STATEMENT OF MR. KENNETH JENKINS

Special Agent In Charge

Criminal Investigative Division

United States Secret Service

Before the Subcommittee on Domestic Monetary Policy and Technology

Committee on Financial Services

U.S. House of Representatives

July 20, 2010

Good afternoon, Chairman Watt, Ranking Member Paul and distinguished members of the Subcommittee. I would like to thank you for providing the U.S. Secret Service (Secret Service) an opportunity to discuss U.S. currency issues.

While the Secret Service is perhaps best known for protecting our nation's leaders, we were established in 1865 to investigate and prevent the counterfeiting of United States currency. As the original guardian of the nation's financial payment system, the Secret Service has a long history of protecting American consumers, industries, and financial institutions from fraud. Congress continues to recognize the Secret Service's 145 years of investigative expertise in financial crimes and over the last two decades has expanded our statutory authorities to include access device fraud (18 USC §1029), which includes credit and debit card fraud. Congress has also given the Secret Service concurrent jurisdiction with other law enforcement agencies for identity theft (18 USC §1028), computer fraud (18 USC §1030), and bank fraud (18 USC §1344). We take our mission to combat these crimes seriously and as a result, the Secret Service is recognized worldwide for our investigative expertise and innovative approaches to detecting, investigating, and preventing financial crimes.

As you are aware, the Secret Service officially became a part of the Department of Homeland Security in March of 2003. Though our agency is no longer a component of the Department of the Treasury, we continue to maintain our historic ties and a robust partnership in the safeguarding of our currency and other payment systems. The Secret Service strongly believes that economic security is a central element of homeland security; therefore, the safeguarding of our financial infrastructure and monetary framework continues to be a paramount objective of our investigative efforts.

New Federal Reserve Notes

Rapid and continual technological advancements have enabled criminals to more easily conduct and expand a variety of crimes. These advancements mean counterfeit currency and other obligations can be reproduced quickly and efficiently. Today's criminals need relatively little knowledge or specialized training to print counterfeit currency or other financial obligations. A counterfeiter or criminal organization can utilize equipment ranging from inexpensive digital

devices such as scanners, computers, printers and multi-function devices, to large commercial presses, to flood a region with counterfeit currency.

The Secret Service is aggressively combating the production and circulation of counterfeit currency on several fronts. With our partners in the Department of the Treasury and the Federal Reserve, we are continuing with the redesign of our currency. As a member of the Advanced Counterfeit Deterrence Steering Committee (ACD) and the Interagency Currency Design Committee (ICD), we have an active role in the research, design, and introduction of new currency. The Secret Service continually evaluates the methods currently employed by counterfeiters and studies cutting-edge anti-counterfeiting technologies to enhance future redesigns of U.S. currency. This partnership was highlighted on April 21, 2010, with the unveiling of the redesigned $100 Federal Reserve Note. The new design for the $100 note not only retains the effective security features from the previous design but also contains two new security features: the 3-D Security Ribbon and the Bell in the Inkwell. The 3-D Security Ribbon is woven into the paper and shifts from *100s* to *bells* depending on how you tilt the paper. The Bell in the Inkwell feature includes a color-shifting bell in a copper inkwell. The bell changes from copper to green, an effect which makes the bell seem to appear and disappear within the inkwell. These advanced security features will hinder potential counterfeiters from producing high-quality notes that can deceive consumers and merchants.

Trends in Counterfeiting

Due to the dollar's value and widespread use overseas, it continues to be a target for transnational counterfeit activity. Of the approximately $908 billion dollars of genuine U.S. currency in circulation, roughly two-thirds of that amount circulates outside of our borders.

Despite our considerable success in reducing the amount of U.S. counterfeit currency in circulation, 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, as not all nations report that information, the Secret Service received approximately $69 million in counterfeit that was passed to the American public in FY 2009 alone—a combination of money the Secret Service has seized within the United States that has been passed to the public, as well as money that has been processed through the Federal Reserve system. 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.

Currently, more than 38 percent of all counterfeit currency passed domestically was printed outside of the United States using traditional printing techniques, predominately offset printing. The rest of the counterfeit currency passed domestically last year was produced within the United States by individuals using digital technology such as computers, scanners, printers, and multi-function devices. The most commonly passed counterfeit note domestically is the $20, whereas the most commonly passed note overseas is the $100.

The Secret Service has also observed that counterfeit notes produced on "bleached" paper are both a domestic and international concern. The "bleaching" process consists of the counterfeiter taking a lower denomination genuine U.S. note, usually a $5 bill, and removing the printed ink through a labor-intensive process commonly referred to as "bleaching." This "bleaching" process creates a blank note of genuine U.S. currency paper that retains many of its "distinctive counterfeit deterrents" and is, of course, made of the "distinctive paper" adopted by the Treasury Department. The counterfeiter then transfers an image of a higher denomination U.S. note, usually from a $100 bill, onto the "bleached" genuine paper. Domestic counterfeiters, as well as counterfeiting operations based in Colombia, Nigeria, and Italy have all produced significant quantities of counterfeit notes that were printed on "bleached" genuine U.S. currency notes. Counterfeiters have also targeted foreign currency, using "bleached" Venezuelan and Iraqi currencies to produce counterfeit U.S. $100 bills.

