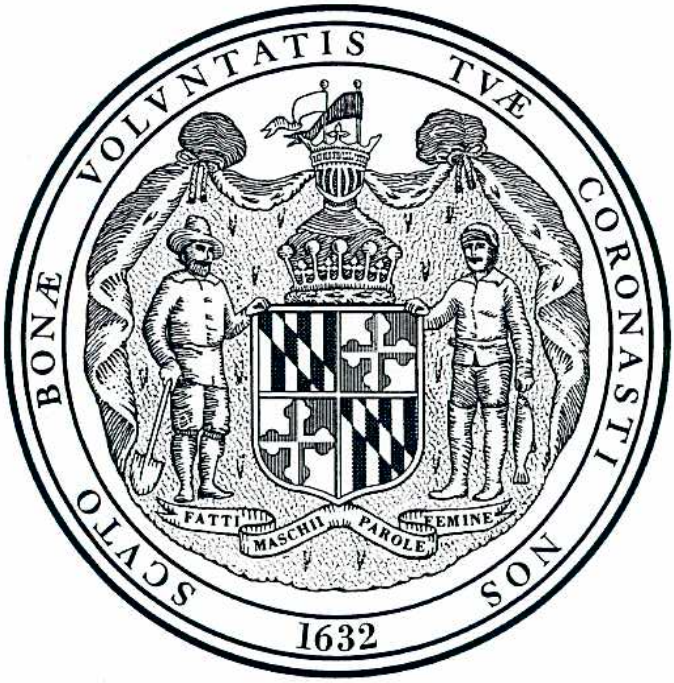
# Task Force to Study Identity Theft




Annapolis, Maryland
December 2007

**For further information concerning this document contact:**

Library and Information Services
Office of Policy Analysis
Department of Legislative Services
90 State Circle
Annapolis, Maryland 21401

Baltimore Area: 410-946-5400 • Washington Area: 301-970-5400
Other Areas: 1-800-492-7122, Extension 5400
TDD: 410-946-5401 • 301-970-5401
Maryland Relay Service: 1-800-735-2258
E-mail: libr@mlis.state.md.us
Home Page: http://mlis.state.md.us

MARYLAND GENERAL ASSEMBLY
TASK FORCE TO STUDY IDENTITY THEFT

December 31, 2007

The Honorable Martin J. O'Malley, Governor of the State of Maryland
The Honorable Thomas V. Mike Miller, Jr., President of the Senate
The Honorable Michael E. Busch, Speaker of the House of Delegates
The Honorable Members of the Maryland General Assembly

Ladies and Gentlemen:

The Task Force to Study Identity Theft was created by Chapters 241 and 242 of the Laws of Maryland of 2005 and was directed to (1) study the problems associated with identity theft in Maryland, including repairing one's credit history and the adequacy of current Maryland law in deterring identity theft, privacy laws in other states and at the federal level that address identity theft; (2) consult with relevant State and federal agencies and other experts on identity theft; (3) survey State agencies to determine compliance with State and federal laws relating to the collection and use of Social Security numbers; and (4) make recommendations regarding possible remedies to identity theft, including statutory changes.

Since all of the required appointments of members to the task force were not completed until late 2006, the task force was not able to schedule its first and organizational meeting until November 15, 2006. In its interim report, the task force recommended that, without an extension of its authority, there was insufficient time remaining to competently fulfill the investigative duties required under Chapters 241 and 242 before the date to report final findings and recommendations to the General Assembly (December 31, 2006) expired. The General Assembly, therefore, extended the authority of the task force an additional year, until December 31, 2007 (Chapters 9 and 10 of the Laws of Maryland of 2007).

The 21-member task force met six times between November 15, 2006, and December 6, 2007. At its meetings, the task force heard from several sources, including State and local agencies, federal agencies, business and consumer advocates, law enforcement, and citizens impacted by identity theft.



Room 110 Legislative Services Building · 90 State Circle · Annapolis, Maryland 21401-1991
410-946-5350 · Fax 410-946-5395 · TDD 410-946-5401
301-970-5350 · Fax 301-970-5395 · TDD 301-970-5401

This report describes the activities and statutory and nonstatutory recommendations of the task force. The task force intends to introduce legislation which encompasses a number of its recommendations in the 2008 session.

Sincerely,

Delores G. Kelley
Senate Co-chairman

Susan C. Lee
House Co-chairman

DGK:SCL/KDM/JJJ/ncs

MARYLAND GENERAL ASSEMBLY
TASK FORCE TO STUDY IDENTITY THEFT

# 2006 Roster

---

**Senator Ralph M. Hughes, Co-Chairman**
**Delegate Susan C. Lee, Co-Chairman**

**Senator**

Verna L. Jones

**Delegates**

Susan K. McComas

Doyle L. Niemann

**State, Business, and Consumer Members**

Steve M. Sakamoto-Wengel
*Office of the Attorney General*

John T. Kuo
*Motor Vehicle Administration*
*Maryland Department of Transportation*

Charles W. Turnbaugh
*Division of Financial Regulation*
*Department of Labor, Licensing, and Regulation*

Thomas (Tim) E. Hutchins
*Department of State Police*

Darrin E. Brown
*AARP Maryland*

Room 110 Legislative Services Building · 90 State Circle · Annapolis, Maryland 21401-1991
410-946-5350 · Fax 410-946-5395 · TDD 410-946-5401
301-970-5350 · Fax 301-970-5395 · TDD 301-970-5401

Isabel Mercedes Cumming
*Prince George's County State's Attorney's Office*
*Maryland State's Attorney's Association Representative*

Robert Davis
*Provident Bank*
*Commercial Bank Representative*

A. Marie Day
*Bank of America*
*Credit Card Industry Representative*

Douglas DeLeaver
*Maryland Transit Administration*
*Maryland Chiefs of Police Association Representative*

John Dennison
*Harford County Sherriff's Office*
*Maryland Sheriffs' Association Representative*

Eric Ellman
*Consumer Data Industry Association*
*Consumer Reporting Agency Representative*

Andy Galli
*Maryland Consumer Rights Coalition*
*Consumer Group or Agency Representative*

Johanna Neumann
*Maryland Public Interest Research Group*
*Consumer Group or Agency Representative*

Charles Sharrocks
*Client Network Services, Inc.*
*Technology-related Trade Representative*

Rodney Staatz
*State Employees Credit Union*
*Credit Union Representative*

Jeffrie Zellmer
*Maryland Retailers Association*
*Retail Industry Representative*

**Task Force Staff**

Karen D. Morgan
John J. Joyce

MARYLAND GENERAL ASSEMBLY
TASK FORCE TO STUDY IDENTITY THEFT

# 2007 Roster

**Senator Delores G. Kelley, Co-Chairman**
**Delegate Susan C. Lee, Co-Chairman**

**Senator**

Verna L. Jones

**Delegates**

Susan K. McComas

Doyle L. Niemann

**State, Business, and Consumer Members**

Steve M. Sakamoto-Wengel
*Office of the Attorney General*

John T. Kuo
*Motor Vehicle Administration*
*Maryland Department of Transportation*

Sarah Bloom Raskin
Commissioner of Financial Regulation
*Department of Labor, Licensing, and Regulation*

First Sgt. Robert Smolek
*Maryland State Police*

Henry Greenberg
*AARP Maryland*

Room 110 Legislative Services Building · 90 State Circle · Annapolis, Maryland 21401-1991
410-946-5350 · Fax 410-946-5395 · TDD 410-946-5401
301-970-5350 · Fax 301-970-5395 · TDD 301-970-5401

Isabel Mercedes Cumming
*Prince George's County State's Attorney's Office*
*Maryland State's Attorney's Association Representative*

Robert Davis
*Provident Bank*
*Commercial Bank Representative*

A. Marie Day
*Bank of America*
*Credit Card Industry Representative*

Lt. Douglas McManus
*Maryland Chiefs of Police Association Representative*

John Dennison
*Harford County Sherriff's Office*
*Maryland Sheriffs' Association Representative*

Eric Ellman
*Consumer Data Industry Association*
*Consumer Reporting Agency Representative*

Steve Hannan
*Maryland Consumer Rights Coalition*
*Consumer Group or Agency Representative*

Johanna Neumann
*Maryland Public Interest Research Group*
*Consumer Group or Agency Representative*

Charles Sharrocks
*Client Network Services, Inc.*
*Technology-related Trade Representative*

Rodney Staatz
*State Employees Credit Union*
*Credit Union Representative*

Jeffrie Zellmer
*Maryland Retailers Association*
*Retail Industry Representative*

**Task Force Staff**

Karen D. Morgan
John J. Joyce

# Contents

# Executive Summary

This report describes the activities and recommendations of the Task Force to Study Identity Theft. The task force has made recommendations for several specific pieces of legislation which will be introduced in the upcoming session, recommendations for nonstatutory steps to help in the fight against identity theft, and suggestions for additional study by the General Assembly.

