Consumers Union
Consumer Federation of America
Privacy Rights Clearinghouse
World Privacy Center
U.S. PIRG

September 26, 2006

Ms. Lydia Parnes
Mr. Ronald Tenpas
Executive Directors
Task Force on Identity Theft
By email

Dear Ms. Parnes and Mr. Tenpas,

We were very interested to see announcement of the Interim Recommendations of the Identity Theft Task Force, which has been asked to determine how to improve the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution. As the Executive Directors of the Identity Theft Task Force formed by the President, we ask you to present to the Task Force several additional recommendations for inclusion in the Task Force's final report.

In brief, we suggest:

- Federal agencies should inform consumers about *all* of their identity theft rights, including the right under many state laws to place a security freeze.

- Federal agencies should be required to notify individuals of *all* data security breaches involving sensitive information.

- Agencies developing a universal police report should seek input from consumer and victim advocates on the contents of this form.

- Federal agencies other than the Social Security Administration should be required to stop using SSNs in a manner which causes this number to be printed on cards that individuals are likely to carry in their wallets. In addition, a process should be developed for independent review of other uses of SSNs by federal agencies.

- Federal agencies should do much more to reduce the collection and retention of sensitive personal data and to promote the security of the sensitive personal information they hold or use.

1. Federal agencies should inform consumers about *all* of their identity theft rights, including the right under many state laws to place a security freeze.

The Federal Trade Commission and other federal agencies who undertake to educate consumers about identity theft and data security should inform consumers of their state, as well as their federal, consumer rights. This includes information about the state right to place a security freeze restricting access to consumer reporting files.

Twenty five states have enacted laws giving consumers to right, and the choice, to place a "security freeze" on the individual's consumer reporting file at each major consumer reporting agency. These states contain far more than half the U.S. population. Twenty of the state security freeze laws make the choice to place a freeze available to all consumers, while the remaining handful restrict the use of the freeze to identity theft victims.[1]

A security freeze lets the consumer stop anyone from looking at his or her own credit reporting file for purposes of granting credit, and in most cases, opening other new accounts, unless the consumer chooses to let that particular business look at the consumer's information. When the consumer is not seeking to open a new account, the security freeze effectively prevents anyone else from doing so. Thus, the security freeze provides a much stronger preventative tool than the federal fraud alert process. Consumers Union regularly talks to consumers who think that they have a state security freeze, when in fact what they have is a federal fraud alert. The absence of information about state security freezes on the FTC's otherwise fairly comprehensive ID theft information pages may allow these misconceptions to continue.

At the time of that the Department of Veteran's Affairs announced a security breach involving a massive number of records about individual veterans, consumers residing in California, Connecticut, Louisiana, Maine, Nevada, New Jersey, and North Carolina had the right to place a security freeze on their credit files as a preventative measure. [2] However, they could not learn of this right from the VA's website, nor from the FTC's posted consumer information material. Businesses and universities who incur breaches may also send consumers to the FTC for more information, but that information will

---

[1] For more information about the security freeze, see:
http://www.consumersunion.org/campaigns//learn_more/001842indiv.html

[2] Since the VA breach, security freeze laws have gone into effect in Colorado, Delaware, and Kentucky, and Vermont law has been expanded to give the right to place a freeze to all consumers. Similar laws giving the choice to place a security freeze to all consumers have been passed but are not yet in effect in Utah and Wisconsin. These additional states provide the security freeze tool to consumers after they become victims of identity theft: Kansas, South Dakota, Texas, and Washington (WA covers victims including consumers with a security breach notice plus a police report). A new Illinois law changing from victims only to all consumers takes effect January 1, 2007. For information about specific state freeze laws, with links to instructions on how to place the freeze, see:
http://www.consumersunion.org/campaigns//learn_more/002355indiv.html

remain incomplete for many consumers if it continues to omit information about the state security freeze.

While the security freeze does have costs for many consumers, balanced information about what the freeze is, how it works, how it differs from other mechanisms, and the pros and cons of choosing to place a security freeze would be of undoubted value to U.S. consumers.

Consumers who receive information or assistance from any federal agency on identity theft should receive complete information about the steps that they can take, including the state security freeze.

2. The data breach guidance to agencies should require written individual notice to all individuals whose sensitive personal information has or is reasonably believed to have been accessed or acquired by an unauthorized person.

Studies show that only about half of consumers who are victimized by identity theft know how the thief acquired the sensitive personal information necessary to commit the theft. This suggests that security breaches of data held by private and public entities could be a significant contributor to the ID theft epidemic afflicting Americans.

It is essential that all entities, government and private, to whom individuals entrust their sensitive personal information keep that information safe through strong policies, vigorous supervision over the implementation of those polices and effective auditing mechanisms. Government and private entities that hold sensitive information about individuals should have strong security policies and see that those policies are effective, kept up to date and are rigorously followed.

A strong, “no loophole” requirement to notify all consumers of security breaches affecting records about them is an essential part of data security. A requirement that federal agencies tell individuals about every data security failure involving sensitive information should contribute to a political environment in which data security becomes and remains a high agency priority. Further, early notice should allow consumers the opportunity to take steps, such as placing a state security freeze, ordering a free credit report, or reading their statements more carefully, that may help them to avoid becoming victims of identity theft as a result of the breach. Waiting until all the facts are in about who accessed the data, and why, is too long of a delay.

