CONDUCTING PRIVACY AND CYBERSECURITY DUE DILIGENCE IN M&A

March 29, 2022

Presented by

Mary Alexander Myers, Partner,
Jones Day

WHY PERFORM DUE DILIGENCE?

- Due diligence is an essential part of the corporate transaction cycle, and critical to the parties' negotiation of value and risk
- Due diligence by buyer is also mandated by various laws, including certain data security laws applicable to certain regulated sectors
- Our goal is to protect and inform the client about cyber risks (security, privacy and data issues)
  - Evaluate and quantify legal and business risk related to cyber
- You also learn the ways other companies manage cyber and privacy compliance and risk

RISKS AND POTENTIAL LIABILITIES

- Technology and data create significant risks and potential liabilities
  - Increased vulnerability to cybersecurity risks
  - Need to reconcile new data and technology assets with legacy data and systems
  - Increased data privacy concerns and liability from greater collection, analysis, and use of data
  - Potential misuse of a data on a larger scale
    - E.g., Cambridge Analytica improperly harvested data on 87 million Facebook users without consent

RISKS AND POTENTIAL LIABILITIES

- Evolving legal landscape creates increased litigation and enforcement risk
  - New regulatory requirements to address cybersecurity and data privacy
    - SEC requires disclosure of material cyber risks
    - California Consumer Privacy Act (CCPA) and other state laws grants new data rights
  - More tools for individual litigants
    - CCPA grants private right of action and statutory damages
  - Increased penalties
    - EU General Data Protection Regulation (GDPR) permits fines up to 2-4% of global revenue

YOUR ROLE AS A PRIVACY AND SECURITY ATTORNEY

- Your role in the team is to add value to the transaction by:
  - Identifying those areas of privacy and information security legal and business risks relating to on-premises information technology, data assets, and use of third party technology providers
  - Advise on structuring of transaction to enhance financial return and reduce/manage risk related to these issues
  - Using skills to shepherd the diligence review, prioritize issues, and facilitate the transaction
  - Working as a member of a team that includes the client and other specialists (IT, InfoSec, Risk, HR, Compliance, Procurement, Vendor Management, etc.)
  - Facilitating the consummation of a beneficial transaction for the client

THREE MAJOR PHASES IN SUPPORTING TRANSACTIONS

DD

- Assessing Cyber and Data Privacy Risks During Due Diligence

PA

- Addressing Compliance and Allocation of Cyber Losses and Liabilities in the Purchase Agreement

TSA

- Identifying and Advising on Cyber Risks and Privacy Issues Post-Closing

RISK ASSESSMENT THROUGH DUE DILIGENCE

- Scope of due diligence depends on privacy and information security posture of the target at the outset:
  - What data/IT assets does the target have?
  - Hos critical are these assets to the target's operations or revenue?
  - How does the target manage its data and IT assets?
  - What is the likely cost impact of a cyber incident or privacy?
  - What is the legal liability risk in terms of noncompliance or legal claims?
  - Is the target dependent on third parties for data and IT?
  - What laws apply? CCPA? GDPR? HIPAA? FCRA?

DUE DILIGENCE GOALS – KEY QUESTIONS TO CONSIDER (1)

- Are there vulnerabilities the client may be buying unwittingly?
- Is the client buying a company with undisclosed data breaches or IP/data losses?
- Is the target managing cyber risks effectively and in a manner consistent with industry standards (*i.e.*, is the target likely to even know if it has been compromised)?
- Is the target aware of and effectively managing cyber and privacy risks presented by its major third party providers and business partners?
- Is the target aware of its legal privacy and data security obligations, and is it adequately addressing these obligations as part of its compliance program?
- Do we have enough information to advise the client on how cyber issues could impact the deal, in terms of value, transition and integration, and post-closing risk management?

