Department of Justice

STATEMENT OF

JASON M. WEINSTEIN
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND
NATIONAL ARCHIVES

HEARING ENTITLED

"IDENTITY THEFT: A VICTIMS BILL OF RIGHTS"

PRESENTED

JUNE 17, 2009

Good afternoon, Chairman Clay and Ranking Member McHenry. It is a pleasure to appear before you to testify about the Department of Justice's commitment to the critical goal of investigating and prosecuting of identity theft crimes.

As you know, identity theft is not a new problem. But it is one that continues to evolve as criminals develop more sophisticated and diverse methods to access and exploit the personal information of others. As criminals capitalize on the new opportunities and data made available through networks and the Internet, the Department of Justice (the Department) continues to adapt so that we can fully address these new developments. Reflecting this trend, there are currently over 2,000 active cases related to identity theft pending in the U.S. Attorney's Offices (USAOs), and there has been a 138.2 percent increase in identity theft convictions by USAOs between Fiscal Year (FY) 2004 and FY 2008.

The Department, through its Criminal Division, the Federal Bureau of Investigation (FBI), the USAOs, and other components, along with our other law enforcement partners, has been aggressively investigating and prosecuting crimes that facilitate or constitute identity theft. Today I will highlight some of the Department's historical successes in the prosecution of individuals and organizations involved in the theft and trafficking of personal and financial information, as well as some of our ongoing efforts to tackle this growing problem. Given the short time we have today, this summary cannot capture all of the important work being done by the Department's prosecutors at Main Justice and in USAOs around the country. I hope, however, that it can provide you with a clear picture of some of our efforts to combat identity theft, and a better idea of how they have resulted in some of the most important prosecutions brought over the past few years.

Before getting into specific cases, I will discuss how identity theft has evolved in recent years and the challenges that this evolution poses to the Department and its law enforcement partners. We consistently look for ways to meet these challenges and ensure our continued success. But we recognize that as always, we can and must do more. To that end, it is critical to our success that we build upon and improve the existing coordination mechanisms we have with our international partners and the private sector, and that we explore potential enhancements to the identity theft-related laws. We are very glad to have this opportunity to discuss these issues in particular with you.

I. THE COST OF IDENTITY THEFT

Each year, millions of Americans suffer the costs of identity theft. By one estimate, identity theft became the fastest growing crime in 2008, affecting approximately 10 million Americans – a 25 percent increase over the 8 million reported victims in 2005.[1] This crime "exacts a serious toll on the American public," with annual monetary losses "in the billions of

[1] Senator Patrick Leahy, Statement On Passage Of The Former Vice President Protection Act of 2008, H.R. 5938 (September 15, 2008)

dollars," as recognized in the 2007 Strategic Plan of the President's Identity Theft Task Force.[2] It also, however, imposes other significant costs that extend well beyond the direct financial losses to individual victims. Take as an example an instance in which corporate insiders are compromised or corporate databases are breached to obtain individual personal or financial information in a manner that constitutes identity theft. In such a case, not only do the affected individuals suffer the monetary losses they incur as a result, but the affected businesses must bear the indirect costs of fraud prevention and mitigation of the harm, including potentially significant reputational harm.

Similarly, individual victims may suffer additional indirect costs, including not only financial costs related to potential civil litigation by creditors and the obstacles that can arise in obtaining or retaining credit, but also the substantial time required to repair the damage that the identity thieves caused, such as correcting fraudulent information in credit reports, closing existing bank accounts and opening new ones, and disputing charges with creditors. Furthermore, many identity theft victims report that they must endure the uncertainty of whether and how an identity thief will cause new problems for them. As one victim put it, in connection with the sentencing of an identity thief,

> I am constantly wondering when I will be attacked again. I have no way of knowing who else [the defendant] has distributed my personal information to . . . . It would have been better to have been mugged at gunpoint, since at least then I would have my peace of mind knowing that it was a one-time event.[3]

Many of the identity theft cases that the Department has prosecuted demonstrate that even a single criminal can cause extensive harm to individual victims. In a prosecution by the USAO for the Middle District of Tennessee, for example, one defendant victimized over 100 people, repeatedly using the stolen identities of minor children, the homeless and others to place multiple fraudulent loans on the same property without the knowledge or consent of the true owners. He was ultimately required to pay $5.9 million in restitution and sentenced to 26 years and four months in prison.

