Don't Ignore Privacy and Data Security: Pre-Deal and Negotiation Considerations for Buyers in Merger and Acquisition Transactions

11/21/2017

Almost all parties are required to exchange personal data as part of a merger and acquisition transaction. With data breaches on the rise, any buyer in a M&A transaction cannot afford to ignore privacy and data security concerns. Nor should these issues be avoided to deal with post-closing. Although not exhaustive, below are some essential elements that a buyer should consider in any M&A transaction:

Organization Is Key

Organization and strategy are essential when it comes to privacy and data security issues in merger and acquisition transactions. Although ideal security may be difficult to achieve, it is dangerous to assume without verification that a target company maintains privacy and data security compliance. In delving into a M&A transaction, a buyer should carefully consider:

- What is the goal of the merger or acquisition?
- How does that account for privacy and security issues?

Before Getting Started

Before engaging in any due diligence review, the parties should ensure appropriate security measures been implemented for the transaction process. From a buyer's perspective, performance of the due diligence review may expose the parties to breach risks, as confidential information is shared with third parties. The buyer and seller should both be in agreement with utilizing confidentiality agreements with service providers , and properly scrutinizing any third party vendor data room provider's security and liability through typical vendor management procedures.

Due Diligence Review

Privacy and data security due diligence should enable a buyer to understand the target company's rights and obligations regarding personal data, the structure of its information security program and a history of security incidents to determine whether the target conforms to a buyer's risk appetite and is an appropriate fit for acquisition. A buyer should conduct a thorough analysis of any target company's privacy and information security program to determine how personal information is handled throughout the data life cycle. Among the standard tools for this review include thorough and relevant questionnaires

to a target, audits, assessments, relevant agreements, current policies, and information regarding past infractions, incidents or complaints. The list below of review considerations is not intended to be complete.

Privacy Obligations

A buyer should confirm that a target's policies, notices and contractual obligations comply with applicable law and identify any limitations that may restrict a transfer or a buyer's subsequent use of the personal information. A buyer should:

- Complete an assessment of a target's public statements and any online media or mobile applications;
- Inventory the type of information that is collected, how such information is used and with whom it is shared;
- Review all contractual data transfer limitations or obligations; and
- Confirm that these policies and obligations comply with legal standards and standard industry practices.

The Federal Trade Commission considers statements made to consumers in privacy notices and policies to be legally enforceable promises and a failure to comply with such promises could result in a FTC enforcement action under Section 5 of the FTC Act. The FTC has also established that affirmative consent is required when there is a material change in a privacy policy that impacts previously collected personal information. Therefore, in examining a privacy notice or policy, a buyer should investigate whether:

- A target's privacy policy contains provisions regarding a transfer of assets;
- Any disconnect exists between a target's and a buyer's respective notices and policies;
- Any additional steps, such as affirmative consent or re-scoping the intended use of the data, may be required for the buyer to utilize the target's personal information as intended; and
- Any new jurisdictional requirements or industry-specific regulation may impact the subsequent use of the personal information by a buyer once the transfer is complete.

Vendor Management

Consideration should also be given to an analysis of any outsourced functions and consider whether the target has an adequate vendor management program. In evaluating a target's vendor management, a buyer should:

- Analyze whether the vendor's security practices and policies were appropriately vetted prior to engagement;
- Collect a completed due diligence questionnaire;
- Collect the vendor's latest audit or other security assessment;
- Review the relevant agreements between target and vendor to ensure appropriate contractual protections exists in the business relationship, including security controls, service levels, indemnification, any limitation of liability and termination rights; and
- Confirm ongoing monitoring has been performed on the vendor services to ensure the most current legal requirements and other applicable regulatory or industry standards are included as part of the vendor management program.

Governance and Related Issues

It is important to understand the framework involved in managing data assets. An inventory of data assets is also an important part of a due diligence review for a buyer. Some targets may provide a data map or other organizational chart. Regardless of format, identifying the systems on which data is stored, the employees or other parties who may have access to it, the related security and governance measures should be reviewed in any M&A transaction. Some factors to investigate include:

- Where is personal information stored?
- What systems are used to access the personal information?

- Who has access to personal information? Is there more than one touchpoint?
- What is the target's data retention policy?
- What is the target's data destruction policy?
- Is in encryption utilized by target? If so, when and using what standards?
- Does the target have remote management or bring-your-own-device policies?

