Caveat Emptor – Increased Regulatory Scrutiny of Consumer Privacy and Data Security in M&A

Merger and acquisition (M&A") agreements frequently contain no privacy or data security representations and warranties, or only a short form representation and warranty that is not appropriately customized for a particular transaction. This approach occurs especially in situations where neither the acquirer nor the target are ecommerce businesses, retailers or in regulated industries such as financial services, health care or services targeted to children. Buyers should think twice about giving short shrift to these issues in other acquisitions, however, because if a company conducts even a minimum amount of business with customers on-line or via mobile devices, it may be subject to privacy and data security laws.

The failure to obtain adequate privacy and data security representations and warranties from the seller could expose a buyer to significant liability and integration problems. This is particularly true if the proposed transaction is structured as a merger or stock purchase, where the buyer assumes the seller's past liabilities, including liabilities for privacy and data security compliance issues.

1. Increased Regulatory Scrutiny of M&A Transactions

Government agencies and regulatory bodies are reviewing privacy and data security issues in M&A transactions with increased scrutiny. For example, when Facebook acquired WhatsApp in February 2014, the US Federal Trade Commission ("FTC") warned both Facebook and WhatsApp that the parties' failure to abide by WhatsApp's privacy notice would constitute a deceptive act under the FTC Act. European data protection authorities also stated that if Facebook used WhatsApp's user data it would violate numerous European data protection and privacy laws.

The FTC also closely scrutinized Barnes & Noble's acquisition of Border's customer database. Barnes & Noble acquired Border's customer database which contained over 45 million customers' names, email addresses and purchase history from Border's bankruptcy auction. Border's privacy notice stated Barnes & Noble would not share its customers' "personal information" without their consent. The Consumer Privacy Ombudsman appointed by the bankruptcy court specified that Barnes & Noble must obtain opt-in consent from each customer before using the customer's "personal information." The FTC also weighed in on the matter and stated that any transfer of "personal information" in connection with the bankruptcy may only take place with customer's opt-in consent or with significant restrictions on the transfer and use of the "personal information."

2. Standard Privacy and Data Security Representations and Warranties

When a M&A agreement contains a privacy and data security representation and warranty, it typically only requires a target company to warrant that it has: (a) operated its business at all times in compliance with all applicable privacy and data security laws; (b) complied with its corporate polices applicable to data privacy, data security and "personal information" at all times; and (c) not experienced any incident in which "personal information" or other sensitive data was or may have been stolen or improperly

accessed. "Personal information" is often either undefined or defined vaguely as "personally identifiable information from any individuals, including without limitation any customers, prospective customers, employees and/or third parties."
This type of a standard representation will not necessarily protect a company from all the types of liability that can arise from breach of privacy and data security laws.

3. Issues for Buyers to Consider

A. Type of Business and Scope of the Term "Personal Information"

The definition of "personal information" differs based on the jurisdictions and laws at issue. A generic definition of "personal information" may not fully capture all information the seller collects, uses, discloses or processes that is subject to privacy and data security regulations. If the scope of the definition of "personal information" is too narrow, the buyer could be liable for deficiencies in the seller's use, collection, or disclosure of information not included in the definition.
Buyers should conduct thorough due diligence to fully determine: (1) the type of information the seller collects; (2) what the seller does with that information; (3) the seller's policies relating to such information; (4) what foreign laws might be implicated; and (5) how the seller has to transfer information to the buyer in the context of the transaction. Once this information is collected and analyzed, privacy counsel can determine the scope of how "personal information" is defined in the representation and warranty to insure the buyer is adequately covered.

B. No Requirement to Provide All Versions of Privacy Notice

Many privacy and data security representations do not require the seller to represent it has disclosed all of the versions of the privacy notice(s) that it has used. If this information is not provided to the buyer, the buyer cannot fully perform diligence on the seller to determine whether it has conducted its business in accordance with such policies or whether the privacy notices contain material omissions of the seller's privacy practices. The seller may also not fully understand what restrictions exist on the use of the "personal information."
It is important for a buyer to be aware of the terms of all the seller's privacy notices in assessing the value and liabilities of a seller. Beyond the issues raised by multiple versions of notices, buyers will confront issues arising from notices that do not address the use of information post-acquisition. Often privacy notices are silent about the transfer of "personal information" in the event of a merger or acquisition or, alternatively, may restrict how a buyer may use a seller's "personal information" post-closing. For example, the buyer might be required to adhere to the seller's privacy policy or obtain opt-in consent to use the "personal information" owned by the seller.
Furthermore, the restrictions contained in various versions of the privacy notices may differ. In this case, a deeper dive is required to determine what information was collected, used, processed or disclosed while each policy was in effect and whether such restrictions might be applicable to the buyer. Different requirements create the potential for violations or confusion.

C. Overly Broad Data Security Representations

Broad representations may require a seller to disclose the potential or actual theft or improper disclosure of "personal information" through the disclosure schedule, but this disclosure may not benefit either the buyer or the seller.

Under many data security laws, companies must get authorization from law enforcement authorities prior to disclosing breaches or potential breaches as to avoid compromising any on-going investigation. Prematurely disclosing this information could cause both the seller and buyer to be in breach of applicable data security laws even if a non-disclosure agreement is in place and damage relationships with regulatory authorities.

In any case, often indemnities and escrows will be a more appropriate way of addressing a potential or actual data security breach, because one can tailor indemnity to the breach, rather than using a broad representation and warranty with disclosure of breaches in the disclosure schedule.

D. Third Party Contracts

Standard privacy and data security representations frequently do not require sellers to represent that the seller has contractually required its third party service providers who access, use, process or further disclose "personal information" to adhere to the seller's privacy practices and all applicable laws. This is particularly problematic if the seller does not have a well-defined internal corporate policy of requiring third party vendors to contractually adhere to its privacy practices and applicable laws, because it will not be captured by the 'compliance with corporate policies' representation. Use of a representation on this topic will result in indemnification of the buyer from the seller for any deficiencies.

4. Conclusion

Due to increased scrutiny from regulatory authorities, buyers in M&A transactions should pay close attention to the privacy and data security practices of potential targets and ensure that the M&A agreement adequately protects them from potential liability, permits them to easily integrate the target and use the seller's data as needed for business purposes. Experienced privacy and data security lawyers can help craft tailored provisions to protect buyers and allocate risk appropriately with full understanding by all parties.

http://blog.helenchristakos.com/