Statement of

A.T. Smith
Assistant Director
U.S. Secret Service

Hearing before the
House Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit

"Cyber Security Threats to the Financial Sector"

September 14, 2011

Good morning Madam Chair, Ranking Member Maloney and distinguished members of the Subcommittee. 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. To put it in perspective, that is nearly four times the amount of data collected in the archives of the Library of Congress[1]. 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.

[1] U.S. Library of Congress. (n.d.) *Library of Congress: Web Archiving FAQs.* Retrieved from http://www.loc.gov/webarchiving/faq.html#faqs_05.

Trends in Cyber Crimes

Advances in computer technology and greater access to personal information via the Internet have created a 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 may indicate that organized cybercriminals are becoming more willing 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 a 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 the FBI, 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.

Collaboration with Other Federal Agencies and International Law Enforcement

Cyber criminals may operate in a world without borders; however, the law enforcement community is constrained by jurisdictional boundaries. The successful investigation and adjudication of these transnational cyber crime cases is time and resource intensive.

In order to successfully perform its protective and investigative responsibilities, the Secret Service has cultivated relationships with state, local, and foreign law enforcement. Its domestic and international offices continue to serve as the platform from which the Secret Service expands its network of partners. The success of this approach is seen in a number of cases including the Secret Service's investigations into the complex network intrusions of TJX and Heartland Payment Systems – two of the largest data breach investigations ever prosecuted in the United States.

In addition, the Secret Service has been responsible for apprehending members of foreign organized criminal groups, such as the CarderPlanet criminal organization, that target the U.S. financial infrastructure through online intrusions and theft and exploitation of stolen financial information. Through extensive work and international coordination, the Secret Service was able to apprehend:

- A pioneer in the criminal world for developing a model in which he hired teams of hackers to target the financial industry to harvest card track data by the millions.
- A criminal who targeted home equity lines of credit maintained by persons on the list of wealthiest Americans. After traveling to the United States from his home in Russia he was apprehended and subsequently admitted to stealing millions of dollars.
- A co-founder of CarderPlanet, who also appears to have a background in law enforcement. The suspect is alleged to have created the first fully automated online store for selling stolen credit card data. Working with our international law enforcement partners, the suspect was identified and apprehended as he was boarding an international flight to Russia.
- A criminal who ran a variety of schemes with his partners in the former Soviet states while residing in Southern California. He is currently facing an array of charges in California.
- A criminal whose trafficking in stolen financial information was so brazen that Russian authorities worked with the Secret Service to secure a six-year prison sentence for the suspect in the Russian Federation.

The Secret Service, in conjunction with its many law enforcement partners across the United States and around the world, continues to successfully combat these crimes by adapting our investigative methodologies. Our success is due in part to the cooperation of these partners in more than a dozen international law enforcement agencies.

Currently, the Secret Service operates 24 offices abroad, including one in Beijing, China, which recently opened on September 11, 2011. While each office has 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.

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.

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 IP addresses 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.

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 142 domestic and 24 international field offices; and
- maximizing technical support, research and development in part with DHS Science and Technology Directorate, 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 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.

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.

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.

The Secret Service is committed to safeguarding the nation's financial payment systems. Responding to the increase in cyber crime and the growing 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, remaining innovative in it approach, providing training for law enforcement partners and raising public awareness.

Madam Chair, Ranking Member Maloney, and distinguished members of the Subcommittee, 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.