ROLE AND OPERATIONS OF THE UNITED STATES SECRET SERVICE

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JUNE 29, 2010

Serial No. 111–140

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE
57–153 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
TAMMY BALDWIN, Wisconsin
CHARLES A. GONZALEZ, Texas
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
DANIEL MAFFEI, New York
JARED POLIS, Colorado

LAMAR SMITH, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM ROONEY, Florida
GREGG HARPER, Mississippi

PERRY APELBAUM, *Staff Director and Chief Counsel*
SEAN MCLAUGHLIN, *Minority Chief of Staff and General Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

ROBERT C. "BOBBY" SCOTT, Virginia, *Chairman*

PEDRO PIERLUISI, Puerto Rico
JERROLD NADLER, New York
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
ANTHONY D. WEINER, New York
MIKE QUIGLEY, Illinois
TED DEUTCH, Florida

LOUIE GOHMERT, Texas
TED POE, Texas
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
J. RANDY FORBES, Virginia
TOM ROONEY, Florida

BOBBY VASSAR, *Chief Counsel*
CAROLINE LYNCH, *Minority Counsel*

CONTENTS

JUNE 29, 2010

ROLE AND OPERATIONS OF THE UNITED STATES SECRET SERVICE

TUESDAY, JUNE 29, 2010

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2 p.m., in room 2141, Rayburn House Office Building, the Honorable Robert C. "Bobby" Scott (Chairman of the Subcommittee) presiding.

Present: Representatives Scott, Conyers, Pierluisi, Jackson Lee, Quigley, Gohmert, and Goodlatte.

Staff Present: (Majority) Bobby Vassar, Subcommittee Chief Counsel; Joe Graupensperger, Counsel; Veronica Eligan, Professional Staff Member; (Minority) Caroline Lynch, Counsel; and Kelsey Whitlock, Minority Legislative Assistant.

Mr. SCOTT. The Subcommittee will come to order. And I am pleased to welcome you today on the hearing before the Subcommittee on Crime, Terrorism, and Homeland Security, an oversight hearing on the United States Secret Service.

The role of the Secret Service has expanded greatly since it was created in 1865 to fight counterfeiting U.S. currency. The Service became part of the Treasury Department in 1883 and took many additional investigative responsibilities with respect to safeguarding the payment and financial systems of the United States. It wasn't until 1894 that the Secret Service started protecting our Presidents on a part-time basis and in 1901 on a full-time basis. That protective role has grown substantially since that time.

Now, as a component of the Department of Homeland Security, the Service continues to focus on the investigation of counterfeiting and a wide variety of other schemes which financially defraud individuals, organizations, and our government. The Secret Service has led in the investigation of some of the most extensive instances of computer intrusion and data theft ever uncovered, such as the TJX and the Heartland cases. The TJX case involved a breach of more than 45 million credit cards. In the Heartland Payment Systems case, 130 million credit card accounts were compromised.

With increasing frequency of such breaches, the high volume of consumer data compromised, the Subcommittee will want to know what challenges law enforcement faces in preventing and investigating these crimes. While the size of some of these cases is astounding, I am also interested to know how we can have law en-

forcement do more to assist individual citizens whose credit cards or other personal information is stolen. The impact of these thefts on individuals can be very damaging, if not devastating.

I believe the key reason for such crime proliferating is that the perpetrators know that they are unlikely to be caught or even have their cases investigated. They know that thefts below certain threshold amounts do not get the attention of law enforcement. The result is a credit card company doesn't charge the customer who proves that the charge is unauthorized, the card holding victim is made whole because they don't have to pay, and the perpetrator keeps the proceeds of the crime without having to face any serious risk of consequences.

These cases aren't so complicated that they can't be solved if the appropriate amount of resources is devoted to them, and I want to know from the Director why more cases are not pursued.

I also want to mention something of interest to me that is not part of the usual investigative or protective mission of the Secret Service, and that is because of the Secret Service's unique experience in threat assessment and protection of individuals at national security special events.

The Service was called upon recently to assist in the preparation of a report studying threat assessment and preventing violence in institutions of higher education. A report was prepared in the wake of the 2007 tragedy at Virginia Tech. As the author of the House-passed Campus Safety Act, which has been waiting for 2 years for the Senate to act upon it, I am very interested in this issue.

The Secret Service has an important and varied mission, and the Subcommittee is pleased to have the opportunity to discuss these and other issues relating to the agency. Today we will have one witness, Mark Sullivan, the Director of the Secret Service. And before we proceed with his statement, it is my pleasure to recognize the Ranking Member of the Subcommittee, the gentleman from Texas, Judge Gohmert.

Mr. GOHMERT. Thank you, Chairman Scott. Welcome, Director Sullivan. Thank you for joining us today for this hearing.

The Secret Service was formed in 1865 to address the prevalence of counterfeit U.S. currency. An estimated one-third to one-half of all the currency in circulation following the Civil War was counterfeit. And at the recommendation of Treasury Secretary Hugh McCulloch, President Lincoln established a commission to study this rapidly growing problem. And on April 14, 1865, he created the U.S. Secret Service to implement the commission's recommendations. Ironically, this was one of President Lincoln's last official acts. He was assassinated later that same day.

Housed within the Treasury Department, the Secret Service began this operation July 5, 1865, and shut down more than 200 counterfeiting plants in its first year. But it would take 36 years and two more presidential assassinations, James Garfield in 1881 and William McKinley in 1901, for Congress to expand the Service's mission to include protection of the President. Every President since 1901 has been protected by the Secret Service. The Service's protection responsibilities have expanded since then to include the First Family, the Vice President, former Presidents, visiting heads of states and others. The Service's investigative authority has also

expanded over the years to include other financial crimes such as identity theft, credit and debit card fraud, and financial institution fraud.

The Service continues its original task of shutting down counterfeiting operations both here and abroad. Through the Project Colombia Initiative and Peruvian Counterfeit Task Force, the Service provides support to local law enforcement investigations in Colombia, the largest producer of counterfeit U.S. currency, and Peru a growing competitor.

Since 1994, the Service provided forensic and technical support to the National Center for Missing and Exploited Children, including polygraph exams, handwriting, and fingerprint analysis and voice print comparisons. The Service operates Electronic Crimes Task Forces to investigate hacking, phishing, skimming, malware attacks, and other electronic crimes.

The Service also operates a national network of 38 Financial Crime Task Forces to investigate crimes associated with the Nation's economic crisis, particularly mortgage fraud. Since 2006, the Service has referred over 400 mortgage fraud cases for prosecution.

These are but a few of the Service's investigative responsibilities. It is clear that the Secret Service is not merely in charge of protecting our President, but also plays a major important role in investigating large scale financial electronic crimes. For that reason, I do look forward to the testimony of our witness and would yield back at this time.

Thank you, Chairman.

Mr. SCOTT. Thank you. We have been joined by the Chairman of the full Committee, the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Chairman Scott and Judge Gohmert. I am glad we have so many of our Members of the Committee out.

