

The background features a glowing blue digital globe with a network overlay of nodes and lines. A large, glowing blue padlock icon is positioned on the right side, partially overlapping the globe. Two horizontal red bars are located above and below the main title.

PRIVACY AND SECURITY

Best Practices in M&A Transactions

BY ELIZABETH B. VANDESTEEG, PARTNER,
HEIDI HOCKBERGER, ASSOCIATE &
LAUREN A. WILEY, ASSOCIATE, LEVENFELD PEARLSTEIN LLC


As new privacy laws become effective across the United States, it is more important than ever to consider data privacy and cybersecurity as a key issue in any M&A transaction, including a sale under section 363 of the Bankruptcy Code. While certain industries such as technology and health care may be more susceptible to privacy concerns, any business that collects, stores, or retains consumer data should consider data privacy regulations. To date, data privacy laws are currently in effect in California, Colorado, Connecticut, and Virginia, with several additional potential new laws on the horizon. Whether representing the buyer or seller in a M&A transaction, it is important to understand:

- Whether any of the current privacy laws are applicable to the target company.
- Whether the target company is compliant with applicable laws.
- If not, what would be required to bring the target company into compliance, either pre- or post-closing.

Due Diligence

The due diligence process is the primary method through which a buyer will determine a target company's privacy and data

continued on page 22



After determining which privacy laws are at play, the seller should seek to limit any privacy or security representations and warranties to only those privacy laws that are applicable to the target company.

continued from page 21

security compliance. A buyer's due diligence request list should include tasks similar to the following:

- 1 Identify the states where the target company does business.
- 2 Provide copies of all privacy policies and procedures.
- 3 Describe any data or security breaches.
- 4 Describe what processes are in place to prevent a data or security breach.
- 5 Confirm whether any of the target company's clients or customers are domiciled in any of the states that have current privacy laws.
- 6 Describe the personally identifiable information and sensitive information collected by the target company.
- 7 Confirm whether the target company sells or shares personally identifiable information.
- 8 Confirm whether the M&A transaction will involve the sale of personally identifiable information.

Many of the above issues will help a buyer determine which laws are applicable as a threshold matter, allowing the buyer to further assess whether the company is in compliance with a particular law. Privacy-related diligence requests should also be tailored to the nature of the target business. For example, companies in the health care industry and those dealing with financial information must be aware of requirements under HIPAA

and the Payment Card Industry Data Security Standard (PCI-DSS).

It is also important for the target company to understand that data privacy laws and regulations to which it may be subject, as this knowledge will inform what representations the target company can make when negotiating the purchase agreement.

Negotiating the Definitive Document—the Buy Side

When negotiating the purchase agreement in an M&A transaction, a buyer should seek broad data privacy and cyber security representations from the seller or target company. This could include requiring the company to represent that the target company has not violated any applicable data security laws or that the target company has at all times maintained sufficient policies and procedures regarding data privacy and information security. Buyers should also require companies to represent that they have not suffered any actual or suspected security breaches, and, to the extent such a breach has occurred, the seller should disclose it. To the extent a data breach is uncovered during diligence, a buyer may likely seek a specific indemnity for any claims arising out of that data breach.

Negotiating the Definitive Document—the Sell Side

After determining which privacy laws are at play, the seller should seek to limit any privacy or security representations and warranties to only those privacy laws that are applicable to the target company. Broad language suggesting that the company is subject to "all data privacy laws" may subject the company to a higher standard, such as the requirements under the California Consumer Protection Act (CCPA), that it is not otherwise

required to meet. A seller may also consider adding look-back periods to data privacy representations, limiting the target company's exposure to for any potential non-compliance in the past three or five years.

