Statement of Mr. Michael P. Merritt

Assistant Director
Office of Investigations
U. S. Secret Service

Before the Senate Homeland Security and Governmental Affairs Committee

U.S. Senate

September 14, 2009

Good morning, Chairman Lieberman, Ranking Member Collins and distinguished members of the Committee. Thank you for the opportunity to address this Committee on the subject of cyber and computer-related crimes and the role of the U.S. Secret Service (Secret Service) in cyber investigations.

While the Secret Service is perhaps best known for protecting our nation's leaders, we were established in 1865 to investigate and prevent the counterfeiting of United States currency. As the original guardian of the nation's financial payment system, the Secret Service has a long history of protecting American consumers, industries, and financial institutions from fraud. Congress continues to recognize the Secret Service's 144 years of investigative expertise in financial crimes and over the last two decades has expanded our statutory authorities to include access device fraud (18 USC §1029), which includes credit and debit card fraud. Congress has also given the Secret Service concurrent jurisdiction with other law enforcement agencies for identity theft (18 USC §1028), computer fraud (18 USC §1030), and bank fraud (18 USC §1344). We take our mission to combat these crimes seriously and as a result, the Secret Service is recognized worldwide for our investigative expertise and innovative approaches to detecting, investigating, and preventing financial crimes.

Trends in Cyber and Computer-Related Crimes

In recent years, the Secret Service has observed a significant increase in the quality, quantity, and complexity of cyber-cases in which perpetrators target financial institutions in the United States. The combination of the information revolution and the effects of globalization have driven the evolution of the Secret Service's investigative mission. The advent of technology and the Internet created a new transnational "cyber-criminal," and as a result the Secret Service has observed a marked increase in cyber and computer-related crimes targeting private industry and other critical infrastructures. For example, trends show an increase in network intrusions, hacking attacks, malicious software, and account takeovers leading to significant data breaches affecting every sector of the American 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 is particularly concerned about cases involving network intrusions of businesses that result in the compromise of credit and debit card numbers and all related personal information. A considerable portion of this type of electronic theft appears to be attributable to organized cyber-groups, many of them based abroad, which pursue both the intrusions and the subsequent exploitation of the stolen data. Stolen credit card information is often trafficked in units that include more than just the card number and expiration date. These "full-info cards" include additional information, such as the card holder's full name and address, mother's maiden name, date of birth, Social Security number, a PIN, and other personal information that allows additional criminal exploitation of the affected individual.

Although network intrusions can be devastating to a company of any size, the subsequent theft of data and customer information often has more dire consequences on a small or medium-sized company that most likely does not have the resources or expertise necessary to properly protect their networks and data. For example, in October 2007, the Secret Service identified a complex fraud scheme in which servers owned by a payroll company were compromised by a network intrusion. Subsequently, four debit card accounts belonging to a small Midwestern bank were compromised, distributed online, and used in a coordinated attack resulting in ATM withdrawals in excess of $5 million. The withdrawals involved 9,000 worldwide transactions in less than two days and the bank had to file for Chapter 11 bankruptcy protection. Our investigation revealed that the criminals compromised the payroll company's database, reset PINs, loaded balances onto the accounts, and removed account withdrawal limits or set the limits at extremely high levels.

Through this investigation, the Secret Service also identified another organized cyber-group in New York City trafficking stolen credit card data that was transmitted by multiple suspects operating in Russia and the Ukraine. Following the investigative leads generated in this case, the Secret Service was able to prevent additional losses by notifying victims of the intrusion and compromise, often before the victims became aware of the illicit activity. For example, the Secret Service discovered that the computer network of a U.S. bank had been compromised. Subsequent notification by the Secret Service enabled the bank to significantly reduce its exposure and avoid potential losses exceeding $15 million. Based on these investigative efforts, the Secret Service identified 15 compromised financial institutions, $3 million in losses, 5,000 compromised accounts, and prevented more than $20 million in potential losses to U.S. financial institutions and consumers.

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 alike. 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 in 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 memberships of approximately 8,000 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, hacking services and other contraband.

