Linfield Magazine

Volume 7
Number 2 *Fall 2010*

Article 18

December 2010

Alumni Profile

Laura Davis
Linfield College

Cyber crime-stopper fights ID theft

Sean Hoar's work takes him all over the world. He recently returned from a trip to the Middle East, where he shared his expertise about digital evidence and cyber crime with investigators, prosecutors and judges.

It's not always best to be right. Just ask Sean Hoar '80. More than a decade ago, Hoar, assistant U.S. attorney for the Department of Justice, singled out identity theft as the crime of the new millennium in an article for a Department of Justice publication that became a seminal piece on the newly emerging subject. With the Internet still in its early stages, Hoar led a team of colleagues to identify potential online crimes even before the private sector began reporting the offenses.

Unfortunately, his forecast proved accurate. According to the Federal Trade Commission, identity fraud continues to increase at a record pace, victimizing over 11 million Americans and resulting in losses of $54 billion in 2009.

Now, Hoar oversees a caseload of complex white-collar and high-tech crime, including identity theft. As a federal prosecutor, he supervises various federal investigations and represents the United States in federal court.

"I work closely with investigators," he says. "Usually, the cases are put together so well that I don't spend too much time in trial."

Hoar made his mark in the cyber crime arena in 1999, when he prosecuted the first case in the United States under the No Electronic Theft Act involving criminal copyright infringement on the Internet. After officials at the University of Oregon discovered significant Internet congestion on their campus system, Hoar's team uncovered a software pirating operation.

"Every day is different," says Hoar. "My cases are very dynamic. I am fortunate to work with well educated, well intentioned agents. The most fulfilling cases are those in which we are able to hold people accountable for victimizing others."

In addition to cyber criminals, Hoar also has targeted narcotics traffickers. Following one case, he received the prestigious Directors Award for his role in prosecuting a heroin trafficking organization based in Southeast Asia, which included a general who was a member of the Supreme Command of the Royal Thai Armed Forces.

Over the years, Hoar has established himself as a leader in the areas of identity theft and cyber crime. He served on the President's Identity Theft Task Force, which developed federal legislation and other action to combat identity theft at a national level. He has written and spoken extensively on the topics of identity theft and cyber crime, and trains investigators nationally and internationally in those areas. Recently, he founded the CyberSafe initiative, a public service project to reduce vulnerabilities in the Internet.

Hoar says his career was shaped by his Linfield experience. He spent two years as student body president, played football and baseball, and was a member of Theta Chi fraternity, and continues to remain involved, serving on the Linfield Alumni Leadership Council and helping to organize the 30th reunion of 1980s graduates.

"Those experiences taught me a lot about myself and helped me identify my strengths," says Hoar, who spoke to incoming Linfield freshmen at orientation. "Linfield was a springboard for tremendous opportunity which allowed me to pursue a very fulfilling career."

– Laura Davis

Fighting back

1. Be cautious about sharing personal information with anyone who does not have a legitimate need for the information.
2. Only carry identity information necessary for daily activities such as a driver's license, one credit or debit card, an insurance card, and regularly used membership cards.
3. Do not place outgoing mail in residential mail boxes. Install a mailbox secured by lock and key and promptly remove delivered mail.
4. Install and enable anti-virus, anti-spyware and intrusion protection software on your computer.
5. If possible, secure by lock and key all financial, medical and other information that may contain personally identifiable information.
6. Promptly review all bills and statements for accuracy. A missing bill may mean a thief has taken over an account.
7. Shred non-essential material containing identity information.
8. Periodically request copies of credit reports.