DUE DILIGENCE GOALS – KEY QUESTIONS TO CONSIDER (2)

- Has the target reported any prior breaches, and provided all relevant information on the status and remediation of each breach?
- Has the target provided cyber risk assessments and audits?
- Is the target subject to breach litigation, agency investigation, or enforcement action, and has it provided all relevant information concerning such matters to evaluate status and materiality?
- Does the target have a privacy compliance program that is compliant with applicable laws (i.e., CCPA, GDPR)?
- Is the target compliance with industry standards like NIST, ISO, and PCI-DSS?

DUE DILIGENCE APPROACHES – PROCESS

- Is the DD checklist complete on cybersecurity and privacy issues?
- Should there be a separate information security/technical DD tracker?
- Is a technical assessment of target's systems/end points required?
- Has the client's infosec team reviewed the target's internal and external information security assessments or certifications?
- Do we need to interview key personnel in charge of information security technology, information management, and privacy compliance (likely yes)?
- Has the target provided all relevant documents evidencing its information security and data privacy compliance and risk management, including third party risk management?

LEGAL CONSIDERATIONS FOR DUE DILIGENCE (1)

- US has no single comprehensive federal privacy and data security law
- Fragmented and dynamic patchwork of:
  - Federal laws and regulations
  - State laws (most notably California, Virginia, Colorado, Massachusetts)
  - Government agency guidelines
  - Industry self-regulatory group guidelines
- Different regulations will apply for cross-border data transfers
- Consult other counsel (e.g., in the EU if GDPR is implicated); but ask corporate team before involving more lawyers
- International data protection and cyber diligence will be more complicated and exacting, so map this early

LEGAL CONSIDERATIONS FOR DUE DILIGENCE (2)

- **Material state laws and regulations**
  - Data breach notification laws
  - Health information protection laws
  - Financial information protection laws
  - Personal information protection program laws
  - Privacy notice requirements
  - Consumer PI collection restriction laws
  - Anti-spam laws
  - Consumer marketing laws

NEGOTIATION OF RISKS IN THE AGREEMENT

- A number of ways to cover infosec and cyber risk in deal documentation
- Price: Incorporating risks in the valuation of the target vs. negotiating remedies in the purchase agreement
- Specific provisions covering scope of “known” vulnerabilities and related post-closing remedies
- General representations and warranties regarding the target’s compliance with its privacy, data protection and security policies and applicable law
- Limitations of indemnification, such as applicability of the indemnity cap or basket to specific or general cyber risks
- Interim Covenants: no real market approach, rarely will a target agree to covenants concerning pre-closing cyber security remediation/ disclosure
- Conditions to Close: where cyber due diligence is continuing after signing or a significant issue has been identified pre-signing, consider termination right under certain circumstances (“MAE” or “Material Cyber Adverse Effect”)

UNDERSTANDING POST-CLOSING RISKS

- Privacy and data security is often relevant to transition services—best to treat it similar to an outsourcing arrangement
- Should target commit to maintaining compliance and, where relevant, assist buyer in maintaining compliance with data privacy and security laws during transition?
- Transition services agreement should contain relevant provisions concerning data privacy and security, in addition to confidentiality
- Is there a need to address cross-border data transfer issues, or foreign legal requirements?
- Are there special known/unknown cyber risks that need to be considered during integration/migration?

THE BEST APPROACH IS AN INTEGRATED APPROACH

- A brave new cyber, privacy and infosec world – threat landscape growing exponentially
- M&A transactions need to have cyber risk on radar for all aspects of transaction
  - Due Diligence
  - Risk Assessment
  - Contract Negotiation
  - Discussion Amongst Principals etc.
  - Post-Close Transition and Integration
- Deal team needs to be aware from outset of core concerns, due diligence items and possible contract approaches
- An integrated due diligence approach that focuses early on key risks that impact value profile, risk profile, transition, and integration activities and business requirements

- *Any presentation by a Jones Day lawyer or employee should not be considered or construed as legal advice on any individual matter or circumstance. The contents of this document are intended for general information purposes only and may not be quoted or referred to in any other presentation, publication or proceeding without the prior written consent of Jones Day, which may be given or withheld at Jones Day's discretion. The distribution of this presentation or its content is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of Jones Day.*