are declared as origin, and what duty rates are applied. Review the same in detail to assess consistency and accuracy.
3. **Evaluate Classification and Valuation Practices**: Determine whether the company has documented internal processes for assigning HTSUS codes and whether it relies on CBP binding rulings, internal

classifications or other guidance. Assess whether the company is valuing its imports correctly and adding all assists and other statutory additions to the value declared to CBP. Request documentation on how intercompany pricing is reflected in customs valuations, if there are any related party imports, and whether transfer pricing adjustments are properly disclosed to CBP.

4. **Country of Origin Determination and Marking**: Review how the company determines country of origin for both marking and tariff purposes. Verify whether products are properly labeled and whether substantial transformation analyses or rules of origin under free trade agreements (*e.g.*, USMCA) are accurately applied. Mislabeling or inaccurate origin claims can result in penalties.

5. **Tariff and Antidumping Duty Liability**: Review whether the company's imports are subject to, or may become subject to, significant tariffs or antidumping and countervailing duties as that could affect the valuation of the deal.

6. **Forced Labor Compliance (UFLPA)**: Specifically inquire into whether the company imports any products with raw materials or components sourced from China or high-risk regions. If so, request supply chain due diligence documentation such as supplier certifications, audit reports, and traceability assessments. Determine whether the company has taken steps to comply with UFLPA requirements, including documentation sufficient to rebut the presumption of forced labor for goods tied to Xinjiang.

7. **Audit History and Regulatory Engagement**: Ask whether the company has undergone any Focused Assessments, Customs-Trade Partnership Against Terrorism (C-TPAT) validations, or other CBP audits. Review any notices of action, penalty assessments, prior disclosures, or warning letters issued by CBP. Evaluate the company's responsiveness to findings and whether remedial measures were implemented.

8. **Broker Management and Power of Attorney (POA) Controls**: Request broker agreements and POAs granted to customs brokers and freight forwarders. Determine whether the company audits its brokers or validates that correct information is transmitted to CBP. Improper broker oversight can create liability, as importers are ultimately responsible for the accuracy of customs filings.

9. **Internal Controls and Training**: Evaluate the company's internal training practices for employees involved in logistics and trade compliance. Determine whether customs compliance is part of onboarding or recurring training programs and whether there is a designated customs compliance officer or team.

Key documents to review include:

- **Customs compliance policies**: reveal organizational intent and structure.
- **Entry filings**: show the accuracy of past customs declarations.
- **Broker agreements**: demonstrate oversight mechanisms.
- **Supplier certifications and audit reports**: critical to UFLPA and origin compliance.
- **CBP audit records**: highlight prior issues and the strength of corrective actions.

A thorough customs diligence effort may reveal underpaid duties, misclassified goods, exposure to penalties under UFLPA, and significant tariff and antidumping and countervailing duty liability. Material issues may warrant pre-closing remediation, indemnification, strong representations and warranties, or conditioning closing on the submission of Prior Disclosures to CBP.

§ 11.05 Other Import/Export Laws

[1] U.S. Antiboycott Laws

[a] Overview

U.S. antiboycott laws are designed to prevent U.S. persons from participating in foreign boycotts that the United States does not endorse. These laws are administered by the Office of Antiboycott Compliance ("OAC") within the Bureau of Industry and Security ("BIS") under the Export Administration Regulations ("EAR"), and by the Internal Revenue Service ("IRS") through reporting obligations under the Internal Revenue Code ("IRC"). The antiboycott provisions of the EAR require U.S. persons to report any requests they have received to take certain actions to comply with, further, or support an unsanctioned foreign boycott even if they rejected such request.

The EAR's antiboycott provisions prohibit:

- Refusals or agreements to refuse to do business with or in a boycotted country or with blacklisted companies.
- Discrimination or agreements to discriminate against a U.S. person based on race, religion, sex, or national origin.
- Furnishing information or agreements to furnish information about business relationships with or in a boycotted country or with blacklisted companies.
- Furnishing information or agreements to furnish information about the race, religion, sex, or national origin of a U.S. person.
- Implementation of letters of credit containing prohibited boycott terms or conditions.
- Taking actions with the intent to evade Part 760 of the EAR.

Violations can result in substantial penalties. Civil penalties under the EAR may reach $374,474 (inflation adjusted) per violation or twice the value of the transaction, and criminal penalties include fines up to $1 million and imprisonment up to 20 years. The IRS can also deny foreign tax benefits for failure to file required boycott reports.

[b] Due Diligence

Antiboycott due diligence seeks to uncover any past or ongoing violations, assess internal controls, and evaluate the company's response to boycott-related requests.

1. **Request and Review Antiboycott Compliance Policies and Procedures**: Start by requesting the company's antiboycott compliance manual, employee training records, and internal guidance on reviewing and responding to foreign contracts. Evaluate whether the company educates employees—particularly in legal, finance, and sales—on how to identify and escalate suspect boycott clauses.
2. **Review Customer and Vendor Agreements**: Request a sample of executed international commercial contracts, letters of credit, and bid tenders. Examine these documents for boycott-

related language, such as commitments not to do business with Israel or requests for compliance with laws of boycotting countries. Pay special attention to contracts with entities based in the Middle East or North Africa.

3. **Evaluate Reporting History and Regulatory Engagement**: Ask whether the company has made any required reports to BIS. Review submitted forms and correspondence with regulators. A failure to report known requests is a potential violation.
4. **Assess Third-Party Involvement**: Inquire whether the company relies on freight forwarders or financial institutions in high-risk jurisdictions and whether there are controls to detect antiboycott language in letters of credit or banking instructions.
5. **Training and Internal Awareness**: Evaluate how frequently employees are trained on antiboycott compliance and whether training content is tailored to commercial staff involved in foreign tenders and contracting.

Key documents include:

- **Antiboycott compliance policies**: indicate whether compliance is proactive.
- **Customer contracts and letters of credit**: reveal any embedded boycott risks.
- **Incident logs and escalation records**: indicate operational compliance.
- **Regulatory filings**: demonstrate compliance with mandatory reporting.

[c] U.S. Census Bureau Export Filings

[i] Overview

The U.S. Census Bureau requires exporters to file Electronic Export Information ("EEI") through the Automated Export System ("AES") for certain shipments leaving the United States. EEI filings are mandatory when shipments exceed $2,500 per Schedule B/HTS line item or when an export license is required. These filings are critical to enforcing export control, trade statistics, and customs regulations.

EEI filings must be accurate and timely. Errors can result in penalties under the Foreign Trade Regulations ("FTR"). Civil penalties can reach up to $10,000 per violation for false or misleading filings.

[ii] Due Diligence

EEI due diligence involves ensuring that the target complies with filing obligations and maintains records in accordance with Census and CBP requirements.

