M&A Insights: Representation and Warranty Insurance Trends, Efforts Standards, and Managing Cybersecurity and Privacy Risks in M&A

December 1, 2022

GIBSON DUNN

RWI Policy Exclusions – Interim Breach

In a transaction with a staggered sign-and-close, most policies historically included an exclusion for losses arising from an "Interim Breach"

- An "interim breach" is a breach where:
  - The facts and circumstances that caused the breach first occurred between signing and closing (the "interim period"); and
  - A member of buyer's deal team obtained actual knowledge of the breach during the interim period
- In practice, interim breaches are rare, given that:
  - even if a breach manifests itself during the interim period, often times components of the breach began pre-signing; and
  - sellers are commonly only required to notify the buyer of a breach post-signing that would give rise to a failure of the buyer's closing condition (often tied to a material adverse effect)
- The reps most commonly implicated by the interim breach exclusion include:
  - Representations regarding customer and supplier relationships
  - Condition of assets (in connection with a casualty event during the interim period)
  - Litigation

Interim Breach Coverage

- In the third quarter of 2022, Aon introduced an excess insurance policy that specifically covers interim breaches
- Market forces have led additional insurance markets to begin offering interim breach coverage as part of both primary and excess policies
- Regardless of whether included in a primary or excess policy, currently interim breach coverage may be available in the following circumstances:
  - An interim period between signing and closing of 60 days or less (with the ability to extend on a case-by-case basis)
  - Deal value of ~$750 million or less (thought interim breach coverage for larger deals may be available in certain circumstances)
- Where interim breach coverage is offered, there is commonly an exclusion for interim breaches that would give rise to a buyer termination right (e.g., a breach that gives rise to a material adverse effect)

The Efforts "Hierarchy": Where Are We Today?

- In practice, lawyers and deal professionals consider there to be a "hierarchy" of efforts standards:
  - "Best efforts" – highest standard
  - "Reasonable best efforts", "reasonable efforts", "commercially reasonable efforts", "good faith efforts"
- Courts do not necessarily draw the same distinctions and case law differs across jurisdictions:
  - In Delaware, courts have interpreted "best efforts" to be on par with "commercially reasonable efforts" and have utilized a "one size fits all" approach to the various reasonableness standards
  - In applying these standards, Delaware courts have consistently considered whether parties had reasonable grounds to take the actions they did and whether they sought to address problems with counterparties
  - In other U.S. jurisdictions (e.g., New York, California), courts have acknowledged that a party may also consider its own economic or other interests in complying with efforts obligations
  - UK courts have drawn distinctions between "best endeavors" and "reasonable endeavors" and where "all" is used to modify the efforts standard
- Generally recognized that the application of these standards is largely dependent on specific facts at hand
- In contexts other than M&A (e.g., real estate), efforts standards may have specific meanings in those narrow circumstances

Practical Implications of Efforts Standards in M&A

- **Know what interpretation you're working with**. Understand courts' interpretation of standards under the governing law of the contract.
- **Use definitions**. Consider using definitions of "Best Efforts", "Commercially Reasonable Efforts" or other efforts standards to provide clarity.
- **Be wary of conflicting standards.** Consider using same efforts standard uniformly throughout an agreement and clearly specify ways in which the obligations might differ.
- **Design parameters around obligations**. In lieu of or in addition to efforts standards, specify actions or inactions considered "reasonable" or place specific limitations on obligations.
  - Consider use of materiality thresholds for both obligations and limitations.
  - Consider specifying how the "reasonableness" determination is to be made and by whom.
  - This approach is often taken on antitrust covenants, interim operating covenants, and earnout obligations.
- **Ensure compliance with standards**. Where efforts standards are used, actively keep counterparties updated on compliance with efforts obligations and coordinate to jointly solve problems that arise. Keep regular documentation on these activities.

Cybersecurity and Privacy Risks

- Cyber concerns are pervasive, and privacy regulation is ever-changing. Potential for liability and reputational exposure is significant.
  - There are lots of examples of messy situations in which a buyer has acquired a target's problems.
    - Ex: Verizon, Yahoo have paid $4.48 billion deal following cyber attacks
    - Ex: Industrials and TMT accounted for 57% of M&A dollar volume in 2021

- Transactions with cross-border aspects raise complex issues, because of the need to consider numerous regulatory regimes.

Targeted
Diligence Process

- Depends on sector, size, consumer focus, international reach, and nature and extent of data collected and used.
- Importance of working with internal teams, and using external experts.
- Critical to understand latest trends in regulatory developments and enforcement, U.S. and globally, particularly given data proliferation and accessibility across jurisdictions.
- Think about orientation in deal and timeframe.
  - Importance of having checklists ready
  - But also going beyond and digging deeply, if deal considerations warrant

Penalties & Risks Highlights

- New state comprehensive privacy laws (e.g., CPRA regulatory penalties; up to $7,500 per each intentional violation (or $2,500 for unintentional violation)).
- CPRA private action in the event of a data breach; statutory damages of up to $750 per consumer per incident.
- TCPA, CAN-SPAM, BIPA class action lawsuits; statutory damages.
- HIPAA and COPPA penalties of up to $50,000 and $49,792 per violation, respectively.
- Data breach lawsuits
- Regulator investigations (increased regulatory scrutiny related to cybersecurity and privacy).

Diligence Red Flags

SPECIFIC RED FLAGS	
• Lack of awareness of applicability of state comprehensive privacy laws (e.g., CCPA/CPRA), and requirements and limitation of exemptions (e.g., B2B / employment)	• Lack of valid consent / disclosure for collection of sensitive information
• Insufficient processes to respond to consumer requests, required contract provisions, disclosure requirements	• Insufficient safeguards to protect personal information and company network
• Lack of awareness of applicability and requirements of sector-specific privacy and security laws (e.g., HIPAA, COPPA, BIPA, CAN-SPAM, TCPA, FCRA, GLBA, etc.)	• Lack of security policies or mere placeholder policies; insufficient incident preparedness, business continuity / disaster recovery plans, and vendor management
• Processing of sensitive data (e.g., health data, biometrics) and/or vulnerable data subjects (e.g., children)	• Breach history, issues with response times, security policies not addressing notification requirements (including deadlines)
• Varying levels of online policy development: no policy, outdated policy, only online policy, or online policies do not match data collection and processing practices	• Past or ongoing claims / investigations

Integrating the Diligence

- Post-closing remediation
  - Materiality and priorities
  - Identification of costs and resources needed
  - Consideration of post-closing governance – data privacy and IT experts
  - Integration of the target's privacy and cyber practices into the buyer's global organization
  - Data sharing issues between target and buyer, particularly in certain jurisdictions (e.g., California, EU)

- Management of specific events
  - Potential cyber incident and/or investigation/claims
  - Impact on the transaction and/or on the business

Common Deal Issues and Trends

- Increasing focus on cyber and privacy related diligence
  - Expanded use of internal and external specialists
  - Development of toolkits
  - Early commencement of review process
  - Managing tensions between buyer and seller regarding scope of diligence exercise
- Increasing focus on cyber and privacy related deal documentation
  - Expanded representations
  - Operating covenants and covenants regarding access to information
  - Indemnification coverage
  - Role of representation and warranty insurance and cyber insurance
- Post-acquisition planning and integration


GIBSON DUNN