II. THE EVOLUTION OF IDENTITY THEFT

As I have already alluded to, two related phenomena have been driving the recent explosion in identity theft. First, both individuals and businesses heavily rely on computers and information technology to store, process, and share confidential personal information. The modern provision of financial services and health care – just to name two examples – would be largely unthinkable without the electronic storage and processing of information. Similarly, individuals engage in a myriad of daily activities that make use of information technology, including online banking, shopping, and email. As a result, there is an increasingly vast amount of confidential personal information routinely stored and shared on computer systems.

---

[2] PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN at 11 (April 2007), *available at* http://www.idtheft.gov/.

[3] *See* United States Attorney's Office, Western District of Washington, Press Release (May 4, 2007), *available at* http://seattle.fbi.gov/dojpressrel/2007/pr050407.htm.

Second, various criminal groups in the United States and abroad recognize how valuable personal confidential information is and explore new ways to gain access to large volumes of such information to make substantial profits from its fraudulent sale. Criminals often use a wide variety of low-tech means of unlawfully acquiring individuals' personal data, ranging from mail theft to compromise of insiders at financial institutions and companies. They also have become adept at exploiting advances in information technology to hack into the computers that store this information. Cybercrime – once the province of the lone hacker – is now big business. It involves large-scale data breaches and the sale of personal confidential information, particularly personal financial information, including credit card and bank account numbers. In fact, large-scale data breaches present one of the most challenging developments in the identity theft problem. Additionally, techniques such as "phishing," the use of fraudulent email and websites to deceive Internet users into disclosing their personal data, and carding, the online trafficking in stolen or fraudulently obtained personal data, are also routinely used by criminals involved in identity theft.

The Internet provides a unique venue through which "carders" can obtain sellable information, advertise and sell stolen data to the highest bidder, and self-organize to facilitate their activities. For example, carders often become members of website forums designed to provide an active marketplace for the sale of, among other contraband, stolen credit and debit card numbers; compromised personally-identifiable information, including an individual's address, phone number, social security number, personal identification numbers (PINs), credit history report, and mother's maiden name; and false identification documents. And once stolen identity information is sold, the purchasers frequently engage in a wide array of fraudulent activity. For example, in recent years, criminal carding organizations engaged in what is known as "PIN cashing" have developed sophisticated networks in which stolen financial information is immediately disseminated to designated groups of criminals who withdraw money from ATMs all over the world within a short time period. In one example, PIN cashers made 9,000 withdrawals worldwide totaling $10 million in less than 48 hours from four compromised prepaid debit card accounts.

Hackers steal information from public and private institutions – everything from large corporate databases to residential wireless networks – using sophisticated tools to penetrate firewalls and automated processes to search for account data or other personal information, export the data, and hide their tracks. Hackers also employ malicious software – such as spyware and keystroke loggers – to collect information from infected computers and send that information back to an identity thief so that it can be sold. Indeed, the marriage of large-scale data-breaches and organized cyber crime represents the latest and most challenging evolution of identity theft. The use of sophisticated, high-tech measures by organized criminal networks represents a significant challenge to the investigation and prosecution of these crimes.

III. THE DEPARTMENT'S RESPONSE TO THE THREAT OF IDENTITY THEFT

Targeting identity theft is an important priority for the Department. In recent years, the Department has aggressively prosecuted a wide variety of identity theft schemes throughout the country, including those involving data breaches and carding. Within the Criminal Division, the

Computer Crime and Intellectual Property Section (CCIPS) investigates and prosecutes these large-scale data breaches and coordinates prosecutions that involve multiple USAOs and foreign countries, the Fraud Section investigates and prosecutes significant fraud cases that involve identity theft, such as healthcare fraud, financial institution fraud, and securities fraud, and the Organized Crime and Racketeering Section partners with these Sections and USAOs to lend its expertise in dismantling the criminal organization. Throughout the country, our USAOs actively investigate and prosecute cases involving data breaches and identity theft.

On the international front, the Office of International Affairs in the Criminal Division supports international cooperation efforts by implementing mutual legal assistance treaties (MLATs) and international conventions that have yielded significant evidence for use in US and foreign prosecutions and by marshaling efforts to extradite international fugitives.

Finally, to facilitate information-sharing and coordination among USAOs and federal agencies in identity-theft matters, the Department also chairs several interagency working groups, such as the Identity Theft Enforcement Interagency Working Group and the recently-established Payments Fraud Working Group, which it co-chairs with the Board of Governors of the Federal Reserve System. The Department also helped to lead the Identity Theft Task Force, which also addressed many of these issues.

