Statement of Mr. A.T. Smith
Assistant Director
Office of Investigations
U.S. Secret Service

Before the Committee on Financial Services
U.S. House of Representatives:
"Hacked Off: Helping Law Enforcement Protect Private Financial Information"

June 29, 2011

Good afternoon Chairman Bachus, Ranking Member Frank, and other distinguished Members of the Committee. Thank you for holding this hearing at the National Computer Forensics Institute (NCFI) and for giving the U.S. Secret Service (Secret Service) the opportunity to discuss our role in protecting cyberspace, particularly as it relates to the safeguarding of our nation's critical financial infrastructure. We are proud of the training program that has been established at this facility and look forward to working with Congress to ensure its continued success.

The Secret Service's dual mission of investigations and protection has evolved over the course of the last century, not because we seek new responsibilities but because the criminal methods used by our adversaries are constantly evolving. Based on our history as an investigative bureau of the Department of Treasury, the Secret Service has jurisdiction to investigate all forms of financial crimes including identity theft, false identification, mortgage fraud, and counterfeit checks. Given that the majority of these crimes today are committed via electronic means, the Secret Service has become very active in the investigation and prevention of cybercrime. As a result of these investigations, and with the development of specialized training programs to equip our agents with the skills needed to gather forensic evidence to successfully prosecute these crimes, the Secret Service's work is critical to the protection of both physical assets and computer networks upon which our economy and our communities rely.

National Computer Forensics Institute (NCFI)

The investigative mission of the Secret Service cannot succeed without the cooperation of local and state law enforcement, the private sector, and academia. Law enforcement and judiciary officials from all over the United States come here to the NCFI for vital digital forensics training necessary to protect our nation's financial infrastructure, commerce,

and well being of our citizens. The NCFI is a testament to the essential cooperation needed to fight the ever evolving cyber threats faced in our increasingly interconnected global community.

The NCFI, which is a result of a partnership between the DHS National Protection and Programs Directorate (NPPD), the Secret Service, the State of Alabama, the City of Hoover, Shelby County, the Alabama District Attorney's Association, and the Alabama Securities Commission, was established to provide computer forensic training and tools to state and local law enforcement officers, prosecutors, and judges to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and conduct electronic crimes investigations. This training also has the benefit of providing state and local law enforcement with the skills and tools to combat a myriad of crimes in their community.

Since the establishment of the NCFI in 2008, DHS-NPPD has transferred $4 million annually to the Secret Service to train state and local law enforcement officials, prosecutors, and judges on the importance of computer forensics to criminal investigations. Responding to the growth of cyber crimes and the level of sophistication these criminals employ requires training, resources and greater collaboration among law enforcement and its public and private sector partners. Thus far, 644 state and local law enforcement officials, 216 prosecutors, and 72 judges representing over 300 agencies from all 50 states and two U.S. territories have received training from the Secret Service through the NCFI. After initial participation in the program, 80 NCFI students have returned to take one or more advanced courses at the Institute over the last three years.

Collaboration Among State, Local, Federal, and International Law Enforcement

While strong collaboration between federal agencies and our international counterparts is critical, there is an increasing awareness that stronger partnerships with state and local law enforcement, prosecutors, and judges are essential to protecting our nation's critical infrastructure. Just as there is recognition that our local first responders are on the front lines of natural disasters and other homeland security challenges, so too must we recognize that many of today's cyber crimes are first investigated by local law enforcement.

In 1995, the Secret Service formed its first Electronic Crimes Task Force (ECTF) in New York City. The concept brought together not only members of federal, state and local law enforcement, but also members of academia and the private sector. Cooperation was needed at all levels to fight this new type of electronic crime that was constantly evolving, often faster than the laws and regulations in place to protect financial infrastructure. Perhaps one of the most important results of this task force was the close partnerships our agents developed with state and local law enforcement, prosecutors, and judges.

The ECTF concept has been replicated in other Secret Service field offices throughout the nation and in two locations internationally. Local law enforcement and judiciary are

not only fighting cyber criminals locally, they are assisting in fighting threats that are emanating from outside the United States which directly affect our citizens and commerce. The NCFI therefore provides crucial training to support our mission and enhances the capacity of local law enforcement to combat a myriad of crimes. Advances in computer technology and greater access to personally identifiable information (PII) 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, malicious software, stolen credit, debit and ATM card data and account takeovers leading to significant data breaches affecting every sector of the world economy.

