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,

modeled after the attached "routine use" recently drafted by the Department of Justice, that would facilitate the disclosure of information in the course of responding to a breach of federal data.

Improved Authentication Methods

Recommendation 5: 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 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

Recommendation 6: To allow identity theft victims to recover for the value of time they spend in attempting to remediate the harms suffered, the Task Force recommends 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.

LAW ENFORCEMENT

Recommendation 7: 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 is 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, the FTC, with support from the Task Force, will 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.

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 restricting the unnecessary use of SSNs, offering guidance on potential substitutes that would be of equal use to the agencies but of no use to identity thieves, and establishing greater consistency when the use of SSNs is unavoidable.

Recommendation 3: To limit the unnecessary use in the public sector of SSNs, the most valuable consumer information for identity thieves, the Task Force recommends the following:

Recommendation 3a: OPM should accelerate its review of the use of SSNs in its collection of human resource data from agencies and on OPM-based papers and electronic forms, and take steps to eliminate, restrict, or conceal their use (including the assignment of employee identification numbers, where practicable). If necessary to implement this recommendation, Executive Order 9397, effective 11/23/1943, which requires federal agencies to use SSNs in "any system of permanent account numbers pertaining to individuals," should be partially rescinded.

It should also be noted that steps are already being taken to facilitate implementation of this recommendation. This month, each OPM program office designated staff to review the use of SSNs in that office, and OPM is prepared to complete its inventory of forms, procedures, and systems that currently display SSNs by October 13, 2006. This new inventory will be the basis for OPM's actions to change, eliminate, or mask the use of SSNs on OPM approved/authorized forms.

Recommendation 3b: 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 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 on the use of SSNs. The policy would include instructions on when SSNs can be displayed, when SSNs must be masked in employee records, and when SSNs must be masked on human resource and payroll system computer screens. The policy could be drafted by November 1, 2006 and would be issued by May 2007, following internal coordination and comment by agencies. OPM would then be prepared to work with the various human resource and payroll systems to implement the changes required by any new policy, with a phased-in implementation expected to take up to 18 months to complete.

Recommendation 3c: OMB should require all federal agencies to review their use of SSNs to determine the circumstances under which such use can be eliminated, restricted, or concealed in agency business processes, systems, and paper and electronic forms, other than those authorized or approved by OPM.

Already, OMB has developed a survey instrument to be in a position to implement this recommendation, which OMB could issue to all agencies this year. To add to this effort, and to ensure consistency, the Task Force will identify factors that agencies should take into consideration in determining whether the use of the SSN is essential to the agency's mission and necessary to ensure program integrity or to maintain national security. The Task Force will also evaluate the availability of practical alternatives to use of the SSN.

4. Publication of a "Routine Use" for Disclosure of Information Following a Breach

A federal agency's ability to respond quickly and effectively in the event of a breach of sensitive personal data is critical to its efforts to prevent or minimize any consequent harms. An effective response may include disclosure of information regarding the breach to those individuals affected by it. Similarly, expeditiously notifying persons and entities in a position to cooperate (either by assisting in informing affected individuals or by actively preventing or minimizing harms from the breach) will help mitigate consequences of a breach. However, the very information that may be most necessary to disclose to such persons and entities will often be information maintained by federal agencies that is subject to the Privacy Act of 1974, 5 U.S.C. § 552a. Critically, the Privacy Act prohibits the disclosure of any record in a system of records, by any means of communication to any person or agency, unless the subject individual has given written consent or unless the disclosure falls within one of twelve statutory exceptions. See 5 U.S.C. §§ 552a(b)(1)-(12).

To address this issue, federal agencies could, in accordance with the Privacy Act exception set forth in subsection § 552a(b)(3), publish a "routine use" that specifically permits the disclosure of information in connection with response and remedial efforts in the event of a data breach. Such

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" recently drafted by the Department of Justice, that would facilitate the disclosure of information to other agencies, entities, and persons in the course of responding to a breach of federal data.[1]

Improved Authentication Methods

5. Developing Alternate Means of Authenticating Identities

In addition to its widespread use by government, the SSN is used throughout the private sector. In particular, the SSN often is used for the dual purposes of identification (to match individuals to records of their information) and authentication (to prove that individuals are who they say they are).[2] Two factors combine to heighten the risk of identity theft: the ready availability of SSNs to identity thieves as a result of their ubiquitous use, and the SSN's use as a sole or primary means of authenticating individuals to open new accounts or obtain other benefits.

