

**Testimony of Deputy Assistant Director
of the Federal Bureau of Investigation**

Steven M. Martinez

**before the House Government Reform Committee's Subcommittee on Technology,
Information Policy, Intergovernmental Relations and the Census**

September 22, 2004

Introductory Statement:

Good afternoon Mr. Chairman and members of the subcommittee. I want to thank you for the opportunity to testify before you today about the FBI's efforts to combat Identity Theft, as well as other overlapping cyber crime problems.

Some studies show that more than 10 million Americans were victimized by Identity Theft in the space of one year, with estimated losses exceeding 50 billion dollars.

These estimates demonstrate the significant impact on U.S citizens and businesses. Accordingly, targeting Identity Theft, and related cyber crime activity, will remain a priority of the FBI.

As you may be aware, the FBI prioritized and restructured its approach to cyber crime, in its many forms, a little more than two years ago, with the establishment of the Cyber Division. Several important premises were acknowledged as the foundation for this re-tooling. These included the need for increased law enforcement collaboration and the recognition that Subject Matter Experts (SMEs) from industry are often better positioned to identify and develop information regarding cyber crime incidents before law enforcement. Also, cyber crime does not often lend itself to a constricted list of terms or definitions. In fact, one incident of cyber crime can often be characterized using different labels such as Identity Theft, Phishing, Credit Card Fraud, Account Hijacking,

Computer Intrusion, Hacking, and even theft of Intellectual Property. Even if a more narrow definition of Identity Theft was adopted by law enforcement, it is important to note that the general public bases its definition on that which is portrayed through the TV, print and web-based media, which to date has been very broad.

In recognition of this fact, and the overriding need to gather the most complete and accurate intelligence as quickly as possible, in December of 2003 the FBI's Internet Fraud Complaint Center was renamed the Internet Crime Complaint Center (IC3). Also during this time period, the FBI focused its efforts on developing joint investigative initiatives with our partners in law enforcement, as well as key Internet E-commerce stake holders. These initiatives targeted escalating cyber crimes, both domestically and internationally, and invariably included numerous incidents which could be characterized as Identity Theft.

It should be noted that Identity Theft in its many forms is a growing problem and is manifested in many ways, including large scale intrusions into third party credit card processors; theft from the mails of printed checks, pre-approved credit card offers and mortgage documents; credit card skimming; Phishing schemes; telephone and bank frauds and other crimes.

Prior Testimony of Assistant Director Jana Monroe regarding SPAM:

When FBI Cyber Division Assistant Director Jana Monroe testified before the Senate Committee on Commerce, Science, and Transportation in May of this year, she reported on the FBI's SLAM-Spam initiative, which was developed jointly with law enforcement, industry, and the Federal Trade Commission, and which continues today. This initiative targets significant criminal spammers, as well as companies and

individuals that use spammers and their techniques to market their products. The SLAM-Spam initiative also investigates the techniques and tools used by spammers to expand their targeted audience, to circumvent filters and other countermeasures implemented by consumers and industry, and to defraud customers with misrepresented or non-existent products.

As you may be aware, SPAM is often the “Front End” of a number of cyber crime scenarios. SPAM, which in some cases has been criminalized with the passage of the Can Spam Act of 2003, is used to invite unsuspecting consumers to provide personal, financial, or credit card information, or to visit another site where malicious code, spyware, or another form of a so-called “Trojan horse” (back door) can be installed on their computer for later use. As a result of this initiative, more than 20 Cyber Task Forces are actively pursuing more than 30 criminal and, in some cases, joint civil proceedings against subjects identified to date.

Operation WEB-SNARE:

Several cases against such spammers were recently included in Operation WEB-SNARE, which, on August 26, 2004, was characterized by the Attorney General as the most successful cyber crime initiative to date. In WEB-SNARE, more than 150 investigations were successfully advanced, in which more than 150,000 victims lost more than \$215 million. This initiative included 150 subjects who were charged, and the execution of 170 search and/or seizure warrants. Many of the investigations included in WEB-SNARE could potentially be characterized as Identity Theft, or related to Identity Theft.

Operations E-Con & Cyber Sweep:

Prior to WEB-SNARE, the IC3 coordinated the development and execution of Operations E-Con and Cyber Sweep with our law enforcement and industry partners. In those initiatives, more than 200 investigations were coordinated among the various law enforcement agencies, resulting in arrests and/or charges of more than 250 individuals for engaging in a variety of cyber crimes including Identity Theft.

