Statement of Mr. Pablo A. Martinez
Deputy Special Agent in Charge
Criminal Investigative Division
U.S. Secret Service

Hearing before the
Senate Committee on the Judiciary

"Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats"

September 07, 2011

Good morning, Chairman Leahy, Ranking Member Grassley and distinguished members of the Committee. Thank you for the opportunity to testify on U.S. Secret Service's (Secret Service) investigative role in combating cyber crime.

As the original guardian of the Nation's financial payment systems, the Secret Service has a long history of protecting American consumers, industries and financial institutions. Over the last two decades, the Secret Service's statutory authorities have been reinforced to include access device fraud (18 USC §1029), which includes credit and debit card fraud. The Secret Service also has concurrent jurisdiction with other law enforcement agencies for identity theft (18 USC §1028), computer fraud (18 USC §1030), and bank fraud (18 USC §1344).

In 2010, the Secret Service's unique multifaceted approach to combating cyber crime led to the arrest of over 1,200 suspects for cyber crime related violations and the examination of 867 terabytes of data, which is roughly the equivalent of 867,000 copies of the Encyclopedia Britannica. These investigations involved over $500 million in actual fraud loss and prevented approximately $7 billion in additional losses. As a result of our efforts, the Secret Service is recognized worldwide for our innovative approaches to detecting, investigating and preventing cyber crimes. Furthermore, in alignment with the President's Comprehensive National Cyber Security Initiative, the Secret Service will continue to raise our overall capabilities in combating cyber crime and related forms of illegal computer activity.

The Administration is aware that in order to fully protect American citizens from cyber threats, certain sections of our current cyber security laws must be updated. Last spring, the Administration released its proposal to address the cybersecurity needs of our country. The legislative package proposed by the Administration addresses key improvements for law

enforcement. Secret Service investigations have shown that complex and sophisticated electronic crimes are rarely perpetrated by a lone individual. Online criminals organize in networks, often with defined roles for participants, in order to manage and perpetuate ongoing criminal enterprises dedicated to stealing commercial data and selling it for profit. The Administration's proposal will better equip law enforcement agencies, such as the Secret Service, with additional tools to combat transnational cyber crime by enhancing penalties against criminals that attack critical infrastructure and by adding computer fraud as a predicate offense under the Racketeering Influenced Corrupt Organizations Act (RICO).

The proposal also includes additional measures to protect consumers against identity theft by standardizing and simplifying the current patchwork of state laws that govern reporting of breaches of personally identifiable information and requiring businesses to notify affected individuals and the government if the business suffers a breach.

Trends in Cyber Crimes

Advances in computer technology and greater access to personal information via the Internet have created a virtual marketplace for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity and complexity of cyber crimes targeting private industry and critical infrastructure. These crimes include network intrusions, hacking attacks, development and use of malicious software, and account takeovers leading to significant data breaches affecting every sector of the world economy. As large companies have adopted more sophisticated protections against cyber-crime, criminals have adapted as well by increasing their attacks against small and medium-sized businesses, banks, and data processors. Unfortunately, many smaller businesses do not have the resources to adopt and continuously upgrade the sophisticated protections needed to safeguard data from being compromised.

The Secret Service has continued its collaboration with Verizon on the 2011 Data Breach Investigations Report (DBIR) to identify emerging threats, educate Internet users, and evaluate new technologies that work to prevent and mitigate attacks against critical computer networks. Researchers from law enforcement and the private sector examined roughly 800 new data breaches. The results from the Verizon study show that two of the noticeable trends in cybercrime over the past couple of years involve the ongoing targeting of Point of Sale (POS) systems as well as the compromise of online financial accounts, often through malware written explicitly for that purpose, with subsequent transaction fraud involving those accounts.

Compared to recent history, it appears that while there were more data breaches in 2010, the amount of compromised data decreased due to the size of the compromised companies' databases. This change demonstrates the willingness of organized cybercriminals to go after the smaller, easier targets that provide a smaller, yet steady, stream of potentially available data. In light of recent arrests and prosecutions following large-scale intrusions into financial services firms, criminals may be weighing the reward versus the risk, and opting to "play it safe".