The task force was created by Chapters 241 and 242 of the Laws of Maryland of 2005 and was directed to (1) study the problems associated with identity theft in Maryland, including repairing one's credit history and the adequacy of current Maryland law in deterring identity theft, privacy laws in other states and at the federal level that address identity theft; (2) consult with relevant State and federal agencies and other experts on identity theft; (3) survey State agencies to determine compliance with State and federal laws relating to the collection and use of Social Security numbers; and (4) make recommendations regarding possible remedies to identity theft, including statutory changes.

Since all of the required appointments of members to the task force were not completed until late 2006, the task force was not able to schedule its first, organizational meeting until November 15, 2006. The task force recommended that, without an extension of its authority, there was insufficient time remaining to competently fulfill the investigative duties required under Chapters 241 and 242 before the date to report final findings and recommendations to the General Assembly (December 31, 2006) expired. The General Assembly, therefore, extended the authority of the task force an additional year (Chapters 9 and 10 of the Laws of Maryland of 2007).

The task force met six times between November 15, 2006, and December 6, 2007. During its meetings, the task force heard from representatives from several relevant agencies and organizations, including the Federal Trade Commission, Federal Bureau of Investigation, U.S. Secret Service, Prince George's County State's Attorney Office, Montgomery County State's Attorney Office, Maryland State Police, Baltimore County Office of State's Attorney, Baltimore County Police Department – Economic Crimes Unit, U.S. Postal Inspection Service, Prince George's County Police Department, Visa USA, Inc., *Privacy Times*, Maryland Bankers Association, Maryland Retailers Association, Maryland Association of Bank Security, Department of Health and Mental Hygiene, Department of Human Resources, Maryland Department of Transportation – Motor Vehicle Administration, Office of Comptroller, Maryland Association of Counties, Maryland Municipal League, Maryland Chamber of Commerce, University System of Maryland, Maryland Independent College and University Association, Maryland Association of Community Colleges, Department of Budget and Management, and the American Civil Liberties Union, as well as consumer advocates and citizens impacted by identity theft issues. Detailed minutes from these meetings, as well as submitted written testimony, are included in this report.

The task force makes the following statutory recommendations to the General Assembly:

***Increased Penalties*:** Based on the recommendations from several law enforcement personnel, business organizations, citizens, and other witnesses, the task force unanimously urges that the penalties for identity fraud be increased and expanded. **The task force specifically recommends that the penalty for felony identity fraud be increased from a maximum 5 to 15 years imprisonment and from $25,000 to $50,000 fine.** Implementing this recommendation would make the felony penalties for identity fraud commensurate with the felony penalties for credit card fraud. In addition, the task force urges that the same penalty be imposed upon a person who commits identity fraud while serving as a "fiduciary" for the victim. Although an individual who is acting as a fiduciary may be affiliated with a financial or other type of institution, the penalty would apply to the individual who commits the offense. The task force also recommends the enhanced penalty if a person commits identity fraud against a "vulnerable adult." Finally, the task force recommends a similarly enhanced penalty for a person convicted of identity fraud who has been convicted of identity fraud on a prior occasion not arising from the same incident. A copy of the legislation that implements this task force recommendation (LR1088/1089) is provided in the Appendices.

***Witness Affidavits and Admissibility of Business Records:*** The task force received several recommendations, particularly from State's Attorneys, for reforms of the rules of evidence to improve the prosecution of identity fraud cases. **The task force recommends that witness affidavits for identity fraud be authorized and that business records be authenticated by the account holder.** The task force endorses legislation that (1) makes personal bank records, business bank records, personal credit card reports, business credit card reports, personal credit card statements, business credit card statements, personal credit card notices, and business credit card notices admissible as evidence and presumed to be authentic if the account holder testifies as to their authenticity in a judicial or administrative proceeding; and (2) adds the crime of identity fraud to the list of offenses for which an affidavit sworn to by a lawful credit cardholder may be introduced as substantive evidence that the credit card or credit card number was taken, used, or possessed without the authorization of the credit cardholder, if at least 10 days before a proceeding at which the State intends to introduce the affidavit, notice is given to the defendant and the defendant fails within 5 days of the proceeding to make a written demand to require the presence of the affiant as a prosecution witness. A copy of the legislation that implements these task force recommendations (LR1172) is provided in the Appendices.

***Unauthorized Possession of Mail:*** **The task force members unanimously recommend that legislation be passed prohibiting a person in Maryland from knowingly and willfully removing, taking, possessing, obtaining, or receiving mail under certain circumstances without the permission of the United States Postal Service or the intended recipient.** This legislation was suggested by the U.S. Postal Service and is similar to House Bill 293 that was introduced in the 2007 session. A copy of the legislation that implements this task force recommendation (LR1127/1128) is provided in the Appendices.

***Credit Card Skimming Devices and Reencoders:*** **The task force recommends that Maryland join 28 other states in making the unauthorized possession and use of certain devices known as "skimmers" and "reencoders" illegal.** The bill would prohibit the unauthorized possession and use of skimming devices that access, read, memorize, or otherwise obtain payment device numbers or personal identifying information. The bill would also prohibit the use of a reencoder to place information encoded on the magnetic strip or stripe of a credit card onto the magnetic strip or stripe of a different credit card or use any other electronic medium that allows such a transaction to occur without the consent of the individual authorized to use the credit card. Penalties would be the same as those for other identity fraud, *i.e.,* if the amount stolen has a value of over $500, the offense would be a felony with the possibility of 5 years imprisonment or a $25,000 fine or both and, if less than $500, a misdemeanor, with the possibility of 18 months imprisonment or a fine of $5,000 or both. A copy of the legislation that implements this task force recommendation (LR1170) is provided in the Appendices.

***Forfeiture:*** **The task force recommends legislation, which was strongly recommended by law enforcement agencies, that would enable a court to order the forfeiture of all property a criminal convicted of identity fraud obtained from the crime.** The task force did not reach full agreement on the details of a specific bill. The task force, however, does unanimously recommend that identity fraud forfeiture legislation be enacted that allows for due process, and fully protects lien holders while allowing for at least part of the proceeds from forfeiture to be distributed to the victims of identity theft.

Since identity fraud offenders are not required to forfeit the proceeds of their crimes, they are able to keep the cash obtained from their crimes or retain the valuables obtained and convert them to cash. After convicted offenders have completed their sentences, they are able to return to society in an advanced financial position. Thus, not only can those offenders who are not apprehended benefit from committing this crime, even those who are convicted can benefit financially. In contrast, victims are left to repair what is left of their finances, often spending additional time and money to do so. While the task force did not have sufficient time to specify the provisions of a forfeiture bill, the task force unanimously believes that forfeiture legislation is necessary to provide much needed justice to the victims of identity fraud.

The task force also makes the following nonstatutory recommendations to the General Assembly:

***Identity Theft Training of Local Law Enforcement Agencies by the Office of Attorney General:*** Based on a need demonstrated by testimony from citizens and law enforcement representatives, **the task force recommends that the Office of the Attorney General develop and provide training in identity theft record and case development to local police departments and State's Attorneys offices.** The task force recommends that the training may be offered through the Internet or other electronic means to save on costs.

***State and Local Agencies:*** Noting a variety of policies and procedures at the State agency and local government level, **the task force recommends that the General Assembly study the feasibility and costs of establishing additional standards for State and local agencies**

**regarding personal information security.** The study should include further review of the information that is collected and the purposes for which it is collected.

***REAL ID Act:*** The task force received testimony concerning the REAL ID Act and its impact on identity fraud. This Act, passed by Congress in 2005, sets standards for state driver's licenses and federally compliant identity cards. To enforce the uniform standards, proposed supporting federal regulations would prevent the use of noncompliant IDs for airline flights, access to federal facilities, and other purposes set by the Department of Homeland Security (DHS). The task force heard testimony that REAL ID would cost almost $50 million for Maryland to implement, with no reimbursement expected from the federal government. Also, the task force heard testimony concerning the increased danger to the security of personal information under REAL ID, and the lack of safeguards under the Act.

