PRESIDENT'S IDENTITY THEFT TASK FORCE
SUMMARY OF INTERIM RECOMMENDATIONS

PREVENTION

Improving Government Handling of Sensitive Personal Data

Recommendation 1: The Task Force recommends that the Office of Management and Budget (OMB) issue to all federal agencies the attached Task Force guidance 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.

Recommendation 2: To ensure that government agencies improve their data security programs, the Task Force recommends 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.

Recommendation 3: To limit the unnecessary use in the public sector of Social Security numbers (SSNs), the most valuable consumer information for identity thieves, the Task Force recommends 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.

Recommendation 4: 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 recommends 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,

PRESIDENT'S IDENTITY THEFT TASK FORCE
INTERIM RECOMMENDATIONS

PREVENTION

Improving Government Handling of Sensitive Personal Data

1. Establishing a Data Breach Policy for the Public Sector

Identity theft and related harms are a consequence of sensitive information about consumers that criminals obtain through theft or other improper means. In many cases, providing notice to the affected individuals can help prevent or mitigate the harms to consumers. Notice permits consumers to take protective actions, while also allowing relevant private sector entities to assist the consumers. Appropriate notice can also enable law enforcement to investigate, punish, and deter crime. At the same time, however, unnecessary or excessive breach notification can overwhelm the public and impose undue burdens and costs on consumers, as well as on government agencies.

Several federal government agencies have suffered high-profile security breaches involving sensitive consumer data over the past several months. These and other agencies have faced difficult decisions about when and how to notify the public of such incidents, and whether the agencies should offer free credit monitoring or other services to those who may be affected. Federal agencies need guidance in how to make these important decisions.

Recommendation 1: The Task Force recommends that the Office of Management and Budget (OMB) issue the attached guidance memorandum, advising federal agencies on steps to take in the event of a compromise of data. The Task Force has developed and formally approved a set of guidelines, produced in Attachment A, that provides the factors that should be considered in deciding whether, how, and when to inform affected individuals of the loss of personal data that can contribute to identity theft, and whether to offer services such as free credit monitoring to the persons affected.

2. Improving Data Security in the Public Sector

The high-profile data breaches suffered by several federal agencies have focused attention on whether the government is doing enough to secure the massive amounts of data held by federal agencies as part of their core missions. The President's Management Agenda (PMA) Scorecard, OMB reports to Congress, Congress' annual security report card, Government Accountability Office reports, and many agency Inspector General (IG) reports show that agency performance in both information privacy and security is uneven. Common findings are that agencies would benefit from increased sharing of best practices, group purchases of automated tools and training courses, and development of a more effective common curriculum for training. OMB and the Department of Homeland Security (DHS) are already leading an interagency Information Systems Security Line of Business (ISS LOB) effort to explore ways to address these issues, including to identify and defend against threats, correct vulnerabilities, and manage risks. The ISS LOB can be a useful forum for

developing best practices and a list of practices that should be avoided in order to protect government information.

Recommendation 2: To ensure that government agencies improve their data security programs, the Task Force recommends that OMB and DHS enhance the activities of the ISS LOB. Specifically, the Task Force recommends that the ISS LOB should (a) outline best practices in the area 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 information held by the government.

3. Decreasing the Use of Social Security Numbers by the Public Sector

One way to reduce the incidence of identity theft is to make it more difficult for criminals to obtain consumer information. Currently, the most valuable consumer information identity thieves can find is the Social Security Number (SSN). SSNs are key to assuming another's identity because they are used to match consumers with their credit histories and many government benefits. Consequently, if federal agencies were to eliminate unnecessary uses of SSNs, they could reduce the opportunities for unauthorized use by identity thieves. The Office of Personnel Management (OPM), which issues or approves many of the federal forms and procedures using the SSN, and OMB, which oversees the management and administrative practices of federal agencies, can play pivotal roles in

employee records, including the appropriate way to restrict, conceal, or mask SSNs in employee records and human resource management information systems.