Security Controls

One of the most important reviews of any due diligence analysis should focus on security controls. Understanding any vulnerabilities of a target's security is critical to evaluating the risk profile of a target. In assessing a target's security program, a buyer should, at minimum, review a target's policies, ongoing assessments and any incidents that could expose a buyer to potential liability.

A buyer should expect to see a holistic security program in place which addresses physical, administrative and technical safeguards. For a target's physical environment, a buyer should obtain guidelines regarding security and access to offices, servers and data centers. From an administrative standpoint, a buyer should review all employment security policies, including the use of background checks and other information gathered during the hiring process.

Much emphasis is placed on technical safeguards for privacy and data security and a buyer's review should appropriately reflect this. An examination of a target's security system and readiness should include:

- What policies are in place? (Including, without limitation business continuity, disaster recovery, incident response, etc.)
- What controls exist on systems where data is stored?
- What internal and external audits or risk assessments or other testing are conducted and how regularly?
- Is the target's system certified to any industry standard?

A buyer should also be aware of any past incidents or other risk it may be acquiring. As part of the due diligence review, a buyer should inquire as to:

- Any past suspected or actual data breaches or other security incidents or regulatory inquiry or ongoing monitoring;
- How a target has previously responded to such breach or incident;
- Has a target issued notice to consumers in relation to such breach or incident;
- Is the target the subject of any pending complaints, litigation, documented breaches or security incidents, regulatory inquiries or monitoring, or fines or sanctions;
- How a target has tracked consumer complaints
- How a target has addressed remediation from any previous audit

Other Considerations

In assessing a target's privacy and data security measures, there are additional practices a buyer may want to consider in evaluating a target, such as:

- Is there a chief data security or privacy officer to oversee proper data management?
- Does the target engage in regular security awareness training for its employees or other representatives? What training materials are used?
- Does the target maintain cyber insurance?

Deal Negotiation Considerations

As with any risk-related issue in any merger or acquisition transaction, privacy and data security issues should be carefully negotiated and addressed in an initial agreement. During negotiation, a buyer should have a clear understanding of:

- What personal information is collected, how it is collected and used by the target;
- Whether the collection and storage of any personal information triggers additional regulatory oversight and increases related risk;
- The volume and value placed on the personal information as an asset in the transaction;
- The applicable laws and industry standards relevant to the personal information;
- The history and current status of the target's compliance program, including any actual or suspected security incidents or program infractions; and
- Relevant contractual obligations.

A key component of any purchase agreement is the risk allocation as expressed through the seller's representations and warranties. After all, a buyer may be assuming a target's past liabilities. Although a buyer's preferred position would be to make them as broad as possible, at minimum a buyer should not accept "qualifiers" on representations and warranties from a seller. These representations and warranties should address, among other items, privacy and security policies and procedures, compliance with laws and regulations and any known incidents. For example, a target's representations and warranties should include the following:

- Seller has not been required to issue, and has not issued, any notifications under any law relating to the actual or suspected unauthorized access or acquisition of personally identifiable information.
- Seller has not undergone any audit or regulatory inquiry from any governmental authority with respect to privacy and/or data security of personally identifiable information and is not subject to any current inquiry from any governmental authority (including complaints from any individuals provided to such governmental authority) regarding same.
- Seller is in compliance with all applicable requirements under law and industry standards (including but not limited to Payment Card Industry standards), as well as regulatory guidance relating to personally identifiable information and data security.
- Seller has obtained appropriate consents from all providers of individually identifiable information.

Also, if a security breach is discovered by disclosure in a schedule to the purchase agreement, a buyer should demand a seller work to remove as many violations or issues as possible from the schedule prior to execution of the agreement. Any issues identified should be addressed and a failure to do so may expose a buyer to lawsuits, regulatory oversight or fines or negative reputational impact. Finally, a buyer should also push for any privacy and data security representations and warranties to be treated as fundamental and excluded from any limitations on survival or liability. A buyer may also consider a separate privacy and data security-specific indemnity.

While no system or procedure is 100% foolproof, it is important to be thorough in understanding privacy and data security for any transaction – from the start-up to IPO to a sale or merger. As markets and products evolve, it is critical to remain proactive in understanding the related risks and liability privacy and data security pose in today's world.