Department of Justice

FOR IMMEDIATE RELEASE
THURSDAY, AUGUST 27, 2004
WWW.USDOJ.GOV

CRM
(202) 514-2007
TDD 202-514-1888

BACKGROUND ON OPERATION WEB SNARE
EXAMPLES OF PROSECUTIONS

CALIFORNIA - CENTRAL DISTRICT

United States v. Jay R. Echouafni et al. (Operation Cyberslam)

Summary: On August 25, 2004, a federal grand jury in the Central District of California indicted Jay R. Echouafni, Chief Executive Officer of Orbit Communication Corporation in Massachusetts, and five other individuals on multiple charges of conspiracy and causing damage to protected computers, after Echouafni and a business partner allegedly hired computer hackers to launch relentless distributed denial of service ("DDOS") attacks against Orbit Communication's online competitors. The indictment and a separate criminal complaint allege that Echouafni and his business partner, Paul Ashley of Powell, Ohio, used the services of computer hackers in Arizona, Louisiana, Ohio, and the United Kingdom to attack the Internet websites of RapidSatellite.Com, ExpertSatellite.Com and Weaknees.Com. The sustained attacks allegedly began in October 2003 and caused the victims to lose over $2 million in revenue and costs associated with responding to the attacks. In addition, the attacks also temporarily disrupted other sites hosted by the victims' Internet Service Providers, including the U.S. Department of Homeland Security and Internet company Amazon.com.
The massive computer networks used to launch the DDOS attacks were allegedly created through the use of computer worms that proliferated throughout the Internet and compromised thousands of vulnerable computers. The infected computers, known as "zombies," were then allegedly used by the co-conspirators to attack the victim computer systems by flooding the systems with massive amounts of data. Echouafni, a U.S. citizen of Moroccan origin, fled from the United States and is the target of an international manhunt led by the FBI. Operation Cyberslam was investigated by the FBI and United States Secret Service with the assistance of the London Metropolitan Police Service and the FBI Legal Attache in the United Kingdom.

United States v. Jie Dong

Summary: On August 20, 2004, the U.S. Attorney's Office in Los Angeles charged defendant Jie Dong in the largest PayPal and eBay fraud scheme in history. A federal criminal complaint alleging that Dong engaged in a sophisticated mail and wire fraud

scheme was filed last week that describes the methodical scheme by a skilled Internet fraudster who stole nearly $800,000 from unwitting victims. Dong conducted over 5,000 fraudulent sales to eBay customers from September to December 2003 after establishing accounts with eBay and PayPal under the username "quainfangcompany."

As part of his scheme, Dong established a positive feedback rating to lure auction fraud victims by selling over $150,000 in low-cost merchandise. In November 2003, however, Dong began selling more expensive items, such as computer hard drives, digital cameras, and DVD players, during the height of the holiday shopping season. In fact, Dong sold an astounding $380,000 in merchandise per week and collected the money through his online PayPal account or by cashing money orders sent directly by the customers. Dong then withdrew the money, sometimes in increments as high as $60,000 at a time, or transferred the money to bank accounts in China and Hong Kong.

Dong's eBay and PayPal accounts were terminated after eBay received a flood of complaints. Dong never sent any of the merchandise purchased by over 5,000 victims. Dong subsequently fled the country and is currently at large. Through the assistance of authorities in China and Hong Kong, and eBay investigators in the United States, more than $280,000 in stolen funds have been frozen and criminal forfeiture proceedings have been filed.

United States v. Calin Mateias

Summary: On August 4, 2004, a federal grand jury in the Central District of California indicted Calin Mateias, an alleged Romanian computer hacker, and five Americans on charges that they conspired to steal more than $10 million in computer equipment from Ingram Micro in Santa Ana, California, the largest technology distributor in the world. The indictment alleges that Calin Mateias, a resident of Bucharest, Romania, hacked into Ingram Micro's online ordering system and placed fraudulent orders for computers and computer equipment. Mateias allegedly directed that the equipment be sent to dozens of addresses scattered throughout the United States as part of an Internet fraud ring. The Justice Department is working closely with Romanian authorities to ensure that Mateias is brought to justice, whether in Romania or the United States.

