U.S. DEPARTMENT OF HOMELAND SECURITY

U.S. SECRET SERVICE

STATEMENT FOR THE RECORD

MARK SULLIVAN
DIRECTOR

BEFORE THE

COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME, TERRORISM
AND HOMELAND SECURITY

U.S. HOUSE OF REPRESENTATIVES

June 29, 2010

INTRODUCTION

Good morning, Chairman Scott, Ranking Member Gohmert and distinguished members of the Subcommittee. Thank you for the opportunity to discuss the U.S. Secret Service's (Secret Service) dual mission of protection and investigation.

As one of the oldest federal law enforcement organizations in the country, the Secret Service has a history of collaborating with local, state, and federal law enforcement in order to fulfill its mission. The Secret Service has benefited greatly from these longstanding relationships as we move forward in carrying out our investigative responsibilities. A few examples of these partnerships include the Secret Service's 38 Financial Crimes Task Forces (FCTF), 29 Electronic Crimes Task Forces (ECTF), the National Computer Forensics Institute (NCFI), the Vetted Anti-Counterfeiting Forces (VACF), and the Peruvian Counterfeit Task Force (PCTF). Evidence of our collaboration was highlighted during the Secret Service's successful investigation into the two largest network intrusions cases in U.S. history: TJX and Heartland Payment Systems.

Today's Secret Service is comprised of 142 domestic and 22 international field offices across 18 countries. We are responsible for investigating violations of laws relating to: counterfeiting U.S. obligations and securities; financial crimes, including credit card fraud; financial institution fraud; identity theft; computer fraud; and computer-based attacks on U.S. financial, banking, and telecommunications infrastructure. While Secret Service field offices are primarily responsible for criminal investigations, they also devote significant resources to assisting with planning protective advance work, conducting protective intelligence investigations, and bolstering permanent and temporary protective details.

Due to the transnational nature of crime, as well as our protective mission, the Secret Service had the foresight to recognize the importance of forging relationships with our international law enforcement partners. While these relationships were previously established to fulfill our protective requirements, they are now being utilized by our foreign field offices to combat and investigate financial crimes affecting the U.S. financial infrastructure.

In fiscal year (FY) 2009, the Secret Service closed 7,803 criminal cases, arrested 5,809 suspects engaged in financial fraud, arrested 2,946 suspects engaged in counterfeit violations, was responsible for seizures in excess of $140 million in assets, prevented $1.8 billion in potential loss to our financial sector, and conducted these investigations so thoroughly that it led to a 99.2% conviction rate for suspects who were indicted. In addition, the Secret Service's total number of criminal seizures increased by 28 percent from FY 2006 to FY 2010, while total seizure amounts during this period increased from $23 million to $130 million. It bears note that approximately 90 percent of all funds seized by Secret Service are returned to the victims.

INVESTIGATIVE OPERATIONS

Although the Secret Service is perhaps best known for protecting the President and our nation's leaders, we were established in 1865 to investigate and prevent the counterfeiting of U.S. currency. As the original guardian of the nation's financial monetary system, the Secret Service has a long history of protecting American consumers, industries, and financial institutions from

fraud. I thank this Committee for its continued recognition of the Secret Service's 145 years of investigative expertise in financial crimes – for over thirty years, this Committee has strengthened our statutory authorities to include access device fraud (18 USC §1029), which includes credit and debit card fraud, identity theft (18 USC §1028), computer fraud (18 USC §1030), and bank fraud (18 USC §1344). Given our innovative approaches to detecting, investigating, and preventing financial crimes, the Secret Service is recognized worldwide for our investigative expertise in these areas.

Counterfeiting

Even though the percentage of U.S. counterfeit currency in circulation is nowhere near the level it was when we were established, recent trends indicate a growing globalization in production and distribution of counterfeit notes. While it is difficult to determine precise figures detailing the amount of counterfeit U.S. currency passed annually overseas because not all nations report that information, the Secret Service seized approximately $69 million in counterfeit that was passed to the American public in FY 2009 alone. Additionally, approximately $108 million in counterfeit U.S. currency was seized prior to distribution last year by the Secret Service and other authorities worldwide. Of this amount, approximately seven percent was seized within the United States.