In addition to demonstrating law enforcement's continued emphasis on cyber crime matters, such initiatives serve as a vehicle to alert consumers and industry about new or evolving schemes to which they may fall victim. Integral to each such initiative are Public Service Advisories or Consumer Be-Ware tips, which are developed in coordination with our federal partners in law enforcement and the FTC, and are included in materials distributed or posted on both law enforcement and industry web-sites. Some examples of these advisories and alerts which have been included in these initiatives have been warnings/alerts regarding Internet employment scams, the Reshipper Fraud, and information regarding Phishing attacks.

Phishing Initiative:

Phishing schemes have a consistent nexus to Identity Theft. Phishing is the creation and use of fraudulent but legitimate looking e-mails and web sites to obtain Internet users' identities and financial account information for criminal purposes. Internet users, who believe they have received an authentic solicitation for information from an entity with which the user has a trusted relationship, are duped into providing their sensitive personal information to criminals who have "spoofed" the e-mails and web sites of the trusted companies and/or government agencies with whom the victims believe

they are interacting. The most frequent targets of interest for criminals conducting such attacks are web sites belonging to the financial services sector, ISPs, and on-line auction venues.

Criminals who engage in Phishing often employ spamming (mass e-mail) techniques to send the Phishing e-mails to thousands or even millions of potential victims nearly simultaneously. Thus, Phishing can be a lucrative criminal enterprise even if only a small percentage of the recipients are deceived into disclosing their personal financial and/or other sensitive information.

Using the Public/Private Alliance model developed for the SLAM-Spam project which proved effective in bringing law enforcement and SMEs to a common venue to address cyber crime, a spin-off initiative is currently being developed to target Phishing. This project is being jointly developed with approximately 40 SMEs from 25 separate industry organizations that have agreed to join law enforcement in this project. This project is being developed jointly between the FBI, U.S. Postal Inspection Service, United States Secret Service, and the FTC, and is expected to be officially launched over the next 30 days.

The Cyber Division is also working closely with the FBI's Criminal Investigative Division, our law enforcement partners, and private industry, on an Identity Theft Working Group, which is actively engaged in intelligence sharing and coordination of public/private investigative efforts to address this crime problem.

International Aspects:

The FBI, through the IC3, has observed a continuing increase in both volume and potential impact of cyber crime with significant international elements. Identifying such

trends, as well as formulating an aggressive and proactive counter-attack strategy, remains a fundamental objective of the FBI's Cyber Division.

In a growing number of cases, Eastern European subjects solicit victims through job postings, email solicitations, and chat-rooms to provide detailed personal information. Once that information is obtained, they use their identities to post auctions on well-known auction sites. Funds obtained through the auction are transferred through several shell accounts, both in the U.S and abroad, and the items sold are never delivered.

In a similar "work at home" variation of this scheme, victims are also required to provide sensitive personal information as part of the application process. Such information is often used to register fraudulent auction sites or to obtain bogus credit cards and may be considered Identity Theft. Once "hired," victims receive packages containing computers and other high-price electronic equipment (usually purchased from on-line retailers with stolen/fraudulent credit cards) with instructions to repackage the items and ship them to locations in Eastern Europe. The victim is provided a cashier's check as payment, typically for several thousand dollars over the amount of the victims' agreed upon salary. Victims are instructed to deposit the check, deduct their salary, and wire the balance to the parent company located in Eastern Europe. Of course, the cashier's checks are later determined to be counterfeit.

West African Re-shippers:

These rapidly expanding schemes often originate in West Africa. A typical scenario includes subject purchases of merchandise from on-line vendors with stolen/fraudulent credit cards, listing a "domestic ship-to location" to allay concerns

regarding suspicious international shipping orders, which are scrutinized and often denied by many E-Commerce merchants.

An expansive network of re-shippers continues to be recruited and utilized by subjects of these schemes. Recruitment is done via Internet Relay Chat (IRC) chat rooms, web based job postings, and even telephone solicitations. In return for the use of their residence or business address, the recruited re-shippers are often allowed to keep certain merchandise as payment, or are paid with counterfeit cashiers checks. New information indicates this scam may also have a European nexus. The potential economic impact is estimated to exceed \$10 billion.