According to the indictment, Mateias began hacking into Ingram Micro's online ordering system in 1999. Using information obtained from his illegal hacking activity, Mateias allegedly bypassed Ingram's online security safeguards, posed as legitimate customers, and ordered computer equipment to be sent to Romania. When Ingram Micro blocked all shipments to Romania in early 1999, Mateias allegedly recruited four of his codefendants from Internet chat rooms to provide him with U.S. addresses to use as "mail drops" for the fraudulently ordered equipment. Four of the codefendants, in turn, allegedly recruited others, including high school students, to provide additional addresses and to accept the stolen merchandise. The defendants in the United States would allegedly either sell the equipment and send the proceeds to Mateias, or repackage the equipment and send it to Romania.

Mateias and his co-conspirators allegedly fraudulently ordered more than $10 million in computer equipment from Ingram Micro. However, Ingram Micro was successful in intercepting nearly half the orders before the items were shipped. All six

defendants are charged with conspiring to commit mail fraud by causing Ingram Micro to ship computer equipment based on the false pretenses that the equipment was ordered by legitimate customers. In addition to the conspiracy count, Mateias is charged with 13 mail fraud counts; two of the defendants with three mail fraud counts; a third defendant with six mail fraud counts; and a fourth defendant with four mail fraud counts for shipments.

This international investigation was handled by the Cyber Crimes Squad in the Los Angeles Field Office of the Federal Bureau of Investigation, which received substantial assistance from the Romanian National Police and the FBI Legal Attache Office in Bucharest. Additionally, the FBI Field Offices in Atlanta; Richmond, Virginia; Miami; Chicago; Albuquerque, New Mexico; El Paso, Texas; Newark, New Jersey; Norfolk, Virginia; Omaha, Nebraska; San Francisco; Seattle; Tampa, Florida; Albany, New York; and San Diego assisted in the investigation.

In a separate case, the United States Attorney's Office for the Western District of Pennsylvania announced the unsealing of an 11-count indictment charging Mateias in another scheme involving shipments of fraudulently ordered merchandise that was sent to co-conspirators in Pennsylvania, Georgia, and Louisiana. [See Western District of Pennsylvania, below.]

CALIFORNIA - NORTHERN DISTRICT

United States v. Robert McKimmey

Summary: On July 29, 2004, Robert McKimmey pleaded guilty in the United States District Court for the Northern District of California to conspiracy to commit theft and downloading of trade secrets, fraud in connection with computers, and interstate transportation of stolen property. McKimmey was employed as Chief Technology Officer of Business Engine Software Corporation ("BES"), a company that creates business enterprise software along with Niku Corporation, one of its competitors. As part of the conspiracy, defendant illegally accessed victim Niku's computer network and applications repeatedly over a 10-month period without authorization; stole, downloaded, and copied things of value including Niku trade secrets; and transmitted some of those things of value including Niku trade secrets to other BES officers and employees - all so that BES could maintain a competitive advantage over Niku. McKinney is awaiting sentencing.

Press Release:
<http://www.usdoj.gov/usao/can/press/html/2004_07_29_mckimmey.html>

United States v. Laurent Chavet

***Summary*:** On July 2, 2004, FBI agents arrested Laurent Chavet on an indictment, filed June 29, 2004, that charged Chavet with allegedly hacking into the computer system of

the Internet search engine Alta Vista to obtain source code, and for recklessly causing damage to Alta Vista's computers.

Press Release:
<http://www.usdoj.gov/usao/can/press/html/2004_07_02_chavet.html>

United States v. Shan Yan Ming

Summary: On July 6, 2004, Shan Yan Ming pleaded guilty in United States District Court for the Northern District of California to an indictment charging him with exceeding his authorized access to computers of a Silicon Valley company that developed a software program used to survey land for sources of natural gas and oil. According to the criminal complaint, he had worked for the victim company, 3DGeo Development, Inc., under an agreement between 3DGeo and PetroChina, a Chinese company which arranged for defendant to travel to California for training on 3DGeo's software. In pleading guilty to the indictment, he admitted that he gained unauthorized access to 3DGeo's computer system with an intent to defraud the company. FBI agents arrested him in September 2002 at San Francisco International Airport as he tried to board a flight to China. A hearing concerning his sentencing is scheduled for September 7, 2004.