OPM already has begun work to implement this recommendation, such as by working to establish a unique employee identifier that can be used in human resource and payroll systems rather than SSNs. Pursuant to the Task Force's recommendation, OPM is also prepared in September 2006 to begin consulting with a working group of agencies to develop a new OPM policy regarding the use of a unique employee identifier and limitations

a "routine use" would serve to protect the interests of the people whose information is at risk by allowing agencies to take appropriate steps to facilitate a timely and effective response, thereby improving their ability to prevent, minimize, or remedy any harms that may result from a compromise of data maintained in their systems of records. For example, such a routine use would permit an agency that has lost data such as bank account numbers to quickly share that information with the appropriate financial institutions, which could assist in monitoring for bank fraud and in identifying the account holders, thereby facilitating the agency's ability promptly to notify the affected individuals. The Department of Justice recently drafted such a "routine use," which is reproduced in Attachment B, and which the Task Force offers as a model for other federal agencies to use in developing and publishing their own "routine uses" as soon as practicable.

Recommendation 4: 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 recommends 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, modeled after the attached "routine use" the agen

[1]The Task Force is aware that for a limited number of agencies, the publication of this routine use will not eliminate all barriers to information sharing. For example, some of the information maintained by the federal banking agencies is bank customer information from financial records. Federal agencies and departments are subject to the Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq., which imposes additional requirements on any federal agency or department wishing to share financial records with another agency or department.

[2] Identification or verification is the process of determining the identity of an individual at the onset of the relationship between the individual and the verifying entity. Authentication is the process of ensuring that the individual is the same as the individual whose identity was initially verified. Thus, verification occurs once with respect to the verifying entity, but authentication can be recurrent, depending on the nature of the relationship between the individual and the authenticating entity.

Both the private and public sectors have made strides in developing improved means of verification and authentication. For example, the Customer Identification Program already requires financial institutions regulated by the federal banking agencies and the SEC to develop and implement procedures for verifying customers' identities when opening new accounts. Technology also can substantially improve the authentication process by, for example, the use of biometrics to authenticate the consumer's identity, making it less likely that a criminal can gain access to another's account. However, many questions remain about emerging technologies, consumer acceptance, and system implementation.

One way to sharpen the focus on improving the means for authenticating the identities of individuals would be to hold public workshops that bring together academics, industry, and entrepreneurs who are developing better authentication systems. These experts can discuss the existing problem, examine the limitations of current processes of authentication, and probe viable solutions that will reduce identity fraud. As an initial step, the FTC and other Task Force member agencies are prepared to announce in the fall of 2006 that they will host such a workshop in the early part of 2007.

Recommendation 5: Because developing 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 should 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.

VICTIM ASSISTANCE

6. 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 conseque

[3] The FTC recently commissioned a new national survey. Although the analysis of the results has not yet been completed and there were some methodological differences from the 2003 survey, it appears that both the number of hours that individual victims spent in recovering from identity theft, and the aggregate hours across the population, have decreased. We note that, in the intervening years, Congress passed the Fair and Accurate Credit Transactions Act,

format that is used by the FTC's Identity Theft Data Clearinghouse, increasing the ability of law enforcement to effectively spot significant patterns of criminal activity.

At present, the FTC has an online complaint form that is used to enter data into its Identity Theft Data Clearinghouse, which is in turn made available to law enforcement nationwide through Consumer Sentinel. The FTC is also prepared to develop a revised online complaint form at www.ftc.gov/idtheft that victims can complete, print, and take to a local law enforcement agency for verification and incorporation into the police department's report system. The victim will then have a valid, detailed police report; the police department will have a record of the crime; and the victim's complaint information will have been entered into the FTC's Identity Theft Data Clearinghouse. The Public Sector Liaison Committee of the International Association of Chiefs of Police supports and has been involved in this effort.

Recommendation 7: To ensure that victims can readily file the police reports necessary to allow them to prevent the continued misuse of their personal information, and to assist law enforcement in analyzing significant patterns of criminal activity in investigating identity theft complaints, the FTC, with support from Task Force members, should 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.

