Bloomberg BNA

Privacy and Security Law Report®



# Buyer Beware: Merger-and-Acquisition Diligence Tips To Reduce Data Privacy & Security Risks

BY BRIAN HENGESBAUGH AND HARRY A. VALETK

A number of market forces, competitive incentives, and even tax liability concerns are fueling mergers and acquisitions, including stock transactions and asset deals, as well as other corporate transactions (e.g., spin-offs of business lines and divisions) in almost every sector of the U.S. economy.

Dealmakers should be looking at data privacy and security when establishing an appropriate valuation of an M&A target, particularly if customer list acquisition or employee data are important to the transaction. But real-world practices among senior dealmakers suggest the opposite. Although a growing number recognize the threats posed by lax data privacy and security controls, not enough are addressing these privacy risks before, during, or after the deal, despite a warning from Securities & Exchange Commissioner Luis Aguilar that ''boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril.''[1]

With this in mind, the following checklist is designed to provide guidance to companies and counsel in the pre-acquisition valuation stage concerning the data privacy risks associated with a potential target. Keep in mind, however, that separate but related issues may arise during other aspects of an M&A transaction (e.g., post-acquisition integration) and other types of corporate transactions, such as pre-transaction restructuring in connection with spin-offs of business lines or divisions.

When conducting these data privacy due diligence activities, it is also good to develop a ″red/yellow/green light″ to adequately perform a risk analysis. **Red light** refers to significant or material data privacy concerns that may affect valuation of the target or should otherwise be carefully considered by key decision-makers (e.g., planned data uses or cross-border transfers that are incompatible with the target's privacy framework, or would otherwise require compliance steps that may be difficult to achieve, like consumer or corporate customer consent). Red light risks are significant in cost, and often raise insurmountable compliance issues. **Yellow light** refers to privacy risks associated with the target's existing privacy framework or the planned integration of that framework into the acquiring company's business operations, where those risks appear to be manageable with moderate funding and appropriate privacy compliance steps. **Green light** refers to elements of the target's privacy program that seem appropriately aligned, designed, and operated to fit within the overall plans to integrate the target into the acquirer's business operations.

The broad questions below offer a framework to help identify key data privacy risks with a target company's existing privacy program, and help flag potential concerns (red light, yellow light, or green light, depending on response provided) with the acquirer's planned uses of the target's personal information.

*Brian Hengesbaugh is a principal in the Chicago office of Baker & McKenzie and a member of the firm's Global Privacy Steering Committee. He focuses on global data privacy and data security issues in business transformations, compliance activities, and incident response/ regulatory inquiries. He can be reached at brian.hengesbaugh@bakermckenzie.com.*

*Harry A. Valetk is of counsel in the New York office of Baker & McKenzie, where he focuses on supporting merger and acquisition transactions involving cross-border data transfers and advising highly-regulated clients on global privacy and data security practices. He can be reached at harry.valetk@bakermckenzie.com.*

[1] Speech, Luis A. Aguilar, Commissioner, SEC, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus (June 10, 2014), available at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.U8VmTnPD-Uk.

 ISSN 1538-3423

**Privacy Policies** matter more today than ever before. Regulators and plaintiff class action counsel continue to rely on them as a basis to file lawsuits against companies that fail to live up to stated promises. Prior to closing a deal, an investor should be confident that all representations about the target company's data collection practices, along with those of its affiliates and subsidiaries (collectively, the Company), are accurately described in any privacy policies. It is also important to compare those practices against the investor's own privacy policy to help identify what steps may be necessary to consolidate acquired databases.

*To-Do List:*

1. Provide copies of the Company's online privacy policy(ies), and list all URLs where the policy is posted.

2. Find out if the Company's privacy policy(ies) accurately represent its information collection, use, and disclosure practices online.

3. Ascertain whether the Company complies with the California Online Privacy Protection Act (CalOPPA), the Children's Online Privacy Protection Act (COPPA), and/or other laws that may apply to disclosures about online data collection practices.

**Marketing and Tracking Technologies.** Too many companies today are embarking on social media and digital marketing campaigns with a limited understanding of data flows—and the laws that apply to collecting and sharing personal information—online in the U.S. or abroad. Some rely entirely on ad agencies to hire and deploy social media and digital marketing activities. Understanding the data privacy risks associated with any acquisition includes knowledge about the types of campaigns, sharing activities, and tools deployed by a target company.

*To-Do List:*

1. Does the Company engage in online behavioral advertising, search engine marketing, or social media marketing activities to (i) consumers; (ii) customer contacts; or (iii) business contacts? Require the Company to describe in detail.

2. Does the Company share any personal information with affiliated or unaffiliated companies for marketing purposes? If yes, require the Company to describe in detail.