Press Release: <http://www.usdoj.gov/usao/can/press/html/2004_07_07_shan.html>

United States v. Robert Lyttle

Summary: On July 15, 2004, a federal grand jury in the Northern District of California returned an indictment alleging that Robert Lyttle, as a member of "The Deceptive Duo," gained unauthorized access to computer systems of various federal agencies in April 2002, including the Department of Defense ("DOD") and the National Aeronautics and Space Administration's ("NASA") Ames Research Center ("ARC"). The indictment alleges that Lyttle gained unauthorized access to DOD computers in Michigan for the purpose of obtaining files that he later used to deface a Web site hosted on computers in Texas. Lyttle also allegedly gained unauthorized access to a NASA ARC computer located at Moffett Field and obtained information from that computer for the purpose of defacing a Web site hosted on the computer.

Press Release: <http://www.usdoj.gov/usao/can/press/html/2004_07_16_lyttle.html>

United States v. Roman Vega

Summary: In June 2004, Roman Vega of Ukraine was extradited from Cyprus to face a 40-count indictment, returned in the Northern District of California, charging Vega with credit card trafficking and wire fraud. According to the Indictment, Vega allegedly used Internet chat rooms to traffic in credit card information of thousands of individuals that had been illegally obtained from sources around the world, including credit card

processors and merchants. Vega was also allegedly an operator of a Web site at www.boafactory.com <http://www.boafactory.com>, where stolen and counterfeit credit card account information was allegedly bought and sold.
___***Press Release***: <http://www.usdoj.gov/usao/can/press/html/2004_06_04_vega.html>

United States v. Michael A. Bradley

Summary: On June 24, 2004, a federal grand jury in the Northern District of California returned an indictment charging Michael A. Bradley with devising a scheme to defraud and extort money from Google. The scheme allegedly involved claims by Bradley that he had developed a software program called "Google Clique" that automated fraudulent "clicks" on "cost-per-click" advertisements utilized by Google. These fraudulent clicks were designed to cause Google to make payments that were supposed to be made only for "clicks" made by legitimate Web surfers. Bradley allegedly claimed that he would sell the software to top spammers if Google did not pay him approximately $150,000, and that Google could lose millions.
___***Press Release***: http://www.usdoj.gov/usao/can/press/html/2004_06_04_bradley.html

FLORIDA - MIDDLE DISTRICT

United States v. Alexander Tobolsky

Summary: On August 25, 2004, Alexander Tobolsky was sentenced in the United States District Court for the Middle District of Florida to 37 months in prison for copyright infringement. Tobolsky had originally been indicted in the Eastern District of Virginia for selling pirated copies of Intuit accounting and finance software through his website and Internet auctions. He sold 2,283 copies that would have had a value of $783,000 if they had been legitimate. Tobolsky agreed to plead guilty to copyright infringement, and his case was sent to the Middle District of Florida where he pleaded guilty.

MASSACHUSETTS

United States v. Patrick Angle

Summary: On August 23, 2004, the United States Attorney's Office in the District of Massachusetts charged a former employee of Varian Semiconductor Equipment Associates, Inc., a large high-technology company headquartered in Gloucester, with computer hacking that caused significant damage to Varian's computer systems. Patrick Angle, of Columbus, Indiana, was charged in a one-count Information with intentionally damaging a protected computer, in violation of 18 U.S.C. § 1030(a)(5)(A)(i), an offense

punishable by a term of imprisonment of up to 10 years. The Information charges that Angle, who had worked for Varian, first in Gloucester and then from his home in Indiana, had become disgruntled with his employment and pending termination. To vent his frustration with Varian, on September 17, 2003, Angle allegedly logged into Varian's computer server in Massachusetts from his Indiana home and deleted the source code for the e-commerce software that he and others had been developing, then covered his tracks by deleting activity logs. Although Varian was ultimately able to recover the deleted material from backups, the company has estimated the cost of the recovery effort to be approximately $26,455. Varian reported the crime to the FBI, which investigated the case, and provided valuable assistance throughout the investigation.

MISSOURI - WESTERN DISTRICT

United States v. Melissa Davidson

Summary: On June 29, 2004, a federal grand jury in the Western District of Missouri indicted Melissa Davidson on two counts of computer fraud under 18 U.S.C. § 1030(a)(4) and two counts of access device fraud under 18 U.S.C. § 1029(a)(5). The government alleged that Davidson, who was employed by Citibank in Kansas City at the time the offenses were committed, accessed without authority confidential customer account information held in a database at Citibank, and was able to find such information belonging to two Citibank customers whose names were also "Melissa Davidson." After going on maternity leave, defendant Davidson allegedly used the purloined account information to gain access to the victims' Citibank accounts via the Internet from a computer in her home, and obtained new Citibank credit cards using the creditworthiness of the victims. The fraudulently obtained credit cards were then used to purchase merchandise. The loss to Citibank is $34,000. The case was investigated by the U.S. Postal Inspection Service.

