crash computers, or knock computers off of the Internet using a denial of service attack. Some cyber-criminals extort companies, however, without explicitly threatening to cause damage to computers. Instead, they steal confidential data and then threaten to make it public if their demands are not met. In other cases, the criminal causes the damage first—such as by accessing a corporate computer without authority and encrypting critical data—and then threatens not to correct the problem unless the victim pays. Thus, the requirement in section 1030(a)(7) that the defendant must explicitly "threaten to cause damage" can preclude successful prosecutions for cyber-extortion under this statute under certain circumstances.

d. Sentencing Guidelines Governing Identity Theft

In recent years, the courts have created some uncertainty about the applicability of the "multiple victim enhancement" provision of the U.S. Sentencing Guidelines in identity theft cases. This provision allows courts to increase the sentence for an identity thief who victimizes more than one person. It is unclear, however, whether this sentencing enhancement applies when the victims have not sustained actual monetary loss. For example, in some jurisdictions, when a financial institution indemnifies 20 victims of unauthorized charges to their credit cards, the courts consider the financial institution to be the only victim. In such cases, the identity thief therefore may not be penalized for having engaged in conduct that harmed 20 people, simply because those 20 people were later indemnified. This interpretation of the Sentencing Guidelines conflicts with a primary purpose of the Identity Theft and Assumption Deterrence Act of 1998: to vindicate the interests of individual identity theft victims.[79]

RECOMMENDATION: CLOSE THE GAPS IN FEDERAL CRIMINAL STATUTES USED TO PROSECUTE IDENTITY-THEFT RELATED OFFENSES TO ENSURE INCREASED FEDERAL PROSECUTION OF THESE CRIMES

The Task Force recommends that Congress take the following legislative actions:

- **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.** Proposed amendments to 18 U.S.C. §§ 1028 and 1028A are available in Appendix E.

- **Add Several New Crimes to the List of Predicate Offenses for Aggravated Identity Theft Offenses.** The aggravated identity theft statute, 18 U.S.C. § 1028A, should include other federal offenses that recur in various identity-theft and fraud cases—mail theft, uttering counterfeit securities, and tax fraud, as well as conspiracy to commit specified felonies already listed in 18 U.S.C. § 1028A—in the statutory list of predicate offenses for that offense. Proposed additions to 18 U.S.C. § 1028A are contained in Appendix E.

- **Amend the Statute That Criminalizes the Theft of Electronic Data By Eliminating the Current Requirement That the Information Must Have Been Stolen Through Interstate Communications.** The proposed amendment to 18 U.S.C. § 1030(a)(2) is available in Appendix F.

- **Penalize Malicious Spyware and Keyloggers.** The statutory provisions in 18 U.S.C. § 1030(a)(5) should be amended to penalize appropriately the use of malicious spyware and keyloggers, by eliminating the current requirement that the defendant's action must cause "damage" to computers and that the loss caused by the conduct must exceed $5,000. Proposed amendments to 18 U.S.C. §§ 1030(a)(5), (c), and (g), and the accompanying amendment to 18 U.S.C. § 2332b(g), are included in Appendix G.

- **Amend the Cyber-Extortion Statute to Cover Additional, Alternate Types of Cyber-Extortion.** The proposed amendment to 18 U.S.C. § 1030(a)(7) is available in Appendix H.

RECOMMENDATION: ENSURE THAT AN IDENTITY THIEF'S SENTENCE CAN BE ENHANCED WHEN THE CRIMINAL CONDUCT AFFECTS MORE THAN ONE VICTIM

The Sentencing Commission should amend 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. This amendment will ensure that courts can enhance the sentences imposed on identity thieves who cause harm to multiple victims, even when that harm does not result in any monetary loss to the victims. The proposed amendment to United States Sentencing Guideline section 2B1.1 is available in Appendix I.

5. TRAINING OF LAW ENFORCEMENT OFFICERS AND PROSECUTORS

Training can be the key to effective investigations and prosecutions, and much has been done in recent years to ensure that investigators and prosecutors have been trained on topics relating to identity theft. In addition to ongoing training by U.S. Attorney's Offices, for example, several federal law enforcement agencies—including DOJ, the Postal Inspection Service, the Secret Service, the FTC, and the FBI—along with the American Association of Motor Vehicle Administrators (AAMVA) have sponsored jointly over 20 regional, one-day training seminars on identity fraud for state and local law enforcement agencies across the country. See Volume II, Part O, for a description of training by and for investigators and prosecutors.