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 websites," operate like online bazaars where criminals converge to trade personal financial data and cyber-tools of the trade. The websites vary in size, from a few dozen members to some of the more popular sites boasting membership of approximately 80,000 users. Within these portals, there are separate forums moderated by notorious members of the carding community. Members 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, brokerage account information, hacking services, counterfeit identity documents and other forms of contraband.

Over the years, the Secret Service has infiltrated many of the "carding websites." One such infiltration allowed the Secret Service to initiate and conduct a three-year investigation that led to the indictment of 11 perpetrators involved in hacking nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers. The investigation revealed that defendants from the United States, Estonia, China and Belarus successfully obtained credit and debit card numbers by hacking into the wireless computer networks of major retailers — including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority and Dave & Buster's. Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks. After the data was collected, the conspirators concealed the information in encrypted computer servers that they controlled in the United States and Eastern Europe. The credit and debit card numbers were then sold through online transactions to other criminals in the United States and Eastern Europe. The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The defendants then used these cards to withdraw tens of thousands of dollars at a time from ATMs. The defendants were able to conceal and launder their fraudulent proceeds by using anonymous Internet-based electronic currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.

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 through ECTFs as well as the support provided by our Cyber Intelligence Section (CIS) and the training provided to our special agents via Electronic Crimes Special Agent Program (ECSAP) were all instrumental to the Secret Service's successful investigation into the network intrusion of Heartland Payment Systems (HPS). An August 2009 indictment alleged that a transnational organized criminal group used various network intrusion techniques to breach security, navigate the credit card processing environment, and plant a "sniffer," a data collection device, to capture payment transaction data.

The HPS investigation – the largest and most complex data breach investigation ever prosecuted in the United States – revealed that data from more than 130 million credit card accounts were at risk of being compromised and exfiltrated to a command and control server operated by an international group directly related to other ongoing Secret Service investigations. During the course of the investigation, the Secret Service uncovered that this international group committed other intrusions into multiple corporate networks to steal credit and debit card data. The Secret Service relied on various investigative methods, including subpoenas and search warrants, to identify three main suspects. Mutual Legal Assistance Treaty (MLAT) requests submitted by prosecutors were also sent via the Office of International Affairs (OIA) of the Criminal Division to foreign countries requesting evidence. As a result of the investigation, the three suspects in the case were indicted for various computer-related crimes. The lead defendant in the indictment pled guilty and was sentenced to twenty years in federal prison. This investigation is ongoing with over 100 additional victim companies identified. The Secret Service is working with our law enforcement partners both domestically and overseas to apprehend the two defendants who are still at large.

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), which "prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts."[1] The Secret Service's ECTFs are a natural complement to CCIPS, resulting in a strong partnership over the years. In the last decade, nearly every major cyber investigation conducted by the Secret Service has benefited from CCIPS contributions.

The recent arrest of an individual charged with being one of the world's most notorious traffickers of stolen financial information, serves as an excellent example of successful cooperation between the Secret Service and its law enforcement partners around the

[1] U.S. Department of Justice. (n.d.). *Computer Crime & Intellectual Property Section: About CCIPS.* Retrieved from http://www.justice.gov/criminal/cybercrime/ccips.html

world. 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. Both the CCIPS and the OIA of the Department of Justice played critical roles in this apprehension. This type of cooperation is crucial if law enforcement is to be successful in disrupting and dismantling criminal organizations involved in cyber crime.

More broadly, the Secret Service maintains an excellent relationship with the Federal Bureau of Investigation (FBI). The Secret Service has a permanent presence at the National Cyber Investigative Joint Task Force, which serves as the coordination and integration center for the identification, mitigation, and neutralization of both criminal and national security threats against the United States. In the last several years, the Secret Service has partnered with the FBI on various high-profile cyber investigations. For example, in May 2010, a joint operation involving the Secret Service, FBI and the Security Service of Ukraine (SBU), yielded the seizure of approximately 143 computer systems – one of the largest international seizures of digital media gathered by U.S. law enforcement – consisting of approximately 85 terabytes of data

Within the Department of Homeland Security (DHS), the Secret Service works closely with NPPD's 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 information with US-CERT. 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);
- Federal Bureau of Investigation's 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.

