November 25, 2002

U.S. Department of Justice
United States Attorney
Southern District of New York
Marvin Smilon, Herbert Hadad
Michael Kulstad
Public Information Office
(212) 637-2600
(718) 422-1870
Katherine M. Choo
(212) 637-2414
Julie Schriebman
(212) 637-2570
Harry Chernoff
(212) 637-2481

U.S. Announces What Is Believed The Largest Identity Theft Case In American History; Losses Are In The Millions

JAMES B. COMEY, the United States Attorney for the Southern District of New York, and KEVIN P. DONOVAN, the Assistant Director in Charge of the New York Field Office of the FBI, today announced the arrest of a defendant, PHILIP CUMMINGS, in what authorities believe to be the largest identity theft case in U.S. history. Mr. COMEY also announced the arrest of LINUS BAPTISTE and the guilty plea of HAKEEM MOHAMMED in related cases.

In a Complaint unsealed today, the United States charged PHILIP CUMMINGS with wire fraud and conspiracy in connection with his participation in a massive identity theft scheme that spanned nearly three years and involved more than 30,000 victims. As alleged in the Complaint, CUMMINGS worked at Teledata Communications Inc. ("TCI"), a company in Long Island that provided the computerized means for banks and other entities to obtain consumer credit information from the three commercial credit history bureaus → Equifax, Experian and TransUnion. TCI provided software and other computerized devices to its client companies that enabled these companies, through the use of confidential computer passwords and subscriber codes, to access and download credit reports of consumers for legitimate business purposes.

As alleged in the Complaint, CUMMINGS worked at TCI from about mid-1999 through about March 2000 as a Help-Desk employee, and was responsible for helping TCI's clients. As such, he had access to these companies' confidential passwords and codes. With these codes, he had the ability to access and download credit reports himself, it was charged.

As alleged in the Complaint, starting in early 2000, CUMMINGS agreed to provide credit reports to a co-conspirator who is now a cooperating witness in the investigation ("CW"), in return for money. CW knew individuals who were willing to pay up to $60 per credit report, and CW offered to split that money with CUMMINGS, it was charged. Thereafter, CW dealt with 20

or more individuals in the Bronx and Brooklyn, who would bring lists to CW filled with names and addresses and/or Social Security numbers, and would ask CW to provide credit reports in those people's names. They would then pay him $60 for each credit report that he was able to provide to them, it was charged, and CW, in turn, would split that money with CUMMINGS.

As alleged in the Complaint, when CW began receiving lists from these co-conspirators in the beginning, he would contact CUMMINGS, and CUMMINGS would bring a laptop computer to the CW's home in New York and download the credit reports and give them to CW. CW in turn would sell them to his co-conspirators on the street.

At some point in 2000, CUMMINGS moved to Georgia but allegedly ensured that the scheme could continue by traveling to New York to download credit reports for CW and then later giving a pre-programmed laptop computer to CW for CW to use to download the reports. He also allegedly taught CW how to access the Credit Bureaus and download the reports.

As alleged in the Complaint, CUMMINGS provided passwords and codes to CW that enabled CW to access all three Credit Bureaus → Equifax, TransUnion and Experian → over time. At various points in the scheme, when CW found that a code and password that CW had been using no longer worked, he allegedly called CUMMINGS. CUMMINGS would then allegedly give him a new password and code to use to continue the scheme. This happened on numerous occasions, th Government charged.

According to the complaints, the other co-conspirators to whom CW sold the credit reports provided, in the aggregate, tens of thousands of names and hundreds of thousands of dollars to CW for consumer credit reports. CW provided the credit reports to these other co-conspirators and split the money that they provided to CW with CUMMINGS.

One entity whose confidential TCI password and subscriber code were allegedly misappropriated in the scheme was Ford Motor Credit Corp. at its Grand Rapids, Michigan, branch. That branch's password and code were used for approximately 10 months to download approximately 15,000 credit reports from Experian. Ford discovered the scheme after reviewing bills sent by Experian for those credit histories and receiving numerous complaints from consumers who had been the subject of identity theft and fraud. After searching its databases, Experian found that the passwords and subscriber codes of Washington Mutual Bank in Florida and Washington Mutual Finance Company in Crossville, Tennessee, had also been compromised, resulting in approximately 6,000 more credit reports for consumers being improperly downloaded.