Finally, of concern to the task force was a recent unsatisfactory audit of the Motor Vehicle Administration (MVA), which would be charged with implementing the Real ID program. The task force was informed that the MVA was confident that it could implement the program successfully and that, in response to the many concerns that had been raised, new regulations from DHS would be forthcoming by February 2008. At the time of the task force's final work session, however, no details of the revised regulations were available. **The task force (with a dissenting vote by the MVA representative), therefore, cautions the General Assembly to delay action on the implementation of the REAL ID Act until the new regulations are promulgated and the relevant standing committees have had the opportunity to be briefed and to review them.**

***Limits on the Storage of Transaction Information by Retailers:*** The task force reviewed legislation that was recently passed in Minnesota prohibiting retailers from retaining personal information taken from credit and debit cards for any longer than the amount of time required to process the transaction. No action was taken on this issue.

# Task Force to Study Identity Theft

## Introduction

This report describes the activities and recommendations of the Task Force to Study Identity Theft. The first part of the report summarizes the establishment of the task force. The second part describes the work of the task force, including its process and sources of information. In the Appendices are copies of legislation that implements many of the task force's statutory recommendations, which will be introduced in the 2008 session. The remainder of the Appendices include copies of the enabling legislation, supporting documentation, and written testimony submitted to the task force.

### Establishment of the Task Force

The Task Force to Study Identity Theft was created by Chapters 241 and 242 of the Laws of Maryland of 2005 and was directed to (1) study the problems associated with identity theft in Maryland, including repairing one's credit history and the adequacy of current Maryland law in deterring identity theft, privacy laws in other states and at the federal level that address identity theft; (2) consult with relevant State and federal agencies and other experts on identity theft; (3) survey State agencies to determine compliance with State and federal laws relating to the collection and use of Social Security numbers; and (4) make recommendations regarding possible remedies to identity theft, including statutory changes.

The enabling legislation directed that the task force consist of the following members:

- two members of the Senate of Maryland, appointed by the President of the Senate;
- three members of the House of Delegates, appointed by the Speaker of the House;
- the Attorney General, or the Attorney General's designee;
- the Superintendent of State Police, or the Superintendent's designee;
- the Commissioner of Financial Regulation;
- the Administrator of the Motor Vehicle Administration, or the administrator's designee;
- the following members, appointed by the Governor:
    - one representative of the Maryland State's Attorneys' Association;
    - one representative of the Maryland Chiefs of Police Association;
    - one representative of the Maryland Sheriffs' Association;
    - one representative of a State-chartered commercial bank or a national banking association with a branch office in the State; and
    - one representative of a State-chartered credit union;

- the following members appointed jointly by the President of the Senate and the Speaker of the House:

  - one representative from the retail industry;
  - one representative from the credit card industry;
  - one representative from a consumer reporting agency;
  - three representatives who are affiliated with a recognized consumer group or agency in the State; and
  - one representative who is affiliated with a technology-related trade group or association in the State.

The President of the Senate was charged with designating one of the members appointed from the Senate of Maryland as co-chair of the task force.

The Speaker of the House was charged with designating one of the members appointed from the House of Delegates as co-chair of the task force.

The Department of Legislative Services was charged with providing staff for the task force.

Since all of the required appointments of members to the task force were not completed until late 2006, the task force was not able to schedule its first, organizational meeting until November 15, 2006. In its interim report, the task force recommended that, without an extension of its authority, there was insufficient time remaining to competently fulfill the investigative duties required under Chapters 241 and 242 before the date to report final findings and recommendations to the General Assembly (December 31, 2006) expired. The General Assembly, therefore, extended the authority of the task force an additional year, until December 31, 2007 (Chapters 9 and 10 of the Laws of Maryland of 2007).

# Work of the Task Force

The 21-member task force met six times between November 15, 2006, and December 6, 2007. At its meetings, the task force heard from several sources, including State and local agencies, federal agencies, business and consumer advocates, law enforcement, and citizens impacted by identity theft. What follows is the detailed report from each of those meetings.

## Session I – Wednesday, November 15, 2006

The task force held its first meeting on November 15, 2006, at which organizational matters were discussed. At this first meeting, task force members introduced themselves and discussed their perspectives on the issue of identity theft.

Co-chairman Susan Lee presented a list of issues on which the task force should focus as it undertakes its work. The issues presented were:

- the scope, extent of the problem, and types of crimes of identity theft in Maryland;

- overview and effectiveness of current Maryland laws, regulations, and policies in deterring, preventing, investigating, and prosecuting crimes of identity theft; review of proposed and enacted privacy and identity theft related legislation in other states and the federal government, including proposed and enacted legislation relating to credit freezes and notification of personal data and information breaches;

- current coordination of local, State, and federal law enforcement agencies in fighting identity theft, including an overview of current law enforcement policies and procedures on, in response to, and reporting of crimes of identity theft and types of assistance rendered to victims;

- overview and examination of policies, procedures, and practices relating to custody, use, disclosure, and distribution of Social Security numbers (SSNs) by State agencies and private entities, including the effectiveness of current laws and policies, procedures, and practices by those entities in protecting individuals' SSNs;

- review of the policies and practices of data collection agencies, credit reporting companies, financial institutions, and other institutions in collecting, using, distributing, transferring, and protecting personal data and information, including the rights of consumers in protecting and accessing their personal information; and

- overview of federal and State relief and remedies available to identity theft victims in restoring their credit reports and ratings, regaining their personal identities, and avoiding arrest for crimes committed in their names; proactive steps Marylanders must take to protect themselves against crimes of identity theft.

Staff then provided a presentation on identity theft. The presentation covered:

- the national incidences and Maryland incidences of identity theft;

- those states and cities with the highest incidences of identity theft and the Maryland jurisdictions with the highest incidences;

- the primary federal laws that address identity theft;

- proposed federal legislation under consideration to further address identity theft;

- an overview of laws that address identity theft enacted by the 50 states;

- a summary of the purpose of security notification laws and credit freeze laws and information on which states had adopted these laws; and

- a summary of the Maryland laws that address privacy, the use of SSNs, prohibit identity fraud, establish the duties of consumer credit reporting agencies, prevent dissemination of false or misleading information through electronic mail, and require policies for the custody of personal information by State agencies.

The chairmen then explained the rationale for asking for an extension of the task force until December 31, 2007, and asked staff to present a draft bill which, with the approval of the task force, would be submitted. The draft would extend the task force and require a report on or before December 31, 2007. After staff explained the provisions that would be included in the extension, the chairmen asked the task force to approve the submission of the draft as a bill during the 2007 session. The task force unanimously approved extending the task force and the submission of the bill which would do so. The task force submitted an interim report containing the recommendation for continuation to the Governor and the leadership of the General Assembly on December 20, 2006. The interim report is contained in the Appendices.

During the 2007 session, Senate Bill 70 and House Bill 26 were introduced by the task force chairmen. They were enacted as Chapters 9 and 10 of 2007. The bills retained the composition of the task force and duties as originally established and extended the task force until January 31, 2008. A final report is required by December 31, 2007.

## Session II – Wednesday, August 22, 2007

To survey State agencies to determine their compliance with State and federal laws on the collection and use of Social Security numbers (SSNs), the task force held its second session on August 22, 2007, on the topic of "State Custody of Social Security Numbers and Other Personal Information."

Due to the time constraints within which the task force operated, the task force did not attempt to query every State agency about this issue. Not every State agency deals with SSNs in ways that impact the public significantly. Instead, the task force opted to query those State agencies that request SSNs and other personal information not only from State employees, but from large numbers of State citizens. The Department of Budget and Management provided information about its oversight and coordinative role regarding the management of SSNs and other personal information from all other Executive Branch agencies.

To further illuminate this important issue, the task force asked the National Conference of State Legislatures (NCSL) to provide information on the laws enacted by all states relating to disclosure of SSNs. NCSL provided information on state legislation enacted from 2002 to 2006. That information is contained in the Appendices. Various selected State agencies and associations participated and were asked to provide information on the following issues:

- How many records containing SSNs and other personal information are maintained? For what purpose is this information collected and used?

- What policies and practices govern when and how SSNs are requested?

- What policies and practices govern the personnel who have access to SSNs and other personal information and under what circumstances these individuals are permitted access?

- What procedures and practices are in place to ensure that access to SSNs and other personal information is limited to only those personnel who need the information to perform their job duties?

