

MyLaptopGPS and Identity Theft Expert: Loss of Laptops Belonging to Health Insurers Have Placed Hundreds of Thousands at Risk of Medical Identity Theft

(BOSTON, Mass. - Feb. 7, 2008 - IDTheftSecurity.com) News reports over the past month indicated that the loss of laptop computers from just three health insurance organizations placed hundreds of thousands of data records in the hands of thieves. All firms with fleets of mobile computing devices need technology like MyLaptopGPS™, which both tracks and deletes sensitive data from missing machines, said Robert Siciliano, a widely televised and quoted personal security and [identity theft](#) expert.

"Thefts of laptop computers from health insurance organizations is nothing new," said Siciliano. "Plenty of examples of this stretch back over the past several years. But familiarity should not breed complacency. If anything, medical information is among the worst types of data to be lost to thieves. For instance, a fraudulently obtained clean health record might help someone with pre-existing conditions obtain health insurance. The right kind of medical record might qualify other thieves for prescription drugs they should have no access to."

CEO of IDTheftSecurity.com and a member of the *Bank Fraud & IT Security Report's* editorial board, Siciliano leads Fortune 500 companies and their clients in workshops that explore consumer education solutions for security issues. A longtime identity theft speaker and author of "The Safety Minute: 01," he has discussed data security and consumer protection on CNBC, on NBC's "Today Show," FOX News, and elsewhere.

Laptop thefts from three health insurance companies made news over the past month:

- The Associated Press reported on Jan. 30 that Horizon Blue Cross Blue Shield had notified 10 percent of its New Jersey customer base of a [laptop computer theft](#). The machine stored more than 300,000 records containing customers' names, Social Security numbers, and other information. On the same day, *InformationWeek* noted that Horizon Blue Cross had invoked a security feature that, according to an unnamed spokesperson for the company, "destroys all the data on the stolen computer" (a functionality MyLaptopGPS shares).
- A Jan. 25th article in the *Boston Herald* reported that a laptop computer containing information on Medicare information on nearly 30,000 customers of Fallon Community Health had gone missing to thieves. Names, dates of birth, some diagnostic information and medical ID numbers were on the machine, which belonged to a third-party contractor that manages Fallon's medical claims. Medical ID numbers, a report from the previous day in *Boston Business Journal* said, are sometimes based on Social Security numbers.
- On Jan. 22, the *Connecticut Post Online* reported the theft of a mobile computer from Health Net, Inc., a large, U.S.-based managed health care provider. The machine contained Social Security numbers and other identifying data on an undisclosed number of Health Net employees, the article noted, quoting a spokesperson saying the "problem... could affect several thousand people." The report went on to quote another health insurance professional, who noted that physicians are "major targets for embezzlement and identity theft."

"Effective technology for laptop computer security can be exceedingly inexpensive to purchase and easy to install," said Dan Yost, chief technology officer at MyLaptopGPS. "Organizations that leave their highly vulnerable mobile computing devices bereft of security technology have little reason to do so. At an affordable price that dwarfs the potential cost of just one laptop theft, MyLaptopGPS secures an entire laptop computer fleet against theft."

[MyLaptopGPS](#) combines Internet-based GPS tracking -- which, for tracking and retrieving stolen laptops, is more effective than other forms of GPS -- with other functionalities to secure mobile computing devices. Users launch MyLaptopGPS' features remotely, protecting data even while the machine is in a criminal's hands. Once connected to the Internet, the software silently retrieves, and then deletes, files from machines as it tracks the stolen or missing hardware -- at once returning the data to its rightful owner and removing it from the lost computer.

MyLaptopGPS also offers SafeRegistry™, a comprehensive system for inventorying entire fleets of mobile computers, as well as a full line of highly renowned SafeTags™, which are police-traceable property tags designed to secure iPods, cell phones, BlackBerry devices, and other mobile property. A [downloadable demo](#) of MyLaptopGPS is available.

The October 2007 issue of *Bank Fraud & IT Security Report*, a newsletter published only in hard copy, ran "The Seven Layers of Laptop Security," an article by Siciliano and Yost. A white paper adaptation of that article [is available](#) from MyLaptopGPS.

Readers may [view YouTube video](#) of "NBC 7 Chicago" footage featuring Yost delivering comments for a televised news report that covered the April 2007 theft of two laptops that stored 40,000 Chicago Public School teachers' Social Security numbers.

According to *USA Today*, theft of personal data more than tripled in 2007. Readers may [view video of Siciliano](#) discussing this news on the new "FOX Business" network. To learn more about identity theft, a major concern for anyone who's lost a laptop computer to thieves, readers may go to [video of Siciliano at VideoJug](#).

###

About MyLaptopGPS

Since 1984, Tri-8, Inc. (DBA MyLaptopGPS.com) has specialized in complete system integration. From real-time electronic payment processing software to renowned mid-market ERP implementations, the executive team at MyLaptopGPS has been serving leading enterprises and implementing world-class data systems that simply work. With MyLaptopGPS™, Tri-8, Inc. brings a level of expertise, dedication, knowledge and service that is unmatched. MyLaptopGPS™'s rock-solid performance, security, and reliability flow directly from the company's commitment to top-notch software products and services for almost 25 years.

About IDTheftSecurity.com

Identity theft affects us all, and Robert Siciliano, CEO of IDTheftSecurity.com and member of the *Bank Fraud & IT Security Report*'s editorial board, makes it his mission to

provide consumer education solutions on identity theft to Fortune 500 companies and their clients. A leader of personal safety and security seminars nationwide, Siciliano has been featured on "The Today Show," CNN, MSNBC, CNBC, "FOX News," "The Suze Orman Show," "The Montel Williams Show," "Maury Povich," "Sally Jesse Raphael," "The Howard Stern Show," and "Inside Edition." The Privacy Learning Institute features him on its Website. Numerous magazines, print news outlets, and wire services have turned to him, as well, for expert commentary on personal security and identity theft. These include *Forbes*, *USA Today*, *Entrepreneur*, *Woman's Day*, *Mademoiselle*, *Good Housekeeping*, *The New York Times*, *Los Angeles Times*, *Washington Times*, *The Washington Post*, *Chicago Tribune*, *United Press International*, *Reuters*, and others.

For more information, visit Siciliano's [Web site](#), [blog](#), and [YouTube page](#).

The media are encouraged to get in touch with any of the following individuals:

John Dunivan
MyLaptopGPS Media Relations
PHONE: (405) 747-6654 (direct line)
jd@MyLaptopGPS.com
<http://www.MyLaptopGPS.com>

Robert Siciliano, Personal Security Expert
CEO of IDTheftSecurity.com
PHONE: 888-SICILIANO (742-4542)
FAX: 877-2-FAX-NOW (232-9669)
Robert@IDTheftSecurity.com
<http://www.idtheftsecurity.com>

Brent W. Skinner
President & CEO of STETrevisions
PHONE: 617-875-4859
FAX: 866-663-6557
BrentSkinner@STETrevisions.biz
<http://www.STETrevisions.biz>