Department of Justice

STATEMENT OF

RITA M. GLAVIN
ACTING ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

HOUSE OF REPRESENTATIVES
HOMELAND SECURITY COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE & TECHNOLOGY

AT A HEARING ENTITLED

"DO THE PAYMENT CARD INDUSTRY DATA STANDARDS REDUCE CYBERCRIME?"

PRESENTED

MARCH 31, 2009

Good morning, Chairwoman Clarke and Ranking Member Lungren. Thank you for your invitation to address the Committee. The Department of Justice welcomes this opportunity to testify about our commitment to combating large-scale data breaches and the payment card fraud that results from such breaches.

As you know, identity theft is not a new problem. However, in recent years, the Information Age has transformed the landscape in which criminals operate, making available a wide array of new methods that identity thieves can use to access and exploit the personal information of others. Criminals have capitalized on these new and far-ranging opportunities. Skilled hackers are now capable of perpetrating large-scale data breaches that leave hundreds of thousands – and in many cases, tens of millions – of individuals at risk of identity theft. Today's criminals now have the opportunity to remotely access the computer systems of government agencies, universities, merchants, financial institutions, credit card companies, and data processors, to steal large volumes of personal information, including individuals' financial information, made available simply by virtue of everyday acts like making credit and debit card retail transactions. 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% increase in identity theft convictions by USAOs between FY04 and FY08. The Department of Justice, through its Criminal Division, the Federal Bureau of Investigation (FBI), the USAOs, and other components, along with our partners at the U.S. Secret Service (USSS) and the U.S. Postal Inspection Service, has been aggressively investigating and prosecuting these data breaches and other criminal activity associated with them, and we are committed to continuing our efforts. Historically, the Department has had tremendous success in identifying, investigating, and prosecuting the perpetrators of these acts**.** But as always, we can and will do more. To that end, the continued and improved coordination with our partners in the international community and the private sector will be critical to ensuring our success, and we are glad to have this opportunity to discuss these issues in particular with you.

The "Carder" Threat

The Department has responsibility for the investigation and prosecution of a wide range of cyber crime cases, but large-scale breaches are of significant concern to us because their fallout can be amplified exponentially when criminals harness the power of the internet to quickly and widely distribute for future fraudulent use the vast quantities of information stolen during these breaches. For example, international organized crime is currently one of the fastest growing threats in the computer intrusion arena, and these groups – who are continuing to expand and become more sophisticated – along with hosts of other cyber criminals, have made large-scale data breaches one powerful part of their profile.

Through activity known as "carding," large volumes of data are stolen, resold, and ultimately used by criminals to commit fraud. In recent years, the problem of "carding" has grown. "Carding" means not only the unauthorized use of credit and debit card account information to fraudulently purchase goods and services, but also a growing

assortment of related activities including computer hacking, phishing, cashing out stolen account numbers, re-shipping schemes, and Internet auction fraud. I will describe some of these schemes in more detail in a moment.

The Internet provides a unique venue in which "carders" can 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.

Once stolen identity information is sold, the purchasers frequently engage in fraudulent activity including, among other things, the use of stolen credit card information to make purchases online and in person, and "cashing," which refers to the act of obtaining money – rather than retail goods and services – with the unauthorized use of stolen financial information. In recent years, criminal carding organizations engaged in what is known as "PIN cashing" have developed sophisticated "cash-out 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 $5 million in less than 48 hours from four compromised prepaid debit card accounts.

The Link Between Carding and Other Crimes

In addition to the financial fraud perpetrated by carders, the Department focuses on criminals who engage in carding activities with a motivation other than personal financial gain. We know, for example, that drug traffickers engage in identity theft for the purpose of financing their activities.

Similarly, there is a well-documented connection between identity theft – in particular as it relates to obtaining fraudulent identification documents, but also as it may relate to credit card fraud – and terrorism. As one example, a convicted terrorist in Indonesia, Imam Samudra, wrote about the use of credit card fraud and carding as a means to fund terrorist activities in his 280-page autobiography. Samudra sought to fund the 2002 Bali nightclub bombings, of which he was convicted, in part through online credit card fraud.