3. Does the Company's website(s) or mobile apps use cookies or other web-based files stored on user devices? If yes, require the Company to provide the following information:

a. Does the Company allow third parties to place their own cookies or files on user computers for (i) display of third party ads on the Company's site; (ii) retargeting of the Company's ads on third party sites; (iii) interaction with social media sites (whether posting to those sites, or merely allowing those sites to capture data); (iv) analytics purposes; or (v) for any other purposes? Require the Company to explain in detail.

b. Does the Company place its own first party cookies, web beacons, Flash cookies, or other tracking technologies on user computers? If so, require the Company to describe the technologies used, the data captured, the purposes of data capture, the purpose or purposes for which the data is used, and whether that data is shared with others.

c. Has the Company undertaken a due diligence process to confirm that its practices for first- and third-party marketing and tracking comply with all U.S. privacy laws (e.g., CalOPPA, including Do Not Track disclosure obligations) and non-U.S. data protection and privacy laws (e.g., European Commission Cookie Directive (2009/136/EC, and its national implementation rules)?

**Cross Border Data Transfers** in this information age are no longer optional; they're essential. Almost every company implements business operations, engages in compliance activities, or otherwise leverages technology or services that require personal information to cross country borders. Even if the personal information remains local, if others outside of that host country can even access it, many data privacy and security laws outside the U.S. would treat this foreign accessibility to personal information the same as a transfer.

*To-Do List:*

1. Does the Company maintain any global or regional databases or applications that store personal data? If so, have the Company identify each and describe the functions (e.g., enterprise resource planning systems, software-as-a-service or other cloud solutions, e-mail, collaboration tools, customer relationship management databases, or the like).

2. Does the Company have an established approach to address cross-border data transfer restrictions under non-U.S. data protection laws (e.g., individual consent, Safe Harbor, standard contractual clauses, binding corporate rules)? Ask the Company to explain in detail.

3. Ascertain whether the Company has completed registrations with any non-U.S. data protection authorities, or taken other steps to comply with non-US data protection laws.

**Employee Data** is often overlooked during the diligence process. Depending on the size of the target organization and whether it has employees outside the U.S., a host of compliance issues may arise.

*To-Do List:*

1. Does the Company have policies governing the collection, use, and disclosure of personal information about its employees?

2. Has the Company obtained consent from or provided notice to employees whose personal information has been transferred outside of the host country? Have the Company explain and provide copies of any forms.

3. Have all employees successfully completed background investigations to the extent permitted by applicable law? (Performing employee background checks outside the U.S. is not always permitted by law.) If not, the acquirer should flag the potential risks from disgruntled employees and other insider threats.

4. Does the Company require its employees to complete data privacy training? If so, how often? Ask the Company to provide the training materials it has used.

**Special Concerns for Highly-Regulated Entities covered by: the Gramm-Leach-Bliley Act (GLBA), Securities and Exchange Commission Regulation S-P, the FTC's Red Flag Rules, COPPA, HIPAA/HITECH Act, and state insurance laws.** Beyond the basic level of diligence applicable to any company doing business today,

  PVLR ISSN 1538-3423

an entirely separate layer of inquiry should be performed on regulated entities to ensure compliance with specific rules that may apply to those businesses. For example, banks, broker-dealers, and financial services firms have numerous obligations under federal and state law separate from those applicable to most companies. Most states have laws governing the use of Social Security numbers. Website operators that collect personal information about children under 13 are subject to COPPA. Health services firms also need to carefully assess operational controls and subcontractor compliance with HIPAA and various other state laws regulating the collection, use, and disclosure of protected health information.

*To-Do List:*

1. Does the Company collect, host, or use protected health information subject to HIPAA? If so, have the Company explain in detail.

2. Is the Company a financial institution subject to the requirements of GLBA?

3. Does the Company offer customers an account designed to allow multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, mobile phone account, utility account, checking account, or savings account? If so, have the Company describe those accounts and how the Company complies with the Red Flag Rules.

**Record Retention and Disposal Policies.** A great deal of personal information is collected and stored by organizations of every size. Suitable information retention and disposal policies are essential to complying with data privacy and security laws (e.g., limits on the retention of personal information when no longer required for legitimate purposes) but also for controlling the potential risks associated with data security incidents (e.g., avoiding situations where the scope of personal data affected by a data security breach is excessively broad because the Company retained personal information well beyond its useful life).

*To-Do List:*

1. Does the Company have a policy requiring the secure disposal of data on electronic media? If so, have the Company provide the policy.

2. Does the Company have a policy requiring the secure disposal of hard copy records (e.g., shredding vendor) when the records are no longer needed for legal or business reasons? If so, have the Company provide the policy.

3. Does the Company maintain a records retention policy? If so, have the Company provide the policy.

**Information Security** is much more than just a yes-or-no inquiry. Every investor should understand the maturity and sophistication levels of any Company's information security program. Consider, for example, how many technical and human resources are charged with protecting the target company's infrastructure?