Director Sullivan, I have a confession to make to you. I was prepared to suggest that you be reassigned because of what happened at the White House, but my able staff has persuaded me that that would be no more fair than holding someone responsible for something that they thought was being covered properly. So I have revised my statement so that—we just want to say this. I don't know how we lost the Social Secretary at the White House, but blaming her is misplaced. The protection of the President of the United States is a job for Secret Service. It is not the Secretary's job or anybody else's. And what I need to know is whether this is preventible. Nobody is perfect. But we are talking about in effect the most influential, if not most powerful single human being on the planet. We don't have time to get his protection right the second time. And I have got to find out whether we can get some certainty that this can never happen again, especially at the White House itself.

The other part of your duties that Chairman Scott referred to, I would like your able men and women behind you to just let me know how many—what was the disposition of all the mortgage fraud cases. We have got so much rip-off coming from the mortgage companies and all the lines of—they resell them, then go out of business. No one can even find them to work out any kind of compromise. We have got foreclosures going on at a record rate in

many of our cities, and that is an area of your responsibility I would like you to deal with.

Thank you, Mr. Chairman.

Mr. SCOTT. Thank you. If other Members have a statement for the record, by unanimous consent, without objection, so ordered.

Our witness today is Mark Sullivan, the Director of the United States Secret Service, who was sworn in as the 22nd Director in 2006. Immediately prior to that he served as Assistant Director of the Office of Protective Operations. He began his Secret Service career as a special agent in the Detroit field office in 1983.

Mr. Sullivan, your total written statement we entered into the record in its entirety. So I would ask you to summarize your testimony. It is usually 5 minutes. But since you are the only witness, do the best you can. We will have the timing light on, but feel free to make your complete statement that you think we need to hear. We have your complete written statement. And so at this point, you may begin your testimony.

TESTIMONY OF MARK SULLIVAN, DIRECTOR, UNITED STATES SECRET SERVICE, UNITED STATES DEPARTMENT OF HOMELAND SECURITY

Mr. SULLIVAN. Thank you. Good afternoon, Chairman Conyers, Chairman Scott, Ranking Member Gohmert. It is my privilege to appear before you today to discuss the current state of the U.S. Secret Service. I will offer brief remarks and ask that my full statement be included in the record.

Before I begin, I would like to recognize the great relationship we have enjoyed with the staff of this Subcommittee for years. Whether it was working to expand our successful Electronic Crime Task Force program or addressing the spike in mortgage and other financial frauds in recent years, your staff has always demonstrated a level of cooperation and professionalism that is appreciated by all of us at the U.S. Secret Service.

Since the majority of our statutory authorities fall under Title 18 of the U.S. Code, the Judiciary Committee has a long distinguished history of working with the U.S. Secret Service on investigative priorities that many in the general public may not recognize we cover. While most people associate the U.S. Secret Service with the protection of the President and Vice President, the special agents in our field offices around the world who make that protection possible also spend roughly half of their time protecting our country's banking and financial system from criminals who seek to harm us.

Although these may appear to be disparate missions on the surface, our protective responsibilities are reliant on the experienced staffing and assets from our investigative field offices to cover daily presidential, vice presidential or other protective travel. They also provide a surge capacity for the U.N. General Assembly, designated NSSEs, and presidential campaigns. Special agents in the field are on the front lines of protecting intelligence cases, responding 24 hours a day, 7 days a week to every threat made toward a Secret Service protectee. In addition, Secret Service field office personnel are responsible for maintaining the excellent relationships we have built through the years with our State and local law enforcement partners.

Finally, but important to understand, is that the special agents you see in close proximity to the President, Vice President or other protectee are not fresh out of our training academy. These agents have spent years in our field offices honing their investigative skills by conducting criminal and protective intelligence investigations. They have also developed their protective skills by performing advance work, providing physical security for visiting heads of state, as well as supporting our permanent protective details. It is through these assignments that special agents in the field develop the expertise, maturity, and judgment needed to succeed in the next phase of their career, a permanent protection assignment.

From our original mandate in 1865 to suppress the counterfeiting of U.S. currency to the complex transnational financial crimes we are investigating today, the U.S. Secret Service has always held two things as sacrosanct, our relationship with law enforcement and other partners and intensive training as a means to prevent bad things from happening. One example of this is our Electronic Crimes Task Force program, or ECTF, that started in our New York field office but has since been replicated in 28 other locations, to include our first internationally ECTF based in Rome, Italy. Membership in our ECTF program includes over 2,100 State, local, Federal and international law enforcement partners, over 3,100 private sector partners, and nearly 300 academic partners. These partnerships are critical to the success of the ECTF program's preventive approach.

Effective collaboration with the banking and financial sector to protect their system networks has led to a stronger business continuity plan and routine risk management assessments of their electronic infrastructure. This collaborative approach also affords the business community direct access to law enforcement if an intrusion is detected. In addition, the research and development that our academic partners bring to the table ensure that all ECTF members are on the cutting edge of technology.

At the core of our ECTF program is the training provided through our Electronic Crimes Special Agent Program, or ECSAP. Nearly 1,200 special agents or 35 percent of the agent workforce has received at least one of three levels of ECSAP training. These special agents are deployed in 98 offices throughout the world and are experts in computer forensics and the preservation and retrieval of electronic evidence. Given the success of ECSAP, the U.S. Secret Service identified a growing need for our State and local law enforcement partners, as well as prosecutors and judges to receive similar training. While this training was provided on an ad hoc basis for years through our electronic crimes State and local program, the Secret Service in partnership with DHS stood up the National Computer Forensic Institute, or NCFI, with the goal of providing a national standard of training for a variety of electronic crimes investigations. By the end of this fiscal year, the U.S. Secret Service through the NCFI will have provided training to 932 State and local law enforcement officials, representing 300 agencies from 50 States and the two U.S. territories.

Since moving to the Department of Homeland Security in 2003, the benefits of our investigative program have been evident.

Whether it was the successful investigation and prosecution of the two largest network intrusion cases in U.S. history or the seizure of more than $20 million of counterfeit U.S. Currency in Lima, Peru during the first year of our operation there, we have contributed to the success of the Department by protecting the banking and financial infrastructure of our country.

Let me be clear, the U.S. Secret Service would be unable to effectively meet our protective mandate if not for the expertise that our special agents develop through conducting criminal investigations in our field offices both here and abroad. If the President schedules a trip to the Pacific Northwest 2 days from now, we would be able to immediately conduct the necessary advance work, including liaison with local law enforcement, to ensure the President's safety. This would not be possible without the strong support of our State and local law enforcement partners and the dedicated men and women across the United States and around the world who serve with distinction as special agents, uniform division officers, and administrative professional and technical personnel.

Despite the demands of our dual mission, the men and women of the U.S. Secret Service are ever vigilant and prepared for the challenges that lie ahead.