Also illustrative of the connection between terrorism and credit card fraud, three British men were convicted in 2007 of inciting terrorist murder via the Internet under the United Kingdom's Terrorism Act of 2000. Younes Tsouli, Waseem Mughal, and Tariq Al-Daour were participants in a network of extremist websites and communication forums through which al-Qaeda statements were issued and which disseminated videos of beheadings, suicide bombings in Iraq, and other jihadi propaganda. The three men also pleaded guilty to conspiracy to defraud banks and credit card companies. Tsouli was sentenced to 16 years in prison, Mughal was sentenced to 12 years in prison, and Al-

Daour was sentenced to 10 years in prison. Al-Daour and his associates used stolen credit card numbers obtained through phishing scams to make more than $3.5 million in fraudulent charges in order to purchase equipment, prepaid cell phones, airline tickets, and other items, to support jihadi groups in the field. Tsouli and Mughal also used stolen credit card numbers to set up and host jihadi websites. Significantly, the investigation revealed that these individuals were members of carding organizations.

The Department's Investigations and Prosecutions

The Department of Justice plays a critical role in combating payment card breaches and the fraud and other criminal activity that results. United States Attorney's offices throughout the country actively prosecute these cases. Within the Criminal Division, the Computer Crime and Intellectual Property Section (CCIPS) also investigates and prosecutes large-scale data breaches and coordinates prosecutions that involve multiple USAOs and foreign countries. In addition, the Fraud Section of the Criminal Division recently established the Payments Fraud Working Group (PFWG), which it co-chairs with the Board of Governors of the Federal Reserve System. The PFWG is an inter-agency cooperative effort between law enforcement and the bank regulatory agencies designed to examine issues related to various payments systems and establish initiatives to protect payments systems against fraud and other misuse. The Department also helped to lead the Identity Theft Task Force, which also addressed many of these issues. Finally, 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.

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 large-scale data breaches and associated criminal activity.

Recent Successes

The Department, in coordination with its various USAOs, has worked with investigative agencies including the USSS, the FBI, and the United States Postal Inspection Service to combat carding and associated crimes, with great success:

- **Dark Market carding forum**. Most recently, on October 16, 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 has resulted in 60 arrests worldwide and prevented an estimated $70 million in economic loss.

- **International hacking ring.** In August 2008, the Department announced the largest hacking and identity theft case ever prosecuted, in which charges were brought by the USAOs in the District of Massachusetts, the Southern District of California, and the Eastern District of New York against 11 members of an international hacking ring, including Maksik, discussed later. 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 13 individuals in Poland and eight in the United States. International cooperation was required to execute search warrants in the United States and in Romania. Significantly, Operation CardKeeper resulted in the U.S. conviction of an individual known online as "John Dillinger." This defendant was sentenced in 2007 to 94 months in federal prison for his carding activity, including aggravated identity theft, access device fraud, and conspiracy to commit bank fraud. 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; he is currently awaiting trial. Max Ray Butler, known online as "Iceman," was the co-founder and administrator of the carding forum Cardersmarket. This case is being prosecuted by the United States Attorney's Office for the Western District of Pennsylvania.

- **"Maksik" and "Lord Kaisersose."** Maksym Yastremskiy, known online as "Maksik," believed to be one of the top traffickers in stolen account information, was arrested for his carding activity in Turkey in 2007. He was also indicted in several U.S. districts as the result of the Department's prosecution of the international hacking ring I discussed earlier. Maksik allegedly sold hundreds of thousands of credit and debit card numbers. One of his customers, an infamous carder known online as "Lord Kaisersose," was previously searched and arrested in France as the result of a joint investigation conducted by the USSS and the French National Police. He is currently awaiting sentencing.

"Operation Firewall"

Much of this successful investigative work has its roots in some of the Department's early efforts to dismantle highly-organized carding enterprises. As just one

example, in 2004, as part of an undercover investigation known as Operation Firewall, the U.S. Secret Service (USSS) and several components of the Department of Justice 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. 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, the credit card industry could have faced 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. This prosecution was the first of its kind – by prosecuting top-tier members of the organization for conspiracy, it held individuals responsible for the criminal offenses facilitated through the carding forum by virtue of their leadership role in a criminal organization that operated solely online. Operation Firewall enabled many of our more recent successes. In addition, the investigation into the Shadowcrew organization also revealed that the defendants were conspiring internationally to commit specific carding-related crimes, including bank fraud, and enabled us to successfully prosecute individuals for that conduct separately.

Operation Firewall, like many of the examples I have mentioned today, also illustrates how we can effectively respond to the increasingly global nature of carding organizations. With the cooperation of law enforcement agencies in the United Kingdom, Canada, Bulgaria, Belarus, Poland, Sweden, the Netherlands, and Ukraine, foreign searches and arrests went smoothly, and foreign individuals were successfully indicted in the United States. In addition, the United Kingdom pursued a separate domestic prosecution of Shadowcrew members, which has led to a number of guilty pleas.