- What policies and practices govern how long SSNs and other personal information are kept and how the information is disposed of when no longer needed?

- How could policies, procedures, and practices be improved to protect SSNs and other personal information and limit or prevent unauthorized disclosures?

## Department of Health and Mental Hygiene

The Department of Health and Mental Hygiene (DHMH), represented by Jim Johnson, Deputy Secretary of Operations; Geneva Sparks, Deputy State Registrar Vital Records Administration; and Charles Lehman, Executive Director of Operations and Eligibility, Medicaid Administration presented information in response to the task force's questions.

DHMH provides a variety of public services that require it to collect personal information. DHMH provided a list of programs that have personal information requirements or SSNs, totaling over 13 million such records. Of these, the Division of Vital Records (DVR) alone keeps 10,320,000 birth, death, marriage, and divorce records on paper within its office. The Maryland Medicaid Program has a total of 2,001,256 open and closed records as of the date of the hearing. Such records are required for a variety of reasons depending on the program or service being provided, including the identification of records, the determination of eligibility for programs, tracking diseases, and billing. DHMH cited federal (*e.g.*, Health Insurance Portability and Accountability Act (HIPAA)) and State (*e.g.*, Maryland Records Privacy Act) privacy laws and regulations that govern access to information. Each program indicated that access to records is "limited by job function." DVR, following guidelines established by the department's Office of Human Resources, has all new hires fingerprinted for criminal background checks. Most programs reported a requirement that personnel sign a confidentiality statement acknowledging responsibility for adhering to standards of confidentiality. Records that include SSNs can be kept indefinitely (*e.g.*, birth and death records collected by DVR). For auditing purposes, DVR maintains applications for certificates for a minimum of two years, although these do not contain SSNs.

During the question and answer period after presentation of testimony, DVR emphasized that it has an urgent need to implement an electronic vital records system and is in the process of doing so. Space limitations within its offices currently prevent all records from being stored in the vault. DVR has tried to balance the need for security with its goal of providing good customer service, which requires staff to have ready access to all records. DVR hopes to implement an automated electronic vital record system by January 2009. Once the new system is implemented, DVR will be able to track access to all records. For security reasons, DVR intends to prohibit electronic information from being stored on laptop computers and will require such information to be maintained on a central network.

## Department of Human Resources

The Department of Human Resources (DHR) was represented at the session by Brian Wilbon, Deputy Director for Operations. DHR's written testimony explained that the department collects and maintains 2.7 million active records with SSNs in automated databases. Aside from those collected by the personnel office of current staff, contractual staff, and applicants, DHR's Inspector General collects 2 million SSNs for the purpose of investigating allegations of public assistance, employee and vendor fraud, and for audits of the 24 local

departments of social services. Additionally, various administrations within the department with programs that provide direct services to the community use SSNs as a tool to determine eligibility, insure accuracy of payments, and interface with various State and federal agencies. Levels of access to the databases are requested and granted based on classification and job function. DHR's data security unit reviews requests for access to ensure appropriateness. Passwords are routinely changed and are protected. Paper records with SSNs are kept in locked filing cabinets. Access is limited by job function. Schedules for retention of information are set by the program administrations within DHR, depending on requirements of State and federal law. Hard copy files are destroyed and electronic information is encrypted.

In response to questions from the task force, Mr. Wilbon testified that, although some DHR personnel handling the database have undergone criminal background checks, not everyone has. The department uses an automated intrusion detection system that checks access to databases, although access rules vary among program administrations. Mr. Wilbon stated that electronic information exchanges between State agencies of personal information were encrypted but expressed concern that personal information sometimes was received "informally" from various unencrypted sources (*e.g.*, blackberries, thumb drives, laptops, and personal handheld devices). DHR recommends that a policy on regulating such exchanges be developed. Mr. Wilbon also confirmed that DHR, like all other State agencies, was exempted from the requirements of the breach notification legislation passed last session by the General Assembly.

## Maryland Department of Transportation

### Motor Vehicle Administration

The Motor Vehicle Administration (MVA) was represented by Christine Nizer, Associate Administrator for Driver and Vehicle Policies and Programs; Sandy Pinder, Associate Administrator of Information Resources; and Rose Bianco, Internal Investigator. To comply with federal and State statutes and regulations, MVA currently has 6,095,608 records containing SSNs. Such personal information is closed to the public as a matter of State law (§ 10-616(p) of the State Government Article). Access to confidential data is limited to job related purposes. MVA employees must have management-approved security access forms and have signed security advisory statements before having access to such information. Mainframe functions mask SSNs except for the last digits, and this restriction will be extended to all other MVA programs by the end of 2007. MVA employs a password policy to prevent unauthorized use of computers. Terminals use biometric physical security. The password changes every 45 days. A security access program makes a record of each time a driving record is accessed. The Social Security Administration conducts periodic audits of MVA on how SSNs are being handled. Only electronic records of SSNs are maintained by MVA, and such records are never purged. The Maryland Department of Transportation is in the planning phase of encrypting data currently stored on the mainframe as well as tapes that go offsite for back-up. In September 2007, MVA will begin a "V" indicator program to permit a victim of identity theft to have a designation placed on the victim's driver's license and record to alert law enforcement officers in traffic stops of the victim's status.

In response to questions from task force members about the expected impact of federal REAL ID legislation on MVA, Ms. Nizer testified that MVA would be required to electronically verify documents which currently do not require such verification. Other added regulations, like added cameras at work stations, are expected. The process MVA will use to provide "V" designations on driver's licenses of victims of identity theft was also explained.

## Office of the Comptroller

Linda Tanton, Deputy Comptroller, provided testimony to the task force on the use and protection of SSNs and other personal information of Maryland taxpayers by the Office of the Comptroller of Maryland. The Comptroller currently has 8.3 million active SSNs in its income tax file, 690,000 accounts with SSNs on a Central Registration file for withholding tax purposes, 157,000 on payroll files, and 1.1 million federal employer identification numbers or SSNs on the R*STARS system that pays the State's bills. The Central Payroll Bureau maintains W-2 files that go back to 1986. The office has almost 250,000 SSNs in a file of holders of unclaimed property. SSNs are also accessed by field agents for enforcement purposes and are used for tax and criminal justice administration. SSNs are requested from the public for the administration of various programs, often as a statutory requirement. The disclosure of tax information is prohibited by Maryland law (§ 13-202 of the Tax General Article). All employees, contractors, and vendors are required to sign a Certificate of Confidentiality. Warnings are issued each time the mainframe is accessed. Access to buildings and offices are controlled. Job descriptions and operating manuals dictate which systems can be accessed by which employees. A logon ID and password system restricts access and maintains an audit log of use. A security officer in each division periodically reviews system access reports, the legislative auditor reviews security for fiscal/compliance audits, and employees are provided periodic training. The Internal Revenue Service also participates in training and conducts audits on the handling of information. To protect taxpayers from identity theft, the office has for several years used the last four digits of SSNs, unless the full SSN is required. Encryption software has been installed in personal notebook computers used in the field, is currently being installed in mainframe computer tape drives so that tapes stored offsite cannot be accessed without authorization, and is used to encrypt e-mail correspondence to taxpayers. Surplus agency personal computers are scrubbed and disposed tapes are burned.

Responding to questions, Ms. Tanton confirmed that the W-2 records from 1986 through 2006 are being maintained electronically rather than on paper and now may be filed electronically by State employees. Such records are kept in perpetuity, for informational purposes. Tax returns are kept in-house for one year, sent to Jessup for storage for two additional years, and then destroyed.

## University System of Maryland

Dr. Donald Z. Spicer, Associate Vice Chancellor and CEO and Lennox Brown, Manager, Information Systems Audit presented testimony to the task force on behalf of the University

System of Maryland (USM). USM is a system of 13 public, four-year and graduate/professional institutions in Maryland, with a total of approximately 160,000 students, faculty, and staff. Collectively, over 2 million records containing SSNs are managed by USM institutions. Within the last 10 years, USM institutions have moved away from public displays of SSNs on class lists, rosters, official and unofficial transcripts, and student identification cards. Since 1999, most USM institutions have begun to use new software that generates a unique primary key for a student's records unassociated with the SSN. The collection and storage of SSNs by various institutions within USM is required by law, for financial aid and employment purposes. Training is in place for faculty and staff on use of a student's personal information. Federal laws, industry security standards, and the State Information Technology (IT) Security Policy and Standards are used by USM to protect information. A USM IT security task force in 2000 developed higher education specific guidelines for IT security. USM's Information System Audit is responsible for performing reviews to ensure the integrity and security of sensitive data, at rest and in transit.

