DAVIS MALM & D'AGOSTINE P.C.

ATTORNEYS AT LAW

REGULATORY AND ADMINISTRATIVE LAW ALERT
SEPTEMBER 2015

THREE IMPORTANT LESSONS FROM THE ASHLEY MADISON DATA BREACH

Many have heard about the recent public disclosure of private information on more than 30 million individuals worldwide collected by the Ashley Madison adult networking website – whose provocative slogan is "Life is Short. Have an Affair." The disclosed information comprises registered names, email addresses, racy photographs, personal questionnaire responses on sexual topics, website transaction details, and partial (last four digits) credit card numbers.

The massive disclosure of this embarrassingly personal information offers three important lessons that extend beyond the specific facts of the Ashley Madison matter.

1. Data Security Plans Should Protect More Than Legally Protected Information.

Written information security plans typically confirm electronic and physical/operational protections for information protected under federal and state laws (i.e., legally defined personal, health, and financial information). The Ashley Madison hack provides an important reminder that data need not be protected by law to be business critical. A breach exposes the importance of such protection. In particular, companies holding trade secrets, or valuable individualized customer or vendor information, should review existing written information security plans to ensure that all business-valuable information is protected.

2. Companies Holding Sensitive Information Should Be Sure to Have Best-in-Class Security.

If your company's success largely depends on maintaining privacy of customer or registrant information, then stinting on security places your entire organization at risk. The Ashley Madison breach provides the latest and most extreme example of how a privacy-oriented business can be harmed from what appears to be lackadaisical electronic security measures. The fallout in this case included a terminated IPO process and a deluge of crippling lawsuits. An Ashley Madison competitor, Adult Friendfinder, experienced a similar breach last year. Top level electronic security and robust internal controls should be high-priority items, and protective measures should be reviewed regularly, including a response plan if a major breach occurs.

3. If You Think Your Organization is Immune to Such a Breach, Think Again.

The reality is that businesses have competitors, organizations have opponents, and any privacy-sensitive business or organization that holds valuable or sensitive personal information of individuals is at risk of having that information exposed, with business-affecting consequences. Even though this is particularly true for organizations that have long maintained tight privacy controls such as adult websites, abortion and reproductive care facilities, controversial public

policy groups, and LGBT rights organizations, similar concerns could apply to law and accounting firms, health clubs and fitness facilities, and a wide variety of online shopping sites. All possess information that could damage the organization if made public.

CONTACT

If you have questions about this alert, please contact one of the authors, Robert J. Munnelly, Jr. or Craig D. Levey, or a member of our Regulatory and Administrative Law Practice.

One Boston Place, Boston, Massachusetts 02108 | phone 617.367.2500 | fax 617.523.6215 | info@davismalm.com.