The Threat of Social Media Diligence on the Confidentiality of the M&A Process: The Problem and Possible Solution

By:Jonathan D. Gworek
March 26, 2014

A version of this article appeared in ABA's Business Law Today.

The buyer and seller in a merger and acquisition (M&A) process often place a high value on the importance of maintaining a confidential process. A buyer is sensitive to the possibility that any leak could invite unwanted competition for the deal. A seller worries that widespread knowledge about an impending M&A transaction and the uncertainty that knowledge creates might cause an unwanted business distraction. Or worse, a seller may fear that if the pending deal becomes known to the public and ultimately falls through, the seller will be left with less leverage among the remaining buyers and could be labeled "damaged goods." Both parties also frequently share a range of concerns about managing the content and timing of an announcement of an M&A transaction to a wide range of constituents such as investors, customers, and suppliers.

Against this backdrop, the widespread use of the Internet and social media in everyday business practices makes it increasingly difficult to maintain confidentiality in a variety of business settings, including M&A. In particular, the increasing use of social media by buyers for purposes of conducting due diligence on a target can easily "tip off" people who would otherwise be unaware. This article looks at the very practical impact of the Internet and "social media diligence" on the confidentiality in M&A transactions and suggests certain practices that the parties might adopt to both mitigate and more fairly allocate this risk.

Social Media's Role in Diligence

In the early stages, the parties to a prospective M&A transaction often limit information about the pending transaction to key members of seller's management and the buyer's M&A diligence team. The parties may intend for this tight control on information to remain in place through the actual closing. While buyers may also desire the same level of confidentiality, the buyer also has to complete a large due diligence review of the seller's business and operations. The buyer can expedite this process by accessing information that sits in the public domain, whether on the seller's website or through social media like LinkedIn and Facebook. For example, if the target is a high technology company, the buyer's technical diligence team may be tasked with assessing the technical capabilities of the seller's engineering and product development team. While the chief technology officer and certain other senior technical employees of the seller may have a biography on the seller's website, this is not likely to be the case below the C-level employee. The most efficient way for the buyer to gather the information necessary to make this initial assessment and create an internal report on the seller's technical team — before moving to the more advanced diligence stage involving joint team meetings and interviews — is likely to be via the review of such publicly available profiles. The same diligence exercise could be performed by the buyer across multiple departments of the seller in parallel.

Risk of Lost Confidentiality Associated with Social Media Diligence

While this practice might seem both efficient and relatively innocuous from the buyer's

perspective, there are inherent risks that result from this approach to diligence. Perhaps the most obvious example of this arises when an employee at the seller notices an inordinate amount of activity on his/her LinkedIn page originating from personnel at the buyer. Upon noticing this trend, this employee may naturally stop and wonder what is underlying this sudden indication of interest. It is not hard to imagine that one such attuned and inquisitive employee might be all that it takes for broader speculation to begin around the seller's water cooler. And if this type of social network diligence is detected by multiple seller employees in parallel, broader speculation is almost certainly going to result. Once this happens, the confidentiality of the pending M&A transaction has essentially been blown internally at the seller. At this point the seller's management has a problem. At minimum it has a distracted employee base. And while the horse may not have yet completely left the barn, the rest of the connected world — including customers, suppliers and the media, to name a few — is one ill-fated Tweet away from being on notice of the pending M&A transaction as well.

Breach of Contract Damages Resulting from Lost Confidentiality

As if the prospect of lost confidentiality is not bad enough, this chain of events could well put the seller in technical breach of the confidentiality agreement between the buyer and seller and at risk for any damages the buyer may incur as a result of this breach. A typical M&A confidentiality provision prohibits not just the use or disclosure of the confidential information of the other party received during the diligence process, but also extends to any information related to the potential transaction itself, including the simple fact that the parties ever entered into discussions. Such agreements typically put the risk of breach on each party in the event of a breach of the agreement by any "director, officer, employee or agent" of such party. Therefore, any leak outside of the company by an employee arising out of the facts described in the prior section could well constitute a breach of the confidentiality agreement by such person's employer. But the leak need not necessarily be outside the company in order to constitute a breach. If the confidentiality agreement limits those seller employees who may be made aware of the transaction and anyone outside of this group learns of the pending M&A transaction, this type of leak could also constitute a seller breach even though the information has not left the company. The damages could be significant in either case. For example, if a second potential buyer learns of the pending sale transaction and as a result makes a successful topping bid and emerges as the buyer, the seller could be saddled with a significant contingent liability in the form of a claim brought by the prior bidder. This would be an unfortunate result. In light of the fact that it was brought about by the prior bidder's diligence methods in the first instance, this may also be considered an unfair result.

