O'Melveny

Alerts & Publications

Venture-Backed M&A: Hot Topics and Recent Developments in 2018

November 5, 2018

KEY CONTACTS

David Makarechian
Silicon Valley
D: +1-650-473-2631

AJ Talt
Silicon Valley
D: +1-650-473-2606

Scott W. Pink
Silicon Valley
D: +1-650-473-2629

Theodore W. Kassinger
Washington, DC
D: +1-202-383-5170

David J. Ribner
Washington, DC
D: +1-202-383-5507

Greta Lichtenbaum
Washington, DC
D: +1-202-383-5249

Eric Amdursky
Silicon Valley
D: +1-650-473-2644

Heather J. Meeker
Silicon Valley
D: +1-650-473-2635

Mergers and acquisitions of venture-backed companies have continued at an extraordinary pace in 2018, with 637 deals reported through the first nine months of the year and a total deal value of over $80 billion.[1] According to the Pitchbook-NVCA Deal Monitor, the exit environment is strong, with total deal value expected to exceed levels reported in 2017.[2] At the same time, the total number of deals annually has gradually declined from a peak of over 1,000 deals in each of 2014 and 2015.[3] The decline in the number of deals may indicate that acquirers are growing selective.

In 2018, venture-backed targets were often of significant size, with distributed operations and innovative business models. Addressing the issues that arise from such targets can be complex. This alert highlights some of the "hot topics" that are areas of focus in venture-backed M&A exits in the torrid market of 2018, including the popularity of representation and warranty insurance, data security and privacy, the Committee on Foreign Investment in the United States (CFIUS), the #MeToo Movement, compliance and corruption risk, and intellectual property concerns.

Representation and Warranty Insurance

One of the most transformative developments in venture-backed M&A is the widespread acceptance of representation and warranty insurance policies (RWI) to address the risk of loss associated with breaches of representations and warranties in the definitive agreement. Aon plc, one of the largest international insurance brokers, estimates that the number of deals that included RWI increased by 96% between 2014 and 2017, with approximately 34% of all M&A deals with an enterprise value between $25 million and $10 billion using RWI in 2017.[4] For venture-backed companies, RWI can be particularly attractive to venture funds that desire to reduce the risk of post-closing liability so that all relevant funds may distributed to their investors. Additionally, venture-backed companies looking to shorten the negotiation period of the M&A transaction may require the buyer to obtain RWI, particularly in auctions.

RWI will only cover unknown breaches of representations and warranties, and will exclude a number of liabilities. Typical exclusions include: breaches of covenants, known breaches, "interim" breaches (those arising between signing and closing), purchase price adjustments, and certain tax matters. By

excluding known breaches, the policy will exclude all liabilities that the acquirer knew about when the policy was bound. This means that losses arising from liabilities not disclosed on a disclosure schedule, but otherwise known by the acquirer through its own diligence or otherwise, will not be covered.

In a typical deal involving seller indemnification without RWI, materiality qualifiers are heavily negotiated as applied to the representations and warranties, as they are important in allocating risk of loss between the acquirer and seller. Most RWI policies insist that disclosures against representations and warranties are made on the basis of a "materiality scrape" in which materiality qualifies are read out of the representations for purposes of determining whether a breach occurred. This is meant to induce the seller to give greater attention to disclosure against representations and warranties.

While an RWI policy may significantly streamline the negotiation of the purchase and sale agreement in venture-backed M&A, the introduction of a representation and warranty policy will not fully eliminate the need to negotiate indemnification provisions. The parties will still need to negotiate indemnification provisions as they relate to the retention amount. In the event that the retention will be split between the acquirer and seller, the parties will need to negotiate the mechanics of that split (e.g., whether there is an initial deductible born by the acquirer). Also, in the event that the underwriter has specific exclusions from the policy, the parties may still need to negotiate indemnification for those items. Finally, as is the case in every M&A deal with indemnification provisions, the normal caps and baskets still need to be negotiated to the extent the seller has some liability under the purchase agreement.