The report also indicates that there has been noticeable increase in account takeovers that result in fraudulent transfers from the victim's account to an account under the control of the

perpetrator. This increase can be directly tied to the continued rise of malware variants created to capture login credentials to financial websites. The Secret Service and the financial services community are working together to combat this growing trend. The Financial Services Information Sharing and Analysis Center (FS-ISAC) has teamed up with the Secret Service, Department of the Treasury, Department of Justice and many other agencies to create the Account Takeover Task Force (ATOTF), which focuses on prevention, detection and response to account takeovers.

The increasing level of collaboration among cyber-criminals raises both the complexity of investigating these cases and the level of potential harm to companies and individuals. For example, illicit Internet carding portals allow criminals to traffic stolen information in bulk quantities globally. These portals, or "carding forums," operate like online bazaars where criminals converge to trade personal financial data and cyber-tools of the trade. The websites vary in size; some of these criminal forums are limited to a few hundred members while others boast memberships of tens of thousands of users. Within these portals, there are separate forums moderated by senior and experienced members of the carding community who discuss tactics and techniques for overcoming security controls and pursuing complex fraud schemes. Criminal purveyors on these forums buy, sell, and trade malicious software, spamming services, credit and debit card data, personal identification data, bank account information, brokerage account information, hacking services, counterfeit identity documents and other forms of contraband.

The effects of the criminal acts extend well beyond the companies compromised, affecting millions of individual card holders in one of the incidents. Although swift investigation, arrest, and prosecution prevented many consumers from direct financial harm, all potential victims were at risk for misuse of their credit cards, overall identity theft, or both. Further, business costs associated with the need for enhanced security measures, reputational damage and direct financial losses are ultimately passed on to consumers.

Collaboration with Other Federal Agencies and International Law Enforcement

While cyber-criminals operate in a world without borders, the law enforcement community does not. The increasingly multi-national, multi-jurisdictional nature of cyber crime cases has increased the time and resources needed for successful investigation and adjudication. The partnerships developed with other law enforcement entities, the private sector and academia through our Electronic Crimes Task Forces, the support provided by our Cyber Intelligence Section, the liaison established by our overseas offices, and the training provided to our special agents via Electronic Crimes Special Agent Program were all instrumental to the Secret Service's successful investigation into the network intrusion of Heartland Payment Systems – the largest and most complex data breach investigation ever prosecuted in the United States.

Recognizing these complexities, several federal agencies are collaborating to investigate cases and identify proactive strategies. Greater collaboration within the federal, state and local law enforcement community enhances information sharing, promotes efficiency in investigations, and facilitates efforts to de-conflict in cases of concurrent jurisdiction. For example, the Secret Service has collaborated extensively with the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS), a key partner in preventing, investigating and prosecuting

computer crimes. The Secret Service's Electronic Crimes Task Forces are a natural complement to CCIPS, and have resulted in an excellent partnership over the years. In the last decade, nearly every major cyber investigation conducted by the Secret Service has benefited from CCIPS contributions. Successful investigations such as the prosecution of the Shadowcrew criminal organization, E-Gold prosecution, and TJX and Heartland investigations, were a result of this valued partnership.

One of the main obstacles that agents investigating transnational crimes encounter are jurisdictional limitations. The Secret Service believes that to fundamentally address this issue, appropriate levels of liaison and partnerships must be established with our international law enforcement counterparts. Currently, the Secret Service operates 23 offices abroad, each having regional responsibilities to provide global coverage. The personal relationships that have been established in those countries are often the crucial element to the successful investigation and prosecution of suspects abroad.

Mitigation and prevention are keys to reducing the threat from cyber criminals. Recognizing this reality, the Secret Service has strengthened its partnership and collaboration with the National Protection and Programs Directorate's (NPPD) United States Computer Emergency Readiness Team (US-CERT), which provides response support and defense against cyber intrusions or incidents for the Federal Civil Executive Branch (.gov) domain, as well as information sharing and collaboration with state and local government, industry and international partners. As the Secret Service identifies malware, suspicious IPs and other information through its criminal investigations, it shares this information with US-CERT. To support such collaboration, US CERT recently published Early Warning Indicator Notices (EWINs) on information gathered through Secret Service investigations. The Secret Service looks forward to building on its full-time presence at US-CERT, and broadening this and other partnerships within the Department.