The Secret Service's approach to protecting U.S. currency includes working jointly with domestic and international law enforcement partners to aggressively investigate the source of the illicit production of counterfeit in order to minimize its collective economic impact. Today, the Secret Service continues to target strategic locations throughout the world where significant counterfeiting activity is detected through our work as part of joint task forces with our international law enforcement partners. Our investigative experience has proven that, in addition to an immediate response by the law enforcement community, the effective suppression of counterfeiting operations requires a close partnership between our international field offices and their local law enforcement counterparts.

The Secret Service's permanent presence in 22 international offices in 18 countries has been pivotal in establishing the required relationships to successfully suppress foreign-based counterfeiting operations. For example, Project Colombia is a continuation of the Secret Service's efforts to establish and support VACF. Since its inception in 2001, Project Colombia partners have seized approximately $239 million in counterfeit U.S. currency, arrested more than 600 suspects, suppressed nearly 100 counterfeit printing plants, and reduced the amount of Colombia-originated counterfeit passed within the United States by more than 80 percent.

As a collateral effect of our investigative successes in Colombia, the criminal element has relocated to other parts of South America. For example, from FY 2008 to FY 2009, the Secret Service noted a 156 percent increase in worldwide passing activity of counterfeit U.S. currency emanating from Peru. These counterfeit notes, referred to as the Peruvian Note Family, have emerged as one of the leading domestically passed notes in the last 18 months. In response to the increase in passing activity of the Peruvian Note Family, which was second only to the domestic passing of digital counterfeit in FY 2008, the Secret Service formed a temporary PCTF in collaboration and partnership with Peruvian law enforcement officials. Since opening in

Lima, Peru on March 15, 2009, the PCTF has yielded 38 arrests, 17 counterfeit plant suppressions, and the seizure of more than $20.6 million in counterfeit U.S. currency. Due to the overwhelming success of the PCTF, the Secret Service and Peruvian law enforcement officials have agreed to extend operations for an additional six-month period in FY 2010.

To highlight PCTF successes, during the spring of 2009, PCTF agents and members of the Peruvian National Police (PNP) developed critical investigative leads through the use of confidential informants to obtain information on counterfeit operations in Lima, Peru. PCTF agents and PNP officers executed four search warrants on target locations where counterfeit U.S. Federal Reserve Notes (FRN) were suspected of being manufactured. The four search warrants resulted in the arrest of ten suspects and the seizure of $9.84 million in counterfeit FRNs, eleven lithographic presses, photo equipment, 15 lithographic plates, and numerous sets of negatives for the Peruvian note.

As new technologies continue to yield sophisticated criminal methods, the challenges facing law enforcement are significant as large quantities of counterfeit currency and other obligations can be reproduced quickly and efficiently. The collaboration with international law enforcement agencies in Latin America and around the world is critical for the Secret Service to successfully combat distribution and foreign counterfeit production.

Identify Theft and Other Fraud

Through our work in the area of financial crime, the Secret Service has developed a particular expertise in the investigation of identity theft, false identification fraud, credit card fraud, debit card fraud, check fraud, and bank fraud. In FY 2009, agents assigned to Secret Service offices across the United States arrested over 5,800 suspects for financial crimes violations. These suspects were responsible for approximately $442 million in actual fraud loss to individuals and financial institutions.

As counterfeiters have begun to use digital processes to commit their crimes, the Secret Service has observed a marked increase in the quality, quantity, and complexity of financial crimes, particularly offenses related to identity theft and access device fraud. Criminals often seek the personal identifiers generally required to obtain goods and services on credit, such as Social Security numbers (SSNs), 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 (PINs).

Electronic Crime and Cyber Investigations

The advent of technology and the Internet has created a new transnational "cyber-criminal," and as a result, the Secret Service has observed a distinct increase in cyber 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.