According to the Complaint, Equifax determined that the password and subscriber codes for Ford's Decatur, Illinois, branch had been used improperly to download 1,300 credit reports from its databases in September and October 2002. The passwords and codes of Washington Mutual Finance's branch in St. Augustine, Florida, were used to download another 1,100 credit reports, and more than 4,000 additional credit reports were downloaded using the passwords and codes of six more entities: Dollar Bank in Cleveland, Ohio; Sarah Bush Lincoln Health Center in Illinois; the Personal Finance Company in Frankfort, Indiana; the Medical Bureau in Clearwater, Florida; Vintage Apartments in Houston, Texas; and Community Bank of Chaska in Chaska, Minnesota.

As alleged in the Complaint, Central Texas Energy Supply's codes were used improperly to download approximately 4,500 credit reports from TransUnion in September 2002.

All of the companies described above whose codes were compromised and misused have all been confirmed as TCI client companies, according to the Complaint.

As alleged in the Complaint, the number of victims in this case exceed 30,000, and the Government is in the process of determining the extent of the loss. To date, more than $2.7 million in financial loss has been confirmed. Consumers whose credit reports have been stolen in this scheme have reported many forms of identity fraud. As alleged in the Complaint, bank accounts holding tens of thousands of dollars in savings have been depleted; credit cards have been used to the tune of thousands of dollars without authorization; address changes have been made to accounts at various financial institutions; checks, debit cards, ATM cards and credit cards have been sent to unauthorized locations; and identities of victims have been assumed by others.

In a related case, LINUS BAPTISTE was arrested on October 29, 2002 on a wire fraud charge related to the CUMMINGS case. According to that Complaint, phone numbers registered to BAPTISTE's residence were used to dial into Equifax's databases and download 400 - 600 credit reports in August 2002 in the scheme. Credit reports, laptop computers and a document bearing CUMMINGS' name were found in BAPTISTE's home.

In a related case involving fraud perpetrated on several of these victims, on July 30, 2002, a defendant using the name HAKEEM MOHAMMED was charged with mail fraud in connection with an address change made to a line of credit opened by two of the Ford victims and the opening of accounts and lines of credit in the names of two other Ford victims. MOHAMMED entered a guilty plea to mail fraud and conspiracy charges on October 2, 2002, and is scheduled to be sentenced before United States District Judge GERALD E. LYNCH on January 8, 2003.

CUMMINGS is expected to be presented in Manhattan federal court this afternoon on the Complaint unsealed today. If convicted, CUMMINGS faces, with respect to the wire fraud charge, a maximum term of 30 years' imprisonment and a maximum fine of $1 million or twice the pecuniary gain or loss resulting from the offense. CUMMINGS faces, with respect to the conspiracy charge, a maximum term of 5 years' imprisonment and a maximum fine of $250,000, or twice the gross gain or loss resulting from the crime.

Mr. COMEY stated: "With a few keystrokes, these men essentially picked the pockets of tens of thousands of Americans and, in the process, took their identities, stole their money and swiped their security. These charges and the potential penalties underscore the severity of the crimes. We will pursue and prosecute with equal vigor others who may be involved."

Mr. DONOVAN stated: "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 the bank vault from an insider. But the potential windfall was probably far greater than the contents of a bank vault and, using 2lst century technology, they didn't even need a getaway car. Using the

same technology, we determined what was done and who did it, proving that technology is a double-edged sword."

Mr. COMEY praised the investigative efforts of the Federal Bureau of Investigation and thanked the United States Secret Service and the United States Postal Inspection Service for assisting in the investigation as well. Mr. COMEY also stated that the investigation is continuing.

Assistant United States Attorneys KATHERINE M. CHOO and JULIAN SCHREIBMAN are in charge of the CUMMINGS and BAPTISTE prosecutions. Assistant United States Attorney HARRY CHERNOFF is in charge of the MOHAMMED prosecution.

The charges contained in the Complaints are merely accusations, and the defendants are presumed innocent unless and until proven guilty.

Persons who believe they may have been victims of identity theft are advised to contact the Federal Trade Commission at: 1-877-ID THEFT (1-877-428-4338) or via e-mail at WWW.FTC.GOV.

02-247

###