Mr. Chairman, distinguished Members of the Committee, this concludes my opening statement. I would be more than happy to answer any questions at this time.

[The prepared statement of Mr. Sullivan follows:]

PREPARED STATEMENT OF MARK SULLIVAN

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.

11

Mr. SCOTT. Thank you very much. We will begin and recognize ourselves under the 5-minute rule. I will begin with the gentleman from Puerto Rico.

Mr. PIERLUISI. Thank you very much, Chairman Scott. Thank you, Director Sullivan, for appearing before us.

Beyond its protective function, the Secret Service plays other key roles, some of which you have mentioned. I am particularly interested in its work in the area of financial crimes as it may relate to money laundering, And I will tell you where I am coming from. I represent Puerto Rico, and we have had a lot of drug trafficking in Puerto Rico, as well as the Caribbean since the mid '90's. Back then I was Attorney General. We were designated as a High Intensity Drug Trafficking Area as a result of efforts on my part, and I am particularly interested in what, if anything, you are doing, your agency is doing in the Caribbean relating to money laundering, which I know is happening.

I know—let me say up front—that your agency participates in Financial Crime Task Forces throughout the Nation. I wonder whether you are participating in High Intensity Drug Traffic Area programs throughout the Nation, including in Puerto Rico. And I want to see what commitment you have regarding this terrible crime that happens and that generates violence, among other things.

Mr. SULLIVAN. Thank you for that question. Sir, what we instruct all of our agents in the field to do is to have an impact in that community where they oversee for that particular office. Nationally we are in partnership with DEA for that very reason when it comes to drug trafficking and the other financial type crimes that are involved with drug trafficking.

Now, I can't give you the particulars as far as what we are doing in the Caribbean. I can tell you that we are very active down there. We do see a lot of money laundering that our people are involved in. I can tell you that it is evident to me just in the seizures that I see, the asset forfeiture seizures that I see—last year, our asset forfeitures were up 35 percent. 90 percent of those asset forfeitures are going back to the victim.

But I can tell you that that is an area that we do pay attention to, that we do ensure that we do partner up. As you know, we have an office in Puerto Rico. And I do believe that our people down there are very involved in this particular type of criminal activity, as well as our office in Miami, which is the office that, you know, San Juan reports to.

Mr. PIERLUISI. I tell you, one thing that concerns me is that with all of this attention—and it is due attention—that the Mexican border is receiving from us, I hope that we don't forget that the southern most border of the U.S. Is the one you have in Puerto Rico and the USVI, and that these drug trafficking organizations and the related money laundering organizations are like moving targets. If you do not have a global or regional approach, you are wasting your time and effort. To the extent you are paying attention to, let's say, the Mexican border, you cannot forget that they simply change routes, they change their focus. So I just urge you to keep an eye on the Caribbean as well because otherwise your efforts could be fruitless.

Mr. SULLIVAN. Congressman, what we are seeing—and you have hit on a very important point—everything now is transnational. I mean, all of our crimes are of borderless type crimes. And that is why we have seen again—we are looking to replicate the Financial Crime and the Electronic Crime Task Forces we have here domestically. We are looking to expand those internationally. And, you

know, that is part of our foreign field office strategy, is for these financial—it fits very well within both our protective mission and with our investigative mission.

So I agree with you wholeheartedly and I would be more than happy to get some information for you on what we are doing down in Puerto Rico. And we can get it back to your staff if you like.

Mr. PIERLUISI. I thank you.

Mr. SULLIVAN. Thank you, sir.

Mr. SCOTT. The gentleman yields back. The gentleman from Texas.

Mr. GOHMERT. Thank you again, Mr. Chairman. Director Sullivan, it is good to see you again.

I understand one of the many things that your agency gets into investigating at least is mortgage fraud. What is the most common form of mortgage fraud that your department ends up investigating?

Mr. SULLIVAN. You know, I would say straw buyers.

Mr. GOHMERT. Straw buyers?

Mr. SULLIVAN. Yes, sir. We just were involved in a task force that went—it was Broken Dreams. It was generated by the Attorney General along with—the FBI was involved, several other Federal and State and local law enforcement agencies, a nationwide initiative. It went from, I believe, March through April. During the course of that time, I believe we had about 22 officers working about 40 different mortgage fraud investigations. We arrested, I believe—or charged 70 people and we uncovered about $135 million worth of fraud and mortgage fraud. And I would say for the most part what we are seeing is straw buyers.

Mr. GOHMERT. One of the things that we have seen going through September and October of 2008 were the mortgage-backed securities. And it seemed that one type of fraud was straw buyers, as you mentioned. But one is people approaching fraud in the manner in which they pushed people into loans they couldn't afford and ultimately loans that had no chance of succeeding and then banding—another type seemed to me in cases where it appears they knowingly put together a whole bunch of really bad loans and put a big thick document with it to make it a security and then sold the securities as mortgage-backed securities and unfortunately without recourse, so that even though they were bad loans all packaged together and it certainly seems they should have been knowingly put together, they are sold, people left with millions and millions of dollars and left others holding those bad papers and bad securities. And then the credit default swaps to insure the MBSs and all that kind of thing.

But I was just wondering through the course of your investigations if you saw any of the laws that needed to be tightened up to help prevent that kind of thing? I have wondered about eliminating the ability to sell mortgage-backed securities without recourse. It seems as if maybe if the generators of these loans had recourse back against them, they would be a whole lot more careful.

But I was just curious if you saw some things we maybe could do to help cut back on loan fraud.

Mr. SULLIVAN. You hit on a very good point, you know, because we are seeing collusive—you know, there are collusive people.

There are insiders there that are manipulating documents to qualify people that just aren't qualified for that particular loan. You know, one of the things I have seen is, you know, that various people are going in and claiming bankruptcy. And bankruptcy will delay the system in that the call on these loans now will be delayed. And I think that is an area that maybe we might want to look at, is these people claiming bankruptcy as a technique to put off the inevitable before the debt loan has to be called in. So all payment now is forgiven or delayed. And to me that was an area that I believed we should take another look at.

Mr. GOHMERT. And I appreciate that. One of the things that has come up this week, of course, is making public the arrest of Russian spies. And we know the President, with whom your agency is charged with protecting, had just met with and sat down with the President from Russia. And I am curious. Is the Secret Service in their role as protectors of the President made aware of information indicating we are meeting with the President who has spies all around? Is that part of your packet of knowledge when you protect a President?

Mr. SULLIVAN. Yes, sir. I could not ask for better cooperation than we get from the intelligence components and from the FBI. We get very good information from their very good briefings from them. I am briefed every single day. But our partners out there are very good about providing any information to us that will enable us to do our job better and protect the President better.

Mr. GOHMERT. I am glad. So would the President be made aware of that, too, so he knows what exactly he is dealing with?

Mr. SULLIVAN. Sir, that would not be our role to provide him with that information.

Mr. GOHMERT. But you may have the information but the man you are protecting may not?

Mr. SULLIVAN. No. I would say, sir, that that information would be provided to him by the people that provide him with intelligence information.