The combined force of all of these efforts, along with the efforts of the FBI and the Department's other law enforcement partners, has resulted in a number of benchmark prosecutions that highlight the range of the Department's efforts to address the growing problem of identity theft, and in particular, that facilitated by large-scale data breaches.

A. "OPERATION FIREWALL"

Much of the Department's successful investigative work targeting carding has its roots in the Department's earliest efforts to dismantle highly-organized carding enterprises. As just one example, in 2004, as part of an undercover investigation known as Operation Firewall, the Department and the U.S. Secret Service (USSS) coordinated the search and arrest of more than 28 members of the "Shadowcrew" criminal organization, located in eight states in the United States and six foreign countries. This operation required significant international cooperation among the law enforcement agencies of the United Kingdom, Canada, Bulgaria, Belarus, Poland, Sweden, the Netherlands, and Ukraine. Members of the group were later charged in a 62-count indictment with trafficking in at least 1.5 million stolen credit and bank card numbers that resulted in losses in excess of $4 million. As part of this takedown, the USSS disabled the Shadowcrew website. We believe that had the organization not been interrupted, there might have been hundreds of millions of dollars in additional losses. Instead, the Shadowcrew criminal organization's activity stopped, and to date, with the exception of two fugitives, all of the domestic Shadowcrew defendants have pleaded guilty and received sentences of up to 90 months in prison.

B. RECENT SUCCESSES

Building upon these early efforts, in recent years, the Department has had increasing success combating identity theft through the investigation and prosecution of carders and large-scale data breaches, including:

- **Dark Market carding forum.** In late 2008, the FBI announced the results of a two-year undercover operation, conducted in conjunction with CCIPS, targeting members of the online carding forum known as Dark Market. At its peak, the Dark Market website had over 2,500 registered members around the world. This operation resulted in 56 arrests worldwide and prevented an estimated $70 million in economic loss.

- **International hacking ring.** In August 2008, the Department and USSS announced the largest hacking and identity theft case ever prosecuted, in which charges were brought in three districts against 11 members of an international hacking ring, including Maksym Yastremskiy, known online as "Maksik" and believed to be one of the top traffickers in stolen account information, with alleged sales of hundreds of thousands of credit and debit card numbers. The various defendants – who were from the United States, Estonia, Ukraine, the People's Republic of China, and Belarus – were charged with, among other things, the theft and sale of more than 40 million credit and debit card numbers obtained from various retailers including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21, Dave & Buster's, and DSW.

- **Operation CardKeeper** – Operation CardKeeper, led by the FBI and the USAO for the Eastern District of Virginia, resulted in the arrests of thirteen individuals in Poland and eight in the United States after significant international cooperation. Operation CardKeeper also resulted in the U.S. conviction of an individual known online as "John Dillinger," who was sentenced in 2007 to 94 months in federal prison for his carding activity, including aggravated identity theft, among other things. Computers seized from him revealed more than 4,300 compromised account numbers and full identity information for over 1,600 individual victims.

- **"Iceman."** In late 2007, a major supplier of tens of thousands of credit card accounts to carding forums was indicted for wire fraud and identity fraud. Max Ray Butler, known online as "Iceman," was the co-founder and administrator of the carding forum Cardersmarket. He is currently awaiting trial.

C. INTERNATIONAL LAW ENFORCEMENT COOPERATION

As these cases illustrate, identity thieves and cybercriminals responsible for many of these large scale data-breaches live in and operate from foreign jurisdictions. In certain cases, hackers both in the United States and abroad route communications through computers located in so-called "hacker havens." In other cases, the hackers themselves operate in foreign countries that law enforcement consider to be "hacker havens." They do this to exploit the many hurdles faced by law enforcement in investigating transnational crimes. The Department continues to

cooperate with foreign law enforcement in prosecuting individuals in the United States. Although the Department's principal law enforcement mission is prosecuting individuals in the United States, the Department also recognizes that an important tool in combating identity theft and cybercrime involves assisting foreign law enforcement in bringing successful prosecutions in their own countries. A number of recent investigations begun in the U.S. have resulted in successful prosecutions in foreign countries long considered to be so-called "hacker havens." For example, based on close cooperation between the Department, the FBI, and the Romanian National Police Cybercrime Divisions, prosecutors from that country's Directorate for Investigating Organized Crime and Terrorism arrested eleven Romanian citizens on fraud and identity theft charges in November 2007. They were part of a criminal organization that specialized in "phishing" information from computer users, imprinting credit and debit card information onto counterfeit cards, and then using those cards to obtain cash from ATMs and Western Union locations. Romanian police officers executed 21 search warrants and seized computers, card reading and writing devices, blank cards, and other equipment. More recently, between February 2008 and March 2009, over 40 defendants were charged in Romania – along with 12 in the United States – for their participation in a sophisticated hacking scheme involving the theft of corporate bank account information, and the use of that stolen information in a variety of fraudulent transactions.