Although increasingly difficult to accomplish, the Secret Service has managed to infiltrate many of the "carding websites." One such infiltration allowed the Secret Service to initiate and conduct a three-year investigation that led to the identification and high-profile 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 they collected the data, the conspirators concealed the data in encrypted computer servers that they controlled in the United States and Eastern Europe. They then sold some of the credit and debit card numbers via 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 fraud proceeds by using anonymous Internet-based electronic currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.

The total actual loss associated with this investigation is still being assessed. However, one of the corporate victims has already reported expenses of almost $200 million resulting from the intrusion.

In both of these cases, the ripple effects of the criminal acts extend well beyond the company compromised. In one example alone, millions of individual card holders were affected. Although swift investigation, arrest, and prosecution prevented many consumers from direct financial harm, all of the potential victims were at risk for misuse of their credit cards, overall identity theft, or both. Also, costs suffered by businesses, such as the need for enhanced security measures, reputational damage, and direct financial losses, are ultimately passed on to consumers.

Collaboration with Other Federal Agencies; State and Local Law Enforcement; Private Sector; and Academia

While cyber-criminals operate in a world without borders, the law enforcement community does not. The multi-national, multi-jurisdictional nature of these cyber-crime cases has increased in complexity and, accordingly, increased the time and resources needed for successful

investigation and adjudication. For example, in the TJX investigation, the Secret Service not only worked with domestic law enforcement partners, but also with officials from Thailand, the United Arab Emirates, Turkey, Ukraine, Spain, Belarus, Estonia, and Germany. The complexity of this three-year investigation involved personnel from our San Diego, Miami, and Boston Field Offices working in close coordination with personnel from our Headquarters Divisions.

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. 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:

- National Protection and Program Directorate's (NPPD) – Office of the Under Secretary;
- NPPD's National Cyber Security Division (US-CERT);
- NPPD's Office of Infrastructure Protection;
- Department of Homeland Security's Science and Technology Directorate (S&T);
- White House Homeland Security Staff;
- Department of Justice National Cyber Investigative Joint Task Force (NCIJTF);
- Each Federal Bureau of Investigation 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;
- National Security Council;
- The Drug Enforcement Administration's International Organized Crime and Intelligence Operations Center;
- EUROPOL; and
- INTERPOL

To continue to fulfill our obligation 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 and continues to dismantle some of the largest known transnational cyber-criminal organizations by:

- providing the necessary computer-based training to enhance the investigative skills of special agents through our **Electronic Crimes Special Agent Program (ECSAP)**;
- collaborating with other law enforcement agencies, private industry, and academia through our 28 **Electronic Crimes Task Forces (ECTF)**;
- 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 **Criminal Intelligence Section (CIS)**;
- providing state and local law enforcement partners with the necessary computer-based training, tools, and equipment to enhance their investigative skills through the **National Computer Forensics Institute (NCFI)**;

- maximizing partnerships with international law enforcement counterparts through our **international field offices**; and
- maximizing technical support, research and development, and public outreach through the Secret Service **CERT Liaison Program (CLP)** at Carnegie Mellon University.

Electronic Crimes Special Agent Program (ECSAP)

A central component of the Secret Service's cyber-crime investigations is its Electronic Crimes Special Agent Program (ECSAP). This program is comprised of 1,148 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 extensive training in forensic identification, preservation and retrieval of electronically-stored evidence. ECSAP agents are computer investigative specialists and among the most highly-trained experts in law enforcement, qualified to conduct examinations on all types of electronic evidence. This core cadre of special agents is 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 and focus:

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 is designed to provide Secret Service agents and our state and local law enforcement partners with a basic understanding of computers and electronic crime investigations. The BICEP program has proven so effective that the Secret Service has incorporated it into its core curriculum for newly hired special agents.

Currently, the Secret Service has 823 special agents trained at the BICEP level.

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.

Currently, the Secret Service has 161 special agents trained at the ECSAP-NI level.

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. The forensically obtained digital evidence is utilized in the prosecution of various electronic crimes cases, as well as criminally focused protective intelligence cases.

Currently, the Secret Service has 164 special agents trained at the ECSAP-CF level.