Mr. GOHMERT. Thank you. I thank the Chair.

Mr. SCOTT. Thank you. The gentleman yields back. The gentleman from Illinois.

Mr. QUIGLEY. Thank you, Mr. Chairman. Welcome, Director.

You mentioned in your opening statement—I believe it was $20 million that was counterfeit money from Peru; is that correct?

Mr. SULLIVAN. I believe that is correct, sir.

Mr. QUIGLEY. I understand that Peru and Colombia are major sources of counterfeit money coming into the United States. Forgive the 101 question. Is it just the drug trade or is it other money launderers that are the people they are dancing with here to bring money into this country?

Mr. SULLIVAN. I think it is a combination of both of those things. You know, back in 2001, we saw that there was a large quantity of counterfeit money coming into this country being manufactured in Colombia. And at that time, we formed a partnership with the Colombian law enforcement, with a vetted group of Colombian law enforcement. And over the next 8 to 9 years, we have seized, I believe, about $250 million in counterfeit coming out of Colombia. We have arrested about 700 people. And I believe we have made about

100 or so counterfeit plant seizures down there. And the majority of those all do involve some nexus to the drug trade.

Meanwhile, the fastest growing region now in South America for the manufacture of counterfeit currency is Lima, Peru. And so we have pretty much mimicked the same strategy that we did in Colombia back in 2001. And back in March of 2009, we entered into a partnership with our Peruvian law enforcement partners. And so far, that has yielded about $20.5 million, I believe. I think we have arrested somewhere around 35 or 40 people. And I think we have about maybe 17 or 18 plant seizures.

Mr. QUIGLEY. So does the new technology in our currency, do they just keep matching it somehow? Or is it easier to catch because of the new technology, the water marks and so forth?

Mr. SULLIVAN. You know, they do try to replicate that. What is interesting is when we first began—and up until about maybe 15 years ago—the majority of all the counterfeit currency that we saw being manufactured here in the U.S. was all offset printing. All the offset printing we see now is being done in foreign countries, whether it be in Europe or in South America. All of that counterfeit currency that is offset printing is coming mainly foreign. And that is where all of our plant seizures are coming from.

The majority of the counterfeit currency that we see here domestically is mainly computer or ink jet generated. And as I said, they do attempt to replicate the security features. Some people do a fair job with it, other people not as well. And the bottom line is we tell all people who come in contact with money to take a real hard look at the money that they are handling.

Mr. QUIGLEY. And it is your understanding or you get briefed as to where the next generation of our currency is going? It is more advances coming as well?

Mr. SULLIVAN. Yes, sir. As a matter of fact, they just rolled out the new $100 bill. It will be coming out, I believe, in February of 2011. But we work with our partners at Treasury, at the Bureau of Engraving and Printing, and with the FRB to make sure that we have the right security features in our currency and keep up with anyone who is trying to defeat those features.

Mr. QUIGLEY. Thank you. I yield back.

Mr. SCOTT. Thank you. The gentleman from Virginia.

Mr. GOODLATTE. Thank you, Mr. Chairman. And, Mr. Sullivan, thank you for joining us today.

It seems to me that your work in the Electronic Crimes Task Force gives your service a unique insight into some of the vulnerabilities in our Nation's critical infrastructure. As a member dedicated to making sure we get any cybersecurity legislation right, I would be interested in hearing from you what you believe are some of the most important things we need to do to secure our Nation's critical infrastructure.

Mr. SULLIVAN. One of the things that we see when you look at the two identity theft cases that we worked back in 2008/2009, one was a cyber intrusion where 40 million identities were stolen. The next one was a cyber intrusion with about 130, 140 identities stolen. And I think the one thing is that people have to evaluate the systems and they have to make sure that they are protected as well as they can be protected.

I think it goes back to—I think you also have to look at partnerships. I think all of us have to look at this as a collaborative effort. That is why I believe, sir, that these Electronic Crime Task Forces are so important, because we bring into play here not only State and local law enforcement, we also bring in academia, we bring in the business community, we bring in a wide range of people. It is not just the traditional law enforcement effort, but it is a true community effort. And I think it is really important for us to take that approach.

Mr. GOODLATTE. Thank you. Would you be willing to work with me to explore this issue further?

Mr. SULLIVAN. Absolutely, sir.

Mr. GOODLATTE. Thank you. Could you go into more detail about electronics benefits transfer fraud? Is this related to food stamp benefits? Is that——

Mr. SULLIVAN. I think it can be anything, you know. You look at again the evolution of our investigations. 20 years ago if somebody was getting a Social Security benefit, they got it via a Treasury check. And we used to see Treasury checks stolen, forged, cashed. You know, today those benefits are, you know, transferred via wire. You know, everything now is being done via wire.

Mr. GOODLATTE. That is a broader category than just the cards that people carry when they purchase foods under the SNAP program?

Mr. SULLIVAN. I think just about any type of payment you can think of would be included in that category.

Mr. GOODLATTE. Are there any trends in terms of the type of perpetrator who commits this type of fraud?

Mr. SULLIVAN. Do you mean as far as the electronic fund transfers?

Mr. GOODLATTE. Yeah, EBT fraud.

Mr. SULLIVAN. I think these are all people that are just looking for vulnerabilities. I think these are the type of people that have a high degree of a technology background, which again there is more and more increasing in our population now. But again, I look at this as a crime of opportunity, the same as I looked at these type of crimes when it was paper. You know, now it is electronic. You know, 50 years ago if somebody was going to rob a bank, they used a gun. Today they use a keyboard. Again, that is why I go back to it is so important for us to protect our critical infrastructure and our payment systems.

Mr. GOODLATTE. What criteria does this task force use to prioritize the field investigations that it conducts?

Mr. SULLIVAN. Again, we want to make an impact on the community. So we leave it up to our agents in charge working with their State and local law enforcement partners, with the business community, with the financial industry, with academia to determine what the impact is there. We meet with the U.S. Attorney's Office. We get the guidelines for prosecution. But we also look to State and local prosecution. And one of the things that we have found is that an investigation initially may not appear to be a large high dollar or large dollar investigation. It might appear to be only $1,000 fraud. But what we have found is as we start to peel back on that, we realize that maybe this group is affiliated with a bigger

group. So we do take a pretty hard look at everything that is referred to us and then we prioritize and make sure that whatever we are working does have an impact on the community.

Mr. GOODLATTE. Thank you. Thank you, Mr. Chairman.

Mr. SCOTT. The gentleman yields back. Does the Chairman have questions? Okay.

Ms. Jackson Lee is recognized for 5 minutes.

Ms. JACKSON LEE. Mr. Sullivan, welcome.

Mr. SULLIVAN. Nice to see you.

Ms. JACKSON LEE. Since I am going to start off with a question of the state dinner, thank you for the manner in which the Secret Service addressed its responsibility and the manner in which you appeared before a number of Committees, I believe. And we appreciate that kind of stand-up-manship, if you will. And I know you prefer not to have to do that on a regular basis, but I do appreciate it very much.