United States v. Soji Olowokandi

Summary: On June 1, 2004, a federal grand jury in the Western District of Missouri in Kansas City, Missouri, returned an indictment charging five individuals with conspiracy to commit identity theft, access device fraud, and unlawful access of a protected computer. The case originated in Columbia, Missouri, where defendant Ganiyat Ishola was employed in the Natural Resources Conservation Service ("NRCS"), which is a division of the United States Department of Agriculture.

The indictment alleges that Ishola, a U.S. citizen from Nigeria, stole several pages from an employee roster, which contained the names and corresponding social security numbers of federal employees. Ishola allegedly gave the roster to her boyfriend, Soji Olowokandi, a Nigerian citizen on an expired student visa. According to the indictment, Ishola and Olowokandi took the stolen information to Chicago, Illinois, where they gave the roster to another Nigerian, Abdulazeez Temitayo Surakatu, who is also named as a

defendant in the indictment. The indictment alleges that unknown members of the conspiracy used a computer to access the Internet for the purpose of applying for credit cards, using the stolen NRCS employee information. Also, the indictment names Spiros Grapsas, Roy Ndidi Eledan, and Craig Parker, as conspirators whose roles were to provide mail drops where the credit cards could be mailed as well as bank account where "convenience checks" could be deposited. The total of the actual and intended loss described in the indictment is $231,500.

The United States Department of Agriculture Office of the Inspector General conducted the investigation.

NEW YORK - SOUTHERN DISTRICT

United States v. Jason Smathers and Sean Dunaway

Summary: On June 23, 2004, Jason Smathers, 24, a software engineer employed at America On Line ("AOL"), and Sean Dunaway, 21, were arrested at their residences in Harpers Ferry, West Virginia, and Las Vegas, Nevada, respectively, on conspiracy charges filed in Manhattan federal court, arising from their scheme to steal AOL's entire subscriber list, and to use the list to send massive amounts of unsolicited commercial e-mails -- also known as "spam" -- to millions of AOL's customers. This case is reportedly one of the first in the nation prosecuted under the recently-enacted CAN-SPAM law.

As charged in the criminal complaint, in May 2003, Smathers, using his skills as a computer engineer and his inside knowledge of AOL's computer system, misappropriated a list of 92 million AOL customer account "screen names." The Complaint further alleges that in May 2003, Dunaway purchased the list from Smathers, and then sold the list to other spammers for $52,000, and also used the list to promote his own Internet gambling operation. The Complaint further charges that Dunaway claimed to have purchased an updated version of AOL's customer list, which Dunaway also sold.

According to the Complaint, AOL, one of the world's leading Internet service providers, with a customer base of approximately 30 million subscribers, maintained its customer list in a database referred to as the "Data Warehouse," in a secure computerized location in Dulles, Virginia. As described in the Complaint, access to that database was limited by AOL to a small number of AOL employees. According to the Complaint, Smathers worked in AOL's Dulles offices, but was not authorized to access or copy the customer information in the Data Warehouse in April and May 2003, when he stole the list. However, as alleged, in April and May 2003, Smathers, using the computerized employee identification code of another AOL employee, improperly gained access to the Data Warehouse database, and began assembling a complete list of AOL's customer account screen names and related zip codes, credit card types (but no credit card numbers), and telephone numbers of AOL customers. The Complaint notes that there is no evidence that anyone gained access to or stole customers' credit card account numbers -- which AOL stores in a separate, highly secured data location apart from the Data Warehouse.

A search of Smathers's work computer conducted in May 2004, as alleged in the Complaint, revealed that in approximately April 2003, Smathers and another individual

discussed various techniques by which to spam AOL customers, as well as the large profits that could be made from spamming.

The Complaint charges that, in or about May or June 2003, Sean Dunaway (who is not an employee of AOL) told a confidential source (the "Source") that he (Dunaway) had obtained from an AOL insider a computerized list of 92 million AOL screen names for millions of AOL customers. The Source purchased the list (together with another individual), and paid Dunaway $2,000 per letter of the alphabet (i.e., all the AOL screen names beginning with that letter), or $52,000 total, for the entire customer list. In or around March 2004, the Source obtained a second list, from Dunaway which Dunaway described as an updated version of the original list, for $32,000, which contains fewer screen names than the earlier list (approximately 18 million). According to the Complaint, the Source used both lists to send spam to AOL's customers in 2004 (i.e., after January 1, 2004, when the CAN-SPAM law went into effect), for purposes of marketing herbal penile enlargement pills.