ATTACHMENT A

MEMORANDUM FROM THE IDENTITY THEFT TASK FORCE

Chair, Attorney General Alberto R. Gonzales
Co-Chair, Federal Trade Commission Chairman Deborah Platt Majoras

SUBJECT: Identity Theft Related Data Security Breach Notification Guidance

The Identity Theft Task Force ("Task Force") has considered the steps that a Department or agency should take in responding to a theft, loss, or unauthorized acquisition of personal information that poses a risk of subsequent identity theft. This memorandum reports the Task Force's recommended approach to such situations, without addressing other notification issues that may arise under the Privacy Act or other federal statutes when the data loss involves sensitive information that does not pose an identity theft risk.

I. Background

Identity theft, a pernicious crime that harms consumers and our economy, occurs when individuals' identifying information is used without authorization in an attempt to commit fraud or other crimes.[1] There are two primary forms of identity theft. First, identity thieves can use financial account identifiers, such as credit card or bank account numbers, to commandeer an individual's existing accounts to make unauthorized charges or withdraw money. Second, thieves can use accepted identifiers like social security numbers ("SSNs") to open new financial accounts and incur charges and credit in an individual's name, but without that person's knowledge.

This memorandum describes three related recommendations: (1) Agencies should immediately identify a core response group that can be convened in the event of a breach; (2) If an incident occurs, the core response group should engage in a risk analysis to determine whether the incident poses problems related to identity theft; (3) If it is determined that an identity theft risk is present, the agency should tailor its response (which may include advice to those potentially affected, services the agency may provide to those affected, and public notice) to the nature and scope of the risk presented. The memorandum provides a menu of steps for an agency to consider, so that it may pursue such a risk-based, tailored response. Ultimately, the precise steps to take must be decided in light of the particular facts presented, as there is no single response for all breaches. This memorandum is intended simply to assist those confronting such issues in developing an appropriate response.

---

[1]Federal laws define "identifying information" broadly. *See, e.g.,* The 1998 Identity Theft Assumption and Deterrence Act (Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028)) and the Fair and Accurate Credit Transactions Act (15 U.S.C. §§ 1681-1681x, as amended). This memorandum focuses on the type of identifying information generally used to commit identity theft.

II. Data Breach Planning

Considering these factors together should permit the agency to develop an overall sense of where along the continuum of identity-theft risk the risk created by the particular incident falls. That assessment, in turn, should guide the agency's further actions.

IV. Reducing Risk After Disclosure

While assessing the level of risk in a given situation, the agency should simultaneously consider options for attenuating that risk. It is important in this regard for the agency to understand certain standard options available to agencies and individuals to help protect potential victims:

A. Actions that Individuals Can Routinely Take

The steps that individuals can take to protect themselves will depend on the type of information that is compromised. In notifying the potentially affected individuals about steps they can take following a data breach, agencies should focus on the steps that are relevant to those individuals' particular circumstances, which may include the following:

- Contact their financial institution to determine whether their account(s) should be closed. This option is relevant only when financial account information is part of the breach.

[6]A fraud alert is a mechanism that signals to credit issuers who obtain credit reports on a consumer that they must take reasonable steps to verify the consumer's identity before issuing credit, making it harder for identity thieves to secure new credit lines. It should be noted that, although fraud alerts can help prevent fraudulent credit accounts from being opened in an individual's name, they also can delay that individual's own legitimate attempts to secure credit.

[7]State laws vary with respect to usability and cost issues, which individuals will need to consider before deciding to place a credit freeze.

[8]A variety of factors may influence a service member's decision to place an active duty

the agency should notify the bank or other entity that handles that particular transaction for the agency.

Agencies may take two other significant steps that can offer additional measures of protection – especially for incidents where the compromised information presents a risk of new accounts being opened – but which will involve additional agency expense. First, in recent years, some companies have developed technologies to analyze whether a particular data loss appears to be resulting in identity theft. This data breach analysis may be a useful intermediate protective action, especially where the agency is uncertain about whether the identity-theft risk warrants implementing more costly additional steps such as credit monitoring (see below) or where the risk is such that agencies wish to do more than rely on the individual action(s) identified above.

