December 4, 2003

U.S. Department of Justice
United States Attorney
Central District of California
CONTACT: Elena Duarte
Assistant United States Attorney
(213) 894-8611
Thom Mrozek, Public Affairs Officer
(213) 894-6947

Former Global Crossing Employee Convicted of Posting Threats on His Internet Website and

Distributing Information to be Used in Identity Theft

LOS ANGELES → A Manchester, New Hampshire man was found guilty this afternoon of eight felony counts related to a website where he posted thousands of Social Security Numbers and other personal information belonging to employees of Global Crossing.

William Sutcliffe, 42, was convicted of thee counts of making interstate threats to injure or kill and five counts of transferring Social Security Numbers with the intent to aid and abet another felony.

During a four-week trial, the federal court jury that convicted Sutcliffe heard evidence that he was employed by Global Crossing as a computer technician until September 2001, when he was fired by the communications company. Soon after his termination, Sutcliffe established a website → EvilGX.com → the name of which referenced Global Crossing's stock symbol. Sutcliffe also picketed outside Global Crossing's Beverly Hills offices and held a sign referring people to his website.

The website contained personal information about many Global Crossing employees. In addition to Social Security Numbers, the website had phone numbers, home addresses, dates of birth and other data. The website also contained threats to publish even more information about additional employees, and links to other websites that discussed the ease with which identity fraud could be committed by an individual with the required personal information of another, such as birthdate and social security number.

The five counts of transferring Social Security Numbers relate to thousands of SSNs that Sutcliffe posted on his website. The jury in this case was told that Sutcliffe posted the SSNs of as many as 8,000 Global Crossing employees at any given time.

As employees realized their personal information was being made public, Global Crossing filed a lawsuit and obtained a temporary restraining order directing Sutcliffe not to publicize information he obtained while he was a Global Crossing employee. After a process server

attempted to deliver a copy of the TRO to him, Sutcliffe threatened to kill the process server on EvilGX.com. Sutcliffe also threatened Global Crossing's assistant general counsel on the website.

Sutcliffe is scheduled to be sentenced on March 22 by United States District Judge A. H0oward Matz. As a result of the guilty verdicts on the eight felony charges, Sutcliffe faces a maximum possible penalty of 30 years in federal prison.

This case is the result of an investigation by the Federal Bureau of Investigation. CONTACT: Assistant United States Attorney Elena Duarte

(213) 894-8611 Release No. 03-167

###

October 7, 2003

U.S. Department of Justice
United States Attorney
Eastern District of Pennsylvania
Patrick L. Meehan
Suite 1250, 615 Chestnut Street
Philadelphia, PA 19106
Contact: Rich Manieri
Media Contact
(215) 861-8525

Disgruntled Philadelphia Phillies Fan Charged with Hacking into Computers Triggering Spam E-mail Attacks

Victims Include Reporters At Philadelphia Inquirer And Daily News

October 7, 2003 - PHILADELPHIA → United States Attorney Patrick L. Meehan today announced the unsealing of an indictment returned on September 25, 2003, against ALLAN ERIC CARLSON. Agents of the Federal Bureau of Investigation arrested Carlson this morning at his residence. Carlson is charged with "hacking" into computers around the country, hijacking or "spoofing" the return addresses of e-mail accounts of reporters at the Philadelphia Inquirer and the Philadelphia Daily News and e-mail accounts at the Philadelphia Phillies, and launching spam e-mail attacks. He is also charged with identity theft for illegally using the e-mail addresses of the reporters. The indictment charges that Carlson, a disgruntled Philadelphia Phillies fan, hacked into computers of unsuspecting users and from those computers launched spam e-mail attacks with long messages voicing his complaints about the Phillies management. The indictment charges that when launching the spam e-mails, Carlson's list of addressees included numerous bad addresses. When those e-mails arrived at their destinations, the indictment charges

that they were “returned” or “bounced” back to the person who purportedly sent them → the persons whose e-mail addresses had been “spoofed” or hijacked. This caused floods of thousands of e-mails into these accounts in a very short period of time. “Fans have the right to voice their displeasure but these were electronic attacks with serious consequences,” said Meehan, who created a separate Computer Crime section in his office in 2001. “By flooding the victim computer systems with spam e-mails, those systems and the businesses they support were severely affected. You can boo, you can turn off the TV, but you can’t hijack the e-mail address of an unsuspecting user and call it passion.” Meehan also noted that this is the first use of an identity theft statute against an e-mail spammer. If convicted, Carlson faces a maximum possible sentence of 471 years imprisonment, $117,250,000 in fines and a special assessment of $7,800.

DEFENDANT ADDRESS AGE

ALLAN ERIC CARLSON 1232 East Lexington Drive Apartment A

Glendale, California 91206 DOB: 12/28/1963

The case was investigated by the Federal Bureau of Investigation. It has been assigned to Assistant United States Attorney Michael L. Levy, Chief, Computer Crimes.

###