Nonetheless, the amount, focus, and coordination of law enforcement training should be expanded. Identity theft investigations and prosecutions involve particular challenges—including the need to coordinate with foreign authorities, some difficulties with the application of the Sentencing Guidelines, and the challenges that arise from the inevitable gap in time between the commission of the identity theft and the reporting of the identity theft—that warrant more specialized training at all levels of law enforcement.

RECOMMENDATION: ENHANCE TRAINING FOR LAW ENFORCEMENT OFFICERS AND PROSECUTORS

- **Develop Course at National Advocacy Center (NAC) Focused Solely on Investigation and Prosecution of Identity Theft.** By the third quarter of 2007, DOJ's Office of Legal Education should complete the development of a course specifically focused on identity theft for prosecutors. The identity theft course should include, among other things: a review of the scope of the problem; a review of applicable statutes, forfeiture and sentencing guideline applications; an outline of investigative and case presentation techniques; training on addressing the unique needs of identity theft victims; and a review of programs for better utilizing collective resources (working groups, task forces, and any "model programs"— fast track programs, etc.).

- **Increase Number of Regional Identity Theft Seminars.** In 2006, the federal agencies and the AAMVA held a number of regional identity theft seminars for state and local law enforcement officers. In 2007, the number of seminars should be increased. Additionally, the participating entities should coordinate with the Task Force to provide the most complete, targeted, and up-to-date training materials.

- **Increase Resources for Law Enforcement Available on the Internet.** The identity theft clearinghouse site, *www.idtheft.gov*, should be used as the portal for law enforcement agencies to gain access to additional educational materials on investigating identity theft and responding to victims.

- **Review Curricula to Enhance Basic and Advanced Training on Identity Theft.** By the fourth quarter of 2007, federal investigative agencies should review their own training curricula, and curricula of the Federal Law Enforcement Training Center, to ensure that they are providing the most useful training on identity theft.

6. MEASURING SUCCESS OF LAW ENFORCEMENT EFFORTS

One shortcoming in the federal government's ability to understand and respond effectively to identity theft is the lack of comprehensive statistical data about the success of law enforcement efforts to combat identity theft. Specifically, there are few benchmarks that measure the activities of the various components of the criminal justice system in their response to identity thefts occurring within their jurisdictions, little data on state and local enforcement, and little information on how identity theft incidents are being processed in state courts.

Addressing these questions requires benchmarks and periodic data collection. The Bureau of Justice Statistics (BJS) has platforms in place, as well as the tools to create new platforms, to obtain information about identity theft from victims and the response to identity theft from law enforcement agencies, state and federal prosecutors, and courts.

RECOMMENDATION: ENHANCE THE GATHERING OF STATISTICAL DATA MEASURING THE CRIMINAL JUSTICE SYSTEM'S RESPONSE TO IDENTITY THEFT

- **Gather and Analyze Statistically Reliable Data from Identity Theft Victims.** The BJS and FTC should continue to gather and analyze statistically reliable data from identity theft victims. The BJS should conduct its surveys in collaboration with subject matter experts from the FTC. BJS should add additional questions on identity theft to the household portion of its National Crime Victimization Survey (NCVS), and conduct periodic supplements to gather more in-depth information. The FTC should conduct a general identity theft survey approximately every three years, independently or in conjunction with BJS or other government agencies. The FTC also should conduct surveys focused more narrowly on issues related to the effectiveness of and compliance with the identity theft-related provisions of the consumer protection laws it enforces.

- **Expand Scope of National Crime Victimization Survey (NCVS).** The scope of the annual NCVS should be expanded to collect information about the characteristics, consequences, and extent of identity theft for individuals ages 12 and older. Currently, information on identity theft is collected only from the household respondent and does not capture data on multiple victims in the household or multiple episodes of identity theft.

- **Review of Sentencing Commission Data.** DOJ and the FTC should systematically review and analyze U.S. Sentencing Commission identity theft-related case files every two to four years, and should begin in the third quarter of 2007.

