

**Embed Ensemble. Make applications richer, without rewriting.**

[Click Here For A Demonstration.](#)



**InformationWeek**  
BUSINESS INNOVATION POWERED BY TECHNOLOGY

## VeriSign Worker Fired After Laptop, Employee Info Are Stolen

The computer held unencrypted information on VeriSign's current and former employees.

By Sharon Gaudin, [InformationWeek](#)

Aug. 7, 2007

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=201203456>

A contract worker for VeriSign no longer works for the security company after her laptop, which held employee information, was stolen from her car.

The woman, who worked in VeriSign's human resources department, failed to comply with company policies that mandate that data be encrypted and that employee information not be downloaded on laptop computers, according to Caroline Japic, a spokeswoman for VeriSign, in an interview. Japic added that the employee's contract was not renewed. She said she had no information on whether the contract was terminated prematurely or if it just happened to expire soon after the theft was reported.

[VeriSign](#), which is based in Mountain View, Calif., offers security services, including digital certificates and managed firewalls. The company also runs a range of network infrastructures, including two of the Internet's 13 root servers.

The employee, who was not identified, reported to VeriSign and to local police in Sunnyvale, Calif. that she had left her laptop in her car and had parked her car in her garage on Thursday, July 12. When she went out the next morning, she found that her car had been broken into and the laptop had been stolen.

Japic said the worker contacted police and then reported the theft to her employer who also contacted police and began their own internal investigation.

The laptop, according to the spokesman, did not contain information on any of the company's customers but did hold information on current and former employees. Their names, Social Security numbers, dates of birth and salaries were contained, and unencrypted, on the laptop.

While Japic said she did not know how many people were affected by the security breach, she did say that all of VeriSign's employees were notified of the breach. Everyone affected has been offered a year of free credit monitoring.

"The Company has a policy on how to manage laptops that contain sensitive information and company data, which in this case was not followed," the company said in a written statement. "That policy includes not leaving laptops in vehicles in plain view, keeping the amount of confidential and sensitive data stored on laptops to a minimum, and using data encryption tools to protect those sets of data that absolutely must be stored on a laptop. Going forward, we will continue to review our security procedures to prevent future human errors of this type."

Japic said the investigation into the stolen laptop is ongoing.

Last December, [Boeing fired an employee whose stolen laptop](#) contained identifying information on 382,000 current and former employees.

The employee, who hasn't been identified, was fired because he violated company policy by downloading the information onto the laptop and not encrypting it. This was the third laptop theft in two years that resulted in lost employee data at

**Boeing.**

**Business VoIP Guide** - Free 80 page Business VoIP Guide.  
Immediate access. Download now. [ShoreTel.com/BusinessVoIPGuide](http://ShoreTel.com/BusinessVoIPGuide)

[Ads by Google](#)

[Advertise on this site](#)

Copyright © 2007 [CMP Media LLC](#)