FEDERAL IDENTITY THEFT TASK FORCE

Attorney General Alberto Gonzales
Federal Trade Commission Chairman Deborah Platt Majoras

On May 10, 2006, the President signed an Executive Order establishing an Identity Theft Task Force, and directing it to develop a coordinated strategic plan to combat identity theft. The Task Force was specifically directed to make recommendations on ways to further improve the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution. The Executive Order directed the Task Force to deliver the strategic plan to the President within 180 days. By further Executive Order, issued November 3, 2006, the President amended the original order to require submission of the strategic plan by February 9, 2007, or as soon as practicable thereafter as the Chairman and Co-Chairman shall determine.

On September 19, 2006, the Task Force published Interim Recommendations, which can be found at www.ftc.gov/opa/2006/09/idtheft.htm.

The Task Force, in working to produce a final strategic plan to the President, is considering, among other things, various ways to improve the coordination and effectiveness of criminal prosecution of identity theft; to enhance data protection for sensitive consumer information maintained by the public sector, private sector, and consumers themselves; to provide more comprehensive and effective guidance for consumers and the business community; and to improve recovery and assistance for consumers following a breach or misuse of their information. The Task Force members have focused their work on the following four areas:

- Keeping sensitive consumer data out of the hands of identity thieves through better data security practices and by educating consumers to protect themselves;
- Making it more difficult for identity thieves, when they are able to obtain consumer data, to use the information to steal identities;
- Assisting the victims in recovering from crime; and
- Deterring identity theft by aggressively prosecuting and punishing those who commit the crime.

Although there is no legal requirement that the Task Force formally solicit public comment, the Task Force believes that seeking further comment on these issues will supplement the research and analysis already conducted, provide further information about the proposals it is considering, and identify areas where additional recommendations may be warranted. It is not expected that the Task Force will respond directly to particular comments or suggestions. Rather, the Task Force will use submitted comments to supplement the outreach and analysis already conducted. The Task Force invites comments on the following issues and questions:

I. MAINTAINING SECURITY OF CONSUMER DATA

The Task Force Interim Recommendations addressed data security in the public sector by calling for examination by federal agencies of their collection and uses of Social Security numbers (SSNs), the piece of information that is often most effective in committing identity theft. The Task Force also recommended that the Office of Management and Budget conduct a survey to assess how well agencies protect the sensitive consumer data they maintain, and recommended that the Office of Personnel Management identify and eliminate the gratuitous use of SSNs in human resources forms used by federal agencies. The Task Force is considering

whether additional measures, including the following, should be taken to further enhance the protection of sensitive consumer information and thus keep it out of the hands of identity thieves:

1. Government Use of SSNs

Because SSNs are frequently used to facilitate identity theft, the Task Force currently is exploring ways to achieve reduced reliance on SSNs by federal, state, and local government. To the extent this is important, what steps (including working with state and local governments to highlight and discuss the vulnerabilities created by the use of SSNs and to explore ways to eliminate unnecessary use and display of SSNs) could help to achieve this goal? On a related issue, please provide any comments that you may have on what information could be used as a substitute for SSNs.

2. Comprehensive Record on Private Sector Use of SSNs

The Task Force, in seeking to address the extent to which the availability of SSNs to identity thieves creates the possibility of harm to consumers, is considering whether to recommend that the Task Force investigate and analyze how SSNs are currently used in the private sector, and how these uses could be modified or limited to help minimize the unnecessary exposure of SSNs and/or to make them less valuable in committing identity theft. Would such an effort be helpful in addressing the problem of identity theft? To what extent would such an effort be the appropriate way to gather this information?

3. National Data Security Standards

The Task Force is considering whether to recommend that national data security requirements be imposed on all commercial entities that maintain sensitive consumer information. Would such national requirements be helpful in addressing any deficiencies in

current data security practices? If so, what would be the essential elements of such a requirement? Does the need for such a national standard, if any, vary according to economic sector, business model, or business size? On a related note, please provide any comments that you may have on the costs of imposing a national data security requirement on businesses.

4. Breach Notice Requirements for Private Sector Entities Handling Sensitive Consumer Information

The Task Force is considering whether to recommend that a national breach notification requirement be adopted. Would such a breach notification requirement be helpful in addressing any deficiencies in the protocols currently followed by businesses after they suffer a breach? If so, what would be the essential elements of such a national breach notification requirement? Does the need for such a national standard, if any, vary according to economic sector, business model, or business size?