The Secret Service is committed to ensuring that all its information-sharing activities comply with applicable laws, regulations, and policies, including those that pertain to privacy and civil liberties.

Private Sector Partnerships

The Secret Service believes that building trusted partnerships among all levels of law enforcement, the private sector and academia is the right model for addressing the challenges of securing cyberspace. It is through such wide-ranging and established partnerships that the Secret Service is able to help expand the collective understanding of cyber crime and continue to augment our prevention, advanced detection, and prosecution efforts. A recent example of our collaboration with the business community involved a joint 2010 Data Breach Investigations Report with Verizon, which analyzed more than 900 breaches, involving more than 900 million compromised records. The widely disseminated report offers recommendations to assist the private sector in securing their networks from both internal and external threats. The recently released 2011 Data Breach Investigations Report (http://www.secretservice.gov/Verizon_Data_Breach_2011.pdf) examined 800 new data compromise incidents since the 2010 report. The 2011 study includes input from The Netherlands' National High Tech Crime Unit.

Network intrusions and cyber crime can be devastating to companies of any size. Theft of data and customer information often has more dire consequences on a small- or medium-sized company that may not have the resources or expertise necessary to properly protect their networks and data. The NCFI adds to our ability to support the private sector during times of crisis by providing the tools and training that local and state law enforcement need to protect businesses, large and small, across the United States.

Successful Cyber Investigations as a Result of NCFI Training

The NCFI initiative has led to numerous successful cyber investigations. For example, a forensic examiner from the Alabama Computer Forensic Laboratories attended the Network Intrusion Responder (NITRO) course offered at the NCFI. After completing the three-week course, he began to work an investigation involving individuals filing fraudulent federal and state tax returns online with a total loss in the hundreds of thousands of dollars. Using skills learned in the NITRO course, he constructed a decoy network to capture all unauthorized network traffic at the consenting owner's Internet connection as well as assisting in securing the owner's real network. The examiner recovered key forensic evidence proving the suspect accessed the decoy network and conducted criminal activity at the online tax website.

Another example of a successful cyber investigation conducted by an NCFI graduate is in July of 2009, the Arapahoe County Sheriff's Office received a complaint from a mortgage lender in the city of Centennial, Colorado. The mortgage lender found more

than 40 applications for payday loans, totaling approximately $200,000, originating from the same IP address. A graduate of the NCFI began to focus on the network intrusion leads in the case, and was able to determine that the logins used were stolen from the account belonging to the owner's wife. The IP address came back to a residence outside of Las Vegas owned by a former employee of the mortgage lender who had knowledge of the company systems to enable him to commit these crimes. Based on the electronic evidence recovered in the investigation and the suspect's home computer, he subsequently confessed to the scheme.

In addition to traditional cyber-related financial cases, NCFI graduates have been able to use the skills learned in the classroom to recover key evidence in traditional criminal investigations. In 2009, an 11 year-old boy was taken from his home near Saginaw, MI. Within hours local law enforcement developed a suspect, a former caregiver / babysitter, and a search warrant was executed on the suspect's residence resulting in the seizure of five computers. A graduate of the NCFI was contacted to conduct a forensic review of the electronic media and, within minutes, the officer recovered evidence from the suspect's computer placing him in an area near Sandusky, OH. Local police were contacted to search a nearby amusement park and found the suspect's car in the parking lot. Less than two hours after the information was located on the computer the child was found unharmed and the suspect was apprehended.

Conclusion

As more information is stored online, 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 criminals. Furthermore, prompt reporting of major data breaches involving sensitive personally identifiable information to the proper authorities will help facilitate a thorough investigation.

The Secret Service is committed to safeguarding the nation's financial payment systems by investigating and dismantling criminal groups involved in cyber crime. Responding to the growth of these types of crimes and the level of sophistication these criminals employ requires significant training, 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. We will continue to be innovative in our investigative approach to cyber crime and cyber security and we are pleased that the Committee recognizes the magnitude of these issues and the evolving nature of these crimes.

Thank you again for this opportunity to testify on behalf of the Secret Service and share some of the many positive impacts of the National Computer Forensics Institute. I will be pleased to answer any questions at this time.