

Ex-employee of Supplier Is Charged in ID Theft
Jim Henry
Automotive News
December 2, 2002

NEW YORK -- The trail in the nation's biggest-ever identity theft case led from Michigan to New York, as federal agents last week arrested three suspects, including an ex-employee of a software supplier of Ford Motor Credit Co.

Federal officials said at least \$2.7 million in losses have been identified; they estimated that there could be more than 30,000 victims.

One suspect, Philip Cummings, worked for Teledata Communications Inc. in Bay Shore, N.Y. Teledata provides Ford Credit and other companies with software for retrieving consumer credit histories from credit bureaus such as Experian of Costa Mesa, Calif.

In May 2002, Ford Credit disclosed that someone electronically impersonating the credit company had gained access to about 13,000 Experian credit reports from April 2001 to February 2002. According to a complaint filed by the U.S. Attorney's office in New York, that was Cummings, who left Teledata in March 2000 and lives in Georgia.

The complaint said Cummings obtained a Ford Credit password while working on a customer help desk at Teledata. That allegedly allowed him to order credit histories, with the bill going to Ford Credit. Cummings allegedly sold the data to other suspects, who allegedly used the records fraudulently to order checks, automated teller machine cards and credit cards. The complaint said Cummings continued to obtain data via a laptop computer even after he left Teledata.

Officials said the other suspects are Hakeem Mohammed of the Bronx, who was arrested Oct. 29 and has pleaded guilty to mail fraud and conspiracy; and Linus Baptiste of New Rochelle, N.Y.

The complaint said there may be 20 or more suspects in New York in Brooklyn and the Bronx.

Ford Credit spokeswoman Melinda Wilson said that the suspects did not use the data to obtain car loans, as far as Ford Credit is aware.

Records also were obtained from other credit bureaus and in the name of other lenders, officials said.

"The defendants took advantage of an insider's access to sensitive information in much the same way that a gang of thieves might get the combination to a bank vault from an insider," U.S. Attorney James Comey said in a written statement. "Using the same technology, we determined what was done and who did it, proving that technology is a double-edged sword."