---

[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 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. The FTC estimated in 2003, based on the results of its Identity Theft Survey Report, that the average identity theft victim spends 30 hours resolving the problems created by identity theft. Those individuals who were victimized most seriously (from both the false opening of new accounts in their names *and* the unauthorized use of their validly-issued credit cards) spent an average of 60 hours resolving the problems. Overall, according to the survey, approximately 297 million hours were expended in one year by consumers attempting to resolve identity theft-related problems.[3]

[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,

While restitution is available for direct pecuniary costs of identity theft offenses, the federal restitution statutes, 18 U.S.C. § § 3663(b) and 3663A(b), do not provide for compensation for this time spent by consumers rectifying accounts and avoiding more harm. Moreover, courts have interpreted the restitution statutes in such a way that would likely preclude the recovery of such amounts from criminal defendants, absent explicit statutory authorization.

In order to better remediate the harm caused by identity theft, the Department of Justice has drafted amendments to the restitution statutes, reproduced in Attachment C, that would allow a victim to obtain restitution from a criminal defendant for the time reasonably spent trying to rectify the consequences of the offense. Under these proposed amendments, the district court judge would determine the amount of time reasonably spent and the value of the victim's time. The Department of Justice can propose that Congress adopt these amendments immediately.

Recommendation 6: The Task Force recommends that Congress amend the criminal restitution statutes, 18 U.S.C. §§ 3663(b) and 3663A(b), based on the attached proposal developed by the Department of Justice, 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.

LAW ENFORCEMENT

7. Development of a Universal Police Report

Victims of identity theft often need police reports documenting the misuse of their information in order to recover fully from the effects of the crime. For example, identity theft victims can use a detailed police report as an "identity theft report" under the Fair and Accurate Credit Transactions Act to request that fraudulent information on their credit report be blocked, or to obtain a seven-year fraud alert on their credit file. Further, identity theft victims also must have a police report to obtain documents relating to fraudulent applications and transactions, and creditors may require a police report before establishing the victim's *bona fides* in challenging a fraudulent account or purchase. Filing a police report also makes it more likely that law enforcement will pursue an investigation of the identity theft.

Some victims report, however, that they are unable to get a police report. FTC complaint data show that during the last three years, about 25% of victims of new-account fraud who sought police reports were not able to obtain them, in part because of overtaxed local police departments and the time involved in preparing what often can be a highly detailed document. Simplifying the process of writing and receiving a police report would both relieve the burden on local law enforcement and allow victims to more easily repair the damage to their credit from the crime. A universal law enforcement report that the victim could complete online and take to the local police department would help achieve this goal. Additionally, the data from such standardized reports would be in a

---

granting consumers new rights and tools for remediating the consequences of identity theft.

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

Given the volume of personal information appropriately collected to carry out myriad government functions, it is almost inevitable that some agencies will, on occasion, lose control of such information. Thus, an important first step in responding to a breach is for agencies to engage in advance planning for this contingency. We therefore recommend that each agency identify in advance a core management group that will be convened upon the identification of a potential loss of personal information. This core group would initially evaluate the situation to help guide any further response. Our experience suggests that such a core group should include, at minimum, an agency's chief information officer, chief legal officer, chief privacy officer (or their designees), a senior management official from the agency, and the agency's inspector general (or equivalent or designee). Such a group should ensure that the agency has brought together many of the basic competencies needed to respond, including expertise in information technology, legal authorities, the Privacy Act, and law enforcement. We recommend that this core group convene at least annually to review this memorandum and discuss likely actions should an incident occur.

