Statement of Mr. Craig Magaw

Special Agent in Charge
Criminal Investigative Division
United States Secret Service

Before the Committee on the Judiciary
Subcommittee on Crime, Terrorism and Homeland Security

U.S. House of Representatives

December 18, 2007

Good afternoon, Chairman Scott, Ranking Member Gohmert and distinguished members of the subcommittee. I would like to thank you for the opportunity to address this subcommittee on the subject of identity crime and the role of the U.S. Secret Service in these investigations.

While the Secret Service is perhaps best known for protecting our nation's leaders, we also investigate a wide variety of financial crimes. In our role of protecting the nation's critical infrastructure and financial payment systems, the Secret Service has a long history of protecting American consumers and the financial industry from fraud. With the passage of legislation in 1984, the Secret Service was provided authority for the investigation of access device fraud, including credit and debit card fraud, and parallel authority with other law enforcement agencies in identity crime cases. In recent years, the combination of the information revolution and the effects of globalization have caused the investigative mission of the Secret Service to evolve.

Through our work in the areas of financial and electronic crime, the Secret Service has developed particular expertise in the investigation of identity theft, false identification fraud, credit card fraud, debit card fraud, check fraud, bank fraud, cyber crime, and computer intrusions. In Fiscal Year 2007, agents assigned to Secret Service offices across the United States arrested over 4,300 suspects for identity theft crimes. These suspects were responsible for approximately $690 million in actual fraud loss to individuals and financial institutions.

These criminals seek the personal identifiers generally required to obtain goods and services on credit, such as Social Security numbers, names, and dates of birth. Identity crimes also involve the theft or misuse of an individual's financial identifiers such as credit card numbers, bank account numbers, and personal identification numbers.

The Secret Service has observed a marked increase in identity theft and access device fraud. Criminals continue to seek new methods of compromising victims' personal and financial information. In the 1980's and 1990's, criminals obtained stolen personal and financial information through traditional means such as, theft of mail, theft of trash from businesses or

victims, home and vehicle burglaries, and theft of a victim's wallet or purse. While these low-tech methods of theft remain popular, criminal activity has evolved to new methods of obtaining large quantities of stolen information.

The recent trend observed by law enforcement is the use of computers and the Internet to launch cyber attacks targeting citizens and financial institutions. Cyber criminals have become adept at stealing victims' personal information through the use of phishing emails, account takeovers, malicious software, hacking attacks, and network intrusions resulting in data breaches.

The Secret Service continues to see a considerable volume of access device fraud, usually in the form of criminal exploitation of stolen credit card data. Of particular concern are those incidents in which large quantities of credit card and related personal data are stolen through electronic intrusions into the networked systems of major retailers or the systems of credit card processors. A considerable portion of this type of electronic theft appears to be attributable to organized groups, many of them based abroad, who pursue both the intrusions, as well as the subsequent exploitation of the stolen data. Stolen credit card data is often trafficked in units that include more than just the card number and expiration date. "Full-info cards" include such additional information as complete name and address information of the cardholder, mother's maiden name, date of birth, Social Security number, PIN, and other personal information that allows additional criminal exploitation of the account. Another marked trend observed in 2007, has been the rise in volume of trafficking in card track data together with PINs; this data allows a criminal to manufacture a fully functional counterfeit card and execute ATM withdrawals or other PIN-enabled transactions against the account.

This stolen information is often sold in bulk quantities on various illicit Internet carding portals. These portals, or "carding websites," can be likened to online bazaars where the criminal element converges to conduct their business. The websites vary in size, from a few dozen members, to some of the more popular sites which boast memberships of approximately 8,000 users. Within these portals, there are separate forums which are moderated by notorious members of the carding community. Members can meet online and discuss specific topics of interest. Criminal purveyors buy, sell, and trade malicious software, spamming services, credit, debit, and ATM card data, personal identification data, bank account information, hacking services and other contraband.

In addition to the exploitation of credit and debit card accounts, many of the more sophisticated online criminal networks are now actively exploiting compromised online financial accounts. Criminals who gain access to victim accounts using online systems then execute fraudulent electronic banking transfers or sell the information to other criminals. The desire to exploit online bank accounts has led to the explosive growth of phishing, as well as the recent wave of "malware" or "crimeware," malicious software designed specifically to harvest account login information from the computers of infected victims. The technical sophistication of the illicit services readily available continues to grow. For example, the online fraud networks are increasingly leveraging the technical capabilities of "botnets" (i.e. networks of thousands of infected computers which can be controlled by a criminal from a central location) for financial attacks ranging in nature from the hosting of phishing and other malicious websites to the

launching of widespread attacks against the online authentication systems of U.S. financial institutions.