Possible Solutions

Both the buyer and seller can take steps to reduce the risk that such an inadvertent leak might occur. One simple way to accomplish this is for the parties to agree that the buyer will not perform any diligence on the target employees using social media. This would require the buyer to obtain the necessary information another way, presumably directly from the seller or other public sources. Recognizing that this may not be practical, an alternative would be to permit the buyer to perform social media diligence, but to require that the diligence be done in a way that does not result in a "tipping off" to target employees by deploying settings that allow the searching party to remain "anonymous" to the target employees. The following provision would accomplish this objective, where "Purpose" refers to the mutual pursuit of the M&A transaction:

> The Buyer shall not use the Internet, including without limitation social networking sites, in connection with diligence or otherwise, to ascertain information about the Seller or its employees, if such practice could inform or alert any employee or consultant of the Seller that the Buyer and the Seller are engaged in discussions regarding the Purpose.

Assuming the parties are in agreement that a buyer's careless diligence practices should not create a risk of breach to the seller, the confidentiality agreement should be further modified to

reflect this allocation of risk. The appropriate provision could operate as a limited exception to the general rule described above that shifts the risk of breach to the seller for the actions of its directors, officers, employees, or agents. The following "tipping exception" serves this purpose when used in conjunction with the prior provision that restricts social media diligence:

> Notwithstanding anything to the contrary set forth herein, the Seller shall not be responsible for a breach of the confidentiality provisions of this agreement if the breach occurs directly or indirectly as a result of the Buyer engaging in activities that violate the provisions of this Agreement prohibiting the use of the Internet, including without limitation social networking sites, to obtain information about the Seller or its employees.

Related Issues

While the scenario described above may be the most obvious source of concern that arises out of Internet and social media diligence, it is certainly not the only one. There are less direct ways in which Internet and social media diligence can leave evidence trails that may provide either the buyer or the seller — or even a third party — with information that can be leveraged into an advantage in the M&A process.

For example, LinkedIn has a view box called "People Also Viewed" that leaves trails of useful business information. This view box shows some of the other profiles that viewers of a certain LinkedIn profile have also recently viewed. This view box information can be used in a variety of ways to infer useful information, none of which require much technical savvy or resourcefulness by today's standards. Using this feature, a seller might be able to ascertain whether or not the M&A team at the buyer that is viewing its employee profiles is also viewing the employee profiles of other prospective targets. This information might be used by the seller to infer that it is the sole target of the buyer. If the seller previously had reason to believe that the buyer was also looking at an alternative acquisition – and possibly using this perception as a point of leverage, whether directly or indirectly — this information might give the seller renewed conviction in the negotiation process.

Alternatively, a seller that previously thought it was the only object of the buyer's affection might look at its employee view boxes and infer that the buyer is in fact doing similar diligence on another prospective target in lieu of the seller. This knowledge could cause the seller to behave more conservatively in the negotiation process. Either way, this is meaningful information to the seller and has been provided to the seller by the buyer indirectly through its social media diligence efforts. This is by no means a one way street. The buyer could use the data to ascertain whether the seller is talking to other potential buyers. And third parties can also monitor this data to make inferences about when a specific company — buyer or seller — might be engaged in an M&A process, and with whom. All of this can be avoided if the buyer and seller either agree not to use social media diligence, or use it in a more limited or discrete manner.

While not a by-product of social networks per se, the parties should also bear in mind the fact that web analytics used by the seller can also be a source of information that could tip off its employees. Even without accessing social media, if a buyer's M&A team is spending an inordinate amount of time browsing the seller's website, web analytics tools used by the buyer will likely flag this activity to certain employees within the seller's company. This could similarly trigger broad speculation among seller employee base.

Conclusion

In summary, the use of the Internet and social media diligence poses risks to the confidentiality of an M&A process and can also leave "fingerprints" that can be used to draw other useful inferences. The stakes are high and the parties in an M&A process would be well served to consider precautions to establish mutually agreeable business processes that will be used during diligence in order to mitigate these risks. The parties should also address allocation of risk in the

event that these safeguards are not sufficient.

For more information on this topic, please contact **Jonathan D. Gworek**.