In response to questions from the task force, Dr. Spicer agreed to provide additional information regarding the practice of USM institution libraries in collecting and using SSNs for collection purposes, whether employees who handle personal information are required to undergo criminal background checks, and if records that were maintained using SSNs are encrypted or use new identifiers when transferred to electronic records. Wireless services require an authentication that the user is affiliated with a USM campus, but further encryption is being considered to protect security of information exchanged in this fashion.

## Maryland Independent College and University Association

Tina Bjarekull, President of the Maryland Independent College and University Association (MICUA), provided testimony to the task force. MICUA represents 18 independent institutions of higher education in Maryland. These institutions maintain personal records of personnel, academic records, student financial and loan information, and medical data. Member institutions enroll about 50,000 students annually and employ about 36,000 workers on a full- or part-time basis. Records of hundreds of thousands of graduates and students who have taken courses are maintained. SSNs are no longer used as unique identifiers in campus transactions. Instead, computer generated numbers are now used. Colleges assign a login ID and an initial password to authorized staff who are only permitted to access records for which they are authorized based on job descriptions. The password is usually changed periodically. Most member institutions follow the policies recommended by the American Association of Collegiate Registrars and Admission Officers on the retention and destruction of personal information.

The task force had questions for President Bjarekull concerning a recent incident in which 30,000 records were reportedly lost from Johns Hopkins University. Apparently, nine tape files, eight containing personnel records and one which contained patient information, were lost by a courier while being transported to be microfilmed. President Bjarekull testified that all affected individuals were notified of the loss of their information. In response to task force member questions as to how Johns Hopkins knew who to contact, President Bjarekull promised to provide follow-up information.

## Maryland Association of Community Colleges

Dr. Deborah Cruise, Vice President for Student Development and Institutional Effectiveness, Harford Community College and Lori Rounds, Chief Technology Officer, Frederick Community College presented testimony to the task force on behalf of the Maryland Association of Community Colleges (MACC). As with the institutions represented by USM and MICUA, member community colleges collect SSNs from students, faculty, and employees. Student IDs no longer employ SSNs, but instead use unique and randomly assigned numbers for such purposes. There are no standardized policies and practices governing the retention of records other than those mandated by statute. Only personnel with a legitimate "need to know" in completing job duties are permitted access to personal information.

## Department of Budget and Management

Becky Burner, Legislative Liaison, presented testimony on behalf of the Department of Budget and Management (DBM). The State Personnel System is decentralized and most personnel functions are carried out at the agency level. SSNs are collected for a variety of reasons: Central Payroll wages and taxes, verification of employee eligibility for benefits, the application and hiring process, drug testing process, and employee relations. DBM is in the process of establishing unique identifiers for use in some of these programs. DBM has an Information Technology Security Policy that establishes minimum levels of compliance with security to which each State agency and their employees and contractors must adhere. Under the policy, each agency must assure the confidentiality of agency information, document that a process is implemented for classifying such information, specify the level of security required to access the information, and develop and implement security training of employees and contractors. Security clearances are required for personnel for the use of nonpublic information. Users are not permitted to store data on electronic media that cannot be adequately secured. Electronic transfers of information must be done by a secure and encrypted method. Laptops and other mobile computing devices may not be used to store nonpublic information unless approved in writing by the agency network support administrator, the agency chief of information technology, and the agency head. The Office of Personnel Services and Benefits has taken a number of precautions to protect confidential employee information, including keeping paper files in a secure file room, training employees in information security, locking work stations when employees are not present, and prohibiting private citizens in the employee work area.

In response to questions from task force members, Ms. Burner said she would investigate whether a written policy existed on notifying affected individuals of security breaches. A breach of security at the Department of Natural Resources led to a notification of impacted persons, according to task force member Steve Sakamoto-Wengel. Although any agency is vulnerable to a dishonest employee, DBM reiterated that it does have a policy that requires criminal background checks for certain "trusted employees." Although DBM's policy is to destroy retired laptop computers, Ms. Burner was unsure if this happened at all agencies. DBM does not audit or monitor agencies on personal information security measures but does provide assistance.

## Session III – Tuesday, September 18, 2007

The task force held its third session on September 18, 2007, on the topic of "Consumers and Businesses: Dealing with Identity Theft." The task force heard testimony from citizens, consumer advocates, business groups, and the Federal Trade Commission on various issues concerning the impact of identity theft on the public.

### Citizen Consumer Panel

Maryland citizens victimized by identity theft were invited to share their personal experiences and concerns with the task force. Each citizen witness was asked to include the following information.

- What were the circumstances where your personal and/or account information was used without consent?

- What steps were taken to rectify the situation? How long did it take to resolve the situation?

- How effective were the police, the businesses, or the creditors in providing necessary assistance so that the problems caused by the unauthorized use of your personal information were resolved as quickly as possible with as little inconvenience to you as possible?

- Were you required to spend your own money to rectify the situation? If so, how much money was spent?

- If you needed to amend credit report information, how easy was that to accomplish? How long did it take?

- Are there any actions that could be taken by government, businesses, and consumer advocate organizations to reduce or prevent identity theft in your opinion?

Mr. Warren Gatewood, a former Baltimore City police officer, informed the task force that his car had been stolen in 1986, containing identification that was later used by another person who was arrested on a different matter. Years after this incident, Mr. Gatewood was terminated from a position at a bank when it was learned that an arrest warrant had been issued in his name arising out of this matter. Although he was able to get the warrant dismissed and his record expunged, as a person with a career in the security field, he is compelled to advise potential employers of this matter and take additional steps to ensure employers of his innocence

(such as providing fingerprint records), and check his record regularly against the possibility that his personal information might be used without his knowledge.

Ms. Virginia Shelp became aware that she was being victimized by identity theft in May of 2005. Thieves had, by phone and Internet, attempted to open credit accounts, successfully established accounts with cell phone companies, and actively enrolled with or attempted to receive services from various utility companies in her name. Ms. Shelp contacted the Federal Trade Commission, placed a fraud alert on her credit information with the three credit bureaus, and attempted to file a police report with the Anne Arundel County Police Department. She was later informed by the Anne Arundel Police that, since the actual theft "took place" in Washington, DC, she would have to file her report in that jurisdiction. Despite filing a total of three reports in Washington, DC, no corrective action was taken against the thieves. Although Ms. Shelp received partial reimbursement for expenses caused by the thefts, her credit rating fell significantly, causing her to be charged higher rates. She stated that she feared retribution against herself and her family if she takes any action against the criminals. She said that she provided information to law enforcement and the relevant businesses about the fraudulent accounts opened in her name. She said that her experience causes her to doubt that businesses will adequately protect any personal information that she provides.

Ms. Cindi Curtis offered both personal testimony as a multiple identity thefts victim and professional testimony as an identity theft risk management consultant, for her company IDTSolutions. In 1998, while completing the application and hiring process for a position as a registered nurse, she was informed that her name, SSN, address, and other personal information had been used 14 years previously by an individual arrested for armed robbery. After turning down that job, she took a registered nurse position that required a Department of Defense security clearance and obtained one, despite this problem. After several additional security clearances over the following 12 years, Ms. Curtis believed that the original problem had been a mistake. In 2006, however, the criminal "record" again came up when a company she worked with instituted new employee files. Ms. Curtis has been forced to use the services of a lawyer and an identity theft protection company to aid her in efforts to clear her name over this incident. Ms. Curtis has also been victimized by an accountant at a company for which she was a contract employee, who used her name and SSN to hide earnings. This led to problems with her credit and the Internal Revenue Service. Additionally, Ms. Curtis's cell phone was stolen three years ago, which has led to several thousands of dollars of bills for which she is not responsible and high service charges to maintain service. She stated that she was frustrated by the "layering" of identity theft occurrences, and that it was difficult to know which problem to address first.

Mr. Michael Johnson testified that, due to having a common name, he has been the victim of the "mis-merging" of his credit records with the records of several other "Michael Johnsons" at the major credit reporting agencies causing significant credit and other problems for him. At least seven other Michael Johnsons' credit histories (including at least one with a spousal credit history) have been incorrectly applied to his identity, leading to the denial of many applications for credit. He has written letters to the credit bureaus and finally hired an attorney to resolve this problem. Mr. Johnson was also denied a driver's license when the record of a person who shared

his name, as well as the same birthday and year, showed an outstanding arrest warrant in New York. He was forced to provide sworn information and photographic evidence of his likeness to overcome this problem.