Data Security and Privacy

Hacking and rules regarding privacy and data protection continue to dominate the headlines in 2018, which has resulted in acquirers being increasingly focused on the target's compliance with privacy laws, the integrity of the target's information technology systems, and the security of the target's data. In May of this year, the General Data Protection Regulation (GDPR) came into force. With the GDPR comes extraterritorial application of EU privacy laws, increases in penalties for non-compliance with those privacy laws, and additional compliance obligations for companies that fall under their regulations—which includes many venture-backed companies.

In the venture-backed M&A context, acquirers often focus on the level of sophistication of the target's data security and privacy team, compliance policies, and infrastructure as they evaluate the risk of the target's potential non-compliance with privacy laws. Acquirers are most concerned about the following issues:

- Civil and regulatory post-closing liability to the acquirer due to a target's non-compliance with GDPR—acquirers can be held liable for a target's

breach of the GDPR even if such breach took place before the transaction.

- Costs to bring the target into compliance with GDPR (or other privacy statutes) post-closing even if no fines are levied against the target by the relevant regulators.
- The target's compliance with other industry-specific regulations that might apply, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for protected health information and Gramm-Leach-Bliley Act (GLBA) for financial institutions.
- The target's ability to continue operations with the existing data as collected by the target. If a target's data was not properly obtained or is subject to transfer and other restrictions, it is at risk of being forfeited or unusable by either the target or the acquirer.
- The target's data security infrastructure. With major data breaches making headlines almost daily, acquirers are inevitably concerned with a target's ability to withstand attacks on its security infrastructure.

These concerns impact how acquirers conduct their diligence and how they negotiate the potential liabilities arising from data security and privacy issues in the definitive agreement. The scope of diligence when evaluating a target's compliance with the GDPR and other applicable statutes and regulations covering the use and collection of personal information should include a detailed review of the target's efforts to comply with such statutes. The first step in reviewing the target's compliance is to understand how the target uses its data. For this reason, the acquirer will want to understand what data is collected, the purpose and legal basis for collecting the data, where the data is stored, and in what jurisdictions the data can be accessed (and whether cross-border transfers are made in compliance with applicable privacy laws). It is also important to identify the third parties the target is using to process data on its behalf and whether it has in place a vendor management program and appropriate data processing contracts to ensure legal compliance and mitigate risk. Additionally, the acquirer should seek to understand how the data will be used in the future and whether there are any planned introductions of new lines of business or new technologies in the target's business plan that may require changes to the target's current data security and privacy policies and infrastructure.

The acquirer will also review the target's privacy policies and/or terms of use of the target's website to ensure that such policies are compliant with the relevant law and reflect best practices. A review of the target's ongoing compliance practices may include its internal compliance function, responses to data subject requests, data retention, and annual updates of its privacy policies to comply with new developments. In addition to compliance, the acquirer will seek to understand the target's information technology systems and the extent of the efforts made to audit systems for security vulnerabilities.

In the cloud and digital storage era, it may be difficult to identify who has access to the target's data. Those with access are likely to include vendors, customers, and employees, among others, and the acquirer will seek to understand how such parties can access the target's data and the relevant security mechanisms in place for such access. The acquirer will also want to review and understand past instances of attacks on its systems, any payments made in ransomware attacks, and steps taken to mitigate vulnerabilities. The acquirer may also consider retaining third-party consultants, particularly if the target is subject to specific industry or legal standards, such as HIPAA.

Companies that collect data of third parties on behalf of its customers may be subject to indemnification obligations with respect to data breaches. The acquirer will inherit these obligations to the extent contracts are assigned to the acquirer.

CFIUS and Restrictions on Foreign Investment

CFIUS is a US government interagency committee, chaired by the Department of the Treasury, that assesses foreign investments in or acquisitions of US businesses for potential national security concerns. CFIUS may impose restrictions on an investment, and the President may formally bar a transaction from proceeding because of national security concerns.

