Global Data Privacy and Security Team

How to Avoid Buying A Data Security and Privacy Liability In An Acquisition: M&A Due Diligence At A Glance

The Federal Trade Commission ("FTC") has held acquirers responsible for the bad data security and privacy practices of the companies that they acquire. Evaluating a potential target's data privacy and security practices, however, can be daunting and complicated by the fact that many "data" issues arise months, or years, after a transaction has closed. For example, the FTC has investigated data security breaches and unlawful data collection practices that occurred long before the company was acquired.

Civil penalty imposed upon acquirer for violations of Children's Online Privacy Protection Act that occurred prior to sale.*	Number of months hackers penetrated a target's systems before the target was acquired and investigated by the FTC.†	Number of months hackers continued to penetrate a target's systems after the target was acquired and investigated by the FTC.‡
3 MILLION	**21** MONTHS	**9** MONTHS

Due diligence questions to consider in a M&A transaction:

- ☑ Has the target received a regulatory inquiry concerning its data privacy and security practices?
- ☑ Has the target received litigation claims concerning its data practices?
- ☑ Has the target tracked complaints submitted to it by consumers?
- ☑ Has the target tracked complaints submitted by consumers to the government?
- ☑ Is the target subject to a sector specific data privacy or security law?
- ☑ Does the target have an appropriate Written Information Security Program ("WISP")?
- ☑ Does the target have an appropriate Incident Response Plan ("IRP")
- ☑ How has the target dealt with prior security incidents and security breaches?
- ☑ Has the target conducted and documented internal security assessments?
- ☑ Has the target conducted and documented external security assessments?
- ☑ If the target accepted payment cards, are any vulnerabilities identified in their most recent Report on Compliance ("ROC")?
- ☑ Do the target's internal privacy policies and procedures comply with legal standards?
- ☑ Do the target's external privacy policies and procedures comply with legal standards?
- ☑ Has the target conducted a data inventory?
- ☑ Has the target conducted a data map?
- ☑ What are the target's data retention policies?
- ☑ With whom does the target share data?
- ☑ Does the target have a vendor management program in place?
- ☑ Have the vendors used by the target provided appropriate contractual protections?
- ☑ Did the target have a system in place to identify privacy or security problems?

Bryan Cave's Global Data Privacy and Security Team helps clients safely collect, utilize, transfer, and monetize data.

For more Information Contact:

David A. Zetoony
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
T: +1 202 508 6000

One Boulder Plaza
1801 13th Street, Suite 300
Boulder, CO 80302-5386 USA
T: +1 303 444 5955

BRYAN CAVE

* *United States (FTC) v. Playdom*, Case No. 11-00724 (C.D. Cal. May 11, 2011)
† *See* Complaint, In the Matter of Reed Elsevier and Seisint, FTC Docket No. C-4226 (July 29, 2008)
‡ Id.