I am just going to start off with you telling us what you have learned from the Indian Prime Minister's state dinner and that series of incidents as it relates to staffing and procedures that may now be in place or generally so in any manner surrounding the White House.

Mr. SULLIVAN. Thank you, Congresswoman. Thank you for the question.

First of all, as I have said from the very beginning, this was a mistake. This was our fault that happened. Somebody made a judgment call and it wasn't the right judgment call. And some individuals got into the White House who shouldn't have gotten in there.

One thing I do want to make clear is these people that did get in did go through every level of security that all the other individuals went through. But it was a mistake, an error. It was a mistake in judgment. It never should have happened, and nobody was more disappointed that that happened than me. And believe me, nobody has been more difficult or harder on us than ourselves regarding those people getting into the White House on that evening.

As I have told you before, this continues to be under investigation, criminal investigation. And I will share with you as much as I can.

One of the things that immediately happened is we did review our procedures, we did review all of our policies. You know, at the White House we put close to 100,000 people through there every month. We have thousands of pass holders at the White House. We have all kinds of workers coming and going from the White House every day. For us, we have to be right though 100 times out of 100. We don't have the luxury of being right 99 times out of 100.

I believe that our policies, our procedures, I believe that they were correct. Again, I just believe that they were not followed. In the meantime, we have worked with our partners at the White House. We have worked with our partners at the State Department. We have worked with all of our partners when it comes to granting access to the White House.

I can tell you since that time, we have had numerous events at the White House. Right after that state dinner, we had numerous Christmas parties at the White House. We have had numerous

events at the White House. We had a state dinner, the Mexican state dinner back in May. All of these have gone off without a flaw.

Ms. JACKSON LEE. Do you feel comfortable that you had a sufficient wake-up call, that you are moving toward, you are moving—I do realize there is a criminal investigation. I would hope that it is indictable to have a reality show. That might be one offense that we might charge those individuals with. But in any event, you just feel that the T's are crossed and the I's are dotted? That is what I think is very important for the American people to hear.

Mr. SULLIVAN. I believe so. You know, Congresswoman, as I told you before, protecting the President is our number one priority, and we are not going to let anything happen to him or his family.

Ms. JACKSON LEE. I understand that.

Mr. SULLIVAN. That was a wake-up call. And I feel very comfortable with our procedures at the White House now, what we are doing at the White House now.

Ms. JACKSON LEE. Let me give you these quick questions. If you can expand on how effective the Electronic Crimes Special Agent Program is because that certainly is—from cybersecurity breaches to fraud on electronic facilities is very important. And then also, as I understand it, you have involvement in the report on the issues raised by the Virginia Tech tragedy, if I am not mistaken. And a number of incidents have happened on our college campuses, from Virginia Tech, Morehouse, UNC. A number of our children attend those schools, and I am wondering where we are with those kinds of incidents.

Lastly, you just mentioned it earlier, your commitment to securing and protecting the White House. Do you have enough resources and staffing as relates to the increased amount of threats that we hear against the White House and, of course, the President?

Mr. SULLIVAN. If it is okay, I will start with the Electronic Crime Task Forces. For us, these have been a huge success, not only the Electronic Crime Task Forces but our Financial Crime Task Forces.

As I have said before, we have 29 Electronic Crime Task Forces and 38 Financial Crime Task Forces. Last year, we opened about 1,100 electronic crime cases and we closed about 1,140. The potential loss that we saw in these investigations was about $533 million. The actual fraud that our investigators saw was about $100 million. And we arrested about 510 people via the Electronic Crime Task Force concept. And we also did 5,450 cyber forensic exams. And out of that, about 42 percent were for State and local law enforcement.

So I would say that these Electronic Crime Task Forces we have around the country have been very successful and have been very collaborative with all of our partners. And also as a result of the Electronic Crime Task Force—and I mentioned it in my opening statement—you know, the National Computer Forensic Institute in Hoover, Alabama, the opening of the NCFI a few years ago has allowed us to train by the end of this year about 940 State and local law enforcement, as well as State and local prosecutors. This for us is a force multiplier. Now these State and local law enforcement, they get the training, they get the equipment that they need to go back out and do their own forensic exams. And again, as I men-

tioned before, every State has been represented as well as, you know, the two U.S. Territories.

As far as Virginia Tech, this was a study that we conducted with the FBI and the Department of Education. What we looked at here, we looked at going back to 1900, I believe, up through 2005, 2007, I believe. We looked at about 150,000—I am sorry. We looked at about 300 incidents from a total of about 150,000 incidents that had transpired during that time to see if we could come up with some type of behavior pattern, to see, you know, exactly what type of individuals we were looking at here, to see if there is any clues prior to the event that maybe could have been identified that could help identify these people as being a potential problem. I do believe that one of the big issues here is that you, you know, do need to have people come forward when they see things about people that may trouble them. And that was one of the things we saw in the study, that there were people after the fact that came back and said that there was some behavior there that they had noticed and just didn't report it to anybody.

But these are really important issues to us. Again, it goes back to us wanting to make an impact on the community. You know, we have people in our Protective Research Division who were involved in this study, and I would like to have them come up and brief, you know, you or your staff and any of the Members on the full findings of the study.

Ms. JACKSON LEE. Do you have enough resources to protect the President?

Mr. SULLIVAN. Ma'am, as I said, our number one priority is to protect the President and we will never compromise on that. And every resource we have is available to protect him.

Ms. JACKSON LEE. Thank you. Thank you very much. I yield back.

Mr. SCOTT. Thank you. I recognize myself for 5 minutes. That doesn't really answer the question.

Are you using all the resources you have? Are there any sources you have asked for and haven't gotten?

Mr. SULLIVAN. No, sir. I don't know an agency head out there that would ever tell you that they have enough resources. Any additional resource, any additional funding that you would support us on, I would be more than happy to take.

Mr. SCOTT. On the question of protecting the President, are there any resources that you think you need that you haven't gotten?

Mr. SULLIVAN. Sir, I work very hard and diligently with the Secretary to ensure that we have all the resources we need to protect the President.

Mr. SCOTT. And what are the results of all of that communication? Do you get the resources you need or don't you?

Mr. SULLIVAN. Sir, right now as a matter of fact I am working with the Secretary on a reprogramming initiative to get some additional resources to protect the President.

Mr. SCOTT. And if you don't get what you need, would you let us know?

Mr. SULLIVAN. You will be the first one to know, sir.

Mr. SCOTT. Thank you. In response to the question from the gentleman from Texas on these loans, some of these loans were called

NINJA loans, N-I-N-J-A, no income, no job or assets. They subsequently, as he indicated, have gotten into the public stream.

Are you pursuing any prosecution for fraud in these packages and loans that had limited value being passed off as bona fide loans?

Mr. SULLIVAN. Sir, if it is a mortgage fraud, it is a criminal violation. We are going to pursue it.