The United States Secret Service, New York Electronic Crimes Task Force, Washington, D.C., Electronic Crimes Task Force, and Las Vegas Electronic Crimes Task Force participated in this investigation.

United States v. William Quinn

Summary: On July 12, 2004, a federal grand jury in the Southern District of New York indicted William Quinn for allegedly obtaining unauthorized access to Verizon computers and posting the access codes for those computers on the Internet. Accessing Verizon's computers in this way would allow hackers to disable phone numbers (including 911, hospitals, etc.) from making or receiving calls. The New York Economic Crimes Task Force conducted the investigation.

United States v. Jacob Jah, et al.

Summary: On June 16, 2004, a federal grand jury in the Southern District of New York indicted three defendants on charges related to allegedly trafficking in counterfeit goods (handbags and other accessories) and then wiring those and other proceeds (in excess of $1 million per month) to China and India as part of a money-laundering/hawala takedown covering New York City; Columbus, Ohio; Detroit, Michigan; Denver, Colorado; and Memphis, Tennessee. The United States Postal Inspection Service investigated the case.

United States v. Ali Aoun, et al.

Summary: On August 5, 2004, a federal grand jury in the Southern District of New York indicted two defendants on charges of conspiracy, trafficking in counterfeit goods, and money laundering, for their alleged sale of counterfeit designer handbags, luggage, wallets, makeup cases, shoes, and other items, out of a storefront in Manhattan. The

counterfeited brands include Louis Vuitton, Fendi, and Christian Dior. The aggregate retail price for the actual goods is in the millions of dollars, and the street value for the knock-offs is just under a million dollars.

United States v. Yu Chun Wang, et al.

Summary: On August 5, 2004, a federal grand jury in the Southern District of New York indicted Yu Chun Wang and three other defendants on charges of conspiracy, trafficking in counterfeit goods, attempted bribery, and money laundering relating to importing of counterfeit Louis Vuitton handbags and luggage from China. The aggregate retail value for the actual goods exceeds tens of millions of dollars, and the street value of the knock-offs is approximately $5.5 million. The bribery charge stems from the defendants allegedly attempting to pay off an undercover Bureau of Immigration and Customs agent who, in a sting, pretended to have an inside Customs contact who could help smuggle contraband.

United States v. Alexei Rodin

Summary: On June 10, 2004, a jury in the Southern District of New York convicted Alexei Rodin of wire fraud and conspiracy. The fraud involved an Internet auction scam in which victims paid money for phantom items on eBay. The victims were all directed via e-mail to send their payments for the nonexistent goods (outboard motors and hydraulic car lifts) to Rodin, who received the money and then wired most of the funds out to a co-conspirator in Latvia.

PENNSYLVANIA - WESTERN DISTRICT

United States v. Calin Mateias [See also Central District of California, above]

Summary: On August 4, 2004, a federal grand jury indictment in the Western District of Pennsylvania against Calin Mateias, a Romanian citizen, on charges of mail fraud and conspiracy was unsealed. The eleven-count indictment, returned by the grand jury on December 3, 2003, named Mateias, age 24, of Bucharest, Romania. The indictment alleges that Mateias conspired in a scheme to defraud Ingram Micro, headquartered in Santa Ana, California, the world's largest distributor of technology products, including computer hardware. The scheme consisted of Mateias, who often used the online nickname "Dr. Mengele," making fraudulent orders for computer hardware over the Internet using the ordering accounts of legitimate Ingram Micro customers. The merchandise was shipped to various "drop" locations in multiple states provided by persons recruited by Mateias. The recruits, which included individuals in the Western District of Pennsylvania, Georgia and Louisiana, would then pick up the hardware and repackage and reship it to Mateias in Romania. The indictment states that, in all, Mateias

was involved in fraudulently obtaining approximately $700,000 worth of computer equipment from Ingram Micro.