As a part of these efforts and to ensure that information is shared in a timely and effective manner, the Secret Service has personnel detailed to the following DHS and non-DHS entities:

- NPPD's Office of the Under Secretary;
- NPPD's National Cyber Security Division (US-CERT);
- NPPD's Office of Infrastructure Protection;
- National Cybersecurity and Communications Integration Center (NCCIC)
- DHS's Science and Technology Directorate (S&T);
- FBI National Cyber Investigative Joint Task Force (NCIJTF);
- Each FBI Joint Terrorism Task Force (JTTF), including the National JTTF;
- Department of the Treasury - Terrorist Finance and Financial Crimes Section
- Department of the Treasury - Financial Crimes Enforcement Network (FinCEN);
- Central Intelligence Agency;
- Department of Justice, International Organized Crime and Intelligence Operations Center;
- Drug Enforcement Administration's Special Operations Division
- EUROPOL; and
- INTERPOL

Secret Service Framework

In line with the Department's focus of creating a safer cyber environment and in order to protect our financial infrastructure, industry, and the American public, the Secret Service has adopted a multi-faceted approach to aggressively combat cyber and computer-related crimes. The Secret Service has dismantled some of the largest known transnational cyber-criminal organizations by:

- providing computer-based training to enhance the investigative skills of special agents through our **Electronic Crimes Special Agent Program**, and to our state and local law enforcement partners through the **National Computer Forensics Institute**;
- collaborating with our partners in law enforcement, the private sector and academia through our 31 **Electronic Crimes Task Forces**;
- identifying and locating international cyber-criminals involved in network intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes through the analysis provided by our **Cyber Intelligence Section**;
- maximizing partnerships with international law enforcement counterparts through our 23 **international field offices**; and
- maximizing technical support, research and development, and public outreach through the **Software Engineering Institute/CERT Liaison Program** at Carnegie Mellon University and the **Cell Phone/PDA Forensic Facility** at University of Tulsa.

Electronic Crimes Special Agent Program

A central component of the Secret Service's cyber-crime investigations is its Electronic Crimes Special Agent Program (ECSAP), which is comprised of nearly 1,400 Secret Service special agents who have received at least one of three levels of computer crimes-related training. These agents are deployed in more than 98 Secret Service offices throughout the world and have received training in forensic identification, preservation and retrieval of electronically stored evidence. ECSAP-trained agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence. These special agents are equipped to investigate the continually evolving arena of electronic crimes and have proven invaluable in the successful prosecution of criminal groups involved in computer fraud, bank fraud, identity theft, access device fraud and various other electronic crimes targeting our financial institutions and private sector.

The ECSAP program is divided into three levels of training:

Level I – Basic Investigation of Computers and Electronic Crimes (BICEP) The BICEP training program focuses on the investigation of electronic crimes and provides a brief overview of several aspects involved with electronic crimes investigations. This program provides Secret Service agents and our state and local law enforcement partners with a basic understanding of computers and electronic crime investigations and is now part of our core curriculum for newly hired special agents.

Level II – Network Intrusion Responder (ECSAP-NI) ECSAP-NI training provides special agents with specialized training and equipment that allows them to respond to and investigate

network intrusions. These may include intrusions into financial sector computer systems, corporate storage servers or various other targeted platforms. The Level II trained agent will be able to identify critical artifacts that will allow effective investigation of identity theft, malicious hacking, unauthorized access, and various other related electronic crimes.

Level III – Computer Forensics (ECSAP-CF) ECSAP-CF training provides special agents with specialized training and equipment that allows them to investigate and forensically obtain legally admissible digital evidence to be utilized in the prosecution of various electronic crimes cases, as well as criminally focused protective intelligence cases.

Electronic Crimes Task Forces

In 1995, 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. Congress further directed the Secret Service in Public Law 107-56 to 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."

The Secret Service currently operates 31 ECTFs, including two based overseas in Rome, Italy and London, England. Membership in our ECTFs includes: 4,093 private sector partners; 2,495 international, federal, state and local law enforcement partners; and 366 academic partners. By joining our ECTFs, all of our partners benefit from the resources, information, expertise and advanced research provided by our international network of members while focusing on issues with significant regional impact.