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 attributed to organized cyber-groups, many of them based abroad, that pursue both the network 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, SSN, a PIN, and other personal information that allows additional criminal exploitation of the affected individual.

The increasing level of collaboration among cyber-criminals makes these cases more difficult to investigate and also increases 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, where members meet online and discuss specific topics of interest. International cyber-criminals 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 six defendants successfully obtained the credit and debit card numbers by "wardriving", the act of searching for Wi-Fi wireless networks by driving around, using a portable computer or PDA, and 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. At the time, the Secret Service investigation of the TJX intrusion represented the largest network intrusion in U.S. history, having compromised 40 million credit card accounts.

Another major investigation was initiated in January 2009, when Heartland Payment Systems detected an intrusion into their processing system. The intruders breached Heartland Payment Systems corporate environment via Structured Query Language (SQL) injection and navigated to the credit card processing environment where a custom packet "sniffer", modified to capture payment transaction data, was recovered.

The Secret Service investigation revealed that over 130 million credit card accounts were at risk of being compromised and that data was ex-filtrated to a command and control server operated by an international group related to other ongoing Secret Service investigations. During the course of the investigation, the Secret Service investigation revealed that this same international group committed other intrusions into multiple corporate networks specifically for stealing credit card and debit card data.

Various investigative methods to include search warrants, Mutual Legal Assistance Treaties, pen traps, and subpoenas have been used to identify three main suspects of this international group. On March 26, 2010, Albert Gonzalez, the hacker responsible for the TJX intrusion, was sentenced to 20 years in prison for his role in the Heartland, Hannaford's, and 7-11 intrusions. Gonzalez will serve this sentence concurrently with his sentence in the TJX intrusion. Furthermore, two unnamed co-conspirators were indicted for their role in this investigation and efforts continue in an attempt to locate these suspects.

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, identity theft, or both. Furthermore, costs suffered by businesses, such as the need for enhanced security measures, reputational damage, and direct financial losses, are ultimately passed on to consumers.

Mortgage Fraud

In recent years, compromised personal indentifying information has been increasingly used to commit mortgage fraud. The Secret Service's aggressive investigation into these cases has had an immediate and direct impact on the financial crimes plaguing our banks, mortgage lenders, and government institutions. From FY 2007-2009, the Secret Service closed 469 mortgage fraud cases nationwide. These cases account for nearly $143.2 million in losses to our financial institutions, with potential losses in excess of $370.5 million. Since 2006, the Secret Service has referred 430 mortgage fraud cases for prosecution.

In response to the rise in mortgage fraud, Congress passed into law the Fraud Enforcement Recovery Act (FERA) of 2009 (P.L. 111-21), which authorized "the United States Secret Service of the Department of Homeland Security, $20,000,000 for each of the fiscal years 2010 and 2011 for investigations involving Federal assistance programs and financial institutions."

On November 17, 2009, President Obama established an interagency Financial Fraud Enforcement Task Force (FFETF) to strengthen efforts to combat financial crime. The Department of Justice-led task force, composed of senior level officials from twenty five departments, agencies, and offices, including the Secret Service, subsequently created a Mortgage Fraud Working Group aimed at confronting this nationwide problem.

In February 2010, the FFETF Mortgage Fraud Working Group organized a national mortgage fraud sweep dubbed "Operation Stolen Dreams," which consisted of the combined criminal and civil efforts of the U.S. Department of Justice, the Secret Service, and multiple federal, state, and local law enforcement agencies. This comprehensive effort resulted in the arrests of 485 individuals. It involved 1,215 criminal defendants and an associated fraud loss totaling $2.3 billion. More specifically, the Secret Service's participation entailed the combined efforts of 22 offices nationwide that resulted in 44 investigations. Our cases alone produced 71 arrests and associated fraud losses exceeding $153 million.