III. Identifying an Incident That Presents Identity Theft Risk and the Level of Risk Involved

A loss of control over personal information, may, but need not necessarily, present a risk of identity theft. For example, a data report showing the name "John Smith," with little or no further identifying information related to John Smith, presents little or no risk of identity theft. Thus, the first steps in considering whether there is a risk of identity theft, and hence whether an "identity theft response" is necessary, are understanding the kind of information most typically used to commit identity theft and then determining whether that kind of information has been potentially compromised in the incident being examined. Because circumstances will differ from case to case, agencies should draw upon law enforcement expertise, including that of the agency Inspector General, in assessing the risk of identity theft from a data compromise and the likelihood that the incident is the result of or could lead to criminal activity.

An SSN standing alone can generate identity theft. Combinations of information can have the same effect. With a name, address, or telephone number, identity theft becomes possible, for instance, with any of the following: (1) any government-issued identification number (such as a driver's license number if the thief cannot obtain the SSN); (2) a biometric record; (3) a financial account number, together with a PIN or security code, if a PIN or security code is necessary to access the account; or (4) any additional, specific factor that adds to the personally identifying profile of a specific individual, such as a relationship with a specific financial institution or membership in a club. For further purposes of this memorandum, information posing a risk of identity theft will be described as "covered information." If a particular data loss or breach does not involve this type of

information, the identity theft risk is minimal, and it is unlikely that further steps designed to address identity theft risks are necessary.[2]

Even where covered information has been compromised, various other factors should be considered in determining whether the information accessed could result in identity theft. Our experience suggests that in determining the level of risk of identity theft, the agency should consider not simply the data that was compromised, but all of the circumstances of the data loss, including

- how easy or difficult it would be for an unauthorized person to access the covered information in light of the manner in which the covered information was protected;[3]
- the means by which the loss occurred, including whether the incident might be the result of a criminal act or is likely to result in criminal activity;[4]
- the ability of the agency to mitigate the identity theft;[5] and
- evidence that the compromised information is actually being used to commit identity theft.

---

[2]OMB has promulgated guidance requiring certain notifications within the government, most notably to the United States Computer Emergency Readiness Team (US-CERT), whenever personal information is compromised, and which applies even where there is no identity theft risk. That reporting guidance remains in full effect.

[3]For example, information on a computer laptop that is adequately protected by encryption is less likely to be accessed, while "hard copies" of printed-out data are essentially unprotected.

[4]For example, as a general matter, the risk of identity theft is greater if the covered information was stolen by a thief who was targeting the data (such as a computer hacker) than if the information was inadvertently left unprotected in a public location, such as in a briefcase in a hotel lobby. Similarly, in some cases of theft, the circumstances might indicate that the data-storage device, such as a computer left in a car, rather than the information itself, was the target of the theft. An opportunistic criminal, of course, may exploit information once it comes into his possession, and this possibility must be considered when fashioning an agency response, along with the recognition that risks vary with the circumstances under which incidents occur. In making this assessment, it is crucial that federal law enforcement (which may include the agency's Inspector General) be consulted.

[5]The ability of an agency or other affected entities to monitor for and prevent attempts to misuse the covered information can be a factor in determining the risk of identity theft. For example, if the compromised information relates to disability beneficiaries, the agency can monitor its beneficiary database for requests for change of address, which may signal attempts to misuse the information, and take steps to prevent the fraud. Likewise, alerting financial institutions in cases of a data breach involving financial account information can allow them to monitor for fraud or close the compromised accounts.

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.
- Monitor their financial account statements and immediately report any suspicious or unusual activity to their financial institution.
- Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. It might take a few months for most signs of fraudulent accounts to appear on the credit report, and this option is most useful when the data breach involves information that can be used to open new accounts. Consumers are entitled by law to obtain one free credit report per year from each of the three major credit bureaus – Equifax, Experian, and TransUnion – for a total of three reports every year. The annual free credit report can be used by individuals, along with the free report provided when placing a fraud alert (which is discussed below), to self-monitor for identity theft. The annual report also can be used as an alternative for those individuals who want to check their credit report, but do not want to place a fraud alert. Contact information for the credit bureaus should be provided, which can be found on the FTC's website.
- Place an initial fraud alert[6] on credit reports maintained by the three major credit bureaus noted above. This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. After placing an

[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.

initial fraud alert, individuals are entitled to a free credit report, which they should obtain beginning a few months after the breach and review for signs of suspicious activity.