1. **Request and Review Export Reporting Policies and Procedures**: Request documentation of EEI-related policies, including filing thresholds, responsibilities for filing (*e.g.*, internal vs. freight forwarder), and record retention procedures. Determine whether internal controls are in place to ensure timely and accurate filings.
2. **Review AES Filing Records**: Request a sample of EEI filings submitted via AES. Evaluate entries for completeness, especially for values, quantities, ECCNs, Schedule B numbers, and license information. Cross-reference with commercial invoices and shipping documents.
3. **Assess Licensing Integration**: Determine whether EEI filings are coordinated with BIS or DDTC licensing, and whether license numbers, license exceptions, and export control classifications are properly reflected in the filings.
4. **Audit History and Error Logs**: Inquire whether the company has received any notices of AES filing errors or has undergone any post-shipment audits. Review any internal or external audits conducted and any corrective actions taken.

5. **Roles and Responsibilities**: Clarify whether the company or its freight forwarder acts as the filer of record and whether Power of Attorney agreements are in place. Improper delegation of filing responsibility may affect accuracy and liability.
6. **Recordkeeping**: Verify that the company retains all EEI submissions and supporting documentation for at least five years, as required by the FTR.

Documents of interest include:

- **Export compliance policies**: foundational for assessing control frameworks.
- **AES filings and shipping documents**: demonstrate compliance history.
- **Licensing data and audit records**: reveal filing accuracy and integration with export control laws.

§ 11.06 U.S. Foreign Corrupt Practices Act (FCPA)

[1] Overview

The U.S. Foreign Corrupt Practices Act ("FCPA"), enacted in 1977 and enforced by both the U.S. Department of Justice ("DOJ") and the U.S. Securities and Exchange Commission ("SEC"), contains two principal provisions: (1) the anti-bribery provisions, which prohibit offering or providing anything of value to foreign officials for the purpose of obtaining or retaining business, and (2) the accounting provisions, which require public companies to maintain accurate books and records and adequate internal controls.

The anti-bribery provisions apply to all (1) U.S. and foreign public companies listed on stock exchanges in the United States ("issuers") and their officers, directors, employees, agents, and stockholders acting on behalf of an issuer; (2) all U.S. persons and businesses ("domestic concerns") and their officers, directors, employees, agents, and stockholders acting on behalf of a domestic concern; and (3) certain persons and entities, other than issuers and domestic concerns, acting while in the territory of the United States. The accounting provisions apply to issuers. Both provisions extend to any non-U.S. subsidiaries of the of the covered entities.

The FCPA's extraterritorial reach, coupled with aggressive enforcement, makes it one of the most significant legal risks in cross-border M&A. Penalties can be significant. Criminal fines for violations of the anti-bribery provisions can reach up to $2 million for companies and $250,000 per violation for individuals and imprisonment for up to five years. Criminal fines for violations of the accounting provisions by corporations and other business entities can be up to $25 million and individuals are subject to a fine of up to $5 million and imprisonment for up to 20 years.

Civil penalties for violations of the anti-bribery provisions for corporations and other business entities can be up to $26,262 (inflation adjusted) per violation. Individuals, including officers, directors, stockholders, and agents of companies, are similarly subject to a civil penalty of up to $26,262 (inflation adjusted) per violation, which may not be paid by their employer or principal. For violations of the accounting provisions in district court actions, the SEC may obtain a civil penalty not to exceed the greater of (a) the gross amount of the pecuniary gain to the defendant as a result of the violations or (b) a specified dollar limitation based on the nature of the violation and potential risk to investors. The SEC may obtain civil penalties both in actions filed in federal court and in administrative proceedings.

Companies are also subject to successor liability for pre-closing FCPA violations committed by an acquired target. Accordingly, comprehensive FCPA due diligence is vital to evaluating enforcement risk and preserving deal value.

[2] Due Diligence

FCPA due diligence seeks to uncover past violations, assess the strength of the target's compliance program, and identify high-risk relationships and geographies. The diligence must include a review of third-party agents, international joint ventures, and other arrangements that create risk under both the anti-bribery and books and records provisions.

1. **Request and Review Anti-Corruption Compliance Policies and Procedures**: Begin by requesting the company's anti-corruption policy, due diligence protocols for third-party intermediaries, internal controls documents, and employee code of conduct, ethics policies and gift and entertainment policies. Evaluate whether the company conducts risk-based assessments and whether compliance policies are tailored to specific markets and risk levels.

2. **Third-Party Intermediary Due Diligence**: Review lists of all third-party agents, consultants, distributors, lobbyists, and local partners etc. used in foreign jurisdictions. Request the due diligence files for each—including background checks, business justifications, contract terms, compensation arrangements, and anti-corruption certifications. Identify any high-risk engagements, such as agents paying a high percentage of contract value or located in high-corruption jurisdictions. Lack of third-party diligence is a major red flag and a common feature of DOJ and SEC enforcement actions.
3. **International Joint Ventures and Affiliates**: Request all joint venture agreements, governance documents, and compliance certifications associated with international partnerships. Assess whether the target exercises sufficient control over the joint venture to ensure FCPA compliance, including implementations of policies and procedures, training, board participation, access to books and records, and audit rights. Determine whether financial controls are aligned with the target's own compliance framework or if the joint venture operates independently in high-risk jurisdictions.
4. **Books and Records, Internal Controls, and Financial Audits**: Evaluate whether the company maintains adequate internal accounting controls to detect and prevent improper payments. Request financial audit reports, internal audit findings, and any whistleblower complaints or internal investigations. Analyze high-risk accounts such as petty cash, marketing expenses, travel and entertainment expenses, commissions, facilitation payments, or charitable donations in sensitive jurisdictions.
5. **Licensing, Permits, and Government Touchpoints**: Identify all interactions with foreign government agencies, including without limitation, customs, tax authorities, land-use authorities, health regulators, or ministries of energy, transportation, or defense. Review procedures for securing permits, licenses, and government contracts. Determine whether these processes are centralized and transparent or conducted by local agents without oversight.
6. **Employee Training and Tone at the Top**: Evaluate the frequency and depth of employee training programs on anti-corruption laws, particularly for sales, finance and government affairs personnel and for employees in high corruption risk jurisdictions. Assess whether senior management communicates a zero-tolerance policy.
7. **Voluntary Disclosures and Government Investigations**: Ask whether the company has ever submitted an FCPA-related voluntary disclosure or been the subject of an inquiry or investigation, whether formal or informal, and whether conducted by a U.S. government entity or local jurisdiction government entity. Review any settlement agreements, monitorships, or independent investigations. Identify follow-up actions and whether remediation has been sustained.