5. Education of the Private Sector and Consumers on Safeguarding Data

The Task Force is considering whether there is a need to better educate the private sector on safeguarding information and on what private sector entities should do if they suffer a data breach. Additionally, the Task Force is considering whether there is a need to better educate consumers on how to safeguard their personal data and how to detect and deter identity theft, through a national public awareness campaign. Are such education campaigns an appropriate way in which to address the problem of identity theft? If so, what should be the essential elements of these education campaigns for the private sector and consumers?

II. PREVENTING THE MISUSE OF CONSUMER DATA

The Task Force is also considering how to make it more difficult for identity thieves, when they are able to obtain consumer data, to use the information to steal identities. In its

interim recommendations to the President, the Task Force noted that developing more reliable methods of authenticating the identities of individuals would make it harder for identity thieves to open new accounts or access existing accounts using other individuals' information. The Task Force accordingly 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. Those workshops will begin in early 2007.

Are there any other measures that the Task Force should consider in addressing how to prevent the misuse of consumer data that has fallen into the hands of an identity thief?

III. VICTIM RECOVERY

The Task Force has been considering the barriers that victims face in restoring their identity. The Task Force has specifically addressed the following issues:

1. Improving Victim Assistance

The Task Force is considering ways in which to provide more effective assistance to identity theft victims, including, but not limited to, providing training to local law enforcement on how best to provide assistance for victims; providing educational materials to first responders that can be used readily as a reference guide for identity theft victims; developing and distributing an identity theft victim statement of rights based on existing remedies and rights; developing nationwide training for victim assistance counselors; and developing avenues for additional victim assistance through the engagement of national service organizations. Would these measures be effective ways to assist victims of identity theft? Are there any other ways to improve victim assistance efforts that the Task Force should consider?

2. Making Identity Theft Victims Whole

The Task Force has issued an interim recommendation that Congress amend the criminal restitution laws to allow identity theft victims to seek restitution from the identity thief for the value of their time in attempting to recover from the effects of the identity theft. Are there other ways in which the government can remove obstacles to victim recovery?

3. National Program Allowing Identity Theft Victims to Obtain an Identification Document for Authentication Purposes

To give identity theft victims a means to authenticate their identities when mistaken for the identity thief in a criminal justice context, several states have developed voluntary identification documents, or "passports," that authenticate identity theft victims. The FBI has established a similar system through the National Crime Information Center, allowing identity theft victims to place their name in an "Identity File." The Task Force is considering whether federal agencies should lead an effort to study the feasibility of developing a nationwide system that would allow identity theft victims to obtain a document or other mechanism that they can use to avoid being mistaken for the suspect who has misused their identity. Would such a system meaningfully assist victims of identity theft? If so, what should be the essential elements of such a nationwide system?

4. Gathering Information on the Effectiveness of Victim Recovery Measures

To evaluate the effectiveness of various new federal rights that have been afforded to identity theft victims in recent years, as well as various new state measures to assist identity theft victims that have no federal counterpart, the Task Force is considering whether to recommend (a) that the agencies with enforcement authority for the Fair and Accurate Credit Transaction Act (FACT Act) amendments to the Fair Credit Reporting Act assess the amendments' impact and

effectiveness through appropriate surveys or other means, and (b) that agencies conduct an assessment of state credit freeze laws, including how effective they are, what costs they may impose on consumers and businesses, and what features are most beneficial to consumers. Are such studies important for formulating a national strategy on how to combat identity theft? Are there any other evaluations that should be done to assess the effectiveness of victim recovery measures?

IV. LAW ENFORCEMENT: PROSECUTING AND PUNISHING IDENTITY THIEVES

The May 2006 Executive Order stated that it shall be the policy of the United States to use its resources effectively to address identity theft, including through "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." The Task Force has accordingly examined various ways, including the following, by which this goal can be achieved.

1. Establish a National Identity Theft Law Enforcement Center

The Task Force is considering whether to recommend the creation of a National Identity Theft Law Enforcement Center, to better coordinate the sharing of information among criminal and civil law enforcement and, where appropriate, the private sector. Such a Center could become the central repository for identity theft complaint data and other intelligence from various sources received by law enforcement, as well as a hub for analysis of that information. The analyses could be used to provide support for law enforcement at state and federal levels in the investigation, prosecution, and prevention of identity theft crimes. The Center also could

develop effective mechanisms to enable law enforcement officers from around the country to share, access, and search appropriate law enforcement information through remote access. The Center could also assist investigative agencies, before they begin a particular investigation, in determining whether another agency is already investigating a particular identity theft scheme or ring. Would the establishment of such a Center assist law enforcement in responding to identity theft? If so, what should be the core functions and elements of that Center?

