United States Department of Justice
United States Attorney's Office
District of Minnesota

B. Todd Jones,
United States Attorney

Jeanne F. Cooney
Director of Community Relations
(612) 664-5611
email: jeanne.cooney@usdoj.gov

News Release

FOR IMMEDIATE RELEASE
Wednesday, February 23, 2011
WWW.JUSTICE.GOV/USAO/MN

Texas man pleads guilty to hacking into computer servers of local company and NASA

MINNEAPOLIS – United States Attorneys B. Todd Jones, of the District of Minnesota, and Rod J. Rosenstein, of the District of Maryland, announced that earlier today in federal court in St. Paul, Minnesota, a 26-year-old Texas man pleaded guilty to hacking into computer networks at a Minnesota business and at NASA. Jeremey Parker, of Houston, Texas, pleaded guilty to one count of wire fraud. He was indicted in the District of Minnesota on October 13, 2010.

In his plea agreement, Parker admitted that from December 23, 2008, through October 15, 2009, he hacked into the computer network of SWReg, Inc., a subsidiary of the cyber-based company Digital River, Inc., of Eden Prairie, Minnesota, in an effort to steal money. SWReg. pays independent software developers who write code. Royalties owed to those developers are accumulated at SWReg. The software developers have the ability to go online, view the royalty balances in their SWReg accounts, and, ultimately, cash out those accounts. When a particular developer cashes out an account, SWReg electronically transfers the money to the developer's bank account, mails the developer a check, or has the developer's PayPal account credited. Parker hacked into SWReg's system, created the money by crediting the SWReg accounts, and then caused that money to be wire transferred to his bank account instead of the accounts of several developers. Parker stole approximately $275,000.

In addition, Parker admitted that on September 24, 2009, he hacked into two computer servers at the National Aeronautics and Space Administration's Goddard Space Flight Center in Greenbelt, Maryland. The servers supported access to data being sent to Earth from satellites gathering oceanographic data. The servers did not have any control over the satellites themselves but, rather, allowed paying members of the scientific community to access the stream of data coming from those satellites. After a period of time, the data was freely available to anyone who wished to log onto a specific NASA website. Once the breach of its computer system was discovered, NASA spent approximately $43,000 to repair the damage. During the time the

website was down for repairs, approximately 3,300 users were denied access to the oceanographic data.

Parker was not officially charged in the District of Maryland in connection with the NASA incident, but the two U.S. Attorneys agreed to have the activity treated as relevant conduct for sentencing purposes in the District of Minnesota. For his crimes, Parker faces a potential maximum penalty of 20 years in prison. U.S. District Court Judge Richard H. Kyle will determine Parker's sentence at a future hearing, yet to be scheduled.

The Minnesota case is the result of an investigation by the Federal Bureau of Investigation. It is being prosecuted by Assistant U.S. Attorney John Docherty. The Maryland case was investigated by the NASA Office of Inspector General, and was prosecuted by Assistant U.S. Attorney Bryan Foreman.

The Justice Department vigorously investigates and prosecutes cyber crimes. It created the Task Force on Intellectual Property (http://www.justice.gov/dag/iptaskforce/) to aid in combating intellectual property crimes both at home and abroad. According to the FBI's Internet Crime Complaint Center's annual report, the FBI received 22.3 percent more cyber crime complaints in 2009 than in 2008, and the total dollar loss from all cases referred to law enforcement ($559.7 million) was more than twice the 2008 figure ($264.4 million). The FBI and the Minnesota U.S. Attorney's Office want to remind people to protect themselves from cyber crime. For more information, visit http://www.justice.gov/criminal/cybercrime/index.html

###