For two reasons, such technology may be useful for incidents involving data for large numbers of individuals. First, the cost of implementing credit monitoring (and the potential to have spent large sums unnecessarily if no identity theft materializes) can be substantial for large incidents because the cost of credit monitoring generally is a function of the number of individuals for whom credit monitoring is being provided. Second, subsequent to any large data breach that is reported publicly, it is likely that an agency will get reports of identity theft directly from individuals in the affected class. Yet, agencies should be aware that approximately 3.6% of the adult population reports itself annually as the victim of some form of identity theft. Thus, for any large breach, it is statistically predictable that a certain number of the potential victim class will be victims of identity theft through events *other than* the data security breach in question. Data-breach monitoring of the type described here can assist an agency in determining whether the particular incident it has suffered is truly a source of identity theft, or whether, instead, any such reports are the normal by-product of the roue i8.0006 Tcw[t-product6rts arw[TJ12qJ1134.2( )]being prng cryp0012 Tcstag Tctll in 0 56 Tw[affch)Tj12

[9]Various credit-monitoring services provide different features and their offerings are constantly evolving. Therefore, agencies may wish to consult with OMB or the FTC concerning the most current, available options.

have been offered in many cases of large data breaches.[1010]

[10]In some instances, monitoring services may even be provided at no cost. Agencies should check the GSA contract schedule.

1. ***Timing***: The notice should be provided in a timely manner, but without compounding the harm from the initialinirom(diate n a)-0.5(nn1he i8hTJetialin07 Tc-19.46c(Timing)Tj/TThe ha5f)3.9(eorceann

[11] There may be other reasons related to law enforcement or national security that dictate that notice not be given to those who are affected. For example, if an agency suffers a breach of a database containing law enforcement sensitive data, immediate notification to potentially affected individuals may be inappropriate – even if the risk of identity theft resulting from that breach is significant – as such notification may result in the disclosure of law enforcement-sensitive or counter-terrorism data.

3. ***Contents***

[12]Agencies may receive updated addresses as a mailer by becoming a direct licensee of the Postal Service or by using a USPS licensed NCOA Link service provider. A current list of service providers is available at http://ribbs.usps.gov/files/ncoalink/CERTIFIED%5FLICENSEES/. For information on address-update and delivery-validation services, contact the USPS at 1-800-589-5766.

[13] As this Task Force has been charged with considering the federal response to identity theft, this routine use notice does not include all possible triggers, particularly those associated with the Privacy Act, such as embarrassment or harm to reputation. However, after consideration of the Strategic Plan and the work of other groups charged with assessing Privacy

Subsection (e)(11) of the Privacy Act requires that agencies publish a Federal Register notice of any new routine use at least 30 days prior to its use and "provide an opportunity for interested persons to submit written data, views, or arguments to the agency." 5 U.S.C. § 552a(e)(11). Additionally, subsection (r) of the Act requires that an agency provide Congress and OMB with

ATTACHMENT C

Text of Amendments to 18 U.S.C. §§ 3663(b) and 3663A(b)

(a) Section 3663 of Title 18, United States Code, is amended by:

(1) Deleting "and" at the end of paragraph (4) of subsection (b);

(2) Deleting the period at the end of paragraph (5) of subsection (b) and inserting in lieu thereof "; and"; and

(3) Adding the following after paragraph (5) of subsection (b):

> "(6) in the case of an offense under sections 1028(a)(7) or 1028A(a) of this title, pay an amount equal to the value of the victim's time reasonably spent in an attempt to remediate intended or actual harm incurred from the offense.".

Make conforming changes to the following:

(b) Section 3663A of Title 18, United States Code, is amended by:

(1) Adding the following after Section 3663A(b)(4)

> "(5) in the case of an offense under this title, section 1028(a)(7) or 1028A(a), pay an amount equal to the value of the victim's time reasonably spent in an attempt to remediate intended or actual harm incurred from the offense.".