For example, the Secret Service's Philadelphia and Fresno offices coordinated an "Operation Stolen Dreams" investigation that involved a suspect who purchased property located in California using a fraudulently obtained SSN belonging to a victim in North Carolina. The suspect used the fraudulently obtained SSN to deed the property to a co-conspirator, who then sold the property to an additional co-conspirator using a fraudulently obtained SSN, this time belonging to a victim in Kansas. The suspects were able to secure loans and then purchase and sell property.

On June 17, 2010, these three suspects were indicted in the Eastern District of California for violations of Title 18, United States Code, Sections 982(a)(2)(A) (Criminal Forfeiture), 1028(a)(7) & (2) (Identity Theft and Aiding & Abetting), 1341 (Mail Fraud), and 1349 (Conspiracy to Commit Mail Fraud). The fraud loss associated with this case is $2 million.

Domestic and International Collaboration

Criminal groups involved in financial and cyber crimes routinely operate in a multi-jurisdictional environment. By working closely with other federal, state, and local law enforcement representatives, as well as international law enforcement, the Secret Service is able to provide a comprehensive network of information sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries.

The Secret Service has established unique and vital partnerships with state, local, and other federal law enforcement agencies through years of collaboration on our investigative and protective endeavors. These longstanding partnerships enabled the Secret Service to establish a national network of 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 38 FCTFs located in metropolitan regions across the country.

To date, the Secret Service has also established 29 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 capability to focus on regional issues. 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.

Partnerships between law enforcement and the private sector are critical to the success of the ECTF's preventive 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 crime. 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.

Another key element of success within the ECTF model is the Secret Service's 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 of all types of electronic evidence. This core cadre of special agents is equipped to investigate the continually evolving arena of electronic crime 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.

These resources allow ECTFs the potential to identify and address possible cyber vulnerabilities before criminals find and exploit 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 model opens the lines of communication and encourages the exchange of information between all academic, private sector, and law enforcement partners.

Community Outreach and Public Awareness

The Secret Service raises awareness of issues related to counterfeit, financial fraud, and electronic crimes, both in the law enforcement community and among 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 counterfeit currency, financial fraud, identity theft, and cyber crime. Agents often address these topics when speaking to academic institutions, civic organizations, and staff meetings involving businesses or financial institutions. In addition, the Secret Service provides training in the form of continuing education to state and local law enforcement. This training includes formal and

informal classes which occur at field office sponsored seminars, police academies, and other various settings.

For example, 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. By the end of FY 2010, the Secret Service will have provided critical training to 932 state and local law enforcement officials representing 300 agencies from 50 states and two U.S. territories.

The Secret Service is committed to providing our law enforcement partners with publications and guides to assist them in combating counterfeit activity, financial fraud, and cyber crime. The Secret Service continues to collaborate with the Department of Treasury and the Bureau of Engraving and Printing to produce and distribute various pamphlets, guides, posters, and visual aids pertaining to counterfeit currency detection.

PROTECTIVE OPERATIONS

Following the assassination of President McKinley in 1901, the Secret Service began protecting the President of the United States. Since then, the Secret Service's jurisdiction has expanded to meet the needs of an evolving security environment. Throughout the 20th century, the protective mission expanded to include the protection of additional designees, including presidential candidates, visiting heads of state and government, designated sites and National Special Security Events (NSSEs). The Secret Service's protective mission includes all activities related to identifying threats, mitigating vulnerabilities, and creating secure environments wherever protectees work, reside, and travel.

During presidential campaigns, NSSEs, and routine protective travel, the Secret Service's domestic and international field office network is an essential component of our protective operations. They not only provide local and regional expertise but serve as a force multiplier for our protective details advancing a visit. Our field office personnel also provide invaluable assistance to the protective details through their well-established, professional relationships with local, state, federal, and international law enforcement partners in their respective districts.

Protection of the President, Vice President, and Other World Leaders

Since taking office in 2009, President Obama and Vice President Biden have maintained extensive domestic and foreign travel schedules. Thus far for FY 2010, the President and Vice President have engaged in 28 overseas visits. These increased travel schedules are also maintained by many former Presidents and their spouses, who have visited 89 foreign countries thus far in FY 2010. Furthermore, Secret Service personnel have coordinated and traveled with other protectees to 146 foreign countries.