The robust venture market has attracted increasing investment from foreign strategic and financial investors. In addition to welcome capital, US targets often see links with foreign investors as potential support for expanding sales abroad. Over the past two years, however, the US government has grown increasingly alarmed by foreign investments, particularly from China, in new and early- stage technology companies. With the Administration's support, Congress responded with CFIUS "reform" legislation—the Foreign Investment Risk Review Modernization Act (FIRRMA)—which became effective on August 13, 2018.

FIRRMA made several important changes to the CFIUS process. These include:

- CFIUS's jurisdiction has been expanded in a way that allows it to review certain non-controlling investments, as well as deals that are structured in a way that aim to evade CFIUS's jurisdiction.
- New mandatory CFIUS filing obligations in transactions involving critical infrastructure, critical technologies, and companies that hold personal data of US citizens in which a foreign government has a "substantial interest" in the foreign investor as well as other investments determined by CFIUS. Parties to such transactions will be required to file these mandatory declarations with CFIUS at least 45 days prior to closing.
- Deadlines were extended. The two key stages of the process may now take as long as 105 days, up from 75 days.

- CFIUS will implement a filing fee equal to one percent of the transaction value up to $300,000.

On October 10, 2018, CFIUS issued interim regulations for a pilot program to implement certain provisions of FIRRMA. Beginning November 10, 2018, the pilot program requires declarations for controlling and non-controlling investments in US businesses that produce, design, test, manufacture, fabricate or develop "critical technology" that is used, or designed for use in connection with 27 specific industries. The rules define "critical technology" to include technologies that are subject to various export controls, and potentially more broadly, "emerging and foundational technologies" subject to the Export Control Reform Act of 2018. The latter group will be defined through a separate rulemaking process lead by the Department of Commerce. The pilot program's 27 industries, defined by NAIC codes, include many that are popular among venture capital investors, including computer manufacturing, optical instruments and lens manufacturing, semiconductors and related device manufacturing, and biotechnology research and development. Failure to file a mandatory declaration may subject the parties to the transaction to a monetary penalty up to the value of the transaction.

Acquirers and targets alike will need to evaluate compliance and transaction risk resulting from FIRRMA not only in an exit, but in investment rounds that include non-US investors prior to an M&A transaction.

The #MeToo Movement and Workplace Violations

In 2018, the venture and technology company communities saw several instances of high-profile allegations of sexual misconduct and workplace harassment. Because of these high-profile cases, acquirers have become more concerned with evaluating the corporate culture and past workplace violations of a target. Some acquirers are even going as far as to hire private investigators to perform background checks on management employees, which can extend to researching such employees' history before their employment with the target began. Acquirers will also want to investigate a target's written policies, training programs, prior claims, and settlement agreements to ensure compliance with state laws, understand the scope of potential liability, and assess whether remedial steps or cultural changes will be necessary.

When reviewing the target's policies, employment claims history, employment agreements, and other relevant documents, there are several identifiable areas of focus:

- Whether sexual misconduct is excluded (either expressly or implicitly) from the definition of "cause" in executive agreements;
- Whether the target is aware of a pattern of misconduct, usually identified in exit interviews, emails, informal complaints (including in social media or traditional news reports), and/or settlement agreements;

- Whether there is higher attrition rate among women, difficulties in recruiting women or those from diverse backgrounds, and/or a large number of settlement agreements; and
- Whether misconduct is being unaddressed and/or covered up, usually identified by reviewing communications between human relations and public relations.

Many acquirers will want to see measures taken in excess of what is required by law. In response, some venture capital funds are requiring their portfolio companies to conduct sexual harassment prevention training for executives and management even if not legally required, as well as implement certain harassment and discrimination prevention policies within a limited number of days of closing a financing round. Targets need to be prepared to explain how they comply with discrimination, harassment, and retaliation laws, and the value and importance they place on maintaining safe and welcoming workplace environments regardless of what the law requires. In many transactions, acquirers are insisting on broader representations and warranties as to workplace conduct, the absence of sexual harassment in the workplace, compliance with labor and employment laws (including laws requiring pay equity based on gender and other protected classifications), and even an absence of claims of sexual harassment or assault by any officers or key employees over the past several years and without regard to whether such persons were employed by the target at the time of such claims.