Key documents include:

- **Anti-corruption compliance manuals and third-party onboarding protocols**: important for assessing governance.
- **Third-party contracts and due diligence files**: critical for evaluating indirect bribery risks.
- **Joint venture documents and audit rights**: central to successor liability analysis.
- **Internal audit and whistleblower logs**: highlight internal control effectiveness.
- **Training materials and board updates**: reflect corporate culture and program maturity.

Where risks are identified, such as payments to state-owned enterprise employees, opaque third-party fees, or missing audit rights in joint ventures, the buyer should consider requiring pre-closing remediation, post-closing audits, indemnification rights and strong representations and warranties.

§ 11.07 Conclusion

Export controls, sanctions regulations, customs laws, antiboycott requirements, and anti-corruption obligations are no longer fringe compliance topics in transactional due diligence—they are central to evaluating the viability, risk, and long-term success of any cross-border transaction. As the legal and regulatory landscape continues to globalize and enforcement becomes more aggressive, failing to uncover regulatory red flags during due diligence can result in steep financial penalties, post-closing liability and disruptions, and reputational harm.

This chapter has outlined a comprehensive framework for conducting due diligence across key U.S. international trade and national security regulatory regimes. A common theme throughout each regulatory domain is the foundational importance of assessing the maturity and effectiveness of the target company's compliance program—its policies, training, internal controls, and prior engagement with regulators. Whether assessing sanctions exposure, export licensing, customs valuation, antiboycott adherence, or anti-bribery safeguards, due diligence begins with documentation to assess internal controls.

Critically, the diligence process should not be confined to a checklist. Legal and compliance professionals must tailor their approach to the industry, geography, and risk profile of the target. The presence of third-party intermediaries, operations in high-risk jurisdictions, dealings in sensitive technologies, or significant interactions with foreign governments should all inform a more focused, in-depth diligence effort. When risks are identified, buyers have a suite of strategic options. They may:

- Restructure the deal to exclude problematic business lines or affiliates.
- Negotiate indemnification rights, representations and warranties, and purchase price adjustments.
- Require specific remediation undertakings in the purchase agreement.
- Condition closing on corrective actions or regulatory disclosures.

Post-closing, the importance of compliance integration cannot be overstated. Acquirers should plan for:

- Immediate implementation of their own compliance policies across the acquired entity.
- Conducting post-closing audits of higher-risk areas.
- Onboarding key personnel with compliance responsibilities.
- Reviewing and potentially renegotiating high-risk third-party contracts.

Successful integration is not merely operational—it is cultural. Compliance must be seen not as a back-office obligation but as a driver of value protection and risk mitigation. In today's enforcement climate, robust due diligence is not only a legal necessity, it is a strategic imperative.

1 Due Diligence in Corporate Transactions Chapter 12.syn

Chapter 12 Special Due Diligence Situations

§ 12.01 Securities Offering Disclosures Due Diligence

[1] Introduction

Disclosure due diligence is an essential stage of preparation and review of an issuer's disclosures in both registered and exempt securities offerings. It generally entails:

- Ensuring that all information required to be disclosed in the registration statement and prospectus or in the private placement memorandum is properly disclosed;
- Confirming that information in the prospectus or in the private placement memorandum is accurate and free of misstatements; and
- Gathering and analyzing all relevant information concerning the issuer to ensure that the prospectus or the private placement memorandum does not contain omissions that would render the disclosure misleading.

[2] Purpose of Due Diligence of Securities Disclosures

The due diligence process for disclosure in securities offerings—particularly for the prospectus in registered offerings—is heavily influenced by the securities law liability framework. While perfecting the prospectus (or the PPM) disclosure is the natural objective of due diligence, the process itself—the *conduct* of due diligence that meets certain standards—holds independent legal significance for liability purposes.

One of the primary incentives for due diligence is to establish the so-called "due diligence defense" for all participants in the offering who are eligible to assert it, thereby insulating them from liability even if the prospectus ultimately contains an imperfection. This is because, in many scenarios, an untrue statement or omission of a material fact alone may be sufficient to trigger liability without requiring proof of scienter or reliance.

Although issuers themselves are not eligible to invoke the due diligence defense in key instances (under Section 11 of the Securities Act of 1933 (the "Securities Act") applicable to registered offerings), they nonetheless benefit from the due diligence process. Enhanced disclosures reduce the risk of incomplete or misleading information, minimize potential investor claims to begin with, and protect the issuer's reputation. Moreover, issuers are almost always obligated to indemnify underwriters (or placement agents) against liabilities arising from securities litigation, providing further motivation to ensure the prospectus or PPM disclosure is robust and accurate.

[3] Disclosure-Related Liability Framework in Securities Offerings

[a] Section 11 Liability

Section 11 of the Securities Act provides the primary civil remedy for purchasers of securities in *registered* securities offerings (and does *not* apply to exempt offerings). Under Section 11, participants in the offering are subject to liability if the registration statement, when it became effective:

(i) "contained an untrue statement of a material fact," or

(ii) "omitted to state a material fact required to be stated therein or necessary to make the statements therein not misleading."

The following securities offerings participants face potential Section 11 liability:

- the issuer;
- all underwriters;
- each person who signed the registration statement (which typically includes principal executive officer, principal financial officer, controller, and the majority of directors of the issuer);
- every person who was a director of the issuer at the time of the filing of the registration statement (whether or not such person signed the registration statement); and
- persons named as experts in the registration statement (to the extent of the expertise portion).

Absent special circumstances, a plaintiff need not demonstrate culpability, causation, or reliance: "bad disclosure" alone suffices to raise a claim under Section 11. To counterbalance this strict liability regime, all participants of securities offering other than the issuer are afforded a due diligence defense. The applicable standard varies depending on whether the participant is an expert and whether the disclosure relates to an "expertised" portion of the registration statement.

Generally, a non-expert defendant must demonstrate that it either:

(i) "after reasonable investigation" had "reasonable ground to believe" that the statements in the registration statement "were true and that there was no omission to state a material fact required to be stated therein or necessary to make the statements therein not misleading" with regard to a non-expertised portion of a registration statement or

(ii) had no reasonable grounds to believe, and did not believe, that the expertise portions were "untrue or that there was an omission to state a material fact required to be stated therein or necessary to make the statements therein not misleading, or that such part of the registration statement did not fairly represent the statement of the expert."

Thus, a "reasonable investigation" absolves non-expert participants of liability. Properly conducted due diligence is exactly the type of "reasonable investigation" that serves this purpose.

The issuer itself is not afforded the due diligence defense and is strictly liable under Section 11 for material misstatements or omissions in the registration statement.