United States v. Frederick Banks

Summary: On July 20, 2004, a federal grand jury in the Western District of Pennsylvania indicted Frederick H. Banks was indicted by on a charge of mail fraud. The one-count indictment named Banks, 36, of Pittsburgh, Pennsylvania.According to the indictment presented to the court, between April 29, 2004 and June 23, 2004, Banks attempted to purchase coins and software through the Internet using counterfeit checks. Banks was arrested pursuant to a criminal complaint on June 24, 2004. Banks was previously indicted for similar conduct on October 7, 2003. In addition, the grand jury in that case returned a superseding indictment on May 4, 2004 charging Banks with mail fraud, money laundering, uttering counterfeited and forged securities, and witness tampering.

The Southwestern Pennsylvania Financial Crimes Task Force conducted the investigation leading to the indictment in this case. The Southwestern Pennsylvania Financial Crimes Task Force comprises United States Postal Inspectors, Special Agents of the United States Secret Service and the Federal Bureau of Investigation, Investigators from the Allegheny County District Attorney's Office, and Detectives from Allegheny County and the City of Pittsburgh.

United States v. Jeffrey Smittle

Summary: On July 15, 2004, Jeffrey Smittle was sentenced in United States District Court to 18 months in prison, followed by three years of supervised release, and was ordered to pay $120,000 in restitution, for unauthorized trafficking in recordings of live musical performances. United States District Judge David Stewart Cercone imposed the sentence on Smittle, 44, of Ceresco, Michigan. Smittle pleaded guilty to the offense in April 2004. Information presented to the court indicated that between January 15, 2002 and November 5, 2002 Smittle was engaged in the business of selling unauthorized recordings of live music concerts. The unauthorized recordings, known as "bootleg" recordings, featured numerous artists, including KISS, Aerosmith, Bob Dylan and Bruce Springsteen. In November 2002, a search of Smittle's former residence on Parkland Drive in Canonsburg, Pennsylvania, resulted in the seizure of more than 11,000 suspected bootleg and counterfeit recordings. Smittle videotaped or audiotaped some of his own bootleg recordings and traded for other recordings with dealers around the country. Smittle sold copies of the bootleg audio and video recordings both over the Internet and at record shows.

The Pittsburgh High Technology Crimes Task Force, which is composed of agents and investigators from the Federal Bureau of Investigation, the United States Secret Service, the United States Postal Inspection Service, the Internal Revenue Service - Criminal Investigation, the Allegheny County District Attorney's Office, detectives from Allegheny County and the City of Pittsburgh, and troopers from the Pennsylvania State Police, conducted the investigation that led to the prosecution of Smittle. The

Canonsburg Police Department and the Recording Industry Association of America also assisted with the investigation.

United States v. Sonya Rosenberger

Summary: On August 24, 2004, a federal grand jury in the Western District of Pennsylvania indicted Sonya Rosenberger on charges of mail fraud. The five-count indictment named Rosenberger, age 27, of Farmington, Pennsylvania, as the sole defendant. According to the indictment, between April 2002 and May 2004, Rosenberger repeatedly defrauded a WTAE-TV contest known as the "Watch 4 Win More" sweepstakes by creating on her computer false contest claim forms with the winning contest number after the station had televised that number. Rosenberger created winning forms for herself and her friends and relatives for which WTAE paid out approximately $95,500, and Rosenberger attempted to collect an additional $20,000 but was unsuccessful because the station discovered the fraud. The Federal Bureau of Investigation conducted the investigation leading to the indictment in this case.

United States v. Alanna Ridenour

Summary: On August 24, 2004, a federal grand jury in the Western District of Pennsylvania indicted Alanna Ridenour on a charge of mail fraud. The one-count indictment named Ridenour, age 45, of Morgantown, West Virginia, as the sole defendant. According to the indictment, between May 2003 and May 2004, Ridenour defrauded a WTAE-TV contest known as the "Watch 4 Win More" sweepstakes by submitting false contest claim forms with the winning contest number after the station had televised that number. Ridenour obtained or manufactured winning forms for herself and her friends and relatives, for which WTAE paid Ridenour approximately $12,000, and Ridenour attempted to collect an additional $19,000 before the station discovered the fraud.

In a separate indictment returned the same day, Ridenour's daughter, Sonya Rosenberger, of Farmington, Pennsylvania, was charged with five counts of mail fraud for carrying out the same scheme for a longer period, from April 2002 to May 2004, in which WTAE paid out a total of approximately $95,500, including the $12,000 received by Ridenour, who was supplied false claim forms in her own name by her daughter. The Federal Bureau of Investigation conducted the investigation leading to the indictment in this case.

