Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Tech M&A Due Diligence Checklist: Sector-Specific Concerns

By **Ed Batts, Carrie LeRoy and Charles Walker** (October 3, 2023, 2:42 PM EDT)


Ed Batts


Carrie LeRoy


Charles Walker

In technology merger and acquisition transactions, critical issues must be evaluated related to a target's intellectual property, and additional, high-impact diligence concerns also need to be evaluated early and with precision.

We detail below a nonexhaustive list of these additional top technology sector-specific legal diligence concerns in acquisitions in an increasingly dynamic merger and acquisition landscape as follows:

Cybersecurity and Data Breach

In today's environment, all companies are vulnerable to cybersecurity incidents.

Even when not consumer facing, a company may house significant and sensitive data regarding its employees, proprietary technology, including source code, customers, suppliers and other counterparties.

What may seem at the outset to be a small cybersecurity issue often balloons into a problem that requires extensive remediation efforts and can be subject to state-by-state notification and country-by-country reporting and remediation requirements.

Further, cybersecurity vulnerabilities that are exploited following the closing of an acquisition can be damaging to the brand and public trust of the acquiror.

An acquiror should require a target company to provide a detailed description of its cybersecurity protocols, policies, procedures, audit results and all recent penetration tests, aka pen tests, and should verify with the target how any issues flagged were remediated.

If a recent pen test is not available, an acquiror should strongly consider engaging a consultant to perform one as part of the diligence process.

Cyberinsurance

Given the increase in cyber incidents over the years, reviewing a target company's insurance policies for any coverage from cyber breaches or other incidents has become an important part of any transaction.

However, these policies often include large exclusions for issues such as ransomware attacks or nation-state attacks.

As such, even with coverage in place, a policy may not provide the expected level of protection. An acquiror, together with counsel, should give careful consideration to how representations and indemnification protections concerning cybersecurity matters, such as pre-closing breaches, are constructed in the definitive agreement.

Further, the acquiror must evaluate both the target company's and its own policies to understand if coverage will exist for historical cyber breaches that are not discovered until after the deal is consummated.

Open-Source Software

Commonly used by software engineers in writing code, certain open-source software kernels in a target company's codebase may come with license terms that can present material issues for a company looking to incorporate and monetize a target company's software.

The most prominent example is "copyleft" or "viral" open-source licenses that, per their terms, require in certain circumstances all modifications to or code incorporated with such code to be released to third parties in source code form.

This could cause significant issues if compliance with these terms would result in the disclosure of otherwise proprietary code or, alternatively, require the acquiror to invest significant time and resources in reengineering the codebase to exclude the copyleft code.

If software is a material asset of the target, acquirors should carefully consider engaging an open-source vendor to perform a code scan that can flag portions of code in the target company's software that are subject to potentially problematic open-source licenses.

Consider having outside counsel engage the consultant to preserve privilege over any findings.

Data Privacy and Data Use

A target company's data can be a valuable asset to an acquiror, but this value can be easily diminished if the target company did not secure the appropriate scope of use for such data.

An acquiror should pay special attention to the target company's data privacy policies, sources and methods of procuring data, procedures and compliance, as well as applicable contractual provisions to ensure any planned use of the data by the acquiror is permitted.

The diligence exercise also needs to include the identification of, and review for compliance with, all applicable privacy laws such as the EU General Data Protection Regulation, California Consumer Privacy Act, California Privacy Rights Act and the ever-expanding patchwork of other similar state, national and international laws and regulations.

The acquiror should confirm that the data can be transferred in the manner contemplated by the transaction by ensuring that the transfer of data upon consummation of the transaction is compliant

with the target company's privacy policy and any applicable laws and regulations.

For example, a target company's privacy policy may require prior consent from the user to transfer its data in a merger or sale. Some policies may also require erasure of data from nonconsenting users, which may preclude the acquiror's use of such data. Consent may also be required for the transfer of certain types of sensitive data, e.g., protected health information.

Adequate Protection of Trade Secrets

For many technology companies, their most valuable intellectual property asset is source code, which is typically maintained as a trade secret — if not patented or patentable subject matter.

Thus, it is important to confirm that the target company engages in industry standard practices and has implemented adequate controls to protect its trade secrets and has not licensed or disclosed its code in a manner that could enable third parties to gain access to the source code.

The target company, may, for example, have agreed to place its source code into an escrow account for the benefit of a third party. Such agreements frequently include provisions that permit the release of source code to the third-party beneficiary in the event of a change of control of the target company.

The implications of such agreements should be considered with respect to the extent that the release of such code could impair the value of the trade secrets or would be inconsistent with the acquiror's intended exploitation of the source code.

Employee Stock Options and 409A Valuations

Technology companies routinely grant employees stock options as part of their compensation packages.

To ensure the options are issued with an exercise price no less than fair market value, a target company should be able to provide yearly 409A valuations by a third-party consultant setting forth the value of the common stock of the target at the time of evaluation.

Note, if the target company experiences a material event, such as a fundraise or execution of a term sheet, the target may no longer be able to reasonably rely on a prior 409A valuation.

It is not unusual to discover during diligence that a target company has issued unallocated stock options after receiving and/or executing a term sheet with an acquiror based on a prior 409A valuation that does not incorporate this material, new valuation information.

Failure to identity and remedy this issue can result in adverse and unexpected tax consequences for both the target company and the employees that were issued these mispriced options — and create dissatisfaction with such employees in the period after an acquisition's closing, precisely when an acquiror will be aiming to retain key technical personnel.

Trade Compliance and Anti-Corruption

Technology companies frequently are global in their sales, and subject both to export control regimes and anti-corruptions laws, such as the U.S. Foreign Corrupt Practices Act, U.K. Bribery Act and France's Sapin II.

These areas often can be afterthoughts in a long list of diligence issues to tackle — however, if not discovered before closing a transaction, the post-closing penalty can include self-disclosure or, worse yet, a whistleblower-triggered investigation by a regulator, each of which can imperil the acquiror's overall brand and business, not to mention financial liability.

Acquirors, in partnership with legal counsel, should evaluate a seller's products and relevant export controls — the Export Administration Regulations and International Traffic in Arms Regulations in the U.S. — as well as compliance with country and individual sanctions.

It is not unheard to discover seemingly immaterial transactions to prohibited states that create significant consequences from regulators.

Likewise, counsel should review a company's corruption compliance program, including specifically, training and any prior whistleblower complaints particularly surrounding high-risk indicia such as "gift" programs or sponsored travel.

Ed Batts, Carrie LeRoy and Charles Walker are partners at Gibson Dunn & Crutcher LLP.

Gibson Dunn associate Jessica Howard contributed to this article.