



# NEWS RELEASE

OFFICE OF THE UNITED STATES ATTORNEY  
WESTERN DISTRICT OF MISSOURI

**TODD P. GRAVES**

---

Contact Don Ledford, Public Affairs • (816) 426-4220 • 400 East Ninth Street, Room 5510 • Kansas City, MO 64106

[www.usdoj.gov/usao/mow](http://www.usdoj.gov/usao/mow)

---

**NOVEMBER 19, 2003**  
**FOR IMMEDIATE RELEASE**

## **BELTON MAN INDICTED FOR COMPUTER HACKING**

**KANSAS CITY, Mo.** – Todd P. Graves, United States Attorney for the Western District of Missouri, announced that a Belton, Mo., man was indicted by a federal grand jury today for the unauthorized computer intrusion at Aventis Pharmaceuticals.

**Thomas S. Millot**, 45, of Belton, Mo., was charged in a single-count indictment returned by a federal grand jury in Kansas City. **Millot** was employed as an NT Information Technology security officer at Aventis' office in Kansas City until Oct. 2, 2000. In that position, Graves explained, **Millot's** primary duties at Aventis were to maintain security access for user accounts, detect and investigate intrusions into the Aventis computer network, and provide information technology security consulting to Aventis.

Aventis is a multi-national maker of pharmaceuticals, based in Strasbourg, France, with offices worldwide, including Kansas City. Those offices are linked together by a network computer system, Graves explained, which means that any computer or server connected to the Aventis network is a "protected computer" under federal law.

The federal indictment alleges that **Millot** gained unauthorized access to the Aventis computer network on nine separate occasions between Dec. 16, 2000, and Aug. 26, 2002, including five occasions after **Millot** left employment with the company.

On Dec. 16, 2000, **Millot** allegedly deleted an Aventis associate's account from the computer network.

According to Graves, it cost Aventis more than \$5,000 to conduct a damage assessment of, verify the security of, and restore the integrity of the Aventis network computer system following the discovery of the unauthorized computer intrusion.

Graves explained that users who want to obtain remote access to the Aventis computer system must have an account PIN number along with an RSA secure ID token number. The secure ID token generates a random number every minute, which the user then enters as a password to access the computer system. While a member of the Access Management Group at Aventis, **Millot** was in charge of assigning secure IDs to employees, as well as maintaining the software that synchronized the RSA secure ID card numbers to the various user accounts.

The federal indictment alleges that on Aug. 18, 2000, **Millot** assigned an RSA card number to the account of a former employee based in Frankfurt, Germany, who had left the company in January 2000. **Millot** then allegedly reset the PIN, and synchronized the card with the server. **Millot** used that account and RSA card access the Aventis system, the indictment alleges.

Graves cautioned that the charge contained in the indictment is simply an accusation, and not evidence of guilt. Evidence supporting the charge must be presented to a federal trial jury, whose duty is to determine guilt or innocence.

The case is being prosecuted by Assistant U.S. Attorney Gene Porter. It was investigated by the Federal Bureau of Investigation.

\*\*\*\*\*

This news release, as well as additional information about the office of the United States Attorney for the Western District of Missouri, is available on-line at  
[www.usdoj.gov/usao/mow](http://www.usdoj.gov/usao/mow)