*To-Do List:*

1. Does the Company maintain an information security program that includes physical, technical, and administrative controls to protect the security, integrity, and confidentiality of personal information about individuals, including consumers, customer contacts, and employees? Ask the Company to provide a copy of the written information security policies, evidence of the due diligence procedures undertaken to identify and establish appropriate controls, evidence of any security audits and results (whether internal or external), and other evidence that supports the program.

2. What specific tools have been deployed? For example, did the Company deploy data loss prevention or encryption?

3. How many exceptions to the Company's policies have been made throughout its operations, and how are such exceptions evaluated and documented?

4. Does the Company have a bring-your-own-device program in place? If so, have the Company describe the administrative and technical controls to prevent unauthorized access to corporate systems and the loss of personal information on employee-owned devices. Also, have the Company describe the steps that it takes to address employee privacy issues with such controls.

5. Does the Company allow personal information about consumers, customer contacts, and employees to be stored on portable devices (e.g., laptops or other mobile devices)? If yes, are all those devices encrypted? Have the Company explain the level of encryption and other controls.

**Data Security Incident Response.** Every company of every size has had data security incidents, but some may have impacted larger populations, resulted in harmful media coverage, or materially damaged the Company's reputation and net worth. Understanding the root cause of any incidents and the steps taken to remediate them allows a savvy buyer to more accurately assess the privacy risk to the deal.

*To-Do List:*

1. Does the Company maintain a data security incident response and breach notification plan? If so, have the Company provide the plan. Have all employees been trained appropriately in their role(s) on how to follow the plan in the event of a known or suspected breach?

2. Has the Company experienced one or more data security incident? If yes:

a. Did the Company perform an investigation to determine the root cause? Have the Company share the findings of that investigation, including a copy of any incident reports.

b. What specific physical, technical, and administrative controls did the Company implement to remediate any deficiencies in its environment?

c. What fines or other consequences accrued to the Company as a result of this incident? Have the company identify all activities arising directly or indirectly from that incident, including:

i. actions by state attorneys general, the Federal Trade Commission (FTC), or other government authorities;

ii. fines from Payment Card Industry Data Security Standard (PCI-DSS) /merchant banks/card brands;

iii. private class actions settlements or determinations;

iv. identifiable customer churn or loss;

v. adverse publicity or media reports; and

vi. other adverse consequences.

3. Has the Company had any data security incidents other than the one identified above? If so, have the Company describe and provide responses to items 2(a)–2(c) for each such incident.

**Authorized Third-Party Subcontractors.** Every company uses subcontractors. Some use more subcontractors than others, and some depend on them more to carry out core business activities. Those subcontractors also often rely on their own service providers to perform services, and must, likewise, access a Company's personal information.

*To-Do List:*

1. Does the Company give any authorized third-party subcontractors access to personal information about its customers or employees? If so, have the Company:

a. identify the vendor(s);

b. identify the type of information provided to each; and

c. identify the nature of the services each provides.

2. Does the Company perform data privacy and security risk assessments on all authorized third-party subcontractors with access to personal information? If yes, have the Company provide the risk assessment questions used to assess each vendor.

3. Does the Company require all third-party subcontractors with access to personal information to agree to specific data privacy and security terms and conditions? If yes, do those provisions include security incident notice obligations? Have the Company provide copies of all of those agreements.

4. Are all authorized subcontractors with access to personal information located locally within the host country?

5. Does the Company use cloud computing services to support any of its operations? Describe the nature of those services, including:

a. whether the cloud services used are multitenant;

b. whether the Company has prior notice and authorization rights (or at least the opportunity to object) to the location and identity of any of the vendor's service providers;

c. whether the Company data resides within regional servers (e.g., in the EU) and other details of the services; and

d. have the Company provide a copy of the terms it has in place with its cloud computing service provider.

**Audits, Claims, and Other Known Issues.** Information about a target's known deficiencies are often available to those who know where to look. Many issues are outlined in internal or external audits, especially if the Company is a regulated entity. A trend in the use of risk and compliance platforms also serves as a source of information about known deficiencies. These tools have become increasingly common among many global or regulated entities with a need to document all internal legal and operational risks, implemented controls, and any known deficiencies.

*To-Do List:*

1. Has the Company's information security program ever been audited (internally or externally)? If yes, have the Company provide the findings and information on remedial steps taken.

2. Does the Company use risk and compliance management software to coordinate and control compliance activities? If yes, have the Company provide all findings related to privacy and data security.

3 Ask the Company to identify any data protection claims brought (or anticipated) against it by consumers, customer contacts, employees or employee representative bodies, state attorneys general, data protection authorities, the FTC, or any other authorities. For each, have the Company give ample detail about the claim(s) and remedial steps taken.

  PVLR ISSN 1538-3423