[b] Section 12(a)(2) Liability and Reasonable Care Standard

Section 12(a)(2) of the Securities Act creates a private cause of action against any person who offers or sells a security, by "means of a prospectus or oral communication" which includes "an untrue statement of a material fact or omits to state a material fact necessary in order to make the statements, in the light of the circumstances under which they were made, not misleading."

Following *Gustafson v. Alloyd Co.*, courts have interpreted Section 12(a)(2) to apply only to public offerings and not to offerings made in reliance on an exemption from registration (with the exception of offerings in reliance on Regulation A).

Like Section 11, Section 12(a)(2) does not require a plaintiff to prove scienter (intent to deceive). However, defendants can avoid liability by showing that they "did not know, and in the exercise of reasonable care could not have known," of the misstatement or omission. Notably, unlike under Section 11, all defendants, including *issuers*, can avail themselves of the reasonable care defense under Section 12(a)(2).

The "reasonable care" standard is widely regarded as less demanding than the Section 11 due diligence standard. Thus, due diligence sufficient to satisfy Section 11 is typically sufficient to establish a Section 12(a)(2) defense.

[c] Section 10(b) of the Exchange Act and Rule 10b-5

Section 10(b) of the Securities Exchange Act of 1934 (the "Exchange Act") and *Rule 10b-5* promulgated thereunder apply to both registered and exempt offerings. Among other things, they prohibit making any

untrue statements of material fact or omitting a material fact necessary to make the statements made not misleading in connection with the purchase or sale of securities.

Unlike Sections 11 and 12(a)(2), however, *Rule 10b-5* is an anti-fraud provision: to prevail, a plaintiff must establish scienter—that the defendant acted knowingly, deliberately, or recklessly—as well as reliance on the misstatement or omission.

Although *Rule 10b-5* does not expressly provide a due diligence defense, demonstrating that a thorough and reasonable investigation was undertaken can help negate allegations of scienter (by showing that the defendants did not act recklessly or with fraudulent intent), which translates into the viability of the due diligence in private offerings.

[d] Other Securities Law Liabilities and Defenses

Robust due diligence also provides protection against other disclosure-based liabilities under federal and state securities laws, including:

- Section 17(a) of the Securities Act prohibits selling securities through material misstatements or omissions. Sections 17(a)(2) and (3) allow for negligence-based claims (no scienter required), although only the SEC—not private plaintiffs—can bring enforcement actions under Section 17(a).
- Section 15 of the Securities Act, addressing control person liability, provides a defense where the control person had no knowledge or reasonable grounds to believe in the existence of the facts causing liability—a defense that can be established through due diligence.
- Companies may also face disclosure-related liability under securities laws of the states where investors reside, frequently referred to as “blue sky” laws. While certain registered and exempt offerings are preempted from the “blue sky” laws registration requirements, such preemption does not extend to state antifraud statutes. Due diligence defense typically serves as one of the means of addressing “blue sky” laws liability.
- Bespeaks caution doctrine and other defenses that protect forward-looking statements of the issuers made in good faith and exempt such statements from antifraud statutes, also incentivize issuers and participants in the offering to conduct due diligence, as similarly “reasonable investigation” vis-à-vis forward-looking statements would typically establish that the forward-looking statements were made on a good faith basis and are not actionable. The issuer itself can rely on bespeaks caution doctrine and other forward-looking statements defenses.

[e] Liability in Exempt Offerings

In exempt offerings, issuers and other participants conducting due diligence are afforded a greater degree of protection against disclosure failures, but still benefit from due diligence for the purpose of antifraud rules.

Inapplicability of Section 11 and Section 12(a) of the Securities Act means that risks associated with potential disclosure liability for offering participants involved in an unregistered offering are somewhat reduced. Nevertheless, the due diligence undertaken in connection with exempt offerings often closely resembles due diligence in registered offerings, especially in larger offerings involving reputable placement agents. This approach is primarily motivated by *Rule 10b-5* and other federal and state antifraud rules and potential reputational concerns of placement agents.

[f] Due diligence defense

Robust due diligence provides protection against other disclosure-based liabilities under federal and state securities laws, including.

Importantly, while each offering participant will need to establish its “reasonable investigation” defense, in practice, due diligence is not typically performed individually by each director, officer, or underwriter. Instead, the issuer’s counsel’s due diligence investigation—if it satisfies the reasonable investigation

standard—is relied upon to establish the defense for directors and officers (provided they appropriately participate). Similarly, lead underwriter's counsel typically performs diligence sufficient for all underwriters' defense. Such reliance does not obviate participation in due diligence by each offering participant to the extent necessary to establish "reasonable investigation," rather, it means that there are typically two main due diligence teams – issuer's and underwriters', and other offering participants participate in due diligence but do not retain their own legal teams to conduct the due diligence.

It is also noteworthy that each offering participant will be separately assessed as to the satisfaction of the "reasonable investigation" standard, and the bar may vary not just across the different types of securities offering participants (for example, the circumstances in which the investigation conducted by underwriters, directors, or selling stockholders will be differently assessed for each category), but may and likely will be different within the same category, at least, when it comes to directors and officers.

In *Escott v. BarChris Construction Corp*, the court articulated significant principles governing the personal liability of directors and officers in connection with securities offerings. Several key criteria emerged from the court's analysis:

- **Level of Involvement**. The extent of a defendant's involvement with the issuer directly influences the diligence standard applied. A newly appointed director is not held to the same standard as a long-serving director who was actively engaged in the issuer's affairs. Nevertheless, even newly appointed directors bear meaningful responsibility for understanding and reviewing disclosure materials.
- **Sophistication and Position**. The court held that individuals possessing greater professional sophistication or relevant expertise are subject to heightened expectations in their due diligence efforts. In *BarChris*, a director who also served as counsel to the issuer was held to an elevated standard. Although there was no evidence questioning his integrity, the court found that the director's legal background and business experience obligated him to identify certain "red flags" that a less sophisticated director might have overlooked.

The court further emphasized several fundamental points regarding the duties of directors in the due diligence process:

- Directors must personally read and understand the prospectus; a failure to do so is not a defense.
- A recent appointment to the board does not excuse a director's obligations with respect to the offering documents.
- Directors have an affirmative duty to ask questions regarding any portion of the prospectus they do not understand.

In-house and outside counsel should give consideration to the approach to preparation of the board meeting agendas and board minutes, specifically, whether and to what extent such documents should build a record of "reasonable investigation" (good faith, diligence, and involvement) of the board members and "reasonable care" of the issuer. This aspect is especially relevant in connection with registered offerings using shelf registration statements and, therefore, incorporating by reference information from Exchange Act filings of the issuer into the prospectus.