- **Track Prosecutions of Identity Theft and the Amount of Resources Spent.** In order to better track resources spent on identity theft cases, DOJ should, by the second quarter of 2007, create an "Identity Theft" category on the monthly report that is completed by all Assistant United States Attorneys, and should revise its departmental case tracking application to allow for the reporting of offenses by individual subsections of section 1028. Additionally, BJS should incorporate additional questions in the National Survey of Prosecutors to better understand the impact identity theft is having on prosecutorial resources.

- **Conduct Targeted Surveys.** In order to expand law enforcement knowledge of the identity theft response and prevention activities of state and local police, BJS should undertake new data collections in specified areas. Proposed details of those surveys are included in Appendix J.

IV. Conclusion: The Way Forward

There is no magic bullet that will eradicate identity theft. To successfully combat identity theft and its effects, we must keep personal information out of the hands of thieves; take steps to prevent an identity thief from misusing any data that may end up in his hands; prosecute him vigorously if he succeeds in committing the crime; and do all we can to help the victims recover.

Only a comprehensive and fully coordinated strategy to combat identity theft—one that encompasses effective prevention, public awareness and education, victim assistance, and law enforcement measures, and that fully engages federal, state, and local authorities and the private sector—will have any chance of solving the problem. This proposed strategic plan strives to set out such a comprehensive approach to combating identity theft, but it is only the beginning. Each of the stakeholders—consumers, business and government—must fully and actively participate in this fight for us to succeed, and must stay attuned to emerging trends in order to adapt and respond to developing threats to consumer well being.

Appendices

APPENDIX A

Identity Theft Task Force's Guidance Memorandum on Data Breach Protocol

September 19, 2006

MEMORANDUM FROM THE IDENTITY THEFT TASK FORCE

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

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.

1. 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.

Considering these factors together should permit the agency to develop an overall sense of where

---

[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.

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[8] 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 initial fraud alert, individuals are entitled to a free credit report, which they should

[8]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.

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.[3] 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.[4] 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.

---

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

[4] 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.

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, 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.*

---

*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.

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 have been offered in many cases of large data breaches.[39] 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.

---

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

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:

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

---

[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.

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.

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.[17] 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

[17] 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.

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.

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.

APPENDIX 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). The Office of Management and Budget, which pursuant to subsection (v) of the Privacy Act has guidance and oversight responsibility for the implementation of the Act by federal agencies, has advised that the compatibility concept encompasses (1) functionally equivalent uses, and (2) other uses that are necessary and proper. 52 Fed. Reg. 12,990, 12,993 (Apr. 20, 1987). In recognition of and in accordance with the Act's legislative history, OMB in its initial Privacy Act guidance stated that "[t]he term routine use . . . recognizes that there are corollary purposes 'compatible with the purpose for which [the information] was collected' that are appropriate and necessary for the efficient conduct of government and in the best interest of both the individual and the public." 40 Fed. Reg. 28,948, 28,953 (July 9, 1975). 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 as follows:[80]

> To appropriate agencies, entities, and persons when (1) the Department suspects or has 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 made to such agencies, entities, and persons is 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.

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.

APPENDIX C

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

Proposed Language:

(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.".

Section Analysis

These new subsections provide that defendants may be ordered to pay restitution to victims of identity theft and aggravated identity theft for the value of the victim's time spent remediating the actual or intended harm of the offense. Restitution could therefore include an amount equal to the value of the victim's time spent clearing a victim's credit report or resolving charges made by the perpetrator for which the victim has been made responsible.

New subsections 3663(b)(6) and 3663A(b)(5) of Title 18 would make clear that restitution orders may include an amount equal to the value of the victim's time spent remediating the actual or intended harm of the identity theft or aggravated identity theft offense. The federal courts of appeals have interpreted the existing provisions of Section 3663 in such a way that would likely preclude the recovery of such amounts, absent explicit statutory authorization. For example, in *United States v. Arvanitis*, 902 F.3d 489 (7th Cir. 1990), the court held that restitution ordered for offenses resulting in loss of property must be limited to recovery of property which is the subject of the offenses, and may not include consequential damages. Similarly, in *United States v. Husky*, 924 F.2d 223 (11th Cir. 1991), the Eleventh Circuit held

that the list of compensable expenses in a restitution statute is exclusive, and thus the district court did not have the authority to order the defendant to pay restitution to compensate the victim for mental anguish and suffering. Finally, in *United States v. Schinnell*, 80 F.3d 1064 (5th Cir. 1996), the court held that restitution was not allowed for consequential damages involved in determining the amount of loss or in recovering those funds; thus, a victim of wire fraud was not entitled to restitution for accounting fees and costs to reconstruct bank statements for the time period during which the defendant perpetuated the scheme, for the cost of temporary employees to reconstruct monthly bank statements, and for the costs incurred in borrowing funds to replace stolen funds. These new subsections will provide statutory authority for inclusion of amounts equal to the value of the victim's time reasonably spent remediating the harm incurred as a result of the identity theft offense.

