Federal Identity Theft Task Force
Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.
Washington, D.C.  20580

As Chair of the U.S. Public Policy Committee of the Association for Computing Machinery (USACM), I welcome the request for comments by the Federal Identity Theft Task Force. Identity theft is a growing trend affecting thousands of Americans each year. It requires a national discussion at the highest levels of government in order to devise appropriate policies to reduce its occurrence. Members of our committee have been involved in issues of digital identity, information security, cyber crime investigation, and other topics for many years. Recently I provided expert testimony before the committee investigating the 2006 Veterans' Administration data breach. Our experience and study has shown us that where identity theft is concerned, two major issues go hand in hand: computer security and privacy.

Well-publicized instances of personal data exposures and misuse have demonstrated the threat of identity theft and corresponding challenges to the adequate protection of privacy. Personal data -- including copies of video, audio, and other surveillance -- needs to be collected, stored, and managed appropriately throughout every stage of its use by all involved parties. However, protecting private, personal data requires more than simply ensuring effective data security. It requires approaching personal data as a steward rather than as a custodian.

As we have detailed in our statement on privacy (http://www.acm.org/usacm/Issues/Privacy.htm, and included with these comments), a holistic, proactive approach to ensuring privacy is necessary, and is an important part of helping minimize the risk of identity theft. This approach gives people more control over their personal data and has the salutary effect of enhancing the early discovery of identity theft. Following the guiding principles of data minimization, consent, openness, access, accuracy, security, and accountability and our associated recommendations will go a long way toward ensuring privacy of stored data and reducing the risk of identity theft. It would help make data custodians into data stewards.

## DATA SECURITY AND DATA BREACH NOTIFICATION POLICIES

A uniform national policy could harmonize company practices for protecting personal data across the United States, but such a policy, if it is not sufficient for protecting personal information, could also undermine consumer protection. We recommend that strong national standards be developed that are based on widely-accepted international data security standards. For example, ISO 17799 on information security management and ISO 18033 on data encryption are comprehensive and detailed security standards that have been adopted by the international community. These are the basis for developing data security plans, but ultimately any data security standards should be technology-neutral and based on the highest possible protections for personal data. Further, notification is often an effective method for ensuring that companies continually improve their security practices. Clearly if there is a breach, regardless of the risk to consumers, a company's security system should be hardened to deal with the vulnerabilities. A national breach notification standard could provide more transparency about ineffective or effective security practices. Last year Congress tried to establish a national breach standard based on varying degrees of risk. At that time, we expressed concern that a risk-based standard would not provide the level of transparency necessary to ensure protection of personal data. In short, implementing lowest common denominator standards for data security or notification is inefficient and raises the possibility of doing more harm than good.

## USE OF SOCIAL SECURITY NUMBERS

Regarding the use of Social Security numbers (SSNs) in data records, the use of SSNs is risky and can cause (and has caused) problems for protecting privacy and reducing identity theft. If they are to be used, there should be clear guidelines limiting and auditing access to this data. Furthermore, SSNs should be used only as an identifier, and not for authentication. Possession of a SSN is not enough to confirm, or authenticate, that a person is the individual assigned to that SSN. Simply because someone has a security pass (identification) does not mean that they are the person who was issued that security pass. They would be authenticated when an authorized agent confirmed that the person presenting the pass is the person assigned to that pass.

Another way to limit access to the SSN (and by extension minimize the risk of identity theft) would be to store the SSN in a separate file linked by some unique, generated number. This decreases the relative risk in holding SSN's in databases by placing it in a less-frequently accessed file, which can also have separate, more stringent, access controls than other personal information in the database. This same practice should apply to any substitutes for a SSN, if they are used in the same ways, and with the same frequency, that SSNs are currently used.

In addition to our recommendations on privacy, we are enclosing a fact sheet on identity and authentication. The general lack of understanding of these principles has indirectly led to many of the instances of identity theft and privacy exposure. We recommend that the Task Force be clear in its use of terms, and help to educate companies and government about these concepts.

## NATIONAL IDENTITY FILES

While the development of national identity files to help restore identity to victims of identity theft has a valuable policy goal in mind, it appears to pose the same kind of risks for identity theft faced by other databases. If this idea were to move forward, it should be limited to those individuals who have had their identities stolen already. Another concern is how to authenticate victims of identity theft over a long period of time.
As the attached fact sheet indicates, it can be difficult to authenticate people based on personal data. With such a system it is important to be very clear on the risks and resources involved, or these files may become another target for identity theft - a very tempting one as these files are intended to serve as the ultimate verification of identity.

Thank you for considering our views. The work of the Task Force is an important step toward increased efforts that help reduce identity theft and encourage more secure, private and reliable computer information. If USACM can provide any clarification to these comments, or answer any other technical questions, please do not hesitate to contact our Public Policy Director, Cameron Wilson, at 202-659-9711 or cameron_wilson@acm.org.

Sincerely,

Eugene Spafford, Ph.D.
Chair
U.S. Public Policy Committee of the Association for Computing Machinery

## About ACM and USACM

With over 80,000 members worldwide, The Association for Computing Machinery is an educational and scientific society focused on advancing computing as a science and a profession. USACM serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matter of U.S. public policy related to information technology.