United States v. Scott Eric Catalano

Summary: On August 25, 2004, the United States Attorney for the Western District of Pennsylvania filed an information against Scott Eric Catalano, charging him with unauthorized access to a computer to obtain files and other account information. The one-count information named Catalano, age 25, of Koppel Pennsylvania.According to the information presented to the court, Catalano accessed without authorization the server of

Allegheny Computer Service from October 14, 2003 through October 17, 2003 to view files and other account information in the course of uploading programs and files used to secure covert access to the server.

The High Tech Crimes Taskforce - consisting of agents and investigators from the United States Postal Inspection Service, the United States Secret Service, the Federal Bureau of Investigation, the Internal Revenue Service - Criminal Investigation, the Allegheny County District Attorney's Office, and detectives from Allegheny County and the City of Pittsburgh -- and troopers from the Pennsylvania State Police conducted the investigation that led to the prosecution of Catalano.

UTAH

United States v. Mark Pentrack

Summary: On June 14, 2004, R. Mark Pentrack was sentenced in the United States District Court for the District of Utah to 135 months imprisonment as a result of his guilty pleas to mail fraud, misuse of a social security number, attempted destruction of evidence, and making a false statement in connection with an Internet fraud scheme. Pentrack offered car parts, aircraft parts, and other items for sale over the Internet, but did not possess those items and did not deliver those items to buyers. To conceal his activities, he hired secretaries in five states outside Utah to receive payments from would-be buyers, used an e-mail service based in Australia and used an anonymizing program when conducting online activities. More than 10 individuals sent Pentrack more than $200,000 in connection with the scheme. After being arrested, Pentrack tried to enlist two people to enter his apartment and remove two computers and other materials relating to his scheme, before federal authorities could find and seize them. He also made false statements concerning his scheme to federal authorities.

VIRGINIA - EASTERN DISTRICT

United States v. Kevin McGandy and Elisa Bescher

Summary: These two individuals are defendants in Operation Revive, a joint investigation by USSS and USPS. The conspirators obtained the identifying information of more than 200 deceased individuals. The conspirators then selected certain of these deceased individuals and established good credit histories for them by putting some of the defendants' personal bills, such as for telephones, in the names of the deceased individuals; opened bank accounts in their names; and added their names to legitimate credit card accounts. After establishing the credit histories, the conspirators applied for credit cards, often online, in the names of the deceased individuals. The conspirators charged more than $500,000 on the credit cards and did not pay the bills. McGandy was sentenced on July 7, 2004 to six months home detention, three years of supervised restitution, and $86,000 in restitution. Bescher pleaded guilty on June 4, 2004. A

previous defendant, Edward Soboleski, was sentenced to 15 months imprisonment and ordered to pay restitution.

United States v. Myron Tereshchuk

Summary: On June 4, 2004, Myron Tereshchuk pleaded guilty in the Eastern District of Virginia to attempting to extort $17 million from an intellectual property firm. For several months, Tereshchuk obtained confidential information belonging to the firm. He obtained customer lists, lists of network passwords, and documents pertaining to the intellectual property of particular clients. Tereshchuk obtained the information by gaining unauthorized access to the victim's computer network and by taking documents placed outside the firm in bins to be picked up by a shredding company. Tereshchuk used the information to embarrass the victim company by sending the confidential information to various clients of the victim. Tereshchuk eventually threatened to release substantially more information unless he was paid $17 million.

Tereshchuk sent most of his emails by war-driving and gaining unauthorized access to wireless access points on computer systems that were not well secured. Through the use of court-ordered email pen registers, other court processes, and surveillance, the FBI caught him in the act of communicating with the victim company while trespassing through a wireless access point.

Press Release:
http://www.usdoj.gov/usao/vae/ArchivePress/JunePDFArchive/04/tereshchuk060804.pdf

WASHINGTON - WESTERN DISTRICT

United States v. Usman Hayat

Summary: On August 20, 2004, Usman Hayat,31, of Islamabad, Pakistan, pleaded guilty in United States District Court in Seattle to one count of transmitting interstate and foreign communications with intent to extort, in violation of Title 18, United States Code, Section 875(d). According to the plea agreement, Hayat contacted Eddie Bauer, Inc. in February 2004, via email, threatening to release photos that Hayat alleged showed child labor being used in the production of Eddie Bauer apparel. Hayat claimed he would post the photos on the Web, or send them to the media or Eddie Bauer's creditors if he was not paid $685,000.