Mr. SCOTT. Are you pursuing those cases now? I mean, it has a name. So people knew what they were doing. Are there cases being pursued now?

Mr. SULLIVAN. Sir, I am not familiar with that. Again, I would say if we are working in mortgage fraud, no matter what name they give it, if it is a fraud, we are pursuing prosecution on that fraud.

Mr. SCOTT. Could you get back with us with a little more specifics? On individual identity theft, what is the role of Secret Service on individual identity theft cases?

Mr. SULLIVAN. On a one person identity theft?

Mr. SCOTT. Yeah. Just run of the mill—well, you steal a lot of credit cards, but for the individual it is an individual case. What usually happens is the bank writes it off and nobody does anything. That is why these guys—why it is such a profitable business. What is the role on individual identity theft? What is the role of the Secret Service on cases like that?

Mr. SULLIVAN. Again, sir, I would say, Mr. Chairman, that we look at every single investigation as they are referred to us. And we have to prioritize all of our investigations. But as I said before, we sometimes have taken a one individual, it looked to be one victim and that has turned into 100 victims. And again, I go back to our Financial Crime Task Forces. And that is why many times those individual type investigations are able to be pursued, because of our partnership with the State and local law enforcements.

Mr. SCOTT. The problem you run into with the individual ID theft, if you get thousands of credit card numbers, if you don't get greedy and only milk each one for a couple of thousand dollars, you are pretty much risk free. What I am asking is, does the Secret Service have any role in creating a risk? And if it is for lack of resources, could you let us know what you would need to pursue these cases so that someone who is milking credit card numbers for just a couple of thousand dollars would incur some risk of investigation and prosecution?

Mr. SULLIVAN. Sir, that is a great point. And believe me, every one of us would love to go after every single person out there. One of the issues we have as well, though, is prosecution of these people. And I think that the issue here is not just us having enough assets to go after these individuals, but also the U.S. Attorney's Office, as well as at State and local prosecutors.

Mr. SCOTT. Well, can you give us an idea what it would cost to create risk for people who are promoting individual credit card fraud? Do you have some idea what we would be talking about if we——

Mr. SULLIVAN. Sir, we can look at that and get back to you on that.

Mr. SCOTT. Okay. You mentioned the campus attacks, targeted violence affects institutions of higher learning. The Campus Safety Act has passed the House twice which would create a research in best practices and training opportunities. You indicated that things aren't happening the way they should be happening. That is what the Campus Safety Act is supposed to cure. Your report just reports it. Don't we need some ongoing training available for institutions of higher education and research for best practices?

Mr. SULLIVAN. Sir, I think that is happening. Again our report went into what happened prior to 2007. I do believe that there is a much greater awareness right now than there was before. I know that we have gone out and done training for some college police, not as much as we would like to do, but for campus police. But I do think that there is a much greater awareness now. I do believe that people are being much more proactive now.

Mr. SCOTT. The campus police officers have endorsed the Campus Safety Act. So maybe we need to look at that and get the Senate to move on it.

The final question is you mentioned protection of the President. You also have the responsibility of protecting former Presidents.

Mr. SULLIVAN. Yes, sir.

Mr. SCOTT. And that protection for Presidents from Clinton back is for their life. And beginning with former President George W. Bush, it is only for 10 years?

Mr. SULLIVAN. Yes, sir.

Mr. SCOTT. Is there any reason to limit protection of Presidents beginning with that presidency for 10 years or should we repeal that limitation?

Mr. SULLIVAN. I think that is something that we all have to take a hard look at. It is something I have given a lot of thought to. As you know, that law was passed over 10 years ago now, I believe. I think that the times are much different than—I think given the current environment, I believe that that is something that we really need to work together on because I do think that the prudent thing to do would be to consider making it lifetime.

Mr. SCOTT. Has any report or recommendation been made?

Mr. SULLIVAN. I have talked to our Congressional Affairs people who are putting something together right now about that very issue, sir.

Mr. SCOTT. We will look forward to hearing it.

Any other questions? The gentleman from Texas.

Mr. GOHMERT. Thank you. And I think that is a great idea at this day and time with former Presidents potentially being targets for people who don't mind blowing themselves up to hurt innocent people. That is a good idea.

But I was hearing the discussion about the Indian state dinner, and it has affected the way things are done over there in getting tour groups in. But in talking to someone on the Oversight Committee, it was my understanding that the Social Secretary—although the White House did not allow her to come, apparently it was a matter of national security, executive privilege or something—that the Social Secretary wouldn't come testify. But she apparently made her own decision not to show up for the dinner when normally Social Secretaries do show up and that left the Se-

cret Service in a terrible quandary as to whether someone would be allowed.

Is that your understanding of why she did not show up that night for the state dinner?

Mr. SULLIVAN. No, sir. We had——

Mr. GOHMERT. Did somebody from Secret Service tell her don't come, we will take care of it, you don't have to be there to say people are okay and approved to come in?

Mr. SULLIVAN. Sir, what I was going to say is we agreed to be the individual——

Mr. GOHMERT. The scapegoat?

Mr. SULLIVAN. The Secret Service agreed to be the people that would be the name checkers. And——

Mr. GOHMERT. Well, you are always the name checkers, right?

Mr. SULLIVAN. Sometimes it is a shared responsibility, whether it is at the White House or at a function outside of the White House.

Mr. SCOTT. Have you gotten it straight? I mean, do we have to go through this again? I mean, do we have any reason to be concerned that the coordination between the Social Secretary's office and the Secret Service, do we have any reason to be concerned that that coordination is not taking place now?

Mr. SULLIVAN. Sir, I can tell you that the coordination between us and this White House, as well as every other White House before, is outstanding.

Mr. GOHMERT. Well, Mr. Chairman, the thing is now we have gone in the mornings when there is tours from having one checkpoint to having two checkpoints a block apart and making hundreds of people wait, much longer than before, having doubled the number of people, now all in uniform instead of plainclothes, when the whole problem was not the morning tours, it was a state dinner. And so I am curious—and I realize our time is up and we've got to go vote, but I would really like to know why it was necessary to completely double the hassle of getting in for a morning tour because of something that happened at a state dinner when, as I understand it, there hadn't been a problem with somebody getting in that wasn't supposed to for a tour. Is that not correct?

Mr. SULLIVAN. No, sir. You know, our methodology has always been a redundant checkpoint and there should always——

Mr. GOHMERT. Well, if it was always redundant, now it is doubly redundant. So anyway, I would appreciate knowing why it was necessary and if we could get a follow-up statement in writing as to why it was necessary to double the redundancy basically for the morning tours.

But thank you, Mr. Chairman.

Mr. SCOTT. The gentleman's time has expired. No other questions, I would like to thank the Director for your testimony today. Members may have additional written questions which we will forward to you and ask that you answer as promptly as possible so that the answer may be a part of the hearing record. The record will remain open for 1 week for submission of additional materials.

