The law allows for penalties of up to $5,000 for improper disposal. The attorney general alone has the authority to pursue violations of the law. There is no private cause of action.

Case Studies and Examples

The following case highlights unclear federal policies about data breach notification. At the time of this incident, federal law did not require agencies to have breach notification policies. There's still no federal law that requires this. However, due to this incident, most federal agencies have implemented internal breach notification policies.

In 2006, an employee of the U.S. Department of Veterans Affairs (VA) took home a laptop computer and external hard drive. The hard drive held the personal information of every veteran discharged since 1975. It was not encrypted. On May 3, 2006, the employee's home was burglarized. Thieves stole the laptop and hard drive. The local police department investigated the burglary.

> **NOTE**
> The U.S. Department of Veterans Affairs is also called the Veterans Administration (VA).

The employee immediately informed his supervisors about the theft. They didn't take the matter seriously. The secretary of the VA didn't learn about it until almost two weeks later. The VA secretary notified the Federal Bureau of Investigations (FBI) about the theft. The FBI began to investigate the theft with the local police department.

The VA issued a statement about the theft on May 22, 2006. It reported the facts about the theft. It also said that the data stolen included names, Social Security numbers, and dates of birth for 26.5 million veterans. It included data on some of their spouses. At the time, the VA reported that the hard drive didn't contain any health or financial information.

Congress was outraged that the VA waited so long to make a public statement. On May 25, 2006, the secretary of the VA appeared at hearings before the U.S. House and Senate to discuss the issue. In his Senate testimony, he stated that he was furious that he was not notified in a timely manner. He also stated that the VA was planning to notify all people affected by the theft. He said that it would take time to prepare the mailing because the VA had to verify addresses. He also said that 26 million envelopes "were not immediately available." The VA began mailing the notification letters on June 9, 2006.

As it carried out its investigation, the VA learned that the hard drive held some health information for 2.6 million people. It also learned that the hard drive contained the personal information of active-duty military personnel.

On June 6, 2006, the VA reported that the hard drive held the data of 1.1 million active-duty troops. It also had information on 430,000 members of the National Guard and 645,000 members of the Reserves.

The police recovered the stolen laptop and hard drive in late June 2006. The FBI reported that a forensic review of the equipment showed that the database containing the personal information hadn't been accessed. In August 2006, the VA mailed a follow-up letter to people affected by the event.

FYI

You can read the VA press release on the incident at *http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1123.*

You can read the Senate Hearing testimony at *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_senate_hearings&docid=f:28754.pdf.*

You can read the VA Inspector General report at *http://www.va.gov/oig/pubs/VAOIG-06-02238-163.pdf.*

You can read the settlement agreement at *http://www.gpo.gov/fdsys/pkg/USCOURTS-dcd-1_06-mc-00506/pdf/USCOURTS-dcd-1_06-mc-00506-0.pdf.*

The VA Inspector General investigated the incident. It found that the VA employee wasn't permitted to take the laptop or hard drive home. The report faulted the employee for using poor judgment in taking the data home. It also faulted the employee for not properly protecting it. The report also criticized VA supervisors for not taking initial reports about the data loss seriously.

In August 2006, police arrested two adults for the theft. Both men pleaded guilty in December of that year. In March 2007, each man was sentenced to six months in prison for stealing the computer equipment. They also were sentenced to three years of probation.

In January 2009, the VA agreed to pay $20 million to veterans whose information was potentially exposed in the incident. It paid this amount to settle lawsuits brought by five veterans groups. The money was used to create a compensation fund. Veterans who wished to make a claim against the fund needed to file claims by November 27, 2009.

Congress created the Veterans Affairs Information Security Act of 2006 in response to the breach. The law requires the VA to create a comprehensive information security program. It also requires it to create breach notification regulations. The VA issued those regulations in April 2008. They require the VA to notify people in the event of a security breach if there's a reasonable risk for the potential misuse of their personal information.[50]

NOTE

The U.S. Government Accountability Office released a report on lessons learned from the 2006 VA incident. You can read the report at *http://www.gao.gov/new.items/d07657.pdf.*