The information revolution of the 1990's has turned our personal and financial information into a valuable commodity, whether it is being collected and brokered by a legitimate company or stolen by an identity thief. This information is no longer only an instrument used to facilitate a financial crime; it is now the primary target of criminals. Consequently, private citizens as well as corporations and financial institutions must take appropriate measures to secure sensitive personally identifiable information. This information is particularly vulnerable when it is stored on personal computers or disclosed over Internet and email connections. Consumers must adhere to comprehensive computer security practices.

Today, hundreds of companies specialize in data mining, data warehousing, and information brokerage. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals. However, businesses can provide a first line of defense against identity crime by safeguarding the information they collect. Such efforts can significantly limit the opportunities for identity crime. Furthermore, the prompt reporting by data brokers of major security breaches involving sensitive personally identifiable information to the proper authorities would ensure a thorough investigation is conducted.

Globalization has made commerce easy and convenient for corporations and consumers. Financial institutions and systems are accessible worldwide. Today's cyber criminals have adapted to this new means of global trade and exploit our dependence on information technology. With the explosion of Internet accessibility world-wide, the criminal element has modified their fraudulent schemes to a new, more anonymous and constantly evolving cyber arena. Having been the target of many of these crimes, the financial sector has some of the most sophisticated security and authentication mechanisms and are constantly evolving their practices to counter this criminal activity Likewise, the Secret Service has modified its investigative techniques to keep pace with emerging technologies.

Criminal groups involved in identity crimes routinely operate in a multi-jurisdictional environment. This creates problems for local law enforcement agencies that generally act as the first responders. By working closely with other federal, state, and local law enforcement representatives, as well as international police agencies, the Secret Service is able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries. This partnership approach to law enforcement is vital to our criminal investigative mission.

The Secret Service's expertise is enhanced through partnerships and identity theft task forces to assist in the national effort to safeguard personal and financial information. These partnerships with other law enforcement agencies and industry representatives perform a crucial role in protecting the financial infrastructure and economic stability of the United States by leveraging the technical expertise and investigative experience of partner agencies.

The Secret Service has established unique partnerships with state, local, and other federal law enforcement agencies through years of collaboration on our investigative and protective

endeavors. These partnerships enabled the Secret Service to establish a national network of Financial Crimes Task Forces (FCTFs) to combine the resources of the private sector and other law enforcement agencies in an organized effort to combat threats to our financial payment systems and critical infrastructures. The Secret Service currently maintains 29 FCTFs located in metropolitan regions across the country. While our FCTFs do not focus exclusively on identity crime, we recognize that stolen identifiers are often a central component of other financial crimes. Consequently, our task forces devote considerable time and resources to the issue of identity crime.

The Secret Service has always employed a proactive, rather than reactive, approach to combating crime. In 1996, the Secret Service established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private sector, and local, state, and federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. The USA PATRIOT Act of 2001, P.L. 107-56, recognized the effectiveness of the New York ECTF and mandated that the Secret Service establish a nationwide network of ECTFs to prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

ECTFs leverage combined resources in an organized effort to combat threats to our financial payment systems and critical infrastructures. Partnerships between law enforcement and the private sector are critical to the success of the ECTF's "focus on prevention" approach. Our ECTFs collaborate with private sector technical experts in an effort to protect their system networks and critical information by encouraging the development of business continuity plans and routine risk management assessments of their electronic infrastructure. Greater ECTF liaison with the business community provides rapid access to law enforcement and vital technical expertise during incidents of malicious cyber crimes. The ECTFs also focus on partnerships with academia to ensure that law enforcement is on the cutting edge of technology by leveraging the research and development capabilities of teaching institutions and technical colleges.

These resources allow ECTFs to identify and address potential cyber vulnerabilities before the criminal element exploits them. This proactive approach has successfully prevented cyber attacks that otherwise would have resulted in large-scale financial losses to U.S. based companies or disruptions of critical infrastructures.

The Secret Service task force models open the lines of communication and encourage the unlimited exchange of information between federal, state, and local law enforcement. Currently, the Secret Service maintains 24 ECTFs in major metropolitan regions across the United States.

Another important goal of the Secret Service is to raise awareness of issues related to identity theft and financial crimes, both in the law enforcement community and the general public. The Secret Service has worked to educate consumers and provide training to law enforcement personnel through a variety of programs and initiatives. Agents from local field offices routinely provide community outreach seminars and public awareness training on the subjects of identity theft and computer fraud. Agents often address these topics when speaking to school groups, civic organizations, and staff meetings involving businesses or financial institutions.

