Testimony of

Ronald J. Tenpas

March 21, 2007

STATEMENT OF RONALD J. TENPAS ASSOCIATE DEPUTY ATTORNEY GENERAL UNITED STATES DEPARTMENT OF JUSTICE ON IDENTITY THEFT BEFORE THE SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE MARCH 21, 2007

Good morning, Madam Chairman and Members of the Subcommittee. I am pleased to appear before you today, on behalf of the Department of Justice, to testify on the topic of identity theft. The Department is strongly committed to the aggressive pursuit of identity theft in all forms, because its effects are both pervasive and substantial. A Bureau of Justice Statistics survey found that in just six months in 2004, 3.6 million U.S. households learned that they were victims of identity theft.1 More recently, a 2007 private-sector survey found that 8.9 million U.S. adults had become victims of identity fraud in the preceding year, leading to losses of nearly $50 billion.2

This morning, I would like to speak with you about the dual roles that the Department of Justice is playing in combating identity theft: first, as the prosecuting agency that seeks to bring identity thieves to justice; and second, as one of the two agencies leading the President's Identity Theft Task Force. In doing so, I will focus on the Department's substantial accomplishments in prosecuting identity theft, and on the work of the President's Identity Theft Task Force, which I serve as Executive Director. Since May 2006, the Task Force has been developing a comprehensive strategic plan for the federal government to combat identity theft more effectively. Because the Task Force is in the final stages of preparing its plan for presentation to the President, I cannot speak to the specific, final recommendations that will be contained in the plan. The Task Force, however, released several interim recommendations in September 2006, and I would be pleased to report on those and the status of their implementation.

Identity Theft Prosecutions

The Department works closely with many investigative agencies, including the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), the United States Postal Inspection Service (USPIS), and the Social Security Administration Office of the Inspector General (SSA OIG), to prosecute identity thieves. Federal prosecutors use a wide variety of federal statutes in prosecuting cases that involve identity theft. These include not only the original identity theft statute (18 U.S.C. § 1028(a)(7)) and the aggravated identity theft statute (18 U.S.C. § 1028A(a)), but other federal criminal statutes applicable to fraud, such as wire fraud (18 U.S.C. § 1343), mail fraud (18 U.S.C. § 1341), access device fraud (18 U.S.C. § 1029), financial institution fraud (18 U.S.C. § 1344), and Social Security fraud (42 U.S.C. § 408(a)(7)). The aggravated identity theft statute enacted in 2004, which carries a mandatory two-year prison sentence, has been a particularly useful tool to the Department in prosecuting identity thieves and ensuring that they receive adequate punishment. Since 2004, DOJ has made increasing use of the

aggravated identity theft statute: in Fiscal Year 2006, DOJ charged 507 defendants with aggravated identity theft, up from 226 in Fiscal Year 2005. In many of these cases, the courts have imposed substantial sentences.

Because identity theft can be involved in a wide range of criminal activities, ranging from fraud to organized crime to terrorism, the Department does not limit its prosecutions to any single type of identity theft. Nonetheless, there are several recurring types of criminal activity in the identity theft prosecutions recently brought by the Department. First, many of the identity theft cases we prosecute involve extensive and often elaborate criminal organizations. The following are just a few examples of these types of identity theft prosecutions:
* On January 24, 2007, in the Southern District of New York, a defendant was sentenced to 34 months imprisonment for his role in a large identity-theft ring that was engaged in, among other things, stealing individual victims' personal identity information, sharing that information over the Internet with other members of the identity-theft ring, and using the information to commit various forms of fraud. The defendant and his co-conspirators stole the identities of at least 175 individuals and victimized a large number of financial institutions. The investigation revealed a large number of e-mails between ring members in which they exchanged credit card numbers, together with expiration dates and threedigit codes. The e-mails also included the personal identity information of a large number of individual victims, including victims' names, addresses, telephone numbers, Social Security numbers, and mothers' maiden names. The defendant and his coconspirators then used the stolen credit card numbers and identity information to commit various forms of fraud, including using the credit card numbers to make purchases over the Internet.3
* On November 21, 2006, in the Eastern District of Virginia, a defendant was sentenced to 134 months imprisonment for aggravated identity theft, production and use of counterfeit credit cards, and conspiracy to utter counterfeit checks. Beginning in August 2005, the defendant and his co-conspirators deposited large-denomination counterfeit checks totaling $318,378.34 into the bank accounts of several local co-conspirators. The defendant and his accomplices obtained over $89,000 from TowneBank before their scheme was detected. During this same period, the defendant enlisted a front desk clerk at a hotel in Virginia Beach to provide him with the credit card information of hotel guests in exchange for cash. Thereafter, the clerk sold to the defendant and another coconspirator in New York City, the names and credit card information of over 100 hotel guests. These stolen credit card account numbers were then used to produce counterfeit credit cards in the names of co-conspirators. The co-conspirators then used these cards to purchase airplane tickets, hotel rooms and rental cars so that they could travel around the country purchasing high-end electronic items, such as flat screen televisions, which were then sold for cash. The losses related to the counterfeit card scheme were more than $340,000.4