Providing protection for the President, Vice President, and other protectees requires more than simply assigning them protective details and protective measures. It requires a comprehensive plan of utilizing personnel and assets, most of which are provided through our network of strategically located field offices around the world. For example, since the beginning of FY 2010, the President, Vice President and 600 visiting foreign heads of state and government have traveled to more than 1,500 domestic locations combined.

Each one of these trips requires the utilization of our field office personnel to undertake protective advance activities, staffing, and liaison with our federal, state, and local partners. In short, our protective mission would be substantially hindered without the framework provided by the Secret Service's field offices, including the established relationships between Secret Service field personnel and our federal, state, and local partners.

Campaign Protection

Although the 2008 presidential campaign and security activities associated with the transition ended just last year, the Secret Service is already beginning the necessary planning and advance work for the 2012 presidential campaign. This early preparation is critical because of the time required to provide advanced protective training to Secret Service employees and partner agencies participating in campaign security activities. In addition, the Secret Service must begin to procure, outfit, and preposition sufficient protective vehicles to transport the expected number of candidates, and to purchase technical security equipment to appropriately secure residences and sites to be visited. Furthermore, we are developing appropriate contingency plans in the event that protective activities for the campaign begin earlier than is traditional, as was the case in 2007.

National Special Security Events

The Secret Service's role in developing security plans for major events was codified when Congress passed into law the Presidential Protection Act of 2000, which authorized the Secret Service to plan, coordinate, and implement security operations at designated events of national significance. This authority was a natural evolution for the Secret Service, as we have led security operations at large events involving the President dating back to our first protective mandate in 1901.

In FY 2010, the Secret Service and its partners successfully coordinated two NSSEs: the 2010 State of the Union Address; and the Nuclear Security Summit in Washington, DC. The security challenges associated with the Nuclear Security Summit in particular were very significant, considering that it was the largest gathering of world leaders in Washington, DC in more than 50 years. During this event, the Secret Service provided protective details for 37 visiting foreign heads of state and government, in addition to the President, Vice President, and several other Secret Service protectees in attendance. Due to its designation as an NSSE, extensive security measures were implemented in and around the Washington, DC Convention Center to protect the venue and individuals participating in the summit. An event of this magnitude cannot be accomplished without the coordination and assistance of our partners. Secret Service personnel

staffed thousands of assignments, with the assistance of our law enforcement, public safety, and military partners.

In addition to current 2012 campaign planning, the Secret Service is also developing security arrangements for future events expected to receive an NSSE designation. One such event is the APEC Summit scheduled for November 2011 in Hawaii. Based on previous summits, the Secret Service is expecting participation by numerous foreign heads of state and government requiring a security detail. At the present time, the Secret Service has identified supervisory personnel for the 2011 APEC Summit. These agents will temporarily relocate to Hawaii to coordinate, in conjunction with the Honolulu Field Office, the NSSE security planning efforts with the appropriate federal, state, and local entities.

Conclusion

In closing, I would like to express my appreciation for the support that Congress and this Committee has shown the Secret Service over the years. What began 145 years ago as a small group of agents responsible for combating the crime of counterfeiting currency has grown into a diverse, internationally respected federal law enforcement agency charged with a unique, dual mission of protecting the nation's critical financial infrastructure and protecting the nation's leaders, visiting heads of state and government, and designated NSSEs.

The Secret Service, in concert with its established partners – public and private, domestic and international, law enforcement and civilian – will continue to play a critical role in preventing, detecting, investigating and mitigating the effects of increasingly complex financial and electronic crimes. The Secret Service will continue to rely on its most valuable asset, its specially trained, dedicated personnel in the field, to investigate these crimes, develop strong cases for prosecution, and bring offenders to justice.

This completes my testimony. I am happy to answer any questions you may have.