Section 363 Sale Considerations

If the transaction is implemented under section 363 of the Bankruptcy Code, additional considerations are relevant to obtaining Bankruptcy Court approval of the transaction. If the sale does not comply with the target's privacy policy—for example, if the policy prohibits selling customer information and the sale includes customer information—the court will appoint a consumer privacy ombudsman to evaluate whether the transaction properly protects personally identifiable information. The court will consider the views of the consumer privacy ombudsman and must also find that the sale complies with applicable non-bankruptcy law, such as the state laws discussed herein. If the sale complies with the target's privacy policy and the buyer agrees to comply with the privacy policy, then Section 363(b)(1) generally will not create additional hurdles.

Representation and Warranty Insurance

R&W insurance has become increasingly popular in M&A transactions, and it presents advantages and disadvantages for both buyers and sellers. R&W insurance allows for longer survival periods for general representations and limits the seller's post-closing liability for a breach of a representation or warranty. Known risks or issues identified during diligence, however, will be excluded from coverage under the R&W insurance policy, and data privacy matters are often on that list of exclusions. Data privacy matters are often excluded for a variety of reasons:



Elizabeth B. Vandesteeg is a partner in the Financial Services & Restructuring Group at Levenfeld Pearlstein LLC. Vandesteeg focuses on identifying risk exposure and mitigating liability for clients, with a concentration in the areas of bankruptcy, creditors' rights, commercial litigation, and data security and privacy. She represents secured creditors, debtors, unsecured creditors, creditors' committees, landlords, and shareholders in bankruptcy courts throughout U.S, as well as representing clients in civil litigation in federal and state courts.



Heidi Hockberger is an associate in the Financial Services & Restructuring Group at Levenfeld Pearlstein LLC. She focuses on advising clients in restructuring and bankruptcy matters. She represents debtors, lenders, landlords, creditor groups, sponsors, and asset purchasers in all aspects of in-court and out-of-court restructuring matters. Hockberger has represented debtors in the energy, retail, telecommunications, healthcare, and cryptocurrency industries in 17 Chapter 11 cases in courts across the country.



Lauren Wiley is a corporate associate at Levenfeld Pearlstein LLC. She advises clients on a variety of corporate matters, including mergers and acquisitions, contract negotiation and drafting, corporate governance, and private equity transactions. In addition, she advises clients on various data privacy and cybersecurity matters, including state law compliance and the creation and maintenance of privacy policies and procedures.

1 The target company did not maintain adequate policies and procedures related to data privacy, such as not maintaining a CCPA-compliant privacy policy on its website as required by the CCPA.

2 The target company suffered a data breach that is ongoing or has potential for future liability or risk.

3 The buyer did not perform thorough diligence on privacy matters, which may occur in a M&A transaction where data privacy concerns are less important than other issues, such as environmental or employment matters.

It is in the best interest of both sellers and buyers to avoid any exclusions to an R&W insurance policy. Adequate privacy and security hygiene and thorough due diligence are the best ways to avoid such exclusions.

Playing the Long Game

Having the appropriate tools and resources at your disposal is key to ensuring a smooth transition before, during, and after an M&A transaction. Before going to market, sellers should take inventory of their current privacy and security practices to identify any gaps or issues that could arise

It is in the best interest of both sellers and buyers to avoid any exclusions to an R&W insurance policy. Adequate privacy and security hygiene and thorough due diligence are the best ways to avoid such exclusions.

further down the line during a sale. Buyers should ask targeted questions during the early stages of diligence to determine which regulations might be at play and whether potential for a data breach is considerable.

We invite you to consider implementing the following best practices no matter what stage of an M&A deal cycle you are in:

- Ensure that the sale or transfer of personally identifiable information is consistent with privacy policies and laws/regulations in the relevant states/countries.
- Institute a privacy policy that aligns with the needs of your industry and jurisdictional requirements.
- Update privacy policies and notices to comply with applicable laws and regulations.
- Foster a culture of overall cybersecurity and privacy awareness within the company.
- Develop clear written guidance on cybersecurity and privacy policies.
- Provide frequent and consistent cybersecurity and privacy training.
- Engage legal counsel to stay current on ever-changing state/federal regulations.
- When in doubt, err on the side of consumer privacy protection. ■