A second category of identity theft cases involves use of the Internet to acquire and trade in people's identifying information on an international scale and other significant instances of unauthorized computer access. The following are just a few examples of the Department's prosecutions of these types of identity thieves:
* On February 9, 2007, in the Eastern District of Virginia, a defendant was sentenced to 94 months for aggravated identity theft, access device fraud, and conspiracy to commit bank fraud. The defendant, who went by the Internet nickname "John Dillinger," was involved in extensive illegal online "carding" activities. He received e-mails or instant messages containing hundreds

of stolen credit card numbers, usually obtained through phishing schemes or network intrusions, from "vendors" who were located in Russia and Romania. In his role as a "cashier" of these stolen credit card numbers, the defendant would then electronically encode these numbers to plastic bank cards, make ATM withdrawals, and return a portion to the vendors. Computers seized from the defendant revealed over 4,300 compromised account numbers and full identity information (i.e., name, address, date of birth, social security number, mother's maiden name, etc.) for over 1,600 individual victims.
* In November 2006, in the Western District of Washington, two defendants pleaded guilty to conspiracy to commit identity theft. According to the indictment, one defendant was employed at a janitorial company and worked at night in a U.S. Bank branch. He joined with other conspirators to steal information on more than 200 bank customers. Using that information, the defendants opened credit accounts in the customers names and used those accounts to purchase expensive items such as laptop computers, flat screen televisions, and airline tickets. In addition, they signed up for on-line banking for accounts that had not previously had on-line banking and then used those accounts to pay their own bills and transfer funds to other checking accounts that they then drained. The indictment charged the defendants with more than $200,000 in fraud against dozens of victims.
* On June 28 and 29, 2006, in the District of New Jersey, four defendants were sentenced to prison terms of up to 32 months for conspiracy to commit credit card and bank card fraud, as well as identification document fraud. As part of their earlier guilty pleas, these defendants admitted to their involvement in the Shadowcrew international criminal organization. Using the website www.shadowcrew.com, the Shadowcrew organization had thousands of members engaged in the online trafficking of stolen identity information and documents, such as drivers' licenses, passports, and Social Security cards, as well as stolen credit card, debit card, and bank account numbers. The Shadowcrew members trafficked in at least 1.7 million stolen credit card numbers and caused total losses in excess of $4 million dollars. The website was successfully shut down following a yearlong undercover investigation that resulted in the arrests of 21 individuals in the United States on criminal charges in October 2004. Additionally, law enforcement officers in six foreign countries arrested or searched eight individuals.

A third category of identity theft cases prosecuted by the Department involves health care fraud and theft of patient information. The following are some examples of the Department's prosecutions in this area:
* On January 24, 2007, in the Southern District of Florida, a federal jury convicted a defendant of all eight counts of a superseding indictment, which charged him with conspiring to defraud the United States, computer fraud, wrongful disclosure of individually identifiable health information, and aggravated identity theft. The case involved the theft and transfer of Medicare patient information from the Cleveland Clinic in Weston, Florida. The defendant purchased the patient information from his codefendant, a former Cleveland Clinic employee, who pleaded guilty on January 12, 2007 and testified against the defendant at trial. The theft resulted in the submission of more than $7 million in fraudulent Medicare claims, with approximately $2.5 million paid to providers and suppliers. This is the first Health Insurance Portability and Accountability Act ("HIPAA") violation case that has gone to trial in the United States. The defendant is scheduled to be sentenced on April 27, 2007.5
* On July 7, 2006, in the Southern District of Florida, three defendants who were indicted by a federal grand jury in a multi-million dollar health care fraud were arrested. The indictment

charged all three defendants with conspiracy to defraud a health care benefits program (Medicare) and defrauding a health care benefits program (Medicare). It also charged two of the defendants with identity theft for fraudulently utilizing Unique Physician Identification Numbers (UPIN) without the physicians' approval or knowledge. It also charged the third defendant with paying kickbacks and bribes to induce the referral of Medicare beneficiaries.6
In addition to our prosecutions, the Department is proud of the investigative efforts and initiatives undertaken by the FBI to combat identity theft. These include the IC3 project, which is a public-private alliance between the IC3 Unit of the FBI and the National White Collar Crime Center. Among other things, IC3 disseminates information on cybercrime and actionable cyber-related investigative leads, including those involving identity theft, to state and local law enforcement. IC3 has also formed an extensive network of relationships with industry, which has been a key to identifying cybercrime and typically associated identity theft.

