Testimony of

Larry D. Johnson

Criminal Investigative Division
U.S. Secret Service
April 13, 2005

Statement of Mr. Larry Johnson

Special Agent in Charge
Criminal Investigative Division
United States Secret Service

Presentation to the Senate Committee on the Judiciary
United States Senate
April 13, 2005

Good afternoon, Chairman Specter. I would like to thank you, as well as the distinguished Ranking Member, Senator Leahy, and the other members of the Committee for providing an opportunity to discuss the subject of information security, and the role of the Secret Service in safeguarding our financial and critical infrastructures.

Background

In addition to providing the highest level of physical protection to our nation's leaders, the Secret Service exercises broad investigative jurisdiction over a wide variety of financial crimes. As the original guardian of our Nation's financial payment systems, the Secret Service has a long history of protecting American consumers and industry from financial fraud. With the passage of new federal laws in 1982 and 1984, the Secret Service was provided primary authority for the investigation of access device fraud, including credit and debit card fraud, and parallel authority with other law enforcement agencies in identity crime cases. In recent years, the combination of the information revolution, the effects of globalization and the rise of international terrorism have caused the investigative mission of the Secret Service to evolve dramatically. The explosive growth of these crimes has resulted in the evolution of the Secret Service into an agency that is recognized worldwide for its expertise in the investigation of all types of financial crimes. Our efforts to detect, investigate and prevent financial crimes are aggressive, innovative and comprehensive.

After 138 years in the Department of the Treasury, the Secret Service transferred to the Department of Homeland Security (DHS) in 2003 with all of our personnel, resources and investigative jurisdictions and responsibilities. Today, those jurisdictions and responsibilities require us to be involved in the investigation of traditional financial crimes as well as identity crimes and a wide range of electronic and high-tech crimes.

The expanding use of the Internet and the advancements in technology, coupled with increased investment and expansion, has intensified competition within the financial sector. With lower costs of information-processing, legitimate companies have found it profitable to specialize in data mining, data warehousing and information brokerage. Information collection has become a common by¬product of newly-emerging e commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by businesses seeking to find the best customers for their products. This has led to a new measure of growth within the direct marketing industry that promotes the buying and selling of personal information. In today's markets, consumers routinely provide personal and financial identifiers to companies engaged in business on the Internet. They may not realize that the information they provide in credit card applications, loan applications, or with merchants they patronize is a valuable commodity in this new age of information trading. Consumers may be even less aware of the illegitimate uses to which this information can be put. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders.

Legitimate business can provide a first line of defense against identity crime by safeguarding the information it collects and such efforts can significantly limit the opportunities for identity crime.

The methods of identity theft utilized by criminals vary. "Low tech" identity criminals obtain personal and financial identifiers by going through commercial and residential trash, a practice known as "dumpster diving." The theft of wallets, purses and mail is also a widespread practice employed by both individuals and organized groups.

With the proliferation of computers and increased use of the Internet, "high tech" identity criminals began to obtain information from company databases and web sites. In some cases, the information obtained is in the public domain, while in others it is proprietary and is obtained by means of a computer intrusion or by means of deception such as "web-spoofing" or "phishing".

The method that may be most difficult to prevent is theft by a collusive employee. Individuals or groups who wish to obtain personal or financial identifiers for a large-scale fraud ring will often pay or extort an employee who has access to this information through their employment at workplaces such as a utility billing center, financial institution, medical office, or government agency. The collusive employee will access the proprietary data base, copy or download the information, and remove it from the workplace either electronically or simply by walking it out.

Once the criminal has obtained the proprietary information, it can be exploited by creating false "breeder documents" such as a birth certificate or social security card. These documents are then used to obtain genuine, albeit false, identification such as a driver's license and passport. Now the criminal is ready to use the illegally obtained personal identification to apply for credit cards or consumer loans or to establish bank accounts, leading to the laundering of stolen or counterfeit checks or to a check-kiting scheme. Our own investigations have frequently involved the targeting of organized criminal groups that are engaged in financial crimes on both a national and international scale. Many of these groups are prolific in their use of stolen financial and personal identifiers to further their other criminal activity.

Agency Coordination

It has been our experience that the criminal groups involved in these types of crimes routinely operate in a multi¬-jurisdictional environment. This has created problems for local law enforcement agencies that generally act as the first responders to their criminal activities. By working closely with other federal, state, and local law enforcement, as well as international police agencies, we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries. This partnership approach to law enforcement is exemplified by our financial and electronic crime task forces located throughout the country. These task forces primarily target suspects and organized criminal enterprises engaged in financial and electronic criminal activity that fall within the investigative jurisdiction of the Secret Service.