Prevention, Detection, and Response

Keeping credit, debit, and other financial account information out of the hands of criminals in the first place is an essential first step in reducing the frequency, and minimizing the impact, of large scale data compromises. Merchants and processors who hold individuals' sensitive financial information are prime targets for hackers and carders. To address this vulnerability, the credit card associations developed a set of security standards, known as the Payment Card Industry Data Security Standards (PCI DSS), for merchants and third party processors. We suggest that all entities that store, process, or transmit credit, debit, and other financial account information should ensure that they comply with all requirements of the PCI DSS in order to improve the security of their computer systems.

As is well understood throughout the security community, however, perfect security is impossible. Therefore, even if 100% compliance with PCI DSS were achieved, it is likely that hackers will continue to develop techniques to exploit the computer systems of companies holding cardholder data. For instances in which those hackers

succeed, efforts by the Department and investigative agencies to investigate, prosecute, and punish hackers and carders are critical to deterring future carders, learning more about the nature of these crimes, and punishing offenders. For continued success on these fronts, it is imperative that 1) victim companies embrace measures to swiftly detect data breaches and system compromises; 2) victim companies report data breaches to law enforcement; and 3) the United States builds upon its existing relationships with international partners to strengthen law enforcement cooperation channels internationally.

Early Detection

Early detection plays two important roles in efforts to combat carding activity. First, it can assist in mitigation of potential damage. When victim companies are notified by law enforcement, credit card companies, or other entities about a potential compromise to their system, they should take all reasonable measures to determine whether a compromise did indeed occur. Successful detection empowers victim companies to take steps to address the vulnerability, fortify their systems, and notify individual victims as necessary. But to date, it has been our experience that following notification, victim companies can not and do not always do enough to determine the scope and severity of data breaches of their computer networks.

Moreover, law enforcement faces continued investigative challenges as a result of delayed detection and response. Often, victim companies detect compromises to their system weeks, months, or years after they occur, and as a result, meaningful investigative leads may have disappeared by the time the compromise is reported to law enforcement, if it is reported at all. Private entities must have the capabilities to identify compromises more quickly. To accomplish this, we recommend that all entities that store, process, or transmit credit, debit, and other financial account information implement security mechanisms designed to detect system breaches, such as tracking and monitoring all access to network resources and cardholder data.

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 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 & Busters case, which was a part of the international hacking ring prosecuted in 2008, when Dave & Busters 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.

International Law Enforcement Cooperation

As illustrated by the array of cases I have mentioned, carders operating in carding forums on the Internet reside in different countries, collaborate freely across borders, and can immediately and widely distribute stolen identity information around the globe. In addition, online carding forums provide networking opportunities for criminals interested in joining together to perpetrate other financial fraud or criminal activity on a global scale. As a result, coordination and cooperation from foreign law enforcement is vital to the success of carding investigations and prosecutions. In this regard, the Identity Theft Task Force's Strategic Plan also recommended that the Department of Justice and other departments and agencies take specific steps to improve coordination and evidence sharing with foreign law enforcement agencies.

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 United States ratified in 2006, assures that other countries enact suitable domestic legislation criminalizing identity theft, in part to facilitate information-sharing under MLATs and the extradition of criminal defendants. 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. This has historically proven effective. Last month, for example, 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 G8 States and proposes "essential elements" of criminal legislation to address identity-related crime. 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 of Justice has begun this process, gathering information from a range of law enforcement authorities. Finally, only by assisting foreign authorities can we expect them to reciprocate with critical evidence for our own investigations. The United States can improve international cooperation, in certain cases, by ensuring that our

legislation provides U.S. authorities with the tools to assist foreign investigations effectively.

Conclusion

As I have attempted to outline for the Subcommittee, the Department has been at the forefront of groundbreaking and historic efforts to identify, prosecute, and punish the perpetrators of large-scale data breaches and the associated identity theft and fraud following from those breaches. In light of the growing sophistication and global scope of the threat, we are committed to continuing and improving our efforts to address this conduct. Thank you for the opportunity to provide the Subcommittee with a brief overview of the Department's role in combating these crimes and the primary issues we must focus on as we press ahead.

Madam Chairwoman, this concludes my remarks. I would be pleased to answer any questions that you or other members of the Subcommittee may have.