Many other investigative agencies, too, including the Secret Service and U.S. Postal Inspection Service, have formed crucial partnerships with the private sector in an effort to combat identity theft. The Secret Service, for example, hosts a portal called the e Information system for members of the law enforcement and banking communities, which provides a forum for members to post the latest information on scams, counterfeit checks, frauds and swindles, and updated Bank Identification Numbers (BINs). In 2005, the USPIS created the Intelligence Sharing Initiative (ISI), a website that allows the Inspection Service and fraud investigators representing retail and financial institutions, as well as major mailers, to openly share information pertaining to mail theft, identity theft, financial crimes, investigations, and prevention methods.

Efforts have also been taken to investigate and arrest identity thieves who operate in foreign countries. For example, between April and November 2006, the FBI's Cyber Division supported "Cardkeeper," a major initiative with the FBI's Richmond, Virginia field office. As part of that initiative, the FBI sent six agents to Bucharest, Romania, to work with the Romanian National Police (RNP) to investigate the Internet intrusions committed by criminals in Romania, and which resulted in harm to U.S. victims. This unprecedented initiative resulted in thirteen arrests in the United States and three searches in Romania. The success of this investigation gave rise to the Romanian Task Force initiative, through which FBI agents are deployed to Romania to work full-time, hand-in-hand with the RNP on cases of mutual interest. The Department intends to continue to work hand-in-hand with all of our law enforcement partners to aggressively investigate and prosecute identity thieves.

President's Identity Theft Task Force
Background

I would like to turn now to the work of the President's Identity Theft Task Force. On May 10, 2006, President Bush issued an Executive Order that established the Task Force.7 The Task Force, under the leadership of the Attorney General as Chairman and Federal Trade Commission Chairman Deborah Platt Majoras as Co-Chairman, includes representatives from 17 departments and agencies, including the Departments of Commerce, Health and Human Services, Homeland Security, Treasury, and Veterans Affairs; the Office of Management and Budget; the Social Security Administration; the Office of Personnel Management; the Federal Reserve Board; the

Federal Deposit Insurance Corporation; the National Credit Union Administration; the Office of the Comptroller of the Currency; the Office of Thrift Supervision; the Securities and Exchange Commission; and the United States Postal Service. Each of these agencies has a unique perspective and expertise in combating identity theft that have been invaluable to the work of the Task Force.

The Executive Order charged the Task Force with implementing the policy to use federal resources effectively "to deter, prevent, detect, investigate, proceed against, and prosecute unlawful use by persons of the identifying information of other persons," including through three specific approaches: (a) increased aggressive law enforcement actions designed to prevent, investigate, and prosecute identity theft crimes, recover the proceeds of such crimes, and ensure just and effective punishment of those who perpetrate identity theft; (b) improved public outreach by the federal government to better (i) educate the public about identity theft and protective measures against identity theft, and (ii) address how the private sector can take appropriate steps to protect personal data and educate the public about identity theft; and (c) increased safeguards that federal departments, agencies, and instrumentalities can implement to better secure government-held personal data.

To carry out its work, the Task Force initially organized four working level subgroups: Criminal Law Enforcement, Outreach and Prevention, Data Security (public and private sector), and Legislative and Administrative Action. All of the Task Force member agencies have worked together in close coordination to develop a coherent and comprehensive response to identity theft. In addition, the Task Force conducted extensive outreach efforts, including soliciting public comments on many of the issues under consideration by the Task Force. The public comments that we received reflected the experiences and views of consumers, identity theft victims, businesses, law enforcement officers, and many others, and will inform the Task Force's recommendations to the President.

Interim Recommendations

As I mentioned, the Task Force is still in the final stages of completing the strategic plan for presentation to the President. We anticipate that the recommendations will build on and ensure effective coordination of robust efforts already under way to prevent identity theft, to assist victims of identity theft, and to investigate and prosecute the identity thieves. We look forward to sharing those final recommendations with this Committee in the coming months.

While the Task Force has been working on making final recommendations to the President, we also made some interim recommendations on September 19, 2006, on which I can report today.

