Testimony by
James E. Farnan, Deputy Assistant Director, Cyber Division,
Federal Bureau of Investigation,
before the
House Financial Services Committee, Subcommittees on
Financial Institutions and Consumer Credit, and
Oversight and Investigations
on April 3, 2003

Thank you for inviting me here today to testify on the topic, "Fighting Fraud: Improving Information Security." Holding this hearing demonstrates your commitment to improving the security of our Nation's information systems and this committee's leadership on this issue in Congress. Our work here is vitally important because the stakes involved are enormous. My testimony today will address the activities of the FBI's Cyber Division as they relate to a broad spectrum of criminal acts involving fraud and information security.

Today there are over 180 million computer users in the United States alone. There are more than 600 million worldwide, and the number is growing. Many of these users are connecting to the Internet, communicating, conducting business, managing financial affairs, searching for information and, unfortunately, committing crimes.

Cyber Vulnerabilities

Anyone with a basic computer interest is probably aware of the existence of security vulnerabilities, at least in a general sense, in our networks and computers. These vulnerabilities are widely discussed in the media. Using a simple Internet search, a 12 year old could locate a variety of hacker tools, then download and implement them. When we first saw the dramatic increase in home computers in early 1990s, we did not worry about attacks on our family computers. Most casual users were not aware that security vulnerabilities even existed. Today, we worry about our systems getting hit with viruses, worms and Trojans. Companies secure web sites and web pages against attacks and defacements. Consumers are concerned that companies are not maintaining adequate security on our personal and financial information as we hear weekly news reports about hackers and new intrusions.

American consumers and businesses increasingly are relying on the Internet to complete transactions. E-commerce is growing in all sectors of the U.S. economy. Most e-commerce transactions are business-to-business (B2B), but e-commerce retail sales reached $46 billion in 2002, up from $36 billion in 2001.[1] When Internet users—be they businesses or consumers—are crippled by Internet fraud schemes, the viability of e-commerce is compromised.

Computer intrusions are a different category from most fraud schemes. Many intrusions are never reported because companies fear a loss of business from reduced consumer confidence

[1] Jennifer Gerlach, ARS Analyst Outlook, January 2003, La Jolla, ARS, Inc.

in their security measures or from a fear of lawsuits. Most of the outsider-intrusions cases opened today are the result of a failure to patch a known vulnerability for which a patch has been issued. Theft of consumer information from a computer system can only be facilitated two ways: by insiders or by outside hackers. Insiders have various motivations, including retribution and money. Outsiders are usually motivated by challenge and/or greed.

The National Research Council issued a report in 2001 titled, "Cybersecurity Today and Tomorrow: Pay Now or Pay Later,"[2] If you have not seen the report, I would urge you to obtain a copy. The report makes a number of significant points and general observations, including a key one for this Hearing:

> "Note also that an attacker...may be able to exploit a flaw accidentally introduced into a system. System design and/or implementation that is poor by accident can result in serious security problems that can be deliberately target in a penetration attempt by an attacker."[3]

If security on a system is inadequate, and someone chooses to exploit the weaknesses, consequences are inevitable. According to the report, there are three things that can go wrong with a computer system or network[4]:

> 1. It can become unavailable or very slow. That is, using the system or network at all becomes impossible, or nearly so.
>
> 2. It can become corrupted, so that it does the wrong thing or gives wrong answers. For example, data stored on the computer may become different from what it should be, as would be the case if medical or financial records were improperly modified.
>
> 3. It can become leaky. That is, someone who should not have access to some or all of the information available through the network obtains such access.

When one of these things happen, the FBI is in a unique position to respond because it is the only Federal agency that has the statutory authority, expertise, and ability to combine the counterterrorism, counterintelligence, and criminal resources needed to effectively neutralize, mitigate, and disrupt illegal computer-supported operations.

The FBI's Cyber Division

The FBI's reorganization of the last two years included the goal of making our cyber

[2] Computer Science and Telecommunications Board (CSTB), National Research Council, Cybersecurity Today and Tomorrow: Pay Now or Pay Later, (Washington, DC, National Academy Press, 2001)

[3] CSTB, page 4

[4] CSTB, page 3

investigative resources more effective. In 2002, the reorganization resulted in the creation of the FBI's Cyber Division.