In response to questions from the task force about the quality of assistance that had been received from law enforcement agencies, Ms. Curtis and Ms. Shelp testified to receiving some initial help, but Ms. Curtis said the police she contacted seemed unsure how to proceed, and Ms. Shelp was frustrated with being sent to Washington, DC, and their seeming unwillingness to pursue her case. Mr. Gatewood was able to use his law enforcement experience and contacts to help his situation, although he confirmed that the expungement he received would not remove reference to his name as an alias in the police files. The citizen panel was gratified to be informed that recent reforms in Maryland law provide for jurisdiction in identity theft cases in the county in which the victim resides, the availability of identity theft "passports" in January 2008, and the Motor Vehicle Administration's adoption of a "V" identifier on driver's licenses and records for victims of identity theft. The identifier will be attached to driver's licenses beginning in October 2007.

## Federal Trade Commission

The Federal Trade Commission (FTC) was asked to provide testimony to the task force in the following areas:

- What steps has FTC taken to improve identity theft enforcement, including assistance provided to state and local governments?

- What are the findings and recommendations of the White House Task Force on Identity Theft and what impact do these findings have on the efforts of FTC to prevent identity theft?

Ms. Betsy Broder, Assistant Director of FTC's Division of Privacy Protection, presented testimony to the task force. She cited statistics indicating that millions of consumers are victimized by the crime of identity theft each year, causing direct costs and threatening consumer confidence in the marketplace. FTC works with federal, state, and local governments along with industry and consumer groups to reduce opportunities for thieves to obtain consumer's personal information and to misuse the information if they do obtain it. FTC brings law enforcement actions against businesses that fail to implement security measures to protect sensitive consumer data, under federal laws like the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, as well as the deceptive acts and practices prohibition of the Federal Trade Commission Act. Since 2001, FTC has brought 14 cases challenging businesses that allegedly failed to reasonably protect sensitive consumer information. For example, in an action against ChoicePoint, a data broker that inadvertently sold sensitive information on more than 160,000 individuals to a criminal gang, the defendant agreed to pay $10 million in civil penalties and $5 million in consumer redress for victims and agreed to undertake substantial new security measures. In

2003, the Fair and Accurate Credit Transactions Act mandated that businesses dispose of consumer information in a safe manner, increased consumers' opportunities to review credit records, and empowered consumers to take steps to limit damage from identity theft if they become victims. FTC has made efforts to increase consumer and business awareness of the need to protect data and prevent identity theft, and the steps to take if victimized, including the launching of a nationwide education program, "Avoid ID Theft: Deter, Detect, Defend." Finally, FTC maintains the Identity Theft Clearinghouse, a national identity theft victim complaint database containing over a million complaints.

In April 2007 the Federal Identity Theft Task Force, comprised of 17 federal agencies and co-chaired by the Attorney General and the FTC Chairman, published a Strategic Plan for combating identity theft. The Task Force Strategic Plan recommends 31 initiatives, focusing on prevention through improvements in data security and customer authentification, victim assistance to ensure victims have the means and support to restore their identity, and deterrence through stronger tools to punish identity thieves. In the public sector, the plan recommends that federal agencies and departments improve internal data security processes, develop breach notification systems, and reduce unnecessary uses of SSNs. The task force also plans to work with state and local governments to eliminate the unnecessary use and display of SSNs. For the private sector, the task force proposed that Congress establish national standards for data security and breach notification that would preempt the numerous state laws on these issues. The plan recommends that the federal task force study the feasibility of developing a nationwide system that would allow identity theft victims to obtain identification documents that verify their identity, similar to the Maryland "passport" system. The plan also asks FTC to assess state laws that grant consumers the right to place credit freezes on their credit reports, with the findings to be used by policy makers in considering whether a federal law would be appropriate. Finally, the plan includes various recommendations for strengthening law enforcement's ability to combat identity theft including providing assistance to state and local governments. For example, the plan recommends increasing the number of identity theft seminars for state and local law enforcement officers, and an increase of resources available to law enforcement over the Internet.

In response to questions at the session, Ms. Broder emphasized that FTC does not enforce the criminal law but focuses on ensuring that commercial entities do not allow identity theft to take place. FTC helps law enforcement by referring victims to the appropriate agency and being a data repository for complaints, so that trends in this area can be discerned. Ms. Broder also spoke of working with the Treasury Department and the U.S. Postal Service to fight instances of identity theft from the U.S. Mail.

## Other Consumer Representatives

The task force heard from a panel of individuals who had particular experiences representing consumers in incidents of identity theft. Appearing were Mr. Evan Hendricks, the founder, editor, and publisher of *Privacy Times*; Mr. Michael Worsham, Esq., a private practice attorney and consumer advocate; and Dr. Edward C. Papenfuse, State Archivist and

Commissioner of Land Records, Maryland State Archives. Each was asked to provide information on the following issues:

- How effective are federal and state laws in preventing identity theft and protecting the rights of consumers who have been victimized by identity theft?

- How effective are federal and state laws in ensuring that the data held by financial institutions, retailers, and credit reporting agencies is protected from unauthorized disclosure?

- What actions could be taken by state and federal governments, businesses, and consumers to reduce or prevent identity theft?

Mr. Hendricks began by stating that Maryland is a recognized legislative pioneer in consumer rights, as evidenced by many of the recent reforms in this area. He emphasized that the credit report (and the production of the report) remains the epicenter of the problems with privacy and identity theft. To get a credit report cleaned up after being impacted by identity theft or other mistake often requires the filing of a lawsuit. Mr. Hendricks blamed this primarily on the automated nature of responses to consumer requests to clear up their reports. Credit bureaus should initiate a "triage" system, so that the more complicated and insidious cases are handled with more care and a dedication to finding the truth of the matter, rather than a computer kicking back standard responses. Mr. Hendricks testified that in light of inconsistent responses to consumer requests for corrections to reports, the credit freeze law enacted in Maryland last session was a good idea. One problem is that there are layers of files within the bureaus and the businesses they serve. The first layer of a file might be produced in response to a request, but the second or third level of files are often held back, in violation of the intent of consumer protection laws that mandate all such files be produced. Mr. Hendricks also expressed concern for the "trigger" problem, which occurs when, within 24 hours after a mortgage application is submitted to a company, the applicant gets inundated with other offers. He said that the law prohibits the selling of information regarding a mortgage or refinancing until after a firm offer is made. Because consumers seem to be getting these offers before they make a firm decision, this discrepancy should be addressed.

Mr. Worsham categorized two types of identity theft: intra-family and everything else. He also spoke of the problem, an example of which the task force heard about earlier with Mr. Johnson, of "mixed file" cases. Mr. Worsham specifically recommended that Maryland law explicitly mandate that credit reporting agencies provide all written documentation provided by consumers who dispute credit items to the creditor or furnisher of the information about which the consumer is disputing and require credit bureaus to do their own independent investigation of such disputes. Cellular and telephone companies, as well as other financial companies, should have the same controls and checks in place for additions to existing service that are placed on the creation of original accounts, including that the request be in writing and have an original signature. Reliance on SSNs as the primary identifier should be strongly discouraged. Mr.

Worsham recommended that requiring credit reporting agencies to provide all written documentation to consumers who dispute credit items would aid in the problem of "mixed-file" cases. Other recommendations included prohibiting SSNs on publicly filed documents, requiring police to take certain steps to investigate the filing of an identity theft complaint, providing the right to request injunctive relief by consumers, providing minimum statutory damages for willful failure to comply with identity theft and credit reporting requirements, and increasing the two-year statute of limitations by extending the current requirements defining the "discovery" period in these cases.

Dr. Papenfuse began by telling the task force of his personal experience as a victim of identity theft, after his mail was stolen from a mail truck and from the mail box of his family's home. His signature was forged on a State reimbursement check, an unsolicited access check, and a State credit union withdrawal check. Despite looking nothing like the victim (the perpetrator was of a difference race and build), the perpetrator was able to conduct business in Dr. Papenfuse's name at various financial institutions. The criminal was eventually caught and sentenced to prison, with the help of court testimony provided by Dr. Papenfuse. Despite this, Dr. Papenfuse was surprised to learn that the criminal had been released from prison at a much earlier date than the requirement of his original sentence. Dr. Papenfuse was not notified of the early release because he was not technically considered the "victim" of the crime, since he had been reimbursed by the bank and the credit union, which were recorded as the "true" victims. Dr. Papenfuse stated that even if a financial institution makes a consumer financially whole, that person still goes through considerable anguish to correct credit report damages. Dr. Papenfuse recommended that State and federal courts improve communication with regard to the identity and records of individuals charged within both systems and be required to maintain an integrated, web-based information system. He would ask for more "truth in sentencing" so that the victims, witnesses, and the public have a better idea of what a sentence truly means, when parole and diminution credits are included. He would like to see a centralized data warehouse of personal data in the custody and shared control of a single accountable governmental archival agency and an independent public records inspector general to ensure the safekeeping of such information.