Because of the global nature of the Internet and the identity theft-related crimes it can facilitate, close coordination and cooperation with foreign law enforcement is vital to the success of identity theft investigations and prosecutions. To that end, the Department serves as the United States point of contact in the G-8 24/7 High Tech Crime Points of Contact network, which consists of more than 50 countries available around the clock to assist other members with high tech issues in criminal cases. The Identity Theft Task Force's Strategic Plan recommended that the Department and other departments and agencies take additional steps to improve coordination and evidence sharing with foreign law enforcement agencies. International cooperation in the arrest and prosecution of cybercrime and identity theft is also a central part of the Department's new strategy to combat international organized crime (IOC), announced in 2008. The Department's strategy recognizes the threat that international organized cyber crime poses to the security and stability of the U.S. economy, particularly to the security of personal financial information and the stability of business, financial and government infrastructures. As set forth in the document announcing the IOC Strategy, "[t]o effectively carry-out cross cutting operations to disrupt and dismantle IOC groups, U.S. law enforcement must capitalize on established relationships with vetted foreign officials and build international partnerships to collaborate in the domestic and foreign prosecution of IOC cases."[4]

We believe that on this front, the United States should continue to press other nations to accede to the Convention on Cybercrime (2001), which will improve cooperation between law enforcement agencies. The Convention, which the U.S. ratified in 2006, assures that other countries enact suitable domestic legislation criminalizing identity theft, in part to facilitate information-sharing under mutual legal assistance treaties and the extradition of criminal defendants.

[4] U.S. Department of Justice, Overview of the Law Enforcement Strategy to Combat International Organized Crime (April 2008), available at http://www.usdoj.gov/ag/speeches/2008/ioc-strategy-public-overview.pdf.

In addition, the United States should continue to work closely with multilateral organizations to urge other countries to review their criminal codes and criminalize identity-related criminal activities where appropriate. The Department has had substantial success in carrying out this recommendation. The Department also has been an active participant since 2008 in the United Nations Office on Drugs and Crime's Core Group of Experts on Identity-Related Crime, which has encouraged efforts to have countries examine their domestic criminal codes and identify areas in which those codes can be revised to address all aspects of identity theft appropriately. Most recently, at the April 2009 meeting of the United Nations Crime Commission, the Department played a substantial role in the drafting and approval of a resolution (for adoption by the United Nations Economic and Social Council later this year) that encourages United Nations Member States to combat fraud and identity theft by ensuring adequate investigative powers and, where appropriate, by reviewing and updating the relevant laws.[5] The Identity Theft Task Force's Strategic Plan also directs the U.S. government to identify countries that are safe havens for identity thieves and to use appropriate diplomatic and enforcement mechanisms to encourage those countries to change their practices. The Department has begun this process, gathering information from a range of law enforcement authorities. The G-8 Roma/Lyon group has also worked to improve international response to identity theft and cybersecurity. In May 2009, the Justice and Interior Ministers of the G-8 met to discuss these issues, among others. The Ministers committed to strengthen international cooperation to combat this type of crime, including continued and improved cooperation with the private sector, increased training, and practical information exchanges on effective law enforcement practices in the field. Additionally, in February 2009, the G-8 Roma/Lyon Group approved for further dissemination a paper that examines the criminal misuse of identification information and identification documents within the G-8 States and proposes "essential elements" of criminal legislation to address identity-related crime. The Department played a substantial role in drafting this paper and in urging its approval by the Roma/Lyon Group.

Finally, law enforcement cooperation can be hampered by our inability, in certain cases, to assist foreign law enforcement agencies. Only by providing assistance to other countries can we expect them to provide critical evidence for our own investigations. Appendix D of the Strategic Plan contained a legislative proposal that would clarify our courts' authority to compel disclosure of evidence to assist foreign law enforcement investigations.