[4] Due Diligence Process

[a] Organization and Scope of Due Diligence

A successful due diligence process involves the collaboration of several teams:

- Issuer and its internal counsel
- Issuer's outside securities counsel
- Lead underwriter's counsel (or placement agent's counsel for exempt offerings)
- Company's accountants

- Various experts, depending on the issuer's business

The lead underwriter is expected to plan and coordinate the due diligence process. Due diligence practices of various banks vary, and the parameters of due diligence for a particular offering are expected to be set at the first due diligence meeting.

The scope of due diligence varies depending on the nature of the issuer's business and industry, the type of securities being offered, the type of form used in connection with the offering (for registered offerings), and the risks perceived by the lead underwriters or placement agents. A due diligence plan is typically discussed during the kickoff meeting and memorialized through diligence request lists and schedules for management presentations, site visits, and third-party verifications.

The due diligence investigation generally encompasses four primary areas:

- **Legal Due Diligence:** Examination of corporate organization, governance, intellectual property, material contracts, regulatory compliance, pending or threatened litigation, environmental matters, and employment issues.
- **Business Due Diligence:** Evaluation of the issuer's operations, competitive positioning, customer base, supply chain, and strategic plans.
- **Financial and Accounting Due Diligence:** Analysis of financial statements, internal controls, accounting policies, tax matters, and any off-balance-sheet arrangements.
- **Management and Governance Due Diligence:** Assessment of management integrity, capabilities, corporate culture, and board oversight.

If companies are eligible to use a short-form registration statement (S-3 or F-3), the timeline of the offering can be extremely condensed, as the registration statement and prospectus incorporate by reference reports filed by the issuer under the Exchange Act. Accordingly, the amount of time to undertake due diligence investigations is drastically reduced compared, for example, to initial public offerings or registered offerings conducted in connection with mergers. However, to our knowledge, no court has held that the shelf takedown format permits a lower standard of due diligence. Accordingly, disclosure controls and procedures and the reviews conducted by the Audit Committee and the board in connection with periodic filings of the issuer become almost "integrated" into the due diligence process in the same manner as filings become a part of the prospectus in such offerings.

[b] Data Room Review and Document Retention

Document review is primarily conducted through virtual data rooms that provide organized access to corporate records, contracts, licenses, litigation documents, and other critical materials. Counsel and underwriters typically maintain internal tracking spreadsheets or memoranda noting:

- Documents reviewed
- Dates of access
- Follow-up questions raised
- Outstanding materials requested

Some firms adopt an "empty box" approach, retaining only a checklist and summaries, while others preserve full copies of reviewed documents for defensive purposes in the event of litigation.

[c] Conduct of Diligence Sessions

A substantial component of the due diligence process is a series of in-person or virtual diligence sessions with the issuer's management and other key personnel. These sessions entail answering pre-distributed questions and are usually structured by topic:

- Financial sessions (with CFO, controller, audit committee, and auditors)
- Legal and regulatory sessions (with general counsel and compliance officers)

- Business operations sessions (with CEO, COO, or divisional heads)
- Technology or intellectual property sessions (with CTO, CIO, or technical staff)
- Specialized sessions addressing environmental, cybersecurity, or sector-specific issues

Each session is designed to elicit a comprehensive understanding of the issuer's risks and to allow for direct questioning and cross-examination by the underwriters' counsel, accounting teams, and underwriters themselves.

In preparing for these sessions, it is customary for participants to review the issuer's publicly available information (e.g., SEC filings, website materials, press releases), third-party news coverage, and any documents already provided through the data room.

[d] Comfort Letters

Comfort letters are a standard component of due diligence in registered offerings and function as one of the key components of the due diligence defense. They are provided by the issuer's independent public accountants and are addressed to the underwriters. Certain unregistered offerings may also entail comfort letters; however, auditors will not issue a comfort letter in an unregistered offering unless the parties receiving the comfort letter make a representation to the auditor that the due diligence process is substantially consistent with a registered offering due diligence (SAS 72 representation letter).

Comfort letters cover, among other things:

- The auditor's independence.
- Compliance of financial statements with applicable accounting requirements in all material respects.
- Agreement of certain financial data in the prospectus with the audited financial statements.
- Various negative assurances, including as to whether anything has come to the auditor's attention during limited procedures that would suggest material misstatements in unaudited interim financials.

While comfort letters do not replace independent diligence by underwriters, they provide a crucial evidentiary component in establishing the due diligence defense with respect to financial disclosures.

[e] Backup Diligence ("Circle-Up")

For factual disclosures that are not subject to auditor comfort letters—such as customer metrics, non-GAAP figures, market rankings, or internal projections—underwriters' (or placement agent's) counsel performs a separate process referred to as "backup" or "circle-up" diligence.

This process involves:

- Circling quantitative and factual assertions in the draft prospectus.
- Requesting backup materials from the issuer supporting each statement (e.g., internal reports, third-party research, press coverage, D&O questionnaires, or analyst reports).
- Comparing source documents to disclosure language to confirm accuracy and eliminate overly pollyannish statements.

If support is lacking or incomplete, the language in the prospectus may be revised to reflect what can be substantiated. Although more manual and document-intensive, this form of diligence plays a critical role in ensuring that the full spectrum of prospectus disclosures—beyond what the auditors cover—is adequately vetted and defensible.

[f] Updating Diligence: Bring-Downs and Closing Certification

The due diligence process does not conclude when the initial prospectus or offering memorandum is filed or finalized. It is customary to conduct bring-down diligence immediately prior to pricing and closing, to confirm that no material changes have occurred since the initial diligence sessions. This includes:

- Updating management interviews
- Reviewing new developments in litigation or regulatory matters
- Obtaining bring-down comfort letters from auditors
- Securing updated management certificates confirming that the disclosure remains accurate

Final certifications, including CFO certificates and officer's certificates, are typically obtained at closing to further document the diligence record and demonstrate continuous monitoring.

[5] Work Product: Negative Assurance (10b-5) Letters and Closing Memoranda

The ultimate goal of the legal due diligence process is often the preparation of a negative assurance letter (commonly referred to as a 10b-5 letter) by issuer's counsel and underwriters' counsel. These letters provide assurances that, based on their due diligence investigation, nothing came to their attention that caused them to believe that the registration statement (or offering memorandum) contains material misstatements or omissions.

Additionally, counsel may prepare internal due diligence memoranda summarizing their findings, listing outstanding risks, and confirming the steps undertaken to support the due diligence defense. Importantly, external due diligence reports are typically not delivered in connection with securities offerings, as such reports may be sought by plaintiffs as evidence.

Another important aspect of attorneys' work product is that attorneys who appear and practice before the SEC have the role of gatekeepers. Failure to withhold or withdraw a negative assurance letter may qualify as willful aiding and abetting securities law violations and entail associated liabilities. The SEC can bring judicial or administrative enforcement actions against attorneys for such failures and regularly exercises its power to do so.