The interim recommendations were intended to address steps that could be taken immediately to combat identity theft, even before the full work of the Task Force was completed. Those recommendations fall under three principal headings: prevention, victim assistance, and law enforcement. I am pleased to report that we have taken significant steps to implement these recommendations already.

Prevention

The first four interim recommendations addressed improving government handling of sensitive personal data:

Recommendation 1 involved establishing a data breach policy for the public sector. The Task Force recommended that the Office of Management and Budget (OMB) issue to all federal agencies the guidance generated by the Task Force that covers (a) the factors that should govern whether and how to give notice to affected individuals in the event of a government agency data breach that poses a risk of identity theft, and (b) the factors that should be considered in deciding whether to offer services such as free credit monitoring.

I am pleased to report that the OMB implemented this recommendation by distributing the Task Force's data breach guidance to all agencies and departments within a day of the Task Force issuing its interim recommendations. This was the first such guidance issued to federal agencies on steps to be taken in the event of a breach. We are confident that, with that guidance, agencies will be better equipped to effectively and quickly respond to data breaches and to mitigate any harms that may arise as a result of a data breach.

Recommendation 2 involved improving data security in the public sector. The Task Force recommended that OMB and the Department of Homeland Security (DHS), through the interagency effort already underway to identify ways to strengthen the ability of all agencies to identify and defend against threats, correct vulnerabilities, and manage risks: (a) outline best practices in the areas of automated tools, training, processes, and standards that would enable agencies to improve their security and privacy programs, and (b) develop a list of the top 10 or 20 "mistakes" to avoid in order to protect government information. These agencies have been working diligently on this task over the last several months, and the OMB anticipates that the resulting guidance will be issued in May 2007.

Recommendation 3 involved decreasing the use of Social Security numbers (SSNs) in the public sector. To limit the unnecessary use in the public sector of SSNs, the most valuable consumer information for identity thieves, the Task Force recommended the following:
* The Office of Personnel Management (OPM), in conjunction with other agencies, should accelerate its review of the use of SSNs in its collection of human resource data from agencies and on OPM-issued papers and electronic forms, and take steps to eliminate, restrict, or conceal their use (including the assignment of employee identification numbers, where practicable).
* OPM should develop and issue policy guidance to the federal human capital management community on the appropriate and inappropriate use of an employee's SSN in employee records, including the proper way to restrict, conceal, or mask SSNs in employee records and human resource management information systems.
* OMB should require all federal agencies to review their use of SSNs to determine where such use can be eliminated, restricted, or concealed in agency business processes, systems, and paper and electronic forms.

This recommendation, too, is in the process of being implemented. OPM is internally conducting a review of all paper and electronic forms and taking steps to eliminate, restrict or conceal SSNs where not needed. Most of the review is complete. Some mitigation plans and activities have been completed but a large number of the actions will rely on the establishment of a Unique Employee Identifier (UEID) that will replace the SSN as the primary key in Federal employee

records. OPM has conducted two agency-wide workgroup meetings to define the scope, structure, and use of the UEID, and is developing requirements and concept-of operations documentation.

In addition, OPM is updating 5 CFR 293 to improve guidance on the restriction, concealment, and masking of SSNs in employee records and human resources information systems. The updated regulation includes comments and suggestions from a cross-agency workgroup and is currently being reviewed internally within OPM. Once completed, it will undergo the normal regulatory process.

Finally, OMB has administered a government-wide survey to assess the extent and nature of agencies' use of SSNs; identify factors to consider when determining whether use of the SSN is mission-essential and necessary to ensure program integrity or national security; and evaluate practical alternatives to use of the SSN. OMB anticipates agency review of its use of SSNs will prompt action to reduce unnecessary use and address vulnerabilities. The survey was conducted in coordination with OPM's evaluation on use of the SSN in employee records for the federal human capital management community. OMB is currently analyzing agencies' responses to the survey.

Recommendation 4 involved publication of a "routine use," under the Privacy Act, for disclosure of information following a breach. Specifically, to allow agencies to respond quickly to data breaches, including by sharing information about potentially affected individuals with other agencies and entities that can assist in the response, the Task Force recommended that all federal agencies, to the extent consistent with applicable law, publish a new "routine use" for their systems of records under the Privacy Act that would facilitate the disclosure of information in the course of responding to a breach of federal data. The Department of Justice has already taken the lead in publishing such a routine use, and we anticipate that other agencies will soon follow.