The Cyber Division addresses cyber threats in a coordinated manner, allowing the FBI to stay technologically one step ahead of the cyber adversaries threatening the United States. The Cyber Division addresses all violations with a cyber nexus, which often have international facets and national economic implications. The Cyber Division also simultaneously supports FBI priorities across program lines, assisting counterterrorism, counterintelligence, and other criminal investigations when aggressive technological investigative assistance is required. The Cyber Division will ensure that agents with specialized technology skills are focused on cyber related matters.

At the Cyber Division we are taking a two-tracked approach to the problem. One avenue is identified as traditional criminal activity that has migrated to the Internet, such as Internet fraud, on-line identity theft, Internet child pornography, theft of trade secrets, and other similar crimes. The other, non-traditional approach consists of Internet-facilitated activity that did not exist prior to the establishment of computers, networks, and the World Wide Web. This encompasses "cyber terrorism," terrorist threats, foreign intelligence operations, and criminal activity precipitated by illegal computer intrusions into U.S. computer networks, including the disruption of computer supported operations and the theft of sensitive data via the Internet. The FBI assesses the cyber-threat to the U.S. to be rapidly expanding, as the number of actors with the ability to utilize computers for illegal, harmful, and possibly devastating purposes is on the rise.

To accomplish its mission, the Cyber Division will form and maintain public/private alliances in conjunction with enhanced education and training to maximize counterterrorism, counterintelligence, and law enforcement cyber response capabilities. The FBI will also maximize the success of cyber investigations through awareness and exploitation of emerging technology.

To support this mission we are dramatically increasing our cyber training program and international investigative efforts. Consequently, specialized units are now being created at FBI Headquarters to provide training not only to FBI cyber squads, but also to the other agencies participating in existing or new cyber-related task forces in which the FBI is a participant. This training will largely be provided to investigators in the field. A number of courses will be provided at the FBI Academy at Quantico.

A typical case will come to the FBI through the Internet Fraud Complaint Center (IFCC), In its fourth year of operation, IFCC has proven to be a very successful clearinghouse, receiving over 75,000 complaints in 2002 on crimes ranging from identity theft and computer intrusions to child pornography.

If the IFCC received an intrusion report from a company in Birmingham, Alabama, we would first attempt to locate where the intrusion took place. That same company may have its servers in Minneapolis, while the intruder is routing attacks through Internet providers in California and Europe. If the servers in Minneapolis were hacked, the Minneapolis Cyber Crime

Task Force would be assigned the lead on the case. The leads could start in California, but end up in Eastern Europe, Nigeria or even back to Birmingham, if an insider was involved. One of the FBI's Computer Analysis Response Teams (CART) would be called upon to preserve computer forensic evidence, and that evidence could be forwarded to one of our new Regional Crime Forensic Labs, now located in Chicago, Dallas and San Diego. The Lab would determine the extent and duration of the intrusion, and whether the attacker came from inside or outside the company. Depending on the sophistication of the intruder, the case can be cracked in a few days or take years. Cases are routinely complex, and often involve international connections. The following cases serve as examples of typical cyber crimes:

Raymond Torricelli, aka "rolex"

Raymond Torricelli, aka "rolex," the head of a hacker group known as "#conflict," was convicted for, among other things, breaking into two computers owned and maintained by the National Aeronautics and Space Administration's Jet Propulsion Laboratory ("JPL"), located in Pasadena, California, and using one of those computers to host an Internet chat-room devoted to hacking.

Torricelli admitted that, in 1998, he was a computer hacker, and a member of a hacking organization known as "#conflict." Torricelli admitted that he used his personal computer to run programs designed to search the Internet, and seek out computers which were vulnerable to intrusion. Once such computers were located, Torricelli's computer obtained unauthorized access to the computers by uploading a program known as "rootkit." The file, "rootkit," is a program which, when run on computer, allows a hacker to gain complete access to all of a computer's functions without having been granted these privileges by the authorized users of that computer.

One of the computers Torricelli accessed was used by NASA to perform satellite design and mission analysis concerning future space missions, another was used by JPL's Communications Ground Systems Section as an e-mail and internal web server. After gaining this unauthorized access to computers and loading "rootkit," Torricelli, under his alias "rolex," used many of the computers to host chat-room discussions.

