June 8, 2004

Alexandria, Virginia

United States
Attorney
Eastern District of of Virginia
United States Attorney
Paul J.McNulty,
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703)299-3700For further information contact:
Sam Dibbley 703-842-4050

Wi-Fi Hacker Pleads Guilty to Attempted $17,000,000 Extortion

Paul J. McNulty, United States Attorney for the Eastern District of Virginia, announced that Myron Tereshchuk, 42, of Hyattsville, Maryland, pled guilty today to one count of attempting to extort $17 million over the Internet. The maximum potential sentence is 20 years imprisonment and a $250,000 fine. United States District Judge James C. Cacheris set sentencing for October 22, 2004. For more than a year, the defendant harassed MicroPatent, an intellectual property firm that produces and distributes patent and trademark information. The defendant sent MicroPatentis clients hundreds of emails, many of which were "spoofed" to resemble authentic MicroPatent correspondence. The emails contained statements derogatory to MicroPatent, attached sexually explicit patent applications, and disclosed MicroPatent documents that were believed to have been confidential. The defendant obtained the confidential information by gaining unauthorized access to MicroPatentis computer network and by searching through the trash set out to be collected by a shredding company at MicroPatentis location in Alexandria, Virginia. The defendant sent emails anonymously by using equipment from his automobile to gain unauthorized access to unsecured wireless computer networks in residences and businesses in Maryland and Virginia. Once the defendant had access to the networks, he often sent the emails using accounts of AOL customers without their knowledge or authorization. On February 3, 2004, the defendant began sending a series of extortionate emails to the president of MicroPatent using the alias "Bryan Ryan" and a free Yahoo email account. To further hide his identity, the defendant accessed the Yahoo account through unsecured wireless access points and the unauthorized use of the University of Maryland computer network and studentsi accounts. In the emails, the defendant demanded $17 million or he would disclose additional MicroPatent proprietary information and launch distributed denial-of-service attacks against intellectual property attorneysi computer systems worldwide. Based on one of the messages, the FBI believed the defendant might be the person attempting the extortion. Thereafter, the FBI, with the assistance of Yahoo, AOL, and the University of Maryland, was able to catch the defendant in the act of sending emails to the president of MicroPatent. At the time of the defendantis arrest at his automobile on March 10, 2003, he was in possession of his laptop, an antenna, and other computer equipment. The FBI searched the defendantis residence on March 10, 2004, and found not only computers and other items related to the attempted extortion, but also the components

for hand grenades, the formula and items necessary for making Ricin, and literature about poisons. Those matters remain under investigation by the FBI and the United States Attorneyis Office for the District of Maryland. United States Attorney Paul J. McNulty stated, “While the Internet has brought our society many benefits, it is also being used by a wide variety of criminals. Some of these criminals have the technical savvy to use new means to try to conceal their identities. This case is proof, however, that law enforcement is keeping up with technological advances and will catch these offenders.” The case was investigated by the FBI and was prosecuted by Assistant United States Attorney Jack Hanly and Michael Stawasz, Trial Attorney, Computer Crime and Intellectual Property Section, United States Department of Justice.

###