APPENDIX D

Text of Amendments to 18 U.S.C. §§ 2703, 2711 and 3127, and Text of New Language for 18 U.S.C. § 3512

The basis for these proposals is set forth in Section III.2 of the strategic plan, which describes coordination with foreign law enforcement.

Proposed Language:

§ 2703. Required disclosure of customer communications or records

(a) **Contents of wire or electronic communications in electronic storage.**—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ~~by a court with jurisdiction over the offense under investigation~~ ***by a court of competent jurisdiction*** or an equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) **Contents of wire or electronic communications in a remote computing service.**—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ~~by a court with jurisdiction over the offense under investigation~~ ***by a court of competent jurisdiction*** or equivalent State warrant; ***or***

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(c) **Records concerning electronic communication service or remote computing service.**—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ~~by a court with jurisdiction over the offense under investigation~~ ***by a court of competent jurisdiction*** or equivalent State warrant;

§ 2711. Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system; and

(3) the term "court of competent jurisdiction" ~~has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation~~ ***means—***

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that–

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or

(iii) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants.

§ 3127. Definitions for chapter

As used in this chapter—

(1) the terms "wire communication", "electronic communication", "electronic communication service", and "contents" have the meanings set forth for such terms in section 2510 of this title;

(2) the term "court of competent jurisdiction" means—

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals ~~having jurisdiction over the offense being investigated~~ *that*–

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of electronic communication service is located;

(iii) is in or for a district in which a landlord, custodian, or other person subject to 3124(a) or (b) is located; or

(iv) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

§ 3512. Foreign requests for assistance in criminal investigations and prosecutions:

(a) Upon application of an attorney for the government, a Federal judge may issue such orders as may be necessary to execute a request from a foreign authority for assistance in the investigation or prosecution of criminal offenses, or in proceedings related to the prosecution of criminal offenses including but not limited to proceedings regarding forfeiture, sentencing, and restitution. Such orders may include the issuance of a search warrant as provided under Rule 41 of the Federal Rules of Criminal Procedure, a warrant or order for contents of stored wire or electronic communications or for records related thereto as provided under 18 U.S.C. § 2703, an order for a pen register or trap and trace device as provided under 18 U.S.C. § 3123, or an order requiring the appearance of a person for the purpose of providing testimony or a statement, or requiring the production of documents or other things, or both.

(b) In response to an application for execution of a request from a foreign authority as described in subsection (a), a Federal judge may also issue an order appointing a person to direct the taking of testimony or statements or of the production of documents or other things, or both. A person so appointed may be authorized to –

(1) issue orders requiring the appearance of a person, or the production of documents or other things, or both;

(2) administer any necessary oath; and

(3) take testimony or statements and receive documents or other things.

(c) Except as provided in subsection (d), an application for execution of a request from a foreign authority under this section may be filed –

(1) in the district in which a person who may be required to appear resides or is located or in which the documents or things to be produced are located;

(2) in cases in which the request seeks the appearance of persons or production of documents or things that may be located in multiple districts, in any one of the districts in which such a person, documents or things may be located; or

(3) in any case, the district in which a related Federal criminal investigation or prosecution is being conducted, or in the District of Columbia.

(d) An application for a search warrant under this section, other than an application for a warrant issued as provided under 18 U.S.C. § 2703, must be filed in the district in which the place or person to be searched is located.

(e) A search warrant may be issued under this section only if the foreign offense for which the evidence is sought involves conduct that, if committed in the United States, would be considered an offense punishable by imprisonment for more than one year under federal or state law.

(f) Except as provided in subsection (d), an order or warrant issued pursuant to this section may be served or executed in any place in the United States.

(g) This section does not preclude any foreign authority or an interested person from obtaining assistance in a criminal investigation or prosecution pursuant to 28 U.S.C. § 1782.