Additionally, the Secret Service provides recurring identity theft training to state and local police departments. This training includes formal and informal classes which occur at police roll calls, field office sponsored seminars, police academies, and other various settings. Currently, the Secret Service provides formal computer training to state and local police departments to allow officers to act as "first responders" in cyber crimes investigations. Officers are trained in basic electronic crimes investigations, network intrusion investigations, and computer forensics.

The Secret Service currently participates in a joint effort with the Department of Justice, the U.S. Postal Inspection Service, the Federal Trade Commission (FTC), the International Association of Chiefs of Police (IACP), and the American Association of Motor Vehicle Administrators to host identity crime training for law enforcement officers. In the last three years, Identity Crime Training Seminars have been held in approximately 20 cities nationwide. These training seminars are focused on providing local and state law enforcement officers with tools and resources that they can immediately put into use in their investigations of identity crime.

The Secret Service has also assigned a special agent to the FTC as a liaison to support all aspects of the Commission's program to encourage the use of the Identity Theft Data Clearinghouse as a law enforcement tool. The FTC has done an excellent job of providing people with the information and assistance they need in order to take the steps necessary to correct their credit records, as well as undertaking a variety of consumer awareness initiatives regarding identity theft.

Additionally, the Secret Service is committed to providing our law enforcement partners with publications and guides to assist them in combating identity theft and cyber crime. As criminals increasingly use computers and electronic storage devices, these items become important pieces of evidence. To ensure proper investigation and successful prosecution, officers need specific instructions pertaining to the seizure and analysis of electronic evidence. To provide this essential knowledge, the Secret Service published the "*Best Practices Guide for Seizing Electronic Evidence*" which is designed as a pocket guide for the police officers and detectives acting as first responders. This guide assists law enforcement officers in recognizing, protecting, seizing, and searching electronic devices in accordance with applicable statutes and policies. This guide has been updated as appropriate, and it is currently issued in its third edition.

The Secret Service also cooperated with several of our task force partners to produce the interactive, computer-based training program known as "*Forward Edge*." *Forward Edge* is a CD-ROM that provides law enforcement and corporate investigative personnel with practical training in the recognition and seizure of electronic storage items. This year we completed an updated version of this training tool and just released "*Forward Edge II*."

In addition, the Secret Service produced an Identity Crime Video/CD-ROM which contains over 50 investigative and victim assistance resources that local and state law enforcement officers can use when combating identity crime. This CD-ROM also contains a short identity crime video that can be shown to police officers at their roll call meetings which discusses why identity crime is important, what other departments are doing to combat identity crime, and what tools and resources are available to officers. The Identity Crime CD-ROM is an interactive resource guide that was made in collaboration with the U.S. Postal Inspection Service, the FTC and the IACP.

To date, approximately 50,000 Identity Crime CD-ROMs have been distributed to law enforcement departments and agencies across the United States. We have distributed over 400,000 *Best Practices Guides* and over 50,000 *Forward Edge* training CD-ROMs to local and federal law enforcement officers nationwide.

In conclusion, I would like to reiterate that identity theft is an evolving threat. Law enforcement agencies must be able to adapt to emerging technologies and criminal methods. The Secret Service is pleased that Congress is considering legislation that recognizes the magnitude of these issues and the constantly changing nature of these crimes. To effectively fight this crime, our criminal statutes must be amended to safeguard sensitive personally identifiable information and to afford law enforcement the appropriate resources to investigate data breaches.

The Secret Service appreciates the Subcommittee's work to enhance penalties and broaden investigative jurisdictions associated with identity theft and cyber crime. H.R. 4175 addresses many of the issues I have discussed in this statement concerning these offenses. H.R. 4175 expands the definition of cyber crime, requires data brokers to notify law enforcement authorities of major security breaches, and increases penalties for identity theft and other violations of data privacy and security. The Secret Service looks forward to working closely with Congress as they address identity crime legislation.

As I have highlighted in my statement, the Secret Service has implemented a number of initiatives pertaining to identity crimes. We have dedicated enormous resources to increase awareness, educate the public, provide training for law enforcement partners, and improve investigative techniques. We will continue to aggressively investigate identity theft offenders to protect consumers. The Secret Service is committed to our mission of safeguarding the nation's critical infrastructure and financial payment systems.

Chairman Scott, Ranking Member Gohmert, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.