Without objection, the Subcommittee stands adjourned.

[Whereupon, at 3 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Statement by the Honorable John Conyers, Jr.
for the Hearing on the

United States Secret Service

before the Subcommittee on Crime, Terrorism, and Homeland Security

Tuesday, June 29, 2010, at 2:00 p.m.
2141 Rayburn House Office Building

Good afternoon. Today's hearing will examine the role and operations of the United States Secret Service.

For many Americans, the Secret Service is most associated with the stereotype of an agent wearing a dark suit and an earpiece, and alertly standing at the President's side.

But the hardworking men and women of the Secret Service have many other important responsibilities in addition to this obviously critical job.

To provide some perspective for today's hearing, I want to make three points about that agency and the interests of this Committee.

First, the protective role of the Secret Service is critical to the operation of our government, and it is much broader than most realize. The Secret Service protects not only the President and Vice President, but numerous others including visiting heads of state and other distinguished visitors to the United States.

Unfortunately, the seriousness of this role is why I must raise the serious lapse in security for the President on November 24th of last year.

On that evening, three individuals, including Michelle and Tareq Salahi, passed through Secret Service checkpoints while not being authorized guests for that night's state dinner for the Prime Minister of India. The bottom line is that people who were not invited to the dinner, or authorized in any way to attend that function, were let into the White House and had personal access to the President, the First Lady, the Vice President, and other dignitaries.

The blame was put by some on the White House social secretary, who is no longer in that position. I think this blame is somewhat misplaced. The people whose job it is to protect the President let him and all of us down. Indeed, Director Sullivan himself has stated that the Secret Service was "deeply concerned and embarrassed" by what happened and the agency's conduct.

This is a very serious matter. I want to hear from the Director about this incident and what the agency has done to hold people accountable and make sure that nothing like this happens again.

I will also want to hear today more about emerging challenges to this security function, and how security lapses will be avoided in the future.

Second, the Secret Service has an investigative role which is becoming even more vital because of the recent state of our economy.

The Service has broad jurisdiction over a variety of financial crimes, such as mortgage fraud. The Secret Service has a particular expertise in this area, and its Mortgage Fraud Working Groups have been a central part of the federal law enforcement effort to combat this type of crime.

This agency has referred more than 430 mortgage fraud cases for prosecution since 2006, and it has taken a substantial role in fighting mortgage fraud in some of the worst hot spots for these schemes.

Between 2003 and 2008, the Secret Service made nearly 29,000 criminal arrests for counterfeiting, cyber investigations and other financial crimes, 98% of which resulted in convictions, and seized more than $295 million in counterfeit currency.

In addition, the Secret Service investigated and closed financial crimes cases where actual loss amounted to $3.7 billion and prevented a potential loss of more than $12 billion.

Third, the Secret Service is a full-fledged law enforcement agency, whose broad and significant functions are of central interest to this Committee.

We value our positive and cooperative relationship with this agency, and we take seriously our continuing responsibility to exercise oversight over its operation. This hearing is an important part of that oversight, and we plan to be even more engaged with the Secret Service in the future.

So, I look forward to hearing from Director Mark Sullivan about the specific issues I have raised, as well as other matters concerning the evolving role of the agency.

SHEILA JACKSON LEE
18TH DISTRICT, TEXAS

WASHINGTON OFFICE:
2160 Rayburn House Office Building
Washington, DC 20515
(202) 225-3816

DISTRICT OFFICE:
1919 SMITH STREET, SUITE 1180
THE GEORGE "MICKEY" LELAND FEDERAL BUILDING
HOUSTON, TX 77002
(713) 655-0050

ACRES HOME OFFICE:
6719 WEST MONTGOMERY, SUITE 204
HOUSTON, TX 77019
(713) 691-4882

HEIGHTS OFFICE:
420 WEST 19TH STREET
HOUSTON, TX 77008
(713) 861-4070

FIFTH WARD OFFICE:
4300 LYONS AVENUE, SUITE 200
HOUSTON, TX 77020
(713) 227-7740

Congress of the United States
House of Representatives
Washington, DC 20515

COMMITTEES:
JUDICIARY
SUBCOMMITTEES:
COURTS AND COMPETITION POLICY
IMMIGRATION, CITIZENSHIP, REFUGEES, BORDER SECURITY, AND INTERNATIONAL LAW
CRIME, TERRORISM AND HOMELAND SECURITY
CONSTITUTION, CIVIL RIGHTS, AND CIVIL LIBERTIES

HOMELAND SECURITY
SUBCOMMITTEES:
CHAIR
TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION
BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM

FOREIGN AFFAIRS
SUBCOMMITTEES:
AFRICA AND GLOBAL HEALTH
MIDDLE EAST AND SOUTH ASIA
TERRORISM, NONPROLIFERATION, AND TRADE

SENIOR WHIP
DEMOCRATIC CAUCUS

CONGRESSWOMAN SHEILA JACKSON LEE, OF TEXAS (TX-18)

COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

Hearing on the Role and Operations of the United States Secret Service

June 29, 2010 2:00 p.m. Rayburn 2141

Mr. Chairman, I thank you for holding this hearing into the roles and functions of the United States Secret Service. I also thank Ranking Member Gohmert for being here, and thank Director Sullivan for taking the time to meet with us today and answer our questions.

The Unites States Secret Service is one of the oldest Federal law enforcement agencies in the country, with a long and distinguished

history going back to 1865. It began its best-known role, the protection of the President, informally back in 1894, and officially in 1901, following the assassination of President McKinley. But its original purpose was to protect the integrity of the currency of the United States, by investigating and suppressing counterfeiting activities. As an outgrowth of that, it now also investigates a great variety of financial fraud, as well as identity theft, etc.

There have been some events in the recent past that have raised a certain amount of concern regarding the USSS and its protection of the President, particularly the Salahi incident, where uninvited "party crashers" were able to meet President Obama, after passing through security checkpoints. I look forward to being enlightened on that matter, and how much a matter for concern it may or may not actually be.

I am particularly concerned about these issues in light of the security environment, with threats against the President's life at an all time high. Last year, various news outlets reported that there had been an increase of 400% in the number of death threats the President received since President Obama's inauguration. That is a rate of, I think, 30 death threats a day against the President of the United

States. I want to know how the Secret Service is adapting to this heightened threat environment. I think we need to determine whether the Secret Service and its agents have absolutely everything they need to ensure the safety of the President.

Again, I want to thank Director Sullivan for being here, and to assure him that we on this Subcommittee welcome his insight into the Secret Service, its functions, and how we can help provide it with the tools it needs to do its job most effectively.