§ 12.02 Conducting Due Diligence in Transactions with Representations and Warranties Insurance

[1] Introduction

Representations and warranties insurance (RWI) has become an important feature of modern mergers and acquisitions, in the United States and globally. This insurance product allows the parties to a transaction to transfer the risk of breaches of representations and warranties from the buyer and the seller to a third party, an insurance carrier. Under an RWI policy, the insurer (also referred to as the RWI carrier) agrees to indemnify the insured parties – typically the buyer and its affiliates in a buy-side policy – for losses arising from breaches of the representations and warranties in the acquisition or merger agreement[1]. In this structure, losses arising from such breaches are covered by the insurer – either as the buyer's sole source of recourse or in combination with limited seller liability – subject to the terms, exclusions, and limits of the RWI policy.

By doing so, RWI alters the economics of indemnification, expedites closings, and simplifies negotiations regarding the content of the representations and warranties and post-closing recourse. However, the increased availability and use of RWI have not diminished the importance of due diligence and detailed disclosure schedules; rather, they have magnified it.

The insurer does not conduct its own exhaustive due diligence review of the target company. Instead, it relies on the buyer's due diligence to determine whether the representations and warranties in the acquisition or merger agreement are supported by an adequate investigation. The insurer's willingness to underwrite unknown risk depends on the perceived rigor and thoroughness of the buyer's due diligence review. Accordingly, due diligence now serves two audiences: the buyer and the insurer. It must provide the buyer with an understanding of the target company and its risk profile while also assuring the insurer that the process was sufficiently thorough to justify and support coverage. This dual purpose requires precision, coordination, and transparency in how transaction counsel plans, executes, and reports on the due diligence process.

[2] How RWI Changes the Due Diligence Landscape

[a] Traditional Role of Due Diligence

Before the widespread adoption of RWI, the primary objective of due diligence was to identify risks that might justify adjustments to the purchase price or specific contractual protections, and to protect the buyer's ability to recover directly from the seller if post-closing losses arose from inaccurate representations or warranties, or from issues or risks identified in advance. The diligence findings informed the drafting of disclosure schedules, indemnification provisions, and closing conditions. In the absence of RWI, the scope of review was largely shaped by the transaction's size, type, and structure; the industry in which the target company operated; and, importantly, the buyer's risk tolerance.

[b] Impact of RWI on Due Diligence

---

[1] RWI policies typically also include coverage for standalone tax indemnities or provide a synthetic tax indemnity. Although tax due diligence is generally conducted by accounting firms, transaction counsel should be cognizant of these provisions and ensure that the client understands how tax due diligence findings interact with RWI coverage.

RWI policies can be structured as either buy-side or sell-side coverage. Although sell-side policies were more common in the early years of the product, the market today is almost entirely dominated by buy-side policies, which are the focus of this discussion.

RWI transforms due diligence from a purely transactional exercise – where indemnification was negotiated exclusively between the buyer and the seller – into part of an underwriting process involving an insurer whose interests overlap – but are not identical – with those of either party.

Although the insurer typically retains legal counsel and receives access to the data room, it does not usually conduct its own independent due diligence or perform a detailed verification of the buyer's review. Instead, the insurer "piggybacks" on the due diligence conducted by the buyer and its advisors. The completeness and accuracy of that review directly affect what the insurer will cover and what exclusions will apply.

Insurers evaluate both process and substance. They assess whether the buyer's team reviewed the appropriate categories of information and subject-matter areas, whether specialists addressed issues within their expertise, and whether the final memorandum provides clear and specific conclusions. A "thin" or poorly supported due diligence record can result in exclusions for entire subject-matter areas.

[3] The Due Diligence Memorandum in the RWI Context

[a] The Importance of Accuracy in RWI Transactions

In the context of a transaction involving RWI, the due diligence memorandum must simultaneously (i) inform the buyer about the target company's operations and risk profile, and (ii) provide the insurer with a credible basis for underwriting coverage. Accuracy is central to this dual purpose and therefore underpins the entire due diligence process.

Because known issues are excluded from RWI coverage, the content of the due diligence memorandum directly affects the scope of available coverage; any issue identified in the memorandum will generally be considered as known to the buyer and, as a result, excluded from coverage under the RWI policy. Counsel must therefore be careful not to gloss over informational gaps or use ambiguous phrasing that might later appear misleading. Vague formulations may seem harmless at the drafting stage but can become critical in the event of a post-closing claim. Ultimately, accuracy serves both audiences: it provides the buyer with a reliable assessment of the target company and enables the insurer to evaluate and stand behind the representations and warranties in the transaction documents.

In addition, as part of the underwriting process, the buyer must sign a No-Claims Declaration – at signing and again at closing in the case of a split sign-and-close transaction, or at closing only in the case of a simultaneous sign-and-close transaction – confirming that it is unaware of any breaches of the representations or warranties contained in the acquisition or merger agreement. Any misstatement, omission, or overgeneralization in the due diligence memorandum can undermine that declaration and jeopardize coverage. For this reason, counsel must strike a careful balance between protecting the client and ensuring factual integrity. The memorandum should disclose material issues clearly and accurately, without exaggeration or minimization, and should articulate the limits of the review when necessary.

Insurers treat accuracy seriously. Even an innocent misstatement can create post-closing complications, especially if it appears inconsistent with the No-Claims Declaration, and may also affect the credibility of counsel in future dealings with insurers and brokers. Clarity and careful wording help prevent those misunderstandings.

[b] "Red-Flag" reporting

In insured transactions, due diligence memoranda are typically prepared in a "red flag only" format, focusing on issues that are material to the transaction – those that could materially affect value or result in post-closing losses. Typical examples include an ongoing government investigation or significant pending litigation, a change-of-control provision that jeopardizes a key revenue stream, or exclusivity or non-compete arrangements that restrict the target company's ability to pursue future growth opportunities. By

contrast, yellow-flag issues generally reflect administrative, operational, or procedural matters that can be remediated, or improvements that can be implemented, post-closing without meaningful financial impact. Examples include a subsidiary that has fallen out of good standing but can be easily reinstated, termination rights in commercial agreements that create inconvenience but not substantial risk to the target company's business, or routine customer and vendor contracts that lack signatures. Such matters are usually omitted from the due diligence memorandum and are more appropriately addressed separately, as part of post-merger integration (PMI) recommendations and planning.

Over-reporting immaterial issues in the due diligence memorandum can create confusion as to which risks are material and warrant focused attention from the insurer and its underwriting team. Conversely, under-reporting runs contrary to the principles discussed above regarding accuracy and may cast doubt on the completeness of the review. The practitioner's challenge is to calibrate materiality appropriately to highlight issues that truly affect value or risk allocation, while avoiding unnecessary noise.