In coordination with law enforcement and industry partners, the FBI through the IC3, has identified 19,000 fraudulent transactions this year alone, involving more than \$11 million in losses. Through recently enhanced cooperation with International Law Enforcement in Ghana and Nigeria, 31 individuals have been arrested and 34 seizures conducted in those countries involving approximately \$1 million in merchandise.

IC3 Complaints Involving Identity Theft:

The IC3 is a joint project between the FBI and the National White Collar Crime Center (NW3C). The IC3 receives, on average, more than 17,000 complaints every month from consumers alone (18,999 in July 2004) and additionally receives a growing volume of referrals from key E-commerce stakeholders. Currently, over 25 percent of all complaints to the IC3 involve some use of spam electronic mail.

Of the more than 400,000 complaints referred to the IC3 since its opening in May of 2000, more than 100,000 were either characterized as Identity Theft, or involved conduct that could be characterized as Identity Theft.

Currently the FBI has more than 2,700 pending investigations of cyber crime matters, not including cases involving online sexual exploitation of children (i.e., our “Innocent Images” initiative). Of the more than 1,800 cyber crime investigations opened in FY 2004, 346 individuals have been convicted with more than 942 million dollars in restitutions and recoveries.

Computer Intrusions/Hackers:

Computer intrusions, or hackers, can significantly contribute to the impact and scope of identity theft. In one FBI investigation initiated in 1999, the computer network of a now defunct software E-commerce company was compromised, and credit card information for approximately eight million accounts was obtained by the hackers. The compromised E-commerce company was contacted via email by the hackers who demanded money to keep them from publicly posting the obtained information on the Internet.

The FBI became aware of this crime when numerous field offices received complaints from citizens who were all incorrectly charged for similar small amounts on their credit card statements. Through investigative efforts, these complaints were all linked to the hacking of the E-commerce company’s system. This case has expanded into a major FBI initiative in which field offices across the country have opened approximately 50 spin-off investigations in the network compromise and extortion of over 100 United States banks and E-commerce providers by Eastern European hacking groups.

Thirty million credit card accounts, including subscriber information, have been stolen as a result of these systems being compromised. The subscribers’ information

obtained through these computer intrusions contained enough information to create false identifications, open bank accounts, apply for loans, and otherwise pose as the original cardholder. Based on a consensus figure of \$500 per account, this represents a potential loss of \$15 billion.

This investigation required the FBI to build upon its international relationships and establish strong ties with foreign law enforcement agencies. Thus far, three of the main subjects of this group have been prosecuted in the U.S., and two others have been prosecuted abroad. Currently, there are five outstanding complaints against the remaining international subjects.

Participation of InfraGard Membership:

InfraGard is an FBI program that began in the Cleveland Field Office in 1996 as a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. Today InfraGard has expanded to all FBI Field Offices with approximately 13,000 members ranging from representatives of Fortune 500 companies to the owners of small ISPs.

At its most basic level, InfraGard is a cooperative undertaking dedicated to sharing information and intelligence derived from various FBI cyber related investigations. InfraGard provides a forum for dialogue and relationship building between policy makers, private companies, and the law enforcement community on a number of issues. Its goal is to enable two way information flow so that the owners and operators of systems and networks can better protect themselves, and, as a result, the United States Government can better discharge its law enforcement and national security responsibilities.

The InfraGard membership regularly provides intelligence and referrals that assist law enforcement's efforts to identify and counter the most significant criminal and national security threats to our country's networks.

Available Statutes:

In addition to the CAN SPAM ACT of 2003, such schemes might be prosecuted through Title 18, USC 1028 (Fraud and related activity in connection with Identity documents), Title 18, USC 1029 (Fraud and related activity in connection with Access Devices), Title 18, USC 1030 (Fraud and related activity in connection with computers), Title 18 USC 2319 (Criminal Infringement of a copyright), Title 18 USC 1343 (Fraud by Wire), Title 18 USC 1341 (Mail Fraud), and Title 18 USC 1028A (Identity theft penalty enhancements).

Conclusion:

Once again, I appreciate the opportunity to come before you today and share the work that the Cyber Division has undertaken to address the problem of Identity Theft. The FBI's efforts in this arena will continue, and we will continue to keep Congress informed of our progress in protecting the America's citizens and economy.