2. Ability of Law Enforcement to Receive Information from Financial Institutions

Because the private sector in general, and financial institutions in particular, are an important source of identity theft-related information for law enforcement, the Task Force is considering:

(a) whether the Justice Department should initiate discussions with the private sector to encourage increased public awareness of Section 609(e) of the Fair Credit Reporting Act, which enables identity theft victims to receive identity theft-related documents and to designate law enforcement agencies to receive the documents on their behalf;

(b) whether relevant federal law enforcement agencies should continue discussions with the financial services industry to develop more effective fraud prevention measures to deter identity thieves who acquire data through mail theft; and

(c) whether the Justice Department should initiate discussions with the credit reporting agencies on possible measures that would make it more difficult for identity thieves to obtain credit based on access to a victim's credit report.

Would such measures meaningfully assist law enforcement efforts in combating identity theft

and/or meaningfully assist in forming partnerships between law enforcement and the private sector? Are there any other measures that could be implemented to strengthen the relationship between the private sector and the law enforcement community in responding to identity theft?

3. The Investigation and Prosecution of Identity Thieves Who Reside in Foreign Countries

To address the fact that a significant portion of the identity theft committed in the United States originates in other countries, the Task Force is considering whether there are ways that the United States can work with foreign countries to better address this problem, including:

(a) whether the Department of Justice and the Department of State should formally encourage other countries to enact suitable domestic legislation criminalizing identity theft;

(b) whether the U.S. Government should continue its efforts to promote universal accession to the Convention on Cybercrime and assist other countries in bringing their laws into compliance with the Convention's standards;

(c) whether the U.S. Government should encourage those countries that have demonstrated an unwillingness to cooperate with U.S. law enforcement in criminal investigations, or have failed to investigate or prosecute offenders aggressively, to alter their practices and eliminate safe havens for identity thieves;

(d) whether the U.S. Government should recommend that Congress amend the language of 28 U.S.C. § 1782 and 18 U.S.C. § 2703 to clarify which courts can respond to appropriate foreign requests for electronic and other evidence in criminal investigations, so that the United States can better provide prompt

assistance to foreign law enforcement in identity theft cases; and

(e) whether federal law enforcement agencies should assist, train, and support foreign law enforcement through the use of Internet intelligence-collection entities.

Would such measures meaningfully assist U.S. law enforcement in its ability to investigate, identify, and prosecute foreign-based identity thieves who are committing crimes in the United States? Are there any other measures that could be implemented to achieve this goal?

4. Prosecutions of Identity Theft

The Task Force is considering whether steps can be taken to increase the number of state and federal prosecutions of identity thieves, including (a) requiring each United States Attorney's Office to designate an identity theft coordinator and/or develop a specific Identity Theft Program for each District, including evaluating monetary thresholds for prosecution, (b) formally encouraging state prosecutions of identity theft, and (c) creating working groups and task forces to focus on the investigation and prosecution of identity theft. Would these measures meaningfully assist in increasing the number of identity theft prosecutions? Are there any other measures that can be implemented that would increase state and federal prosecutions of identity thieves?

5. Targeted Enforcement Initiatives

The Task Force is considering whether to propose that law enforcement agencies undertake special enforcement initiatives focused exclusively or primarily on identity theft, including specific initiatives focused on (a) unfair or deceptive means to make SSNs available for sale; (b) identity theft related to the health care system; and (c) identity theft by illegal aliens. Additionally, the Task Force is considering whether to recommend that federal agencies,

including the SEC, the federal banking agencies, and the Department of Treasury review their supervisory and compliance programs to assess whether they adequately address identity theft and create sufficient deterrence. Would these special initiatives be useful in prosecuting and punishing identity thieves? Are there any other such special enforcement initiatives that could make a difference in deterring and punishing identity thieves?