- For residents of states in which state law authorizes a credit freeze, consider placing a credit freeze on their credit file.[7] This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. A credit freeze cuts off third party access to a consumer's credit report, thereby effectively preventing the issuance of new credit in the consumer's name.
- For deployed members of the military, consider placing an active duty alert on their credit file.[8] This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. Such active duty alerts serve a similar function as initial fraud alerts, causing creditors to be more cautious in extending new credit. However, unlike initial fraud alerts, they last for one year instead of 90 days. In addition, active duty alerts do not entitle the individual to a free credit report. Therefore, those placing an active duty alert should combine this option with a request for obtaining the annual free credit reports to which all individuals are entitled.
- Review resources provided on the FTC identity theft website, www.ftc.gov/idtheft. The FTC maintains a variety of consumer publications providing comprehensive information on breaches and identity theft.
- Be aware that the public announcement of the breach could itself cause criminals engaged in fraud, under the guise of providing legitimate assistance, to use various techniques, including email or the telephone, to deceive individuals affected by the breach into disclosing their credit card numbers, bank account information, SSNs, passwords, or other sensitive personal information. One common such technique is "phishing," a scam involving an email that appears to come from a bank or other organization that asks the individual to verify account information, and then directs him to a fake website whose only purpose is to trick the victim into divulging his personal information. Advice on avoiding such frauds is available on the FTC's web site http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt166.htm.

B. Actions that Agencies Can Take

If the breach involves government-authorized credit cards, the agency should notify the issuing bank promptly. If the breach involves individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government employee salaries, or any benefit payment,

---

[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 alert–for example, if there are stateside family members who need easy credit access, the alert would likely be counterproductive.

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 routine incidence of identity theft.

Second, and typically at great expense, agencies may wish to provide credit-monitoring services. Credit monitoring is a commercial service that can assist individuals in early detection of instances of identity theft, thereby allowing them to take steps to minimize the harm (although credit monitoring cannot guarantee that identity theft will not occur). A credit-monitoring service typically notifies individuals of changes that appear in their credit report, such as creation of a new account or new inquiries to the file.[9]

In deciding whether to offer credit monitoring services and of what type and length, agencies should consider the seriousness of the risk of identity theft arising from the data breach. Particularly important are whether incidents have already been detected and the cost of providing the service. Such costs can be substantial, although rates are often subject to negotiation; bulk purchase discounts

[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.[10] The length of time for which the service is provided may have an impact on cost as well. In addition, the agency should consider the characteristics of the affected individuals. Some affected populations may have more difficulty in taking the self-protective steps described earlier. For example, there may be groups who, because of their duties or their location, may warrant special protection from the distraction or effort of self-monitoring for identity theft.

Agencies should also be aware that, to assist the timely implementation of either data breach analysis or credit monitoring, the General Services Administration (GSA) is putting in place several government-wide contracting methods to provide these services if needed. Thus, an agency's contract officer, working with GSA, should be able promptly to secure such services and to develop cost estimates associated with such services.

Finally, it is important to note that notification to law enforcement is an important way for an agency to mitigate the risks faced by the potentially affected individuals. Because an agency data breach may be related to other breaches or other criminal activity, the agency's Inspector General should coordinate with appropriate federal law enforcement agencies to enable the government to look for potential links and to effectively investigate and punish criminal activity that may result from, or be connected to, the breach.

V. Implementing a Response Plan: Notice to Those Affected

Having identified the level of risk and bearing in mind the steps that can be taken by the agency or individual to limit that risk, the agency should then move to implement a response plan that incorporates elements of the above. Agencies should bear in mind that notice and the response it can generate from individuals is not "costless," a consideration that can be especially important where the risk of identity theft is low. The costs can include the financial expense and inconvenience that can arise from canceling credit cards, closing bank accounts, placing fraud alerts on credit files, and/or obtaining new identity documents. The private sector and other government agencies also incur costs in servicing these consumer actions. Moreover, frequent public notices of such incidents may be counterproductive, running the risk of injuring the public and, by making it more difficult to distinguish between serious and minor threats, causing citizens to ignore all notices, even of incidents that truly warrant heightened vigilance. Thus, weighing all the facts available, the risks to consumers caused by the data security breach warrant notice when notice would facilitate appropriate remedial action that is likely to be justified given the risk.