Electronic Crimes Task Forces (ECTF)

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. Congress has since 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 has established 28 ECTFs, including the first international ECTF based in Rome, Italy. Membership in our ECTFs include: 299 academic partners; over 2,100 international, federal, state, and local law enforcement partners; and over 3,100 private sector partners. The Secret Service ECTF model is unique in that it is an international network with the capabilities to focus on regional issues. For example, the New York ECTF, based in the nation's largest banking center, focuses heavily on protecting our financial institutions and infrastructure, while the Houston ECTF works closely with partners such as ExxonMobil, Chevron, Shell, and Marathon Oil to protect the vital energy sector. By joining our ECTFs, all of our partners enjoy the resources, information, expertise, and advanced research provided by our international network of members while focusing on issues with significant regional impact.

Criminal Intelligence Section (CIS)

Our Criminal Intelligence Section (CIS) collects, analyzes, and disseminates data in support of Secret Service investigations nationwide and overseas and generates new investigative leads based upon its findings. CIS leverages technology and information obtained through private partnerships 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 developed 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 (NCFI)

The National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, the Department of Homeland Security (DHS), and the State of Alabama. 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 basic electronic crimes investigations.

Since opening on May 19, 2008, the Secret Service has provided critical training to 564 state and local law enforcement officials representing over 300 agencies from 49 states and two U.S. territories.

Collaboration of International Partners

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 foreign law enforcement counterparts. Currently, the Secret Service operates 22 offices abroad, each of which has regional responsibilities providing 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.

Computer Emergency Response Team (CERT)

In August 2000, the Secret Service and Carnegie Mellon University Software Engineering Institute (SEI) established the Secret Service CERT Liaison Program (CLP). The role of the CLP is threefold: (1) technical support; (2) research and development; and (3) public outreach and education.

The CLP is a collaborative effort with over 150 scientists and researchers engaged in the fields of computer and network security, malware analysis, forensic development, and training and education. Supplementing this effort is research into emerging technologies being employed by cyber-criminals, and development of technologies and techniques to combat them.

The objectives of the CLP are: to broaden the Secret Service's knowledge of software engineering and networked systems security; to expand and strengthen Secret Service partnerships and relationships with the technical and academic communities; to provide an opportunity for the Secret Service to work closely with CERT, SEI, and Carnegie Mellon University; and to provide public outreach and education.

Heartland Payment Systems Case

As an example, the partnerships developed through our ECTFs, the support provided by our Criminal Intelligence Section, the liaison established by our overseas offices, and the training provided by ECSAP were all instrumental to the Secret Service's successful investigation into the network intrusion of Heartland Payment Systems (HPS). An August 2009 indictment alleges that a transnational organized criminal group used various network intrusion techniques to

breach security, navigate the credit card processing environment, and plant a "sniffer" to capture payment transaction data.

The Secret Service investigation revealed data from more than 130 million credit card accounts at risk of being compromised and ex-filtrated 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 search warrants, the use of Mutual Legal Assistance Treaties with our foreign law enforcement partners, and subpoenas to identify three main suspects. As a result of this investigation, the three suspects in the case were indicted and charged with various computer-related crimes.

This case represents the largest and most complex data breach investigation ever prosecuted in the United States.

Conclusion

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 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 and DHS continue to collaborate closely with the private sector to improve coordination and communication on cyber issues.

As I have highlighted here, the Secret Service has implemented a number of initiatives on cyber and computer-related crimes. Responding to the growth in these types of crimes and the level of sophistication these criminals employ demands an increasing amount of resources and greater collaboration. Accordingly, we dedicate significant resources to increasing awareness, educating the public, providing training for law enforcement partners, and improving investigative techniques. The Secret Service is committed to our mission of safeguarding the nation's critical infrastructure and financial payment systems. We will continue to aggressively investigate cyber and computer-related crime to protect consumers.

In conclusion, I would like to reiterate that cyber-crime remains an evolving threat. It is not a threat of the future; it is very much here. Law enforcement agencies must be able to adapt to emerging technologies and criminal methods. The Secret Service is fully involved in the federal government's new approach to cybersecurity. We are dedicated to the government's collective effort to adopt innovation in our approach to cyber-crime and cybersecurity and to stay ahead of this ever-changing threat. The Secret Service is pleased that the Committee 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.

Chairman Lieberman, Ranking Member Collins, 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.