Statement of John R. Large
Special Agent in Charge
Criminal Investigative Division
Office of Investigations
U. S. Secret Service

Before the

House Committee on the Judiciary
Subcommittee on Crime, Terrorism and Homeland Security
U.S. House of Representatives

Hearing on
"Combating Organized Retail Crime – The Role of Federal Law Enforcement"

November 5, 2009

Good morning, Chairman Scott, Ranking Member Gohmert and distinguished members of the Subcommittee. Thank you for the opportunity to testify today on the investigative responsibilities of the United States Secret Service (Secret Service).

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

To accomplish its investigative mission, the Secret Service operates 142 domestic offices (including domicile offices) and 22 foreign offices in 18 countries. The agency works closely with other federal, state, and local law enforcement, as well as other U.S. government agencies and foreign counterparts to maximize its efforts.

Financial Fraud and Electronic Crimes

In recent years, the combination of the information revolution and the effects of globalization have caused the investigative mission of the Secret Service to evolve. Through our work in the areas of financial and electronic crime, the Secret Service has developed particular expertise in the investigation of identity theft, false identification fraud, credit card fraud, debit card fraud, check fraud, bank fraud, and cyber crime, including computer intrusions. In Fiscal Year 2008, agents assigned to Secret Service offices across the United States arrested over 5,600 suspects for financial crimes violations. These suspects were responsible for approximately $442 million in actual fraud loss to individuals and financial institutions.

The Secret Service continues to observe 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, 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).

In the 1980s and 1990s, criminals obtained stolen personal and financial information through traditional means, such as theft of mail, theft of trash from businesses or victims, home and vehicle burglaries, and theft of a victim's wallet or purse. While these low-tech methods of theft remain popular, criminal activity has also evolved so that criminals now employ newer, more high-tech methods for obtaining large quantities of stolen information.

Recent trends observed by law enforcement show that today's criminals continue to seek to compromise victims' personal and financial information through the use of computers and the Internet to launch cyber attacks targeting citizens and financial institutions. Cyber criminals have become adept at stealing victims' personal information through phishing emails, account takeovers, malicious software, hacking attacks, and network intrusions resulting in data breaches.

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, and the subsequent exploitation of this data. A considerable portion of this type of electronic theft appears to be attributable to organized cyber groups, many of them based abroad, which pursue both the intrusions and the subsequent exploitation of the stolen data. Stolen credit card information is often trafficked in units that include more than just the card number and expiration date. These "full-info cards" include additional information, such as the card holder's full name and address, mother's maiden name, date of birth, Social Security number, a PIN, and other personal information that allows additional criminal exploitation of the affected individual.

Another rising trend is the increase in volume of trafficking "card track data" together with PINs. This data allows a criminal to manufacture a fully functional counterfeit credit or debit card and execute ATM withdrawals or other PIN-enabled transactions against an account.

The increasing level of collaboration among cyber-criminals raises both the complexity of investigating these cases and the level of potential harm to companies and individuals alike. Illicit Internet carding portals allow criminals to traffic stolen information in bulk quantities globally. These portals, or "carding websites," operate like online bazaars where criminals converge to trade in personal financial data and cyber-tools of the trade. The websites vary in size, from a few dozen members to some of the more popular sites boasting memberships of approximately 8,000 users. Within these portals, there are separate forums moderated by notorious members of the carding community. Members meet online and discuss specific topics of interest. Criminal purveyors buy, sell, and trade malicious software, spamming services, credit, debit, and ATM card data, personal identification data, bank account information, hacking services and other contraband.

In addition to the exploitation of credit and debit card accounts, many of the more sophisticated online criminal networks are now actively exploiting compromised online financial accounts. Criminals who gain access to victim accounts using online systems then execute fraudulent electronic banking transfers or sell the information to other criminals. The desire to exploit online bank accounts has led to the explosive growth of phishing scams, as well as the recent wave of malicious software, also known as "malware" or "crimeware," which is specifically designed to harvest account login information from the computers of infected victims. The technical sophistication of the illicit services readily available continues to grow. For example, the online fraud networks are increasingly leveraging the technical capabilities of "botnets" (i.e. networks of thousands of infected computers which can be controlled by a criminal from a central location) for financial attacks ranging in nature from the hosting of phishing and other malicious websites to the launching of widespread attacks against the online authentication systems of U.S. financial institutions.

The information revolution of the 1990s has turned our personal and financial information into a valuable commodity, whether it is being collected and brokered by a legitimate company or stolen by an identity thief. This information is no longer only an instrument used to facilitate a financial crime; it is now the primary target of criminals. Today, many companies have access to or store customer's personal financial information. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals.

Globalization has made commerce easy and convenient for corporations and consumers – financial institutions and systems are readily accessible worldwide. Today's cyber-criminals have adapted to this new means of global trade and subsequently seek to exploit our dependence on information technology. With the explosion of Internet accessibility world-wide, criminals have modified their fraudulent schemes to a new, more anonymous and constantly evolving cyber arena. As a result, the Secret Service has modified its investigative techniques to keep pace with emerging technologies.

With this expansion of cyber crime, online auction houses have found themselves the victims or even the unwitting participants in organized criminal conspiracies. The Secret Service, while continuing to investigate financial crimes, has also opened criminal investigations into these organized cyber groups. The Secret Service has found these cases primarily evolve from access device fraud investigations, wherein, criminals who fraudulently purchase merchandise from traditional and online retailers and then resell the merchandise through online auction houses. In the recent past, the Secret Service, working closely with online auction houses, has successfully investigated and prosecuted several of these groups.