Members of these task forces, including representatives from local and state law enforcement, prosecutors' offices, private industry and academia, pool their resources and expertise in a collaborative effort to detect and prevent electronic crimes. The value of this crime fighting and crime prevention model has been recognized by Congress, which authorized the Secret Service (pursuant to the USA PATRIOT Act of 2001) to expand our Electronic Crime Task Forces (ECTF) initiative to cities and regions across the country. Additional ECTFs have been added in the last two years in Dallas, Houston, Columbia (SC), Cleveland, Atlanta and Philadelphia, bringing the total number of such task forces to 15.

The Secret Service ECTF program bridges the gap between conventional cyber-crimes investigations and the larger picture of critical infrastructure protection. Secret Service efforts to combat cyber-based assaults that target information and communications systems supporting the financial sector are part of the larger and more comprehensive critical infrastructure protection and counterterrorism strategy.

As part of DHS, the Secret Service continues to be involved in a collaborative effort targeted at analyzing the potential for financial, identity and electronic crimes to be used in conjunction with terrorist activities. The Secret Service takes great pride in its investigative and preventive philosophy, which fully involves our partners in the private sector and academia and our colleagues at all levels of law enforcement, in combating the myriad types of financial

and electronic crimes. Central to our efforts in this arena are our liaison and information exchange relationships with the U.S. Immigration and Customs Enforcement (ICE), the Department of the Treasury, the Department of State, the Federal Bureau of Investigation and our Joint Terrorist Task Force participation.

The Secret Service is actively involved with a number of government-sponsored initiatives. At the request of the Attorney General, the Secret Service joined an interagency identity theft sub¬committee that was established by the Department of Justice (DOJ). This group, which is comprised of federal, state, and local law enforcement agencies, regulatory agencies, and professional organizations, meets regularly to discuss and coordinate investigative and prosecutorial strategies as well as consumer education programs.

In a joint effort with DOJ, the U.S. Postal Inspection Service, the Federal Trade Commission, the International Association of Chiefs of Police and the American Association of Motor Vehicle Administrators, we are hosting Identity Crime Training Seminars for law enforcement officers. In the last two years we have held seminars in eighteen cities nationwide including Denver, Colorado; Raleigh, North Carolina; Orlando, Florida; Rochester, New York; and Santa Fe, New Mexico. Identity Crime seminars scheduled for the upcoming months include Boise, Idaho; Providence, Rhode Island; and Baltimore, Maryland. These training seminars are focused on providing local and state law enforcement officers with tools and resources that they can immediately put to use in their investigations of identity crime. Additionally, officers are provided resources that they can pass on to members of their community who are victims of identity crime.

It is through our work in the areas of financial and electronic crime that we have developed particular expertise in the investigation of credit card fraud, identity theft, check fraud, cyber crime, false identification fraud, computer intrusions, bank fraud, and telecommunications fraud. Secret Service investigations typically focus on organized criminal groups, both domestic and transnational. As Secret Service investigations uncover activities of individuals or groups focusing on doing harm to the United States, appropriate contact is immediately made and information is passed to those agencies whose primary mission is counterterrorism.

Finally, the best example of interagency and multi-jurisdictional cooperation came on October 24, 2004, when the Secret Service arrested 30 individuals across the United States and abroad for credit card fraud, identity theft, computer fraud and conspiracy. These suspects were part of a multi-count indictment out of the District of New Jersey and were involved in a transnational cyber "organized crime" underground network that spanned around the world. In addition to the 30 arrests, 28 search warrants were served simultaneously across the United States. Internationally, 13 search warrants were served in 11 different countries in conjunction with this Secret Service-led investigation. Central to the success of this operation was the cooperation and assistance the Secret Service received from local, State and other federal law enforcement agencies as well as our foreign law enforcement partners and Europol.

This case began in July of 2003, when the Secret Service initiated an investigation involving global credit card fraud and identity fraud. Although the catalyst for the case came from a more "traditional" crime of access device fraud, the case evolved into a very technical, transnational investigation. The aforementioned criminal activity primarily occurred over the Internet. After the initial act(s) of fraud, suspects would exchange contraband (such as counterfeit credit cards and counterfeit driver's licenses). This case, entitled Operation Firewall, developed into a multilateral effort involving 18 Secret Service domestic offices and 11 foreign countries. As the lead investigative office, the Secret Service Newark Field Office conducted a complex undercover operation involving the first ever wiretap on a computer network.

Chairman Specter and Senator Leahy, 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.