The fifth recommendation addressed development of alternate authentication methods. Because developing reliable methods of authenticating the identities of individuals would make it harder for identity thieves to access existing accounts and open new accounts using other individuals' information, the Task Force recommended that the Task Force hold a workshop or series of workshops, involving academics, industry, and entrepreneurs, focused on developing and promoting improved means of authenticating the identities of individuals. We are pleased to report that the first workshop will be hosted by the FTC on April 23 and 24, 2007. That public workshop, "Proof Positive: New Directions in ID Authentication," will explore methods to reduce identity theft through enhanced authentication. The workshop will facilitate a discussion among public sector, private sector, and consumer representatives, and will focus on technological and policy requirements for developing better authentication processes, including the incorporation of privacy standards and consideration of consumer usability issues. The FTC is seeking public comments in planning the agenda for the workshop, and is inviting parties interested in participating as panelists to notify the agency. The FTC is also inviting comments on ways to improve authentication processes to reduce identity theft, including, but not limited to, comments on the following questions: How can individuals prove their identities when establishing them in the first place? What are some current or emerging authentication technologies or methods - for example, biometrics, public key infrastructure, and knowledge-

based authentication -- and what are their strengths and weaknesses? To what extent do these technologies meet consumer needs, such as ease of use, and to what extent do they raise privacy concerns?

Victim Assistance

Recommendation 6 involved expanding the types of restitution for identity theft victims. One reason that identity theft can be so destructive to its victims is the sheer amount of time and energy often required to remediate the consequences of the offense. This may be time spent clearing credit reports with credit-reporting agencies, disputing charges with individual creditors, or monitoring credit reports for additional impacts of the theft. To allow identity theft victims to recover for the value of time they spend in attempting to remediate the harms suffered, the Task Force recommended that Congress amend the criminal restitution statutes to allow for restitution from a criminal defendant to an identity theft victim, in an amount equal to the value of time reasonably spent by the victim attempting to remediate the intended or actual harm incurred from the identity theft offense. The Department transmitted that proposed amendment to Congress on October 4, 2006. We look forward to working with this Committee to ensure that those amendments are enacted into law.

Law Enforcement

Recommendation 7 involved development of a universal police report. The Task Force recommended that the FTC and other Task Force members develop a universal police report, which an identity theft victim can complete, print, and take to any local law enforcement agency for verification and incorporation into the police department's report system. This recommendation is intended to ensure that victims can readily obtain the police reports that they need to take steps to prevent the misuse of their personal information by identity thieves, and to ensure that their complaint data are entered in a standardized format that will allow complaints to flow into a central complaint database and that thereby would assist law enforcement officers in responding to such complaints.

This recommendation, too, has been implemented. The FTC posted the standard police report form on its website in October 2006. The form is based on the online complaint form found at www.ftc.gov/idtheft, and when printed by the consumer, can be used as the basis for a police report. The FTC and others are publicizing the form's availability to law enforcement, and encouraging police departments to refer identity theft victims to the form. Use of the form should streamline the efforts for law enforcement, and enable more victims to obtain police reports, and continue their efforts to restore their good name.

* * *

In conclusion, we welcome this Subcommittee's interest in the problem of identity theft, and look forward to working with the Subcommittee and Committee in the future. Madam Chairman, that concludes my prepared remarks. I would be pleased to take questions from you and other members of the Subcommittee.

1 See Bureau of Justice Statistics, U.S. Dep't of Justice, Bulletin: Identity Theft, 2004 (April 2006), available at http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

2 See JAVELIN STRATEGY & RESEARCH, 2007 IDENTITY FRAUD SURVEY REPORT: IDENTITY FRAUD IS DROPPING, CONTINUED VIGILANCE NECESSARY (February 2007).
3 See U.S. Attorney's Office, Southern District of New York, Press Release (January 24, 2007), available at http://newyork.fbi.gov/dojpressrel/pressrel07/identitytheft012407.htm.
4 See U.S. Attorney's Office, Eastern District of Virginia, Press Release (November 22, 2006), available at http://www.usdoj.gov/usao/vae/Pressreleases/11-NovemberPDFArchive/06/20061122ross_charlesnr.pdf.
5 See U.S. Attorney's Office, Southern District of Florida, Press Release (January 24, 2007), available at http://miami.fbi.gov/dojpressrel/pressrel07/mm20070124b.htm.
6 See U.S. Attorney's Office, Southern District of Florida, Press Release (July 7, 2006), available at http://miami.fbi.gov/dojpressrel/pressrel06/mm20060707.htm.
7 See Executive Order 13402, Strengthening Federal Efforts to Protect Against Identity Theft (May 10, 2006), available at http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html.