(h) As used in this section –

(1) the term "foreign authority" means a foreign judicial authority, a foreign authority responsible for the investigation or prosecution of criminal offenses or for proceedings related to the prosecution of criminal offenses, or an authority designated as a competent authority or central authority for the purpose of making requests for assistance pursuant to an agreement or treaty with the United States regarding assistance in criminal matters; and

(2) the terms "Federal judge" and "attorney for the Government" have the meaning given such terms for the purposes of the Federal Rules of Criminal Procedure.

APPENDIX E

Text of Amendments to 18 U.S.C. §§ 1028 and 1028A

The basis for these proposed amendments is set forth in Section III.D.4.a of the strategic plan, which describes gaps in the identity theft statutes.

Proposed Amendment to Aggravated Identity Theft Statute to Add Predicate Offenses

Congress should amend the aggravated identity theft offense (18 U.S.C. § 1028A) to include other federal offenses that recur in various identity-theft and fraud cases, specifically, mail theft (18 U.S.C. § 1708), uttering counterfeit securities (18 U.S.C. § 513), and tax fraud (26 U.S.C. §§ 7201, 7206, and 7207), as well as conspiracy to commit specified felonies already listed in section 1028A—in the statutory list of predicate offenses for that offense (18 U.S.C. § 1028A(c)).

Proposed Additions to Both Statutes to Include Misuse of Identifying Information of Organizations

(a) Section 1028(a) of Title 18, United States Code, is amended by inserting in paragraph (7) the phrase "(including an organization as defined in Section 18 of this Title)" after the word "person".

Section 1028A(a) of Title 18, United States Code, is amended by inserting in paragraph (1) the phrase "(including an organization as defined in Section 18 of this Title)" after the word "person".

(b) Section 1028(d)(7) of Title 18, United States Code, is amended by inserting in paragraph (7) the phrase "or other person" after the word "individual".

Rationale:

Corporate identity theft whereby criminals assume the identity of corporate entities to cloak fraudulent schemes in a misleading and deceptive air of legitimacy have become rampant. Criminals routinely engage in unauthorized "appropriation" of legitimate companies' names and logos in a variety of contexts: misrepresenting themselves as officers or employees of a corporation, sending forged or counterfeit documents or financial instruments to victims to improve their aura of legitimacy, and offering nonexistent benefits (e.g., loans and credit cards) in the names of companies.

One egregious example of corporate identity theft is represented on the Internet by the practice commonly known as "phishing," whereby criminals electronically assume the identity of a corporation in order to defraud unsuspecting recipients of email solicitations to voluntarily disclose identifying and financial account information. This personal information is then used to further the underlying criminal scheme—for example, to

scavenge the bank and credit card accounts of these unwitting consumer victims. Phishing is just one example of how criminals in mass-marketing fraud schemes incorporate corporate identity theft into their schemes, though phishing also is designed with individual identity theft in mind.

Phishing has become so routine in many major fraud schemes that no particular corporation can be easily singled out as having suffered a special "horror story" which stands above the rest. In August 2005, the "Anti-Phishing Working Group" determined in just that month alone, there were 5,259 unique phishing websites around the world. By December 2005, that number had increased to 7,197, and there were 15,244 unique phishing reports. It was also reported in August 2005, that 84 corporate entities' names (and even logos and web content) were "hijacked" (i.e., misused) in phishing attacks, though only 3 of these corporate brands accounted for 80 percent of phishing campaigns. By December 2005 the number of victimized corporate entities had increased to 120. The financial sector is and has been the most heavily targeted industry sector in phishing schemes, accounting for nearly 85 percent of all phishing attacks. *See, e.g. http://antiphishing.org/apwg_phishing_activity_report_august_05.pdf.*

In addition, major companies have reported to the Department of Justice that their corporate names, logos, and marks are often being misused in other types of fraud schemes. These include telemarketing fraud schemes in which communications purport to come from legitimate banks or companies or offer products or services from legitimate banks and companies, and West African fraud schemes that misuse legitimate banks and companies' names in communications with victims or in counterfeit checks.

Uncertainty has arisen as to whether Congress intended Sections 1028(a)(7) and 1028A(a) of Title 18, United States Code to apply only to "natural" persons or to also protect corporate entities. These two amendments would clarify that Congress intended that these statute apply broadly and may be used against phishing directed against victim corporate entities.