In May 2006, an internationally recognized telecommunications company contacted the Secret Service regarding the theft of approximately 20,000 cell phones from their plant in a major U.S. metropolitan area. The phones had left a warehouse in a shipment of five large pallets, and only two reached their final destination. The investigation led to employees of a nationally identified shipping company. The employees were interviewed regarding the missing shipments and eventually a manager of the shipping company confessed to running a stolen cell phone operation. The scheme involved cell phones that were sold to a re-seller at $75-$100 per phone, usually valued at $120-$150. Some of the phones were resold from a network of small collusive shops and some were sold at other venues, such as online auction houses. As a result of the investigation, the Secret Service recovered $1,549,000 of merchandise from a suspect's residence and all suspects in this case were arrested on federal charges for Aiding and Abetting, Conspiracy, and Access Device Fraud.

In October 2007, members of a Secret Service Electronic Crimes Task Force (ECTF), in cooperation with a District Attorney's Office, began an investigation into the criminal activities of an identified international currency transmittal service. The investigation revealed that suspects associated with this currency transmittal service recruited numerous individuals to sell fraudulently obtained merchandise over online auction houses. These proxy sellers advertised and took orders and/or bids for electronic merchandise at a significantly reduced price. Using stolen credit card information, the suspects purchased the ordered merchandise and then shipped it directly to the purchaser, or through another remailer. To date, the known fraud loss attributed to the group exceeds $4 million. Since the launch of the investigation, fourteen defendants have

been arrested and are now in the United States and one defendant is currently in custody overseas awaiting extradition to the United States.

In March 2008, the Secret Service was contacted by a credit card issuing bank regarding credit cards that were compromised at a local restaurant. Subsequent investigation revealed four suspects were using "skimmed" credit card numbers to purchase gift cards from nationally identified retail stores. Upon obtaining the gift cards, the subjects would purchase electronic merchandise and sell those items and other gift cards through various online auction houses. All suspects associated with this case were subsequently arrested on federal charges for Access Device Fraud, Aggravated Identity Theft, and Conspiracy.

Fostering Partnerships and Combining Resources

Criminal groups involved in financial crimes routinely operate in a multi-jurisdictional environment. By working closely with other federal, state, and local law enforcement representatives, as well as foreign 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 partnerships enabled the Secret Service to establish a national network of Financial Crimes Task Forces (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 37 FCTFs located in metropolitan regions across the country.

Further, in 1996, the Secret Service established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private sector, and local, state and federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. Congress has since directed the Secret Service in Public Law 107-56 to establish a nationwide network of ECTFs to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

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

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 on 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.

Additionally, the National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, the Department of Homeland Security (DHS), and the State of Alabama. The goal of this facility is to provide a national standard of training for a variety of electronic crimes investigations. The program offers state and local law enforcement officers, prosecutors, and judges the training necessary to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and conduct basic electronic crimes investigations.

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

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 school groups, 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.

The Secret Service currently participates in a joint effort with the Department of Justice, the U.S. Postal Inspection Service, the Federal Trade Commission (FTC), the International Association of Chiefs of Police (IACP), and the American Association of Motor Vehicle Administrators to host identity crime training for law enforcement officers. In the last four years, Identity Crime Training Seminars have been held in over 18 cities nationwide, with two more expected by the end of the year. These training seminars are focused on providing local and state law enforcement officers with tools and resources that they can immediately put into use in their identity crime investigations.

In addition, 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 aides pertaining to counterfeit currency detection.

Specific instructions pertaining to the seizure and analysis of electronic evidence should be provided to officers to ensure proper investigation and successful prosecution of cyber crime offenses. To provide this essential knowledge, the Secret Service published the "*Best Practices Guide for Seizing Electronic Evidence*." This pocket guide was designed for police officers and detectives acting as first responders and helps guide law enforcement officers in recognizing, protecting, seizing, and searching electronic devices in accordance with applicable statutes and policies. The guide continues to be updated, and it is currently issued in its third edition.

The Secret Service also has collaborated with several of our law enforcement and corporate partners to produce the interactive, computer-based training programs known as "*Forward Edge*" and "*Forward Edge II*." The *Forward Edge* series is a CD-ROM that provides law enforcement and corporate investigators with practical training in order to recognize and seize electronic storage items.

Finally, the Secret Service produced an Identity Crime Video/CD-ROM, which contains over 50 investigative and victim assistance resources that local and state law enforcement officers can use when combating identity crime. This CD-ROM also contains a short identity crime video that can be shown to law enforcement which discusses why identity crime is important, what other departments are doing to combat identity crime, and what tools and resources are available. The Identity Crime CD-ROM is an interactive resource guide that was made in collaboration with the U.S. Postal Inspection Service, the FTC and the IACP.

Conclusion

As I have highlighted in my statement, the Secret Service is committed to our mission of protecting the integrity of U.S. currency and safeguarding the nation's critical financial infrastructure and financial payment systems. Although the Service's core responsibilities remain the same, our methods of investigation have changed to keep pace with emerging technologies. Through successful partnership with public and private task force members, the Secret Service continues to adapt to the ever evolving cyber criminal environment. The Secret Service dedicates significant resources to aggressively investigate all offenses within our purview to protect consumers and financial institutions.

This concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.