Cyber Intelligence Section

Another example of our partnership approach with private industry is our Cyber Intelligence Section (CIS) which collects, analyzes, and disseminates data in support of Secret Service investigations worldwide and generates new investigative leads based upon its findings. CIS leverages technology and information obtained through private sector partnerships as well as evidence obtained from Secret Service investigations and undercover operations to monitor developing technologies and trends in the financial payments industry for information that may be used to enhance the Secret Service's capabilities to prevent and mitigate attacks against the financial and critical infrastructures.

CIS has an operational unit that investigates international cyber-criminals involved in cyber-intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. The information and coordination provided by CIS is a crucial element to successfully investigating, prosecuting, and dismantling international criminal organizations.

National Computer Forensics Institute

The National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, NPPD, the State of Alabama and the Alabama District Attorney's

Association. The goal of this facility is to provide a national standard of training for a variety of electronic crimes investigations. The program offers state and local law enforcement officers, prosecutors, and judges the training necessary to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and conduct electronic crimes investigations.

Since the establishment of NCFI on May 19, 2008, the Secret Service has provided critical training to 932 state and local law enforcement officials representing over 300 agencies from all 50 states and two U.S. territories.

Computer Emergency Response Team/Software Engineering Institute (CERT-SEI)

In August 2000, the Secret Service and Carnegie Mellon University Software Engineering Institute (SEI) established the Secret Service CERT Liaison Program to provide technical support, opportunities for research and development and public outreach and education to more than 150 scientists and researchers in the fields of computer and network security, malware analysis, forensic development, training and education. Supplementing this effort is research into emerging technologies being used by cyber-criminals and development of technologies and techniques to combat them.

The primary goals of the program are: to broaden the Secret Service's knowledge of software engineering and networked systems security; to expand and strengthen partnerships and relationships with the technical and academic communities; to provide an opportunity to work closely with CERT-SEI and Carnegie Mellon University; and to present the results of this partnership at the quarterly meetings of our ECTFs.

In August 2004, the Secret Service partnered with CERT-SEI and the Department of Homeland Security's Science and Technology Directorate to publish the first ever "Insider Threat Study" examining the illicit cyber activity in the banking and finance sector. Due to the overwhelming response to this initial study, the Secret Service and CERT-SEI, in partnership with DHS S&T, are working to update the study. An updated study, expected to be released in late 2011, will analyze actual incidents of insider crimes from inception to prosecution. The research team will share its findings with federal, state, and local law enforcement, private industry, academia and other government agencies.

Cell Phone/Forensic Facility

The U.S. Secret Service Cell Phone Forensic Facility at the University of Tulsa conducts training, examinations, and research in the field of mobile device forensics to include skimmers, cell phones, and GPS units. The facility's mobile device forensic capabilities are among the best in the world. Agents trained at the facility complete examinations in the field with the more problematic devices submitted to the facility for examination. University of Tulsa students, who are a part of the national Cyber Corps Scholarship for Service Program, work in collaboration with special agents on mobile device research projects year round.

To date, 49 special agents have been trained in Basic Mobile Device Forensics; 48 special agents have been trained in Advanced Mobile Device Forensics; 31 special agents have been trained in Mobile Device Forensics Refresher; and 45 special agents have been trained in Advanced Android Forensics. The success of this program is clear, with over 5,000 mobile device examinations conducted since 2008.

Conclusion

As more information is stored in cyberspace, target-rich environments are created for sophisticated cyber criminals. With proper network security, businesses can provide a first line of defense by safeguarding the information they collect. Such efforts can significantly limit the opportunities for these criminal organizations. Furthermore, the prompt reporting of major data breaches involving sensitive personally identifiable information to the proper authorities will help ensure a thorough investigation is conducted.

The Secret Service is committed to safeguarding the Nation's financial payment systems by investigating and dismantling criminal organizations involved in cyber crime. Responding to the growth in these types of crimes and the level of sophistication these criminals employ requires significant resources and greater collaboration among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates significant resources to improving investigative techniques, providing training for law enforcement partners and raising public awareness. The Secret Service will continue to be innovative in its approach to cyber crime and cyber security and is pleased that the Committee recognizes the magnitude of these issues and the evolving nature of these crimes.

Chairman Leahy, Ranking Member Grassley, and distinguished members of the Committee, 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.