At the direction of law enforcement, Eddie Bauer communicated with Hayat via email and ultimately provided Hayat with a plane ticket to Seattle. In the plea agreement, Hayat admits he traveled to Eddie Bauer headquarters in Redmond, Washington, and met with undercover agents in order to collect the $685,000 he had demanded. At the meeting, Hayat showed the agents photographic negatives that he claimed showed child labor. Federal agents provided him with $500,000 cash. Hayat reviewed the money and

agreed to meet the agents the next day to open bank accounts and deposit the money. Hayat was arrested before leaving the Eddie Bauer offices.

According to Eddie Bauer officials, the company regularly audits the Pakistani factories where its apparel is produced and those audits have found no evidence of the use of child labor in the manufacture of Eddie Bauer products. In response to the allegations made by Hayat, Eddie Bauer recently ordered a round of unannounced inspections. According to Eddie Bauer officials, again no evidence of the use of child labor in the manufacture of Eddie Bauer products was found. Hayat has agreed to pay $21,559.00 in restitution to Eddie Bauer.

The case was investigated by agents of the FBI and the United States Secret Service working as part of the Northwest Cyber Crimes Task Force (NWCCTF). The Northwest Cyber Crimes Task Force comprises agents from the FBI, United States Secret Service, Internal Revenue Service, Washington State Patrol, and the Seattle Police Department. The NWCCTF investigates computer hacking, Internet fraud, and other computer-related crimes.

United States v. Jeffrey Lee Parson

Summary: On August 11, 2004, Jeffrey Lee Parson, 19, of Hopkins, Minnesota, pleaded guilty in United States District Court in Seattle, to intentionally causing and attempting to cause damage to a protected computer. Parson was indicted in 2003 for sending out a variant of the MS Blaster computer worm on August 12, 2003. Parson's worm is referred to by a number of different names including the "B" or "teekids" variant of the MS Blaster worm.

According to the plea agreement, Parson admitted that he created his worm by modifying the original MS Blaster worm and adding a mechanism that allowed him to have complete access to infected computers. Parson then infected approximately fifty computers that he had previously hijacked with his worm. From those fifty computers, Parson's worm spread to other individual computers. Parson's worm then directed those infected computers to launch an attack against a Microsoft web site. Attorneys for the government calculate that more than 48,000 computers were infected by Parson's worm. Parson's attorneys dispute that calculation.

The MS Blaster worm case was investigated by the Northwest Cyber Crime Task Force and, in particular, by agents of the Federal Bureau of Investigation and the United States Secret Service. Key support for the investigation also was provided by the Department of Justice's Computer Crime and Intellectual Property Section and several United States Attorney's Offices around the country, particularly the District of Minnesota and the Southern District of California.

United States v. James Robert Murphy

Summary: On June 29, 2004, James Robert Murphy, 38, of Columbia, South Carolina pleaded guilty in the United States District Court for the Western District of Washington in Seattle to two counts of use of a telecommunications device (the Internet) with intent to annoy, abuse, threaten or harass. Murphy was indicted in April 2004 for sending

harassing e-mails to Seattle resident Joelle Ligon and to other employees of the City of Seattle.

In his plea agreement, Murphy admits he had a sporadic romantic relationship with Ligon from 1984-1990. In May of 2002, Murphy began sending dozens of uninvited and harassing e-mails and facsimile (fax) messages to Ligon and her co-workers. Murphy hid his identity with special e-mail programs and created the "Anti Joelle Fan Club" (AJFC) and repeatedly sent threatening e-mails from this alleged group. Murphy disseminated false information about Ligon's background to her co-workers. The harassment escalated over time with Murphy sending pornographic material and making it appear that Ligon was sending the pornographic material to her co-workers at the City of Seattle. Even after Ligon was able to identify her harasser and get a court order barring contact, Murphy violated the order by sending an e-mail denying he was the harasser.

This case was investigated by the Northwest Cyber Crime Task Force, composed of the FBI, United States Secret Service, Internal Revenue Service, Seattle Police Department, and Washington State Patrol. The NWCCTF investigates cyber-related violations including criminal computer intrusions, intellectual property theft, child pornography and Internet fraud. The task force brings federal, state and local law enforcement agencies together to share intelligence and conduct joint investigations.

###

04-584