In response to questions, Dr. Papenfuse allowed that there may be "big brother" concerns over his recommendation of a centralized data warehousing agency of information, but that, at least, there should be "inter-operability" among relevant agencies to keep better track of such information. Dr. Papenfuse also said that consumers spend a great deal of time trying to get cashiers, bank tellers, and others who handle personal information to do the basic checking and verification that should be done as a matter of course.

## Credit Card Company

Mr. Mark MacCarthy, Senior Vice President, Public Policy, Visa USA, Inc., presented testimony to the task force from the perspective of the credit card industry. Mr. MacCarthy was asked to speak about the following issues:

- Generally speaking, what actions do federal and state laws require credit card companies to take to protect the personal and financial information of customers?

- What other initiatives has Visa USA undertaken to protect personal and financial information that are not required by federal and state laws?

- What is the annual cost to Visa USA of identity theft, especially in terms of refunds or financial credits to affected customers and the cost of efforts to secure databases of personal and financial information?

- What actions could be taken by government, businesses, and consumers to reduce or prevent identity theft?

Mr. MacCarthy testified that, as the "leading consumer e-commerce payment system in the world," Visa considers it a top priority to develop technology, products, and services to protect consumers from the effects of identity theft and account fraud. There is no "silver bullet" that will erase fraud, so multiple tools and tactics must be used. Visa has a "zero liability" policy that protects cardholders from liability for fraudulent use of their credit cards. Visa has instituted a customer information security program to keep member information protected and confidential that includes data security standards, provisions for monitoring compliance, and sanctions for failure to comply. Visa supports the common set of data security standards used by various credit card organizations and has launched an accelerated compliance program to provide merchants with financial incentives. Visa also has security programs that focus specifically on small businesses. Visa employs "cutting-edge" technologies to monitor transactions on a global basis to detect and stop fraud and has implemented a number of other security measures to achieve the same result. As a result of these measures, fraud conducted within the Visa system ranges from five to six cents for every $100 of transactions. This represents a significant reduction from the early 1990s when the fraud rate was almost 20 cents for every $100 of transactions. Mr. MacCarthy testified that banking institutions, including credit card issuers, are among the "most highly regulated and closely supervised" of those that handle and process sensitive consumer information. He cited the guidance given the industry under Title V of the federal Gramm-Leach-Bliley Act (GLBA) in limiting disclosure of customer information, protection of the information from unauthorized access or use, and the notification of customers of security breaches. Mr. MacCarthy stated that the GLBA regulations and guidance make it unnecessary to design a completely new system to address identity theft. Visa takes no position on pending legislation in this area but favors reasonable risk-based security and notification requirements, stronger penalties for identity theft, and additional resources for state and local law enforcement to combat these crimes.

In response to task force member questions, Mr. MacCarthy asserted that problems with credit card solicitations have already been addressed by the U.S. Patriot Act, which requires the industry to take steps to ensure that the actual identity of the applicant is known, keep a database

of fraudulent applications, and check new applications against the database. Regulations require a new credit check once an application is received. The data reflects that these prescreened applications are not, in fact, a significant source of fraud. He confirmed that a request for an address change on an application is a red flag that triggers additional scrutiny of such an application. Mr. MacCarthy cited data that shows over 90 to 95 percent compliance with data security standards in the industry. He testified that giving consumers the choice of "opting-out" of information-sharing is better for consumers than the "opting-in" alternative that has been suggested. The use of an "opt-in" system would hinder data mining used to assist consumers. The solution, according to Mr. MacCarthy, is to ensure that people understand their options.

## Banking Panel

The banking industry was represented by Ms. Kathleen Murphy, President and Chief Executive Officer of the Maryland Bankers Association (MBA); Mr. Kevin Smith, Senior Vice President and Corporate Security Director of the Chevy Chase Bank and Chairman of the MBA's Security Committee; Ms. Eartha Morris, Senior Vice President of Management of Consumer Information at Provident Bank; Mr. Michael Briggs, Legal Counsel, Gordon, Feinblatt, Rothman, Hoffberger and Hollander; and Ms. Mindy Lehman, MBA's Vice President of Government Affairs. This panel was asked to provide information to the task force on the following issues:

- Generally speaking, what actions do federal and state laws require banks to take to protect the personal and financial information of customers?

- What other initiatives have banks undertaken to protect personal and financial information that are not required by federal and state laws?

- What is the annual cost to Maryland banks of identity theft, especially in terms of refunds or financial credits to affected consumers and the cost of efforts to secure databases of personal and financial information?

- What actions could be taken by government, financial institutions, and consumers to reduce or prevent identity theft?

Ms. Murphy prefaced the banking panel's presentation by stating that banks are heavily regulated by the FDIC, Comptroller, Federal Review Board, and the Commissioner of Financial Regulation. Banks now operate under stringent requirements to know the customer before opening an account due to provisions in the U.S. Patriot Act. She also said that the banking industry does not regard identity theft as a cost of doing business, but as a trust and market stability issue. Citing statistics compiled in the *2006 Identity Fraud Survey* published by Javelin Strategy & Research, identity theft is down 12 percent, with 500,000 fewer victims in 2006 than

2005. Ms. Murphy stated that data demonstrate that prevention against the majority of identity theft crimes (about 63 percent) is within the control of the consumer.

Mr. Briggs presented a compilation of current federal and state laws and regulations governing banks and the protection of personal data, stating that they are comprehensive and aggressive.

Mr. Smith remarked that Maryland had a unique approach to the issue of consumer protection and a reputation for "getting out in front" of such issues. He reminded the task force that identity theft, although it recently has received a great deal of attention, is an "old crime" – in essence, the crime of fraud. Mr. Smith testified that member banks prevent $20 million in fraudulent transactions each year by using a pattern analysis of all transactions. Approximately 70 percent of the fraud cases involve a fake check. The industry has not waited to be given "red flag" guidelines on steps to prevent identity fraud since it directly suffers costs if such attempts are successful. Mr. Smith said the U.S. Patriot Act mandates that banks require identification, signatures, and other information to open new accounts. While mistakes may be made on the "front line" (*e.g.*, bank tellers), there are security backstops requiring analyses and comparisons to look for tell-tale signs of fraud. Nearly all banking institutions have identity theft repair programs for consumer victims. Although Mr. Smith testified that it was hard to accurately determine costs related to identity theft, there was probably an estimated $12 to $18 cost for every banking card that required re-issuance due to being compromised.

Ms. Morris testified that member banks actually exceed the requirements of federal and state regulation in their efforts to prevent fraud. Banks check and monitor transactions, issue fraud alerts, use encryptions and firewalls against unauthorized data access, and listen to consumer complaints and concerns. Additionally, banking customers are provided services to monitor their accounts and step-by-step information if they find themselves victimized by identity theft.

Ms. Lehman spoke about the role of the banking customer in incidents of identity theft. According to the Javelin Report, about 7 out of 10 cases of identity theft are within the control of customers rather than the financial institution. They include stolen wallets, theft by associates or family members, and the hacking of their personal computers. In response, the banking industry has conducted public information campaigns to raise consumer awareness of the problem. For example, the task force was provided material for the "Shred It or Dread It" campaign. Ms. Lehman said that there is evidence that these efforts are working, citing a 12 percent decline in the number of adult victims of identity theft and a corresponding decline in the amount of losses from such crimes. Credit was given to increased customer awareness, better procedures used by financial institutions, and the increase of online banking.

## Retail Panel

Speaking for the retail industry, the task force took testimony from Mr. Damien Walter, a Loss and Prevention investigator for the Target Corporation, and Mr. Jeffrie Zellmer, the

Legislative Director of the Maryland Retailers Association and a member of the task force. The panel was asked to provide information about the following issues:

- Generally speaking, what actions do federal and state laws require retailers to take to protect the personal and financial information of customers?

