CORPORATE, TAX & TRANSACTIONAL ALERT

12/21/2017

Evaluating Privacy and Data Security Needs to be Part of Your Due Diligence Process

Given today's regulatory and commercial environment, when considering a potential acquisition, priority should be given to evaluating the target's privacy policies and data security measures. Information technology assets and data are integral components of every business, but these assets also represent a significant source of legal, business and even reputational risk. If risks are identified early in the M&A process, buyers can manage and mitigate any potential risk and liability. Attention should also be paid to post-closing integration and whether the target's systems and data should be merged with any existing systems and data that the buyer may have.

Sellers may not be able to share existing data with a buyer pre-closing, particularly if the buyer is a strategic acquirer. Despite this, buyers should be assessing the type and volume of data collected and maintained, how the data is collected and stored, how it is shared, how it is transferred, how it is disposed of, how it is protected and related data retention policies. This can help a buyer to evaluate any gaps in regulatory compliance. Particular attention should be paid to analytics performed on data, geo-location tracking, cookies and other tracking technologies used, social media and mobile platforms, as use of these technologies can represent an additional set of benefits, risks and liabilities.

Privacy concerns and data security are still an emerging source of regulatory concern. For this reason, there is no single comprehensive law governing these issues. Instead there are federal laws and regulations, state laws (with California and Massachusetts being the most restrictive), government agency guidelines on best practices, and industry self-regulatory group guidelines all regulating these issues. The SEC promulgates rules governing these issues as well. Cross-border M&A transactions can include additional regulatory schemes.

Buyers should make sure to always request the target's internal and public privacy policies, notices and statements. The target's information security policy should be assessed to determine if it meets applicable legal requirements. It is a best practice for companies that handle sensitive data to have a written information security program. Security measures should include policies, routine risk assessment, physical safeguards of the on-site premises and technical safeguards (such as user access, encryption, intrusion detection and prevention systems, and management of third-party systems such as cloud storage and data loss prevention systems).

The purchase agreement should contain standard representations and warranties regarding the target's compliance with privacy and information security laws, compliance with its own policies, absence of past breaches, any claims or disputes related to this topic and confirmation that execution of the purchase agreement will not result in any violations of these matters. If the buyer has identified any risks or liabilities through the due diligence process, it may address these concerns through pre-closing conditions, adjustments to purchase price, and post-closing indemnification provisions, possibly including a special escrow.

The corporate attorneys in Roetzel's Corporate, Tax and Transactional Group are well-versed in identifying and managing potential liabilities and risks. Please contact one of the attorneys listed below for assistance with your next acquisition.

Authors
Terrence H. Link II
tlink@ralaw.com

Connie A. Porter
cporter@ralaw.com

Manager
Christopher P. Reuscher
creuscher@ralaw.com