Counterfeit currency also continues to be associated with organized crime and drug trafficking. In one example, in October 2009, the U.S. Drug Enforcement Administration's Organized Crime Drug Enforcement Strike Force (OCDESF), located in New York, New York, contacted the Secret Service's New York Field Office with information concerning counterfeit currency. An OCDESF investigation had yielded reliable information that counterfeit Federal Reserve Notes (FRNs), would be accompanying a shipment of illegal narcotics, expected to arrive via commercial aircraft from Cali, Colombia. Working with the Colombian National Police and a confidential source, OCDESF and Secret Service agents were able to arrest the suspect with a suitcase containing illegal narcotics and a laptop computer bag containing over $150,000 in counterfeit FRNs concealed in the liner and charge him in U.S. District Court, Eastern District of New York.

Counterfeit Suppression

Today, the Secret Service continues to target strategic locations throughout the world where significant counterfeiting activity is detected through joint task forces with foreign law enforcement partners. Our investigative history has shown that the effective suppression of counterfeiting operations requires a close partnership between our domestic and international field offices and their law enforcement counterparts, as well as an immediate response by the law enforcement community.

The Secret Service's permanent presence overseas has been pivotal in establishing the partnerships necessary to successfully suppress foreign-based counterfeiting operations. For example, Project Colombia is a continuation of the Secret Service's efforts to establish and support Vetted Anti-Counterfeiting Forces (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.

In one instance in early 2009, agents from the Bogota Resident Office and officials with the Colombian National Police and the VACF contacted our Madrid Resident Office regarding a counterfeit suspect. Through extensive collaboration between the Secret Service, the VACF, and

the Spanish National Police (SNP), the SNP intercepted a package originating from Colombia, which contained negatives bearing images of counterfeit FRNs. Then, in January 2010, the SNP conducted a search warrant at one suspect's residence and seized $1.3 million in counterfeit U.S. currency, an offset printing press, two computers, photo negatives bearing the image of FRNs, and other items consistent with producing counterfeit currency. Ultimately, five Spanish suspects were charged by the Spanish National Police with violations of fraud and negotiating counterfeit instruments.

Our investigative successes in Colombia have forced these criminal elements to relocate 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 Peruvian Counterfeit Task Force (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 one of the 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. FRNs 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, 11 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 given that 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.

Partnerships

In addition to the increasing complexity of financial and electronic crimes, the Secret Service must contend with the fact that these types of crimes transcend national borders more fluidly than ever before. As a result, our counterfeit and cyber crime investigations require seamless coordination between Secret Service domestic and international field offices, headquarters, and our law enforcement partners throughout the world.

Currently, the Secret Service operates a network of 142 domestic and 22 international investigative field offices across 18 countries, to carry out its investigative and protective responsibilities. By working closely with other federal, state, and local law enforcement

representatives, as well as with international law enforcement officials, the Secret Service is able to establish comprehensive networks of information and resource sharing. The technical expertise and the comprehensive networks of information and resource sharing bridge jurisdictional boundaries. This partnership approach to law enforcement is vital in order for the Secret Service to fulfill its dual mission of protection and investigations. Such communication and cooperation is the blueprint we have successfully developed over the course of many decades of experience.

Electronic Crime and Cyber Investigations

Through our work in the area of financial crime, the Secret Service has developed a particular expertise in the investigation of 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, which 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 information such as the card holder's full name and address, mother's maiden name, date of birth, Social Security number, a PIN, and other personal information that allows additional criminal exploitation of the affected individual.

The increasing level of collaboration among cyber-criminals makes these cases more difficult to investigate and also increases the 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 marketplaces 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.

One of the Secret Service's major investigations into a network intrusion was initiated in January 2009. 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, stealing credit card and debit card data.

Various investigative methods, including search warrants, Mutual Legal Assistance Treaties, pen traps, and subpoenas, were used to identify three main suspects of this international group. On March 26, 2010, one of the suspects, Albert Gonzalez, was sentenced to 20 years in prison for his role in the Heartland, Hannaford's, and 7-11 intrusions and two unnamed co-conspirators were indicted for their role in this investigation. Efforts to locate them are ongoing.

Collaboration and Training

To illustrate the innovative approach to meeting increased investigative demands and collaborate with our law enforcement partners, the Secret Service, in partnership with others in the Department of Homeland Security, developed the National Computer Forensics Institute (NCFI) in Hoover, Alabama. NCFI is a cyber crimes training facility designed to provide state and local law enforcement officers with critical expertise in computer forensics and digital evidence analysis. By the end of 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. These individuals will now be available to serve as a force multiplier and assist the Secret Service with investigations as necessary.

The Secret Service also maintains an ongoing, robust relationship with the International Law Enforcement Academy (ILEA), which has locations in Budapest, Hungary; Bangkok, Thailand; San Salvador, El Salvador and Gabarone, Botswana. The Secret Service's work with ILEA provides a critical opportunity to forge new relationships with international law enforcement partners and share its expertise in combating counterfeiting, financial crimes and cyber crimes. Providing this training to foreign law enforcement partners has allowed the Secret Service to expand its investigative footprint in countries where these types of crimes are proliferating at an alarming rate. In FY2009, the Secret Service, in conjunction with ILEA, trained more than 900 foreign police officers from more than 70 countries.

Additionally, the Secret Service continues our public education and training in an effort to prevent and suppress the manufacturing, distribution and sale of counterfeit U.S. currency domestically and abroad. Secret Service personnel continuously conduct training seminars on topics such as financial crimes and computer forensics in an effort to augment the Secret Service's mission.

Conclusion

In closing, I would like to express my appreciation for the support that Congress 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 highest leaders, visiting heads of state and government, and designated National Special Security Events.

The Secret Service, in concert with its 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 and 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.

Chairman Watt, Ranking Member Paul and distinguished members of the Subcommittee, this concludes my prepared remarks. I would be pleased to answer any questions that you may have.