- What other initiatives have retailers undertaken to protect personal and financial information that are not required by federal and state laws?

- What is the annual cost to Maryland retailers of identity theft, especially in terms of refunds to affected consumers and the cost of efforts to secure databases of personal and financial information?

- What actions could be taken by government, retailers, and consumers to reduce or prevent identity theft?

Mr. Zellmer testified that retailers are subject to many of the same laws and regulations as other financial institutions and make concerted efforts to protect and preserve the personal information of their customers. Mr. Zellmer reminded the task force members that retailers are true victims of such crimes, since identity theft involves the direct cost loss of the merchandise that is stolen as a result. Although cost figures were hard to come by due to the proprietary nature of the information, such losses are extensive. Mr. Zellmer characterized Maryland as being in the "front lines" of legislative responses to the problem of identity theft and consumer protection. Retailers are victimized in a variety of ways by identity thieves, including the interception of information from wireless transactions, the direct theft of information from customers (like identification stolen from cars), and information stolen from customers over the Internet. Mr. Zellmer informed the task force of a recent case in Howard County of a woman prosecuted for falsely claiming to be an identity theft victim to eliminate her debts.

Mr. Walter testified that his data indicated a 130 percent increase in recent years of incidents of attempted identity theft. Retailers like Target have instituted procedures so that a cashier is able to process transactions without seeing the account numbers of the customers. Fraudulent credit applications continue to be a problem of concern. Increasingly, victims are asking for access to in-store video tapes of fraudulent transactions, but store policy is to encourage working with law enforcement agencies to catch the perpetrators. While data indicates that check fraud is decreasing, credit card fraud appears to be on the increase, probably due to the increased use of credit cards in the typical transaction. In response to questions, Mr. Walter advised that the use of a credit card is probably safer for the consumer than the use of a personal check to make a purchase. In the Target Corporation, records of transactions are usually maintained for only 18 months, and the data is restricted to only 120 people within the company. In response to a question about the value of State legislation to prohibit the retention

of personal data by retailers, Mr. Walter replied that the Target Corporation did not have a position.

## Session IV – Tuesday, October 2, 2007

The task force held its fourth session on October 2, 2007, on the topic of "Law Enforcement: Effectiveness of Apprehension and Prosecution of Identity Criminals." The task force heard testimony from federal, State, and local law enforcement agencies and officials on various issues concerning the apprehension and prosecution of those who commit identity theft.

### Prince George's County State's Attorney's Office

The Prince George's County State's Attorney's Office was asked to provide testimony to the task force in the following areas:

- What resources does the Prince George's County State's Attorney's Office allocate to the prosecution of identity theft?

- What is the prevalence of identity theft crimes from the perspective of your office, and how successful has been the prosecution of such offenders?

- What is your assessment of how well existing criminal laws in this area work, whether additional legislation is needed, and what type of personnel and budgetary resources would help in prosecuting and convicting identity theft criminals?

- What are the circumstances under which federal, State, and local prosecutors and law enforcement work together to apprehend, extradite, and ultimately prosecute identity thieves?

- Are there any special issues or concerns that make identity theft crimes harder or easier to prosecute than other types of fraud?

Appearing on behalf of the Prince George's County Office of the State's Attorney were Delegate Doyle L. Niemann and Ms. Isabel Mercedes Cumming, both Assistant State's Attorneys and members of the task force. Both prosecutors have extensive experience in handling economic crimes in Prince George's County, including identity theft.

Delegate Niemann and Ms. Cumming spoke of the various sources of identity theft, emphasizing that only a tiny percentage come from "institutional" sources (like hacking into a bank). They cited examples showing that more than 60 percent of identity theft occurs between people who have a connection with one another (*e.g.* family and friends) and most of the

remainder comes from noninstitutional sources, like mail theft and phishing. They testified that a barrier to apprehending the typical identity theft criminal is that such cases require more extensive investigation than traditional cases, including securing financial records from banks, credit card companies, Internet providers, eye-witnesses and other sources, and pulling together a variety of written and testimonial evidence to link a particular suspect to a specific crime. Records are hard to obtain from companies and other law enforcement agencies that are out of county jurisdiction. Another barrier is that identity theft and other economic crimes are not given a high priority in many law enforcement agencies. The Prince George's County Police Department's Financial Crimes Unit has only two to three detectives and is subject to constant changes in personnel. They testified that this is not uncommon, and only a couple of jurisdictions in the area are reasonably staffed to handle identity theft. They noted that Fairfax County in Virginia has 15 detectives dedicated to economic crimes, Montgomery County has 8 detectives, and Baltimore City has 5 detectives. Prince George's County, however, has the second largest number of complaints, and the police department receives 15 calls per day about identity theft.

Delegate Niemann and Ms. Cumming testified that there is a critical need for more resources to be committed to combating economic crimes like identity theft. They noted that while federal authorities have substantial resources, they usually do not become involved in identity theft until there is evidence of an organized crime ring. They also suggested:

- Raising the penalty for identity theft from a misdemeanor to a felony.

- Changing rules of evidence to allow an individual to introduce and testify about the individual's own financial records rather than requiring the custodian of the business record to appear.

- Change Maryland sentencing guidelines to reflect the dollar amount of the fraud rather than whether it was a first or subsequent offense.

- Add resources available at the State level to local law enforcement like lab facilities, handwriting analyses, and Internet research.

In response to questions from the task force, Delegate Niemann and Ms. Cumming testified that requiring all mail boxes to be the lockable kind like those shared by apartment dwellers and town homes would not necessarily hinder identity thieves. They have been known to pry open such boxes and gain access to the mail of multiple victims. They also noted that Maryland sentencing guidelines do not account for the severity of the crime. A sentence of six months is the guideline whether an identity thief has stolen $500 or $1 million. Federal sentencing guidelines provide longer sentences depending on the severity of the crime.

## Montgomery County State's Attorney's Office

The Montgomery County State's Attorney's Office was asked to provide testimony to the task force in the following areas:

- What resources does the Montgomery County State's Attorney's Office allocate to the prosecution of identity theft?

- What is the prevalence of identity theft crimes from the perspective of your office, and how successful has the prosecution been of such offenders?

- What is your assessment of how well existing criminal laws in this area work, whether additional legislation is needed, and what type of personnel and budgetary resources would help in prosecuting and convicting identity theft criminals?

- What are the circumstances under which federal, State, and local prosecutors and law enforcement work together to apprehend, extradite, and ultimately prosecute identity thieves?

- Are there any special issues or concerns that make identity theft crimes harder or easier to prosecute than other types of fraud?

Appearing on behalf of the Montgomery County Office of the State's Attorney was Mr. Robert Hill, Assistant State's Attorney.

Mr. Hill gave examples of the problems encountered in prosecuting identity theft cases. One example was a case in which a number of credit cards were used in Maryland, but the cardholders were primarily from out-of-state. It was extremely difficult to get the victims to come to Maryland and appear as witnesses since the credit card companies had made them "whole." Many other cases are relatively low level, in terms of the amount stolen and the possible penalties, making it hard to justify the complicated steps required to prosecute these offenses. Because of this, many times the State is not able to proceed but is also unable to get the court to grant a continuance so that the evidence can be obtained. As a result, the charges are dropped. Mr. Hill recommended:

- Amending the Maryland Code so that a witness affidavit may be used in lieu of an appearance by the victim, if the defendant is given notice and fails to object. Even if an objection is made, the court may be more willing to grant a continuance so the witness may be produced at a later time. Specifically, Mr. Hill recommended that § 7-105.1 of the Criminal Law Article be amended to include identity theft. That statute allows victims of motor vehicle theft to submit an affidavit in lieu of a court appearance.

- Changing rules of evidence to allow an individual to introduce and testify about the individual's own financial records rather than requiring the custodian of the business record to appear.

- Allow faxes and emails of business records and correspondence to be used as evidence.

- Allow victims to testify that they did not make the contested purchases without requiring the appearance of the record custodian.

- Amend the Commercial Law Article to designate a forgery affidavit as a business record.

In response to questions from the task force, Mr. Hill reiterated that, unless an agreement is reached in a pre-trial negotiation with the defendant's counsel, currently a witness must be produced in person.

## U.S. Secret Service

The U.S. Secret Service was asked to provide testimony to the task force on the following issues:

- What is the prevalence of identity theft in Maryland and nationally?

- What work does the Secret Service do in the area of fighting identity theft and participating in the federal-state task force on financial crimes?

- What types of identity theft cases does