May 5, 2004

U.S. Department of Justice
United States Attorney
District of Massachusetts
John Joseph Moakley
United States Courthouse
Suite #9200
1 Courthouse Way
Boston, MA 02210
Press Contact: Samantha Martin
(617) 748-3139

Pennsylvania Man Sentenced to Prison for Accessing Massachusetts Investor's On-line Investment Account and Making $46,000 in Unauthorized Trades

A Pennsylvania man was sentenced today following his earlier conviction for the unauthorized access to a protected computer and other crimes in connection to his unlawfully accessing a computer belonging to an individual ("the Investor") residing in Westborough, Massachusetts, and using information gained through that intrusion to make unlawful trades with funds in the Investor's on-line brokerage account.

United States Attorney Michael J. Sullivan and Kenneth W. Kaiser, Special Agent in Charge of the Federal Bureau of Investigation in New England, announced today that VAN T. DINH, age 20, of 236 4th Avenue Phoenixville, Pennsylvania, was sentenced by U.S. District Judge Nathaniel M. Gorton to 1 year and 1 month in prison, to be followed by 3 years of supervised release and a $3,000 fine. Prior to today's sentencing, DINH had paid full restitution to the victim Investor in the amount of $46,986, which represented the entire amount of money taken from the Investor's account.

DINH pleaded guilty on February 9, 2004, to an eight count indictment charging him with causing damage in connection with unauthorized access to a protected computer; committing mail and wire fraud; and of knowingly executing a scheme and artifice to defraud the Investor and others in connection with a security and to obtain by means of false and fraudulent pretenses, money and property in connection with the purchase and sale of a security.

At today's sentencing hearing, the prosecutor read excerpts from DINH's computer diary which Judge Gorton described as "appalling." Including an entry made on June 3, 2002, which read in part, "... I am so proud of myself for my 'hacking business' - I will never regret what I did. I am the best of the best Trickster. I laugh often when mom says she worries - what the (expletive) do you have to worry about. Even if I go to jail - big deal - I will learn something there. Hahaha."

From June 18 through June 27, 2003, DINH purchased approximately 9,120 put option contracts for the common stock of Cisco Systems, Inc. ("Cisco") at the strike price of $15.00 per share through his online trading account at Cybertrader.com. Each put contract DINH purchased gave him the right to sell 100 shares of Cisco common stock at $15.00 per share, if the share value fell

to that price or below, until the contract's expiration which was set for July 19, 2003. DINH paid $10.00 per contract for a total purchase price of approximately $91,200. If the value of Cisco shares had fallen relatively precipitously during the short period of the life of the contracts, DINH would have stood to make a large profit - a highly speculative but potentially very lucrative gamble.

On July 7, 2003, the Investor, a member of Stockcharts.com's stock-charting forum, who lived in Westborough, Massachusetts, received a seemingly benign message from an individual named "Stanley Hirsch," who turned out to be DINH. The Investor responded the email, thus providing his personal email address to "Stanley Hirsch", a/k/a DINH.

On July 8, 2003, the Investor received an email sent to his personal email address inviting him to participate in a so-called "beta test" of a new stock-charting tool. The sender, identified as "Tony T. Riechert," provided a link in the email message to enable the Investor to download a computer program that purported to be the stock-charting application. Tony Riechert was another name, also used by DINH in connection with this scheme.

The purported application sent to the Investor was actually a disguised "Trojan horse" that contained a series of "keystroke-logging" programs which enable one Internet user to remotely monitor the actual keystrokes of another Internet user. A "Trojan horse" is a program in which malicious or harmful code is concealed or hidden inside apparently harmless programming or data, in such a way that it can get control of the breached computer and do its chosen form of damage (for example, as in the instant case, logging keystrokes made on the victim computer).

Once the Investor had installed the program on his computer, DINH was able to use the intrusion programs to identify an on-line TD Waterhouse account held by the Investor and to extract password and login information for that account. By July 10, 2003, approximately nine days before the expiration date of DINH's Cisco options, Cisco's stock was trading at approximately $19.00 per share, making it likely that DINH's $15.00 Cisco put options would be worthless at the time they expired and DINH would stand to lose the entire $91,200 he had paid to purchase the options. On July 11, 2003, DINH used the password and login information for the Investor's online account to place a series of buy orders for the Cisco options, depleting almost all of the account's available cash, approximately $46,986. The buy orders for the Investor's account were filled with 7,200 Cisco put options sold from DINH's account. As a result of the execution of these buy orders, DINH avoided at least $37,000 of losses, (some of the $46,986 in funds taken from the Investor's account went to commission costs). At today's hearing, the prosecutor explained to the Court that the actual loss to the victim in the case was $46,986, but the intended loss was upwards of $59,561. DINH had placed additional purchase orders from the Investor's account which went unfilled only because the Investor's account had already been depleted of funds by DINH. The investigation was conducted by the Federal Bureau of Investigation, the Securities and Exchange Commission's Office of Internet Enforcement, with the cooperation and assistance of the U.S. Attorney's Office for the Eastern District of Pennsylvania and the Department of Justice's Computer Crime and Intellectual Property Section. The prosecution of Internet fraud and other cybercrimes is a key focus of the U.S. Attorney's Office. The U.S. Attorney's Office's Computer Hacking and Intellectual Property Section also known as "CHIPS", was created to prosecute high-technology and intellectual property offenses, including

computer intrusions, denial of service attacks, virus and worm proliferation, Internet fraud, and telecommunications fraud. The case was prosecuted by Assistant U.S. Attorney Allison D. Burroughs in Sullivan's Computer Hacking and Intellectual Property Section of the Economic Crimes Unit and Assistant U.S. Attorney Jonathan Kotlier, Chief of Sullivan's Economic Crimes Unit, with the assistance of William Yurek, Trial Attorney with the Department of Justice's Computer Crime Section.