Assuming that an agency has made the decision to provide notice to those put at risk, agencies should incorporate the following elements into that notification process:

---

[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 initial incident through premature announcement based on incomplete facts or in a manner likely to make identity theft more likely to occur as a result of the announcement. While it is important to notify promptly those who may be affected so that they can take protective steps quickly, false alarms or inaccurate alarms are counterproductive. In addition, sometimes an investigation of the incident (such as a theft) can be impeded if information is made public prematurely. For example, an individual who has stolen a password-protected laptop in order to resell it may be completely unaware of the nature and value of the information the laptop contains. In such a case, public announcement may actually alert the thief to what he possesses, increasing risk that the information will be misused. Thus, officials should consult with those law enforcement officials investigating the incident (which could include the agency's Inspector General) regarding the timing and content of any announcement, before making any public disclosures about the incident. Indeed, even when the decision has been made to notify affected individuals, under certain circumstances, law enforcement may need a temporary delay before such notice is given to ensure that a criminal investigation can be conducted effectively or for national security reasons. Similarly, if the data breach resulted from a failure in a security or information system, that system should be repaired and tested before disclosing details related to the incident.[11]

2. ***Source***: Given the serious security and privacy concerns raised by data breaches, notification to individuals affected by the data loss should be issued by a responsible official of the agency, or, in those instances in which the breach involves a publicly known component of an agency, a responsible official of the component.

There may be some instances in which notice of a breach may appropriately come from an entity other than the actual agency that suffered the loss. For example, when the data security breach involves a federal contractor operating a system of records on behalf of the agency or a public-private partnership (for example, a federal agency/private-sector agreement to operate a program that requires the collection of covered information on members of the public), the responsibility for complying with these notification procedures should be established with the contractor or partner prior to entering the business relationship. Additionally, a federal agency that suffers a breach involving personal information may wish to determine, in conjunction with the regulated entity from which it obtained the information, whether notice is more appropriately given by the agency or by the regulated entity. Whenever possible, to avoid creating confusion and anxiety, the actual notice should come from the entity which the affected individuals are reasonably likely to perceive as the entity with which they have a relationship. In all instances, the agency is responsible for ensuring that its contractor or partner promptly notifies the agency of any data loss it suffers.

---

[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***: The substance of the notice should be reduced to a stand-alone document and written in clear, concise, and easy-to-understand language, capable of individual distribution and/or posting on the agency's website and other information sites. The notice should include the following elements:

- a brief description of what happened;
- to the extent possible, a description of the types of personal information that were involved in the data security breach (e.g., full name, SSN, date of birth, home address, account number, disability code, etc.);
- a brief description of what the agency is doing to investigate the breach, to mitigate losses, and to protect against any further breaches;
- contact procedures for those wishing to ask questions or learn additional information, including a toll-free telephone number, website, and/or postal address;
- steps individuals should take to protect themselves from the risk of identity theft (see above for the steps available), including steps to take advantage of any credit monitoring or other service the agency intends to offer and contact information for the FTC website, including specific publications.

Given the amount of information needed to give meaningful notice, an agency may want to consider providing the most important information up front, with the additional details in a Frequently Asked Questions (FAQ) format or on its website. If an agency has knowledge that the affected individuals are not English speaking, notice should also be provided in the appropriate language(s).

4. ***Method of Notification***: Notification should occur in a manner calibrated to ensure that the individuals affected receive actual notice of the incident and the steps they should take. First-class mail notification to the last known mailing address of the individual should be the primary means by which the agency provides notification. Even when an agency has reason to doubt the continued accuracy of such an address or lacks an address, mailed notice may still be effective. The United States Postal Service (USPS) will forward mail to a new address for up to one year, or will provide an updated address via established processes.[12] Moreover, certain agencies, such as the Social Security Administration and the Internal Revenue Service, may sometimes possess address information that can be used to facilitate effective mailing. The notice should be sent separately from any other mailing so that it stands out to the recipient. If using another agency to facilitate mailing as referenced above, agencies should take care that the agency that suffered the loss is identified as the sender, not the facilitating agency.