Cross-Border Compliance and Risks: Corruption, Economic Sanctions, and Export Controls

In their risk assessments of venture-backed companies with international operations, acquirers are increasingly focused on the target's compliance with the US Foreign Corrupt Practices Act and other anti-bribery laws, which are proliferating in major economies around the world. In the current market environment, an acquirer is likely to perform enhanced diligence of overseas operations, including reviews of the target's compliance policies, whistle-blower reports and steps taken to address such reports, forensic accounting, and background checks by investigative services. Many of these anti-bribery laws include extra-territorial provisions. Acquirers also focus on the target's compliance with US economic sanctions and export control laws, which are typically broader than parallel laws in other countries and have expanded and become more aggressively enforced in recent years.

Generally, acquirers are concerned with four types of risks when evaluating a target's compliance with applicable anti-bribery, economic sanctions, and export control laws:

- Legal Risk: The acquirer will be concerned about acquiring legacy, as well as prospective, legal liability (depending on the circumstances), and structure of the acquisition;

- Financial Risk: The acquirer will be concerned about the remediation costs in connection with bringing the target into compliance;
- Valuation Risk: The acquirer will be concerned about how dependent the target's revenue is on practices that will need to be stopped; and
- Reputational Risk: The acquirer will be concerned about how non-compliance with these laws by a target may negatively impact the acquirer's reputation after the M&A transaction.

The FCPA is enforced by the Department of Justice and the Securities and Exchange Commission. In November 2017, the DOJ formalized its corporate enforcement policy for FCPA violations, providing strong incentives for voluntary corporate disclosure and remediation efforts. In May 2018, the DOJ further clarified its position, stating that these incentives also apply to successor entities in M&A transactions. Therefore, a proper evaluation of a target's compliance with the FCPA is not limited to whether they are currently in compliance; it should include a comprehensive assessment of what steps need to be taken to bring the target into compliance. The Department of Commerce and the Treasury Department, which each have a role in administering the export control and economic sanctions laws, take similar approaches.

Intellectual Property

Addressing intellectual property issues remains an area of focus in venture-backed M&A. Understanding the chain of IP ownership is a fundamental concern. Tracking the chain of IP ownership may become complicated in an era when many early-stage companies are developing in incubators or other shared working spaces, often times sponsored by universities or other corporate entities. Acquirers will want to know where this early intellectual property was developed and to see agreements that clearly assign the intellectual property rights to the target. The absence of such agreements alone may raise questions as to whether the target's intellectual property was adequately protected and appropriately assigned.

Another common problem for venture-backed companies arises when the development of intellectual property takes place by foreign subsidiaries. In the venture context, compliance with local law may not have been prioritized, and it is possible that proper assignments of intellectual property were not obtained by employees and/or contractors of a foreign subsidiary that is developing intellectual property. Additionally, acquirers will want to see functioning inter-company agreements that allow for each entity to have the intellectual property rights they are exercising, whether that be for selling company products, licensing the intellectual property, or developing the intellectual property of the target.

Conclusion

The venture-backed M&A market is ever evolving and affected by political and social trends, economic fluctuations, changes to the law, and changes in the M&A market generally. The issues facing acquirers and targets became more complex in 2018. It is imperative for potential acquirers and targets to work with counsel versant in the variety of issues affecting venture-backed M&A transactions.

---

[1] Dana Olson, *The State of US Venture Capital in 15 Charts*. PITCHBOOK (October 29, 2018).

[2] *Venture Monitor 3Q 2018*, PITCHBOOK & NATIONAL VENTURE CAPITAL ASSOCIATION (October 8, 2018).

[3] *Venture Pulse Q3 2018*, KPMG ENTERPRISE (October 10, 2018).

[4] *M&A Risk and Review*, AON PLC (2018).