6. Amendments to Federal Statutes and Guidelines Used to Prosecute Identity-Theft Related Offenses

The Task Force is considering whether to recommend that Congress amend the identity theft and aggravated identity theft statutes to ensure that identity thieves who misappropriate information belonging to corporations and organizations can be prosecuted, and add several new crimes to the list of predicate offenses for aggravated identity theft offenses, such as mail theft, uttering counterfeit securities, tax fraud, and conspiracy to commit those crimes. The Task Force is also considering whether to recommend that Congress amend 18 U.S.C. § 1030(a), the statute that criminalizes the theft of electronic data, by eliminating the current requirement that the information must have been stolen through interstate communications. Further amendments under consideration by the Task Force include:

- amending 18 U.S.C. § 1030(a)(5) by eliminating the current requirement that the defendant's key-logging or malicious spyware actions must cause "damage" to computers and that the loss caused by the conduct must exceed $5,000;
- amending the cyber-extortion statute, 18 U.S.C. § 1030(a)(7), to cover additional, alternate types of cyber-extortion;
- outlawing pretexting by providing both criminal and civil penalties for such

conduct;

- ! enacting legislation that would make it a felony for data brokers and telephone company employees to knowingly and intentionally sell or transfer customer information without prior written authorization from the customer, with appropriate exceptions for law enforcement purposes;
- ! amending the U.S. Sentencing Guidelines to ensure that an identity thief's sentence can be enhanced when the criminal conduct affects more than one victim; and
- ! amending the definition of "victim," as that term is used under United States Sentencing Guideline section 2B1.1, to state clearly that a victim need not have sustained an actual monetary loss.

Would such amendments meaningfully assist prosecutors in charging, convicting, and ensuring the just punishment of identity thieves? Are there any other potential amendments to the provisions of the United States Code or U.S. Sentencing Guidelines that the Task Force should consider?

7. Training for Law Enforcement Officers and Prosecutors

The Task Force is considering whether to recommend enhancing the training for law enforcement officers and prosecutors who investigate and prosecute identity theft offenses, including by: (a) developing a course at the National Advocacy Center (NAC) focused solely on investigation and prosecution of identity theft; (b) increasing the number of regional identity theft seminars hosted by the U.S. Postal Inspection Service, Justice Department, Federal Trade Commission, U.S. Secret Service, and American Association of Motor Vehicle Administrators;

(c) increasing resources for law enforcement available on the internet, including by ensuring that an Identity Theft Clearinghouse site could be used as the portal for law enforcement agencies to gain access to additional educational materials on investigating identity theft and responding to victims; and (d) reviewing curricula to enhance basic and advanced training on identity theft. Are these measures necessary or helpful to law enforcement officers and prosecutors? Are there any other such training initiatives that the Task Force should consider?

8. Measuring Law Enforcement Efforts

Because there is limited data on law enforcement efforts in the area of identity theft, the Task Force is considering whether additional surveys and statistical analysis are needed, including whether to: (a) expand the scope of the National Crime Victimization Survey; (b) review U.S. Sentencing Commission data on identity theft-related case files every two to four years; (c) track federal prosecutions of identity theft and the amount of resources spent on such prosecutions; and (d) conduct targeted surveys in order to expand law enforcement knowledge of the identity theft response and prevention activities of state and local police. Would such surveys be helpful to the law enforcement community? Are there any other such surveys or measurements that the Task Force should consider? On a related issue, are the data sets that are currently available that relate to the frequency, cost, and type of identity theft sufficient to give us a full understanding of the problem of identity theft?

Form of Comments

The Task Force requests that interested parties submit written comments on the above questions and/or bring to the attention of the Task Force any additional facts or considerations

that would assist in developing a coordinated strategic plan. Comments should be captioned **Identity Theft Task Force** and must be filed on or before Friday, January 19, 2007. Although the Task Force prefers that interested parties file their comments electronically, parties may also submit their comments by mail/hand delivery.

Electronic Filing: If parties choose to submit their comments electronically, they should email the comments to Taskforcecomments@idtheft.gov. The Task Force asks that the email include the parties' contact information and that the substantive comments be attached to the email in Word Perfect, Microsoft Word, or PDF format.

Mail or Hand Delivery: A comment filed in paper form should include "Identity Theft Task Force, P065410," both in the text and on the envelope and should be mailed or delivered to the following address: Federal Trade Commission/Office of the Secretary, Room H-135 (Annex N), 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. Because paper mail in the Washington, D.C. area and at the FTC is subject to delay, parties should consider submitting their comments in electronic form, as prescribed above. The Task Force requests that any comment filed in paper form be sent by courier or overnight service, if possible.