

American Health Information Management Association

<http://journal.ahima.org/2009/02/06/va-to-pay-20-million-in-data-breach-case/#more-157>

- Journal of AHIMA - <http://journal.ahima.org> -

VA to Pay \$20 Million in Data Breach Case

Posted By [Kevin Heubusch](#) On February 6, 2009 @ 7:31 am In [Compliance](#), [Privacy and security](#) |

Last week the Department of Veterans Affairs announced it would pay \$20 million to settle a class action lawsuit resulting from a stolen laptop. The case resonated with a [data breach story](#) ^[1] *Journal* writer Chris Dimick had just written for the current print issue, and he circled back with two law experts featured in the story to get their comments.

First a little background. In 2006 a VA employee took home a laptop that included unencrypted personal information for approximately 26.5 million vets. Several teenagers broke into the employee's house and made off with the laptop.

The employee notified his superiors immediately, but the VA took nearly three weeks to warn vets that their information was at risk.

At that point the story hit the news, which appeared to be the first time that the teens learned there was a treasure trove of names, birth dates, and Social Security numbers on the laptop. About a month later the laptop made its way to the FBI, turned in by an unidentified person seeking the \$50,000 reward. Shortly thereafter, two teens were charged in the theft, with charges pending on another suspect.

There was no happy ending, though. The VA, already no stranger to criticism of its security practices, was subject to a harsh report from its own inspector general. The story played large in the mainstream press, several VA officials were fired, and finally the VA was hit with a class action lawsuit.

Delay at Fault

The agreement is a mediated settlement in which the VA admits no wrongdoing, violation of the privacy act, or any other legal basis for liability. However, its past history of neglecting its information security needs appears to have provided a basis for claims under the privacy act, says [Alan Wernick](#) ^[2], Esq., of Wernick and Associates in Northbrook, IL.

Wernick notes that in 2004 the VA was cited as failing to comply with the Federal Information Security Management Act requirements and in that year and the following it received failing grades from the House Government Reform Committee on its information and computer security programs.

[Reece Hirsch](#) ^[3], JD, is a partner with Sonnenschein Nath & Rosenthal LLP, based in San Francisco, CA. He finds it interesting that the VA settled out of court even though the laptop was recovered and there was no evidence that harm was done. But like Wernick, he notes the VA had a documented history of poor security practices. The reprimand by its own inspector general clearly didn't help its case.

It was the VA's delay in notifying vets that was likely the key fault in the case. "The mistake that seems to be made was the VA's failure to move promptly after the organization had knowledge of the laptop theft," Hirsch says.

Settling the case may also have been a statement to vets, Hirsch suggests. "It looks like the federal government and the VA wanted to send a clear message that they take this seriously," he says. Settling the case "could be a way of showing the veterans they are serious about this."

A Lesson to Take to Heart

The VA case is "something organizations can take to heart," Hirsch says. With weak security policies and apparently no response plan in place, the breach went from bad to worse.

Wernick notes that published reports suggest the VA did not have a data breach plan in place and did not provide staff with adequate (if any) training on handling a data breach.

That's the moral of the story for Wernick. Organizations with sound security policies and procedures in place are more likely to prevent or limit breaches and more likely to respond quickly and effectively when they do happen, he says.

The FCC's [red flags rule](#) ^[4], which go into effect May 1, should help address this gap, Wernick notes. The rule requires organizations that act as creditors (which includes most healthcare organizations) to have identity theft prevention programs in place.

Hirsch finds a similar moral to the VA's story. "You have to be prepared to respond quickly to a breach," he says. "If a member of an organization has knowledge of an incident and you are not in a position to send a breach notice, it could lead to litigation."

The very magnitude of data holdings like the VA's only adds to the necessity.

"With such a large group of people, it is not an easy thing to prepare for a notification, but that is why you need to have a breach plan in place," Hirsch says.

Article printed from Journal of AHIMA: <http://journal.ahima.org>

URL to article: <http://journal.ahima.org/2009/02/06/va-to-pay-20-million-in-data-breach-case/>

URLs in this post:

[1] data breach story:

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_042628.hcsp?dDocName=bok1_042628

[2] Alan Wernick: **<http://www.wernick.com>**

[3] Reece Hirsch: **<http://www.sonnenschein.com/attorneys/index.aspx?aid=0003540>**

[4] red flags rule: **<http://journal.ahima.org/2008/11/21/a-closer-look-at-the-red-flag-rules/>**

© 2008 American Health Information Management Association