[c] Determining the Scope of Review

[i] Reasonable Scope of Review for the Specific Transaction

In traditional transactions, the scope of the due diligence investigation is tailored to the circumstances – principally the size, type, and structure of the transaction; the industry in which the target company operates; and, important, the buyer's risk tolerance. The buyer's risk tolerance is often influenced by budget constraints and by how it chooses to balance cost against perceived exposure. In RWI-backed transactions, the insurer also has a stake in determining scope. The insurer will only agree to insure unknown risks if the buyer's review reflects what a reasonable acquirer would undertake under comparable circumstances. In practice, this expectation can result in a broader scope or a more granular review than the buyer might otherwise have been willing to pursue.

[ii] Justification of Scope of Review

Reasonableness – not exhaustiveness – is the standard. The insurer does not require the buyer and its advisors to review every single document or investigate immaterial issues. What matters is that the scope of review can be justified as reasonable and defensible in light of the transaction's nature and risk profile. Insurers expect the buyer and its advisors to exercise judgment and to document the rationale for any scoping decisions.

For example, if ninety-five percent of the target company's revenue is derived from ten customer contracts, with the remaining five percent spread among fifty smaller customers, limiting the review to the top ten contracts may be defensible – absent specific reasons to review additional agreements, such as red flags identified through other diligence responses or disclosure schedules (for instance, unusual termination, change-of-control, exclusivity or non-compete provisions). Similarly, if the target company has a large volume of contracts based on a standardized template and confirms that there are no material or substantive deviations among them, the buyer may reasonably justify reviewing only a representative sample, both to confirm consistency and to assess substantive terms.

[iii] Underwriting Areas of Focus

The RWI process typically begins with the insurer issuing a Non-Binding Indication Letter (NBIL), which functions as a preliminary term sheet. The NBIL outlines key business terms, including premium pricing, retention amount, coverage scope, and anticipated exclusions. Importantly, it also identifies the areas where the insurer expects heightened due diligence.

Transaction counsel representing the buyer should review the NBIL early and align the diligence plan accordingly. These focus areas should be examined thoroughly and addressed expressly in the due diligence memorandum. This does not mean that diligence should be limited to those topics; rather, they represent issues likely to receive particular scrutiny from the insurer and its advisors during underwriting. For example, if the NBIL highlights prior M&A activity or intellectual property ownership,

the buyer's counsel should ensure that these areas are analyzed in depth and discussed explicitly in the final due diligence memorandum.

[iv] Clear Statement of the Scope

The due diligence memorandum should state the scope of review clearly and explicitly. This is one of the first items the insurer and its counsel will examine, as the stated scope helps define the boundaries of coverage. The memorandum should specify the categories of documents reviewed and any limitations in scope that are material to understanding the analysis. Where appropriate, counsel should also explain why certain documents or subject matters were not reviewed. A concise, transparent statement of scope strengthens both the credibility of the diligence and the defensibility of the coverage position.

[d] Drafting Best Practices

The following drafting principles should guide the preparation of any due diligence memorandum. While they are fundamental in all transactions, they take on heightened importance in transactions involving RWI, where the memorandum not only informs the buyer but also supports the insurer's underwriting process.

[i] Be specific and quantify risk. Identify the precise nature of each issue, quantify potential exposure where possible, and explain the factual or contractual basis for any conclusion. Avoid "open-ended" risk descriptions when the magnitude can be reasonably approximated. Specificity gives both the client and the insurer confidence in the analysis and supports defensibility of the work product.

[ii] Avoid vague formulations. Generic statements such as "potential liability may exist" or "compliance cannot be confirmed" are unhelpful to both the buyer and the insurer. Replace them with concise, fact-based explanations that clarify what is known, what is unknown, and why. If you have requested additional information or documents from the seller to clarify these issues, this should be included in the memorandum and follow-up will be needed. Such formulations often indicate that the scope or depth of the due diligence may have been insufficient, and the buyer's counsel should consider whether further inquiry is warranted.

[iii] Explain the scope of review. Specify what categories of documents or data were reviewed and why that scope was appropriate. If certain items were not reviewed, clarify why (see Section [c][iv] above). A clear statement of scope helps the insurer understand the context and limitations of the analysis.

[iv] Maintain factual integrity. Describe only what the documents and information support. Do not speculate, infer intent, or draw conclusions that extend beyond the available evidence. Precision in language protects credibility with both the client and the insurer.

[v] Focus on red flags. Distinguish between issues that affect deal value or risk allocation and operational matters that can be addressed post-closing. Over-including minor issues can create confusion during underwriting (see Section [b] above). Quantifying risks can help determine whether they constitute red flags.

[vi] Highlight actionable next steps. Identify any consents, regulatory filings, or remediation steps required before closing. Post-integration recommendations should preferably be kept separate (see Section [b] above).

[e] Coordination with Specialist Teams

RWI magnifies the coordination challenges among specialist teams. Each specialist – such as employment, intellectual property, environmental, real estate, and regulatory counsel – may not fully appreciate how an insurer or its counsel will interpret their findings in the context of a transaction involving RWI.

The transaction counsel should circulate a unified due diligence memorandum template or detailed written guidance at the outset of the review to establish expectations regarding format, language, and level of detail. The drafting best practices set forth above serve as a helpful framework for that purpose.

Specialist teams should also be informed early that the due diligence memorandum will be reviewed not only by the client but also by the insurer and its underwriting counsel. They should understand that their reports form part of the underwriting file. Raising this point at the outset helps avoid overly cautious, ambiguous, or heavily qualified drafting that may complicate underwriting or suggest gaps in diligence.

Finally, transaction counsel should review the specialists' findings before the final memorandum is circulated. The objective is to maintain a cohesive narrative, eliminate inconsistencies across disciplines, and identify any areas that warrant additional review or are likely to result in exclusions from RWI coverage (whether because a specific issue has been identified or because diligence in that area was insufficient) and therefore require separate client discussions. A harmonized and well-edited set of specialist inputs signals to the insurer that the buyer's diligence process was coordinated, rigorous, and reliable.

[4] Interaction Between Due Diligence and Disclosure Schedules in RWI Transactions

Disclosure schedules both contain (i) the exceptions to the representations and warranties in the purchase agreement and (ii) definitions or clarifications that further delineate the scope of certain representations and warranties. Because these schedules are directly intertwined with the representations and warranties that form the basis of RWI coverage, they are reviewed closely by the insurer and its underwriting team.

As in traditional transactions, due diligence and disclosure schedules are interdependent. The buyer's due diligence provides the foundation for evaluating the adequacy of the seller's disclosure schedules, and in turn, the disclosure schedules test the completeness and accuracy of the buyer's due diligence.

