Shook, Hardy & Bacon L.L.P.

SEPTEMBER 13, 2012

DATA SECURITY ALERT

PRIVATE LAWSUITS ARISING FROM DATA BREACHES – THE ELEVENTH CIRCUIT WEIGHS IN

Last week, the United States Court of Appeals for the Eleventh Circuit decided *Resnick v. AvMed, Inc.*, No. 11-13694 (11th Cir. Sep. 5, 2012). The Court's opinion addresses some important issues regarding an individual's right to bring a private lawsuit when her personally identifiable information or protected health information is compromised. In its decision, the Court reversed the dismissal of all but two counts in a class action lawsuit that arose from a data breach suffered by an integrated managed care organization.

Background

AvMed, Inc., an integrated managed care organization was the victim of a theft. Two of AvMed's unencrypted laptops containing PHI and PII for approximately 1.2 million current and former AvMed members (Plaintiffs) were stolen. Plaintiffs alleged that an unknown third party used their information for fraudulent purposes 10 to 14 months after the theft.

The operative complaint alleged the following causes of action: negligence, breach of implied and express contracts, unjust enrichment, negligence *per se*, breach of fiduciary duty, and breach of implied covenant of good faith and fair dealing.

The Southern District of Florida dismissed the lawsuit, in part because the complaint failed to allege cognizable injury. The Eleventh Circuit has now reversed the trial court's dismissal on all but two counts, holding that Plaintiffs had standing, alleged a cognizable injury, and adequately alleged causation.

Standing

The Court first addressed the issue of whether Plaintiffs had standing. The Court held that Plaintiffs alleged all three elements necessary to meet the standing requirement:

- **Plaintiffs suffered an injury in fact** – they were victims of identity theft and suffered monetary damages

Shook, Hardy & Bacon understands companies face challenges securing information in an increasingly electronic world.

SHB guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage risks associated with maintaining and using electronic information.

For more information on SHB's data security and data privacy services, please contact:

Al Saikali
(305) 960-6923
asaikali@shb.com

- **Plaintiffs' injuries were "fairly traceable to AvMed's actions"** – Plaintiffs had personal habits of securing their sensitive information yet became the victims of identity theft after the laptops containing their PHI were stolen
- **A favorable resolution of the case in Plaintiffs' favor could redress their injuries** – compensatory damages would redress their injuries.

Cognizable Injury

The Court next dealt with the issue of whether Plaintiffs suffered a cognizable injury. Plaintiffs alleged the following damages: money spent placing alerts with various credit reporting companies, money spent contesting fraudulent charges, money spent purchasing credit monitoring services, lost wages for missing work while filling out police reports, travel related costs, cell phone minutes, postage, and overdrawn amounts in their bank accounts. The Court held that Plaintiffs' allegations of monetary loss and financial injury were cognizable injuries under Florida law, though the Court did not address the validity of each one of these damages elements separately.

Causation

The Court then addressed causation – whether Plaintiffs had alleged sufficient facts showing that the theft of the AvMed computers caused Plaintiffs' injuries. The Court held that Plaintiffs' allegations were sufficient to show that causation was "plausible". Specifically, the Court relied on three allegations: (1) before the breach, Plaintiffs never had their identities stolen or sensitive information compromised; (2) before the breach, Plaintiffs took substantial precautions to protect themselves from identity theft; and, (3) Plaintiffs became the victims of identity theft for the first time in their lives 10 to 14 months after the laptops containing the PHI were stolen.

A key fact for the Eleventh Circuit was that the sensitive information on the stolen laptops was the same sensitive information used to steal Plaintiffs' identity.

With respect to unjust enrichment (the one count that did not require causation), Plaintiffs alleged that a portion of Plaintiffs' monthly premiums went towards AvMed's data security administrative costs, and AvMed should not be permitted to retain that money because AvMed failed to implement proper security measures. The Court allowed this count to proceed.

The Dismissed Counts

The Eleventh Circuit did, however, affirm the dismissal of Plaintiffs' negligence *per se* and breach of covenant of good faith and fair dealing. The negligence *per se* count was based on an allegation that AvMed violated Section 395.3025, Florida Statutes, by disclosing Plaintiffs' health information without authorization. The Court held that because AvMed is a managed-care organization and not

a hospital, ambulatory surgical center, or mobile surgical facility, it was not subject to the statute. The Court dismissed the breach of covenant of good faith and fair dealing count because any failure by AvMed to secure Plaintiffs' data did not result from a "conscious and deliberate act" on AvMed's part.

The Dissent

The opinion included a vigorous dissent that argued Plaintiffs had failed to allege a plausible basis for finding that AvMed caused Plaintiffs to suffer identity theft. The dissenting judge observed that an obvious alternative explanation for the identity fraud existed – an unscrupulous third party that possessed the Plaintiffs' sensitive information might have sold it to identity thieves who opened the fraudulent accounts, or a careless third party might have lost the information that then found its way into the hands of those thieves.

What Are The Takeaways?

First, it is important to note that as of the date of this alert, the opinion is not yet final. That said, the opinion in its current form could lead to a dramatic uptick in data security litigation within the Eleventh Circuit, as plaintiffs will likely use the opinion to argue that the bar for causation in such cases is low and cognizable damages can be extensive (and arguably speculative).

Companies maintaining personally identifiable information and protected health information about residents in the Southeast United States would be well served to ensure that they are taking proactive steps to implement reasonable data security measures in an effort to avoid a data breach. In this instance, for example, encryption of the subject laptops might have prevented the subject lawsuits. ■

For more information about these and other issues relating to data security law, visit Al's blog at www.datasecuritylawjournal.com.

OFFICE LOCATIONS

Geneva, Switzerland
+41-22-787-2000
Houston, Texas
+1-713-227-8008
Irvine, California
+1-949-475-1500
Kansas City, Missouri
+1-816-474-6550
London, England
+44-207-332-4500
Miami, Florida
+1-305-358-5171
Philadelphia, Pennsylvania
+1-215-278-2555
San Francisco, California
+1-415-544-1900
Tampa, Florida
+1-813-202-7100
Washington, D.C.
+1-202-783-8400