D. ASSISTANCE TO IDENTITY THEFT VICTIMS

Beyond addressing the threat through prosecution, the Department also works in coordination with other agencies to aid the victims of identity theft. DOJ's Office for Victims of Crime has provided substantial grants to organizations at the national, regional, state, and city level for programs that provide direct assistance to identity theft victims. The grant recipients are the Identity Theft Resource Center, one of the panel members who will be testifying before this subcommittee, the Victims' Initiative for Counseling, Advocacy, and Restoration of the Southwest, the Maryland Crime Victims' Resource Center, Inc., and Atlanta Victim Assistance. Each of these grantees have developed resources, projects, and protocols that can serve as models for other victim assistance programs.

---

[5] *See* United Nations Economic and Social Council, Document No. E/CN.15/2009/L.2/Rev.1 (April 23, 2009), *available at* http://daccessdds.un.org/doc/UNDOC/LTD/V09/829/09/PDF/V0982909.pdf?OpenElement.

A variety of state and federal programs, as well as non-profit organizations, provide direct assistance to identity theft victims. The Task Force recommended that member agencies develop nationwide victim assistance training for counselors at these programs. Accordingly, DOJ's Office for Victims of Crime (OVC) conducted a national training session, developed in cooperation with the FTC, for victim-witness coordinators in 2007. To increase identity theft victim assistance services, OVC has encouraged Victims of Crime Act (VOCA) victim assistance administrators to expand their program outreach to identity theft victims. OVC also has highlighted identity theft and fraud issues at the VOCA Administrators' Annual Conferences by supporting victim impact workshops to help recognize the needs of identity theft victims and expand program services using VOCA victim assistance dollars. Through these efforts, the Department has helped alleviate some of the difficulties faced by identity theft victims and has assisted them in recovering from the damage caused by identity theft.

IV. STRENGTHENING IDENTITY THEFT LAWS

A. SENTENCING ENHANCEMENTS

In addition to legislation that would improve our ability to cooperate with our international law enforcement partners, the Department believes that there are ways to improve the identity theft laws. Congress should strengthen the penalties for stealing identity information and other related cybercrimes. This could be accomplished both by amending the sentencing provisions of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) and by altering the way in which the U.S. Sentencing Guidelines treat these offenses. At the direction of Congress, the Sentencing Commission recently completed a review of this issue, but their proposed amendments to the Guidelines are minor and do not adequately take into account the scope of the problem or Congress' directive to the Commission. We would be happy to work with Congress to develop a more appropriate sentencing scheme that will deter identity thieves and provide for just punishment of offenders.

B. BREACH REPORTING

Immediate reporting of incidents to law enforcement is also vital to law enforcement's ability to investigate large-scale data breaches. Immediate reporting necessarily relies upon each potential victim company's capacity to promptly detect an incident, but we know from experience that prompt detection will not itself result in a report from the victim company. For a variety of reasons, data breaches are significantly underreported, and as a result, law enforcement efforts to bring criminals to justice are significantly hampered. If law enforcement never learns of the incident, we will not be able to investigate it; if we hear about it too late, we may be unable to preserve critical evidence or identify the perpetrators. On the other hand, several recent successes in tracking down the perpetrators of high-profile data breaches are the direct result of immediate information from victim companies on how the hackers entered and exited their systems, including the specific IP addresses used in the attack. For example, in the Dave & Buster's case, which was a part of the international hacking ring prosecuted in 2008, when Dave & Buster's became aware of intrusions, they took measures to log access to their computers,

block the intruder's further attempts to collect credit and debit card data, and identify for law enforcement the intruder's IP address. While companies like VISA require by policy that all entities that suspect or have confirmed that a security breach occurred must contact federal law enforcement, few laws require the victim company to notify law enforcement. In its April 2007 Strategic Plan, the Identity Theft Task Force recommended the establishment of a national standard requiring entities that maintain sensitive data to provide timely notice to law enforcement in the event of a breach. Because only a handful of state laws currently require reporting to law enforcement and because private sector rules are neither universal nor consistently enforced across the various companies, we urge Congress to consider requiring security breach reports to federal law enforcement using a mechanism that ensures that the USSS and FBI have access to the reports. Any legislation should contain provisions to ensure that breaches are reported to law enforcement prior to notifying individual victims, and to permit law enforcement to seek delayed notification, so that law enforcement has sufficient time to preserve evidence and investigative leads.

This concludes my remarks. I would be pleased to answer questions from you and other members of the Subcommittee.