Insurers expect disclosure schedules to be prepared thoroughly and with specificity, without applying materiality qualifiers or thresholds. In most underwriting processes, insurers and their counsel will request explicit confirmation during the underwriting call that the disclosure schedules were prepared on that basis. Insurers and their advisors review the disclosure schedules closely and request copies of the final schedules before binding the RWI policy. Their objective is to verify that all known risks have been properly disclosed and that no information disconnect exists between the parties.

A disclosure schedule that introduces unexpected information late in the process or conflicts with prior diligence findings can prompt additional underwriting inquiries, the imposition of new exclusions, or adjustments to coverage limits. Accordingly, careful review of the disclosure schedules by buyer's counsel is essential. Every new disclosure should be analyzed in light of the existing due diligence record. If a disclosure reveals an issue not previously identified, the buyer's counsel should determine whether additional diligence is warranted, by requesting and reviewing supplemental documentation, revisiting specific data-room materials, or consulting with relevant specialists. The due diligence memorandum should then be updated to reflect any new findings, even if the resulting assessment is that the risk remains low or adequately mitigated as such analysis will be important to the insurer's review. Where timing constraints make formal updates impracticable, these matters can be addressed separately outside the due diligence memorandum; however, the buyer's counsel should anticipate insurer questions regarding how the new information was evaluated and documented.

[5] The Underwriting Call: Defending the Due Diligence Process

A few days before signing – typically within three days of the anticipated execution date, an underwriting call is organized with the insurer. The underwriting call is the insurer's opportunity to test the adequacy and thoroughness of the buyer's due diligence. Participants usually include the RWI broker; the insurer and its counsel; the buyer's deal team and the relevant specialist attorneys; any other advisors of the buyer who prepared due diligence materials (for example, financial and tax advisors); and key business representatives of the buyer. The insurer circulates an agenda in advance listing topic-specific questions.

[a] Preparation of the Underwriting Call

Preparation is critical. The buyer's corporate transactional counsel should:

- Review the agenda carefully and assign each question to the appropriate team member (including outside tax or financial advisors, and client representatives for business topics or negotiation history).
- Hold an internal pre-call to align on facts, scope, and conclusions and to confirm who will speak to each item.
- Ensure coverage for every agenda item. Each assigned participant should confirm they can address their topic; if any uncertainty remains, identify and resolve it before the underwriting call.

[b] Participation in the Underwriting Call

During the underwriting call, the participants will go through the various questions listed on the agenda. The tone should be factual, measured, and confident. Insurers are not adversaries; their objective is to understand whether the buyer investigated key risk areas with sufficient depth and rigor. Practitioners should avoid alarmist or speculative phrasing. Rather than "there could be liability," describe findings with specificity and context (for example: "the issue has been identified; corrective measures are in progress; potential exposure is approximately $___ based on ___.").

The approach mirrors the due diligence memorandum: accuracy and clarity are paramount. Present facts supported by the review, explain the analysis and reasoning, and note any mitigation underway or planned. A well-managed underwriting call reinforces the insurer's confidence in the diligence process and can directly influence the scope of final coverage.

[c] Follow-Ups after the Underwriting Call

Post-underwriting call questions are common. The buyer's counsel should coordinate promptly with the seller and relevant specialists to provide complete responses, as these inquiries typically relate to due diligence topics or clarifications arising from the discussion.

[6] Post-Signing/Closing Due Diligence and Conditional Exclusions

[a] Post-Signing Due Diligence

In transactions where a significant period elapses between signing and closing, or where new information arises that may affect the accuracy of the representations and warranties, the buyer is generally expected by the insurer to update its due diligence. This follow-up diligence serves two purposes: to confirm that no material changes have occurred in the target company's condition since signing, and to satisfy the insurer that the representations and warranties remain accurate as of closing.

[b] Bring-Down Call

Shortly before closing – typically within a few days, the insurer will conduct a "bring-down call" to confirm that the buyer's due diligence findings remain accurate and that no new issues have arisen since signing. The bring-down call functions as a condensed underwriting call focused on developments during the interim period. The insurer and its counsel will ask targeted questions about any additional due diligence conducted post-signing, changes in the target company's business, or updates to the disclosure schedules.

The buyer's counsel should prepare for this call in the same manner as for the initial underwriting call: by coordinating with the client and relevant specialists, verifying whether any new diligence or material developments occurred, and ensuring that any such developments are accurately described and documented. If additional due diligence was performed, the relevant materials should be provided to the insurer in advance and the buyer's counsel should summarize its scope and findings to facilitate and expedite the insurer's review.

A clear and consistent update during the bring-down call reinforces the insurer's confidence and supports the buyer's representation in the No-Claims Declaration executed at closing.

[c] Exclusions Conditional upon Additional Due Diligence

In some cases, insurers may require additional targeted diligence after signing – or even after closing – on areas they deem insufficiently reviewed during the due diligence process. These situations typically result in conditional exclusions in the RWI policy. Conditional exclusions carve out specific subject matters from coverage unless the buyer completes further diligence within a specified period, often before closing or within thirty to sixty days post-closing, as applicable. If the additional due diligence confirms no material issues, the exclusion may be lifted; however, any issue identified during that review will be treated as a known matter and excluded from coverage. While not ideal, conditional exclusions can provide a practical mechanism to allow the transaction to proceed to signing or closing when time constraints or limited access to information would otherwise delay execution.

[7] Information Sharing and Non-Reliance Letters

All due diligence materials, including, memoranda, specialist reports, related correspondence, and any internal reports prepared internally by the buyer, must be made available to the insurer and its counsel as part of the underwriting process. Insurers rely on these materials to assess the scope and quality of the buyer's investigation and to finalize coverage decisions.

Because the insurer and its counsel are not clients of the buyer's advisors, the materials are shared on a non-reliance basis. The buyer's counsel, as well as other external advisors such as tax or accounting firms, will prepare a non-reliance letter for execution by the insurer. This letter confirms that the insurer may review the materials they prepared but may not rely on them for any purpose, thereby protecting the advisors from exposure to third-party liability.

Each firm's process for issuing non-reliance letters may differ, but these letters generally require internal review or approval (for example, through an opinion or risk-management committee). It is therefore critical to anticipate this requirement early in the deal timeline to avoid delays. Coordination among counsel, brokers, and the insurer is key to ensuring that all necessary non-reliance letters are executed in a timely fashion.

Taken together, these practices enable transaction counsel to conduct due diligence that not only informs the buyer's decision-making but also withstands insurer scrutiny, ensuring that RWI serves its intended function as a tool for efficient, well-managed risk transfer.