---

[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.

Substitute means of notice such as broad public announcement through the media, website announcements, and distribution to public service and other membership organizations likely to have access to the affected individual class, should be employed to supplement direct mail notification or if the agency cannot obtain a valid mailing address. Email notification is discouraged, as the affected individuals could encounter difficulties in distinguishing the agency's email from a "phishing" email.

The agency also should give special consideration in providing notice to individuals who are visually or hearing impaired consistent with Section 504 of the Rehabilitation Act of 1973. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large-type notice on the agency's web site.

5. ***Preparing for follow-on inquiries***: Those notified can experience considerable frustration if, in the wake of an initial public announcement, they are unable to find sources of additional accurate information. Agencies should be aware that the GSA has a stand-by capability through its "USA Services" operation to quickly put in place a 1-800-FedInfo call center staffed by trained personnel and capable of handling individual inquiries for circumstances in which the number of inquiries is likely to exceed the agency's native capacity. Thus, agencies may wish to consider briefly delaying a public announcement to allow them to implement a consolidated announcement strategy, as opposed to a hasty public announcement without any detailed guidance on steps to take. Such a strategy will permit public statements, website postings, and a call center staffed with individuals prepared to answer the most frequently asked questions all to be made simultaneously available.

6. ***Prepare counterpart entities that may receive a surge in inquiries***: Depending on the nature of the incident, certain entities, such as the credit-reporting agencies or the FTC, may experience a surge in inquiries also. For example, in incidents involving a substantial number of SSNs (e.g., more than 10,000), notifying the three major credit bureaus allows them to prepare to respond to requests from the affected individuals for fraud alerts and/or their credit reports. Thus, especially for large incidents, an agency should inform the credit bureaus and the FTC of the timing and distribution of any notices, as well as the number of affected individuals, in order to prepare.

ATTACHMENT B

Proposed Routine Use Language

Subsection (b)(3) of the Privacy Act provides that information from an agency's system of records may be disclosed without a subject individual's consent if the disclosure is "for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section." 5 U.S.C. § 552a(b)(3). Subsection (a)(7) of the Act states that "the term 'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." 5 U.S.C. § 552a(a)(7). A routine use to provide for disclosure in connection with response and remedial efforts in the event of a breach of federal data would certainly qualify as such a necessary and proper use of information – a use that is in the best interest of both the individual and the public.

Subsection (e)(4)(D) of the Privacy Act requires that agencies publish notification in the Federal Register of "each routine use of the records contained in the system, including the categories of users and the purpose of such use." 5 U.S.C. § 552a(e)(4)(D). The Department of Justice has developed the following routine use that it plans to apply to its Privacy Act systems of records, and which allows for disclosure to appropriate agencies, entities, and persons under the following circumstances:[13]

> when (1) it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Agencies should already have a published system of records notice for each of their Privacy Act systems of records. To add a new routine use to an agency's existing systems of records, an agency must simply publish a notice in the Federal Register amending its existing systems of records to include the new routine use.

---

[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 Act considerations, OMB may determine that a combined identity theft/Privacy Act routine use may be preferable.

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 "adequate advance notice" of any proposal to make a "significant change in a system of records." 5 U.S.C. § 552a(r). OMB has stated that the addition of a routine use qualifies as a significant change that must be reported to Congress and OMB and that such notice is to be provided at least 40 days prior to the alteration. See Appendix I to OMB Circular No. A-130 – Federal Agency Responsibilities for Maintaining Records About Individuals, 61 Fed. Reg. 6435, 6437 (Feb. 20, 1996). Once a notice is prepared for publication, the agency would send it to the Federal Register, OMB, and Congress, usually simultaneously, and the proposed change to the system (i.e., the new routine use) would become effective 40 days thereafter. See id. at 6438 (regarding timing of systems of records reports and noting that notice and comment period for routine uses and period for OMB and congressional review may run concurrently). Recognizing that each agency likely will receive different types of comments in response to its notice, the Task Force recommends that OMB work to ensure accuracy and consistency across the range of agency responses to public comments.

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.".