There have been some proposals in other contexts for a so-called “risk based” approach to notice. This is the wrong approach. A risk based approach to notice would, at worst, promote “don’t know, don’t tell,” in which lack of information about nature of the risk posed by the breach may excuse notice. A risk based approach would allow an agency with a public relations incentive to downplay information about a breach by making a choice for the public about the public’s need to know. Such an approach would also deprive consumers of information at the earliest appropriate time. It would reduce the political incentive to have the kind of strong policies,

implementation, and oversight of security that will prevent or reduce the incidence of security breaches.

As the Task Force works to develop proposed guidance to federal agencies on notice of security breaches, it should follow the lead of states such as California, Illinois, Nevada, New York and Tennessee in requiring notice whenever there has been a security breach involving certain specific sensitive personal information of an individual, without any additional delays or "triggers" based on the perceived level of risk.

3. Consumer and victims' advocates should be consulted in the drafting of the universal police report form.

We are very pleased to see the Interim Recommendation to begin work toward a universal police report that would be widely accepted. This will be a major step forward for consumers. In preparing the universal police report form, it will be necessary to acknowledge that in many cases, the information available to the individual consumer who is a victim of identity theft can be quite sketchy. The form must be designed in such a way that it can be useful over a broad array of factual situations, and in circumstances where little is known about the crime, as well as in circumstances where more is known. The form should not require so much information that many victims will be unable to complete it. To reach these goals, the federal agencies working on the form should seek early and sustained input from consumer and other nonprofit organizations that work directly with ID theft victims. Input should also be sought from local law enforcement agencies and from state Attorneys General offices which provide victim information or assistance.

While every effort should be made to encourage wide acceptance of the universal report, federal agencies should not require, and should not permit private entities to require, the use of that report form. Since local police departments will ultimately decide whether to accept the form, consumers in local jurisdictions which choose not to use the report should not be penalized.

4. Federal agencies other than the Social Security Administration should be required to stop using SSNs in a manner which causes this number to be printed on cards that individuals are likely to carry in their wallets. In addition, a process should be developed for independent review of other uses of SSNs by federal agencies.

We strongly agree with the recommendation that the Office of Personnel Management expedite its review of federal use of SSNs of employees, and that the Office of Management and Budget encourage all federal agencies to review their use of Social Security Numbers. Reducing the use of SSNs by federal agencies is an important step, and may set useful standards for changes that private businesses should also make. However, the issue of nonessential use of SSNs is too important to be left to the sole discretion of those agencies which are already using these numbers. This is particularly

so when the SSN is printed on a card that consumers must ordinarily carry with them, such as a Medicare card or a military identification card.

Because of the way in which the Social Security Number is used in the granting of credit, the SSN has become the key to a consumer's financial front door. A thief who has a person's name and SSN is well-positioned to open new accounts for credit and services. New account identity theft can ruin a victim's credit record and deprive consumers of timely economic opportunities such as reasonably priced credit, jobs, and rental units. New account identity theft also imposes a daunting set of tasks to notify creditors, notify credit reporting agencies and dispute credit record information from unauthorized accounts. Federal agencies facilitate theft when they print an SSN on an identification card that consumers ordinarily must carry with them to access services or to enter their place of employment.

In addition to encouraging agencies to review their uses of the SSN, the Task Force should develop a mechanism to evaluate the need for continued use of SSNs by those agencies which decline to restrict their own use of these sensitive numbers. The Task Force should recommend a federal rule against the use of SSNs by federal agencies other than the Social Security Administration on any card issued by the agency and commonly carried by individuals, and should adopt a timeline to phase out all such existing uses. For uses of the SSN by federal agencies other than on wallet cards, the Task Force should create a process by which federal agencies must identify and justify those uses to an entity within the federal government outside of the agency. Under that process, each agency should be required to show that an existing use which it proposes to continue is essential and that there is no reasonable alternative to its use for reasons other than transition costs.

5. Much more should be done to reduce the collection and retention of sensitive personal information and to ensure effective federal agency protection of sensitive personal information.

The largest data breach so far in calendar year 2006 involved a government agency. Increasingly, data security breaches in both government and private entities appear to stem in part from lapses in the implementation of existing policies. It is essential that government agencies be held to a standard not only of having strong data protection polices, but also of ensuring that those policies are fully understood and consistently adhered to at every level of the agency. In addition, more attention should be given to reducing the collection and retention of sensitive personal information by federal agencies. Finally, attention should be given to steps to reduce the risk of human error in the protection of data, including decisions to reduce the amount of sensitive personal data initially collected, standard data purging to remove such data when it is no longer needed for the purpose for which it was originally collected, and technological mechanisms that prevent certain types of data from being copied or transmitted.

Conclusion

These recommendations, like the Task Force's charge, are focused on the federal government's activities. However, the issues of data privacy and data security reach beyond the federal government. In addition to improvements in federal practices, consumers need strong state and federal laws in the areas of data protection, notice and other obligations to consumers when there is a failure to protect sensitive data, and preventative tools including the security freeze.

Very truly yours,

Gail Hillebrand
Consumers Union
West Coast Office
1535 Mission St
San Francisco, CA 94103
(415) 431-6747

Beth Givens
Privacy Rights Clearinghouse

Pam Dixon
World Privacy Forum

Ed Mierzwinski
U.S. PIRG

Travis Plunkett
Consumer Federation of America