RESPONSE TO QUESTIONS FROM MARK SULLIVAN, DIRECTOR, UNITED STATES SECRET SERVICE, UNITED STATES DEPARTMENT OF HOMELAND SECURITY

QFR's and USSS Responses

Hearing on Role and Operations of the United States Secret Service June 29, 2010

1) Cost associated for USSS to be able to investigate all ID theft cases referred to USSS? (Rep. Scott)

Answer - The Secret Service's primary investigative mission is to safeguard the payment and financial infrastructures of the United States. Simply stated, the Secret Service realizes identity crime violates the trust in the U.S. payment systems, which in turn threatens the American economy. To ensure the American tax-payers are receiving maximum benefits from their investment, The Secret Service **primarily** focuses our resources on high-impact cases. The Secret Service measures our results in dismantling, arresting and deterring criminal organizations involved in identity crimes. The Secret Service carefully tracks identity crimes by case types and arrest statistics, as well as an agent's investigative man-hours.

Although the Secret Service primarily focuses its resources on high-impact cases, through our 31 Electronic Crimes Task Forces (ECTF's) and our 38 Financial Crimes Task Forces (FCTF's) the Secret Service works closely with state and local law enforcement agencies to investigate and prosecute all identity theft cases. As a Federal Law Enforcement agency each Secret Service office has to operate within the prosecutorial guidelines established within their area of responsibility by the U.S. Attorney in that district. Consequently, some identity theft cases do not meet the federal prosecutorial guidelines established by that U.S. Attorney's Office. The Secret Service does however work with its state and local partners to properly investigate all financial crimes an attempt to make investigative links between cases with small dollar amounts to see if they are related to a larger organized criminal group. All criminal cases investigated by the Secret Service are conducted by its special agents. Consequently, for the Secret Service to have the ability to investigate every identity theft case referred to us nationwide, the agency would need approximately 150 additional special agents assigned to our various field offices. At the journeyman grade level of a GS-13 the salaries & expenses cost of a GS-13 special agent totals approximately $115,000 per year. Therefore for the additional 150 special agents that the Secret Service would need the total would be approximately $17.2 million dollars.

During fiscal year (FY) 2010, the Secret Service investigated 3,242 identity theft related cases. These investigations resulted in 4,070 foreign and domestic arrests during the same time period. Approximately 46 % of all Secret Service arrests in 2010 involved an identity crime. Although most identity crimes investigations are time intensive, the Secret Service accomplished these arrests in FY 2010 through 483,773 investigative man-hours. While the Secret Service utilizes support personnel to aid in identity crime investigations, approximately 96 percent of the total man-hours were accomplished by agent personnel. The total Secret Service manpower hours spent investigating identity crimes translated to $21,703,210 million dollars for FY 2010.

Highlighting the agency's foreign partnerships initiatives in 2010, the Secret Service coordinated with foreign law enforcement to affect the arrest of 522 individuals wanted for identity crimes. This achievement is over a 300 % increase in foreign arrests in five years.

Capitalizing on the Secret Service's 31 Electronic Crimes Task Forces (ECTFs), today agents pursue criminals across international borders. Although originally started in the New York Field Office in 1987, the Secret Service's ECTF model was greatly enhanced by the 2001 USA Patriot Act. In fact, two of the 31 ECTFs reside outside the United States. Force multiplying the Secret Service's investigative reach is a primary goal of the agency. Foreign law enforcement contacts forged during Presidential and Vice Presidential protective missions have significantly extended the Secret Service ability to dismantle international identity crime organizations. While working in a foreign protective capacity, agents often utilize their contacts to assist in investigations. As a result of these partnerships, these man-hours are not charged to the identity crime investigation cost analysis. The Secret Service has established successful and trusted partnerships in both the law enforcement and business communities around the world in order to effectively combat financial and identity crimes.

2) Why are multiple check-point necessary when accessing the White House for morning tours? (Rep. Gohmert)

Answer - "Pursuant to 18 USC §3056 and §3056A, the United States Secret Service (Secret Service) is responsible for implementing appropriate security procedures to protect the President, First Lady, other protected individuals at the White House, as well as the buildings and grounds that comprise the White House Complex. As part of its overall protective methodology, the Secret Service constantly evaluates and refines these procedures in an effort to respond to evolving threats and identified vulnerabilities at Secret Service protected facilities, including the White House Complex. Further, the Secret Service works with its federal, state, local, military, and other partners to provide a secure environment that is both appropriate and coordinated among all of the entities who have security responsibilities.

In the particular case of tours occurring at the White House Complex, the Secret Service works in close coordination with the Executive Office of the President (EOP), the National Park Service, the U.S. Park Police, and other agencies to provide an adaptable, multi-layered security plan. The various checkpoints, operated by the EOP and the Secret Service, serve distinct functions within this security plan. Some of the checkpoints determine whether individuals arriving at the White House Complex have been scheduled to attend a particular tour. Other checkpoints are responsible for determining whether individuals have been appropriately screened to enter the White House. This closely coordinated process provides appropriate protection for the White House Complex, while still permitting members of the public to access the facility."

3a) What types of crime is the U.S. Secret Service actively investigating in Puerto Rico? (Del. Pierluisi)

Answer - Special Agents of the U.S. Secret Service assigned to the San Juan Resident Office are actively investigating various crimes to include Financial (Counterfeit, Bank Fraud, Credit

Card/Access Device Fraud, Mortgage Fraud, Money Laundering and Check Forgery), Identity Theft and Protective Intelligence.

b) Are members of the USSS working with or assisting other Law Enforcement entities with investigations involving crimes of money laundering and drug trafficking?

Answer -Special Agents of the U.S. Secret Service assigned to the San Juan Resident Office are currently assisting other Federal Agencies with their investigations pertaining to Financial Crimes and prescription drugs. The U.S. Secret Service is currently assisting the following Federal Agencies with the associated crimes; Internal Revenue Service – U.S. Treasury Checks, Bank Loans, Bank Fraud and Mortgage Fraud, Drug Enforcement Administration – Identity Theft, in relation to prescription drugs, Federal Bureau of Investigation – Identity Theft, Bank Fraud and Mortgage Fraud, U.S. Immigration and Customs Enforcement – U.S. Treasury Checks, Bank Loans, Bank Fraud and Mortgage Fraud, U.S. Postal Inspection Service – Mail Fraud, U.S. Treasury Checks, Bank Fraud and Mortgage Fraud and U.S. Department Health and Human Services (HHS) OIG - Identity Theft, in relation to prescription drugs and Health Insurance, Bank Fraud and Wire Fraud.

c) Are members of the USSS assigned to any Local/Federal Task Forces?

Answer - Special Agents in San Juan, are assigned to, or assisting the following task forces; USSS San Juan Resident Office Electronic and Financial Crimes Task Force - created by USSS and include members of the Puerto Rico Police Department, Financial Mortgage Strike Force – created by the AUSA's Office District of Puerto Rico, High Intensity Drug Trafficking Areas program, Joint Terrorism Task Force, SAR Review Team - created by the AUSA's Office District of Puerto Rico and the IRS, Puerto Rico Bank Association, Dominican Republic Bank Association and CARICOM - Association of Chief Commissioners of the Caribbean Islands (focused on crime trend in the Caribbean).