

Justice Breyer Is Among Victims in Data Breach Caused by File Sharing

By Brian Krebs
washingtonPost.com Staff Writer
Wednesday, July 9, 2008; A01

Sometime late last year, an employee of a McLean investment firm decided to trade some music, or maybe a movie, with like-minded users of the online file-sharing network LimeWire while using a company computer. In doing so, he inadvertently opened the private files of his firm, Wagner Resource Group, to the public.

That exposed the names, dates of birth and Social Security numbers of about 2,000 of the firm's clients, including a number of high-powered lawyers and Supreme Court Justice Stephen G. Breyer.

The breach was not discovered for nearly six months. A reader of washingtonpost.com's [Security Fix](#) blog found the information while searching LimeWire in June.

Services such as LimeWire, which are known as peer-to-peer networks, link computers directly, allowing users to swap digital movies, music and files with other users without the need of a central Web site to manage the exchange.

What users may not be aware of is that the software that facilitates file sharing may be configured to allow access to a portion, if not all, of a user's documents.

Robert Boback, chief executive of Tiversa, the company hired by Wagner to help contain the data breach, said such breaches are hardly rare. About 40 to 60 percent of all data leaks take place outside of a company's secured network, usually as a result of employees or contractors installing file-sharing software on company computers.

"We've seen a lot of instances where a company will be working on a product that's not even released yet, and the diagrams for that product are already out on the Net," Boback said. "This case is unique because of the high profile of the targets. The individuals on this list are at a very high risk, almost imminent, of identity theft."

In June, medical records and Social Security numbers for at least 1,000 patients at [Walter Reed Army Medical Center](#) were exposed in a peer-to-peer data breach. In June 2007, the pharmaceutical giant [Pfizer](#) disclosed that an employee who installed peer-to-peer software on a company laptop exposed files containing the names, Social Security numbers, addresses and some compensation information of 17,000 current and former Pfizer employees.

In March, a Seattle man was sentenced to 51 months in prison for using LimeWire and similar networks to dig up personal and financial information on more than 50 people, which he then used to open lines of credit in the victims' names.

Tiversa officials found that more than a dozen LimeWire users in places as far away as Sri Lanka and Colombia downloaded the list of personal data from the Wagner network.

"To me, this was devastating," said Phylp Wagner, founder of the investment firm. "I didn't even know what peer-to-peer was. I do now."

A spokesman for Breyer said the justice had no comment on the security breach, which came to light after the reader notified Security Fix and the blog alerted some of the Wagner clients.

Wagner said his company has contracted with FirstAdvantage of Poway, Calif., which last week sent out letters notifying affected clients of the breach and offering each six months of free credit-report monitoring. He emphasized that the peer-to-peer disclosure never endangered his clients' financial records, which are stored by a separate company. But that may be small consolation to several lawyers on the list who said they recently experienced unexplained financial activity.

"This may explain why two weeks ago I got a \$9,000 cellphone bill from AT&T," said Steven Agresta, a partner with the law firm Alston & Bird. Someone had opened a phone account using his date of birth and Social Security number, but with a different address.

Agresta said AT&T promptly canceled the account and the bogus charges, but he's still checking his credit history and other accounts for signs of fraud.

Of the 2,000 records from Wagner Resource Group that were found online, 700 included Social Security numbers, names and birth dates, while other records included only one or two of those details.

Brian Krebs writes the Security Fix blog, at <http://blog.washingtonpost.com/securityfix>.