Torricelli admitted that, in these discussions, he invited other chat participants to visit a website which enabled them to view pornographic images and that he earned 18 cents for each visit a person made to that website. Torricelli earned approximately $300-400 per week from this activity. Torricelli also pled guilty to intercepting usernames and passwords traversing the computer networks of a computer owned by San Jose State University. In addition, Torricelli pled guilty to possession of stolen passwords and usernames which he used to gain free Internet access, or to gain unauthorized access to still more computers. Torricelli admitted that when he obtained passwords which were encrypted, he would use a password cracking program known as"John-the-Ripper" to decrypt the passwords. He also pled guilty to possessing stolen credit card numbers that he obtained from other individuals and stored on his computer. Torricelli admitted that he used one such credit card number to purchase long distance telephone service.

Much of the evidence obtained against Torricelli was obtained through a search of his personal computer. In addition to thousands of stolen passwords and numerous credit card numbers, investigators found transcripts of chat-room discussions in which Torricelli and members of "#conflict" discussed, among other things, (1) breaking into other computers; (2) obtaining credit card numbers belonging to other persons and using those numbers to make unauthorized purchases; and (3) using their computers to electronically alter the results of the annual MTV Movie Awards. This case illustrates the wide variety of criminal acts which can result from security vulnerabilities.

Raphael Gray, aka "Curador"

On March 1, 2000, a computer hacker using the name "Curador" compromised several e-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom, and stole as many as 28,000 credit card numbers with losses estimated to be at least $3.5 million. Thousands of credit card numbers and expiration dates were posted to various Internet websites.. After an extensive investigation, on March 23, 2000, the FBI assisted the Dyfed Powys (Wales, UK) Police Service in a search at the residence of “Curador,” Raphael Gray. Mr. Gray, age 18, was arrested and charged in the UK along with a co-conspirator under the UK’s Computer Misuse Act of 1990. This case illustrates the benefits of law enforcement and private industry around the world working together in partnership on computer crime investigations.

Bloomberg Extortion

Kazakhstan citizens Oleg Zezov, and Igor Yarimaka were arrested on August 10, 2000 in London, England for breaking into Bloomberg L.P.’s Manhattan computer system in an attempt to extort money from Bloomberg. Zezov gained unauthorized access to the internal Bloomberg Computer System from computers located in Almaty, Kazakhstan. In the Spring of 1999, Bloomberg provided database services, via a system known as the "Open Bloomberg," to Kazkommerts Securities located in Almaty, Kazakhstan. Zezov was employed by Kazkommerts.

Zezov sent a number of e-mails to Michael Bloomberg, the founder and owner of Bloomberg, using the name "Alex," demanding that Bloomberg pay him $200,000 in exchange for providing information to Bloomberg concerning how Zezov was able to infiltrate Bloomberg's computer system. Michael Bloomberg sent e-mail to Zezov suggesting that they meet. Zezov demanded that Michael Bloomberg deposit $200,000 into an offshore account. Bloomberg

> established an account at Deutsche Bank in London and deposited $200,000. Michael Bloomberg suggested that they resolve the matter in London and Zezov agreed.
>
> On August 6, 2000, Yarimaka and Zezov flew from Kazakhstan to London. On August 10, 2000, Yarimaka and Zezov met with officials from Bloomberg L.P., including Michael Bloomberg, and two London Metropolitan police officers, one posing as a Bloomberg L.P. executive and the other serving as a translator. At the meeting, Yarimaka allegedly claimed that he was a former Kazakhstan prosecutor and explained that he represented "Alex" and would handle the terms of payment. According to the Complaint, Yarimaka and Zezov reiterated their demands at the meeting. Shortly after the meeting Yarimaka and Zezov were arrested. On February 27, 2003, the trial of Anatoljevich Zezev concluded with a guilty verdict for computer fraud, extortion, use of interstate communications for extortion, and conspiracy. He faces a maximum of 28 years in prison. This case is an example of a traditional crime facilitated by a computer.

Cyber crime continues to grow at an alarming rate, and security vulnerabilities contribute to the problem. We encourage administrators and security professionals to reduce opportunities for criminals by employing best practices and patching vulnerabilities before they can be exploited. The FBI will continue to aggressively pursue cyber criminals as we strive to stay one step ahead of them in the cyber crime technology race.

I thank you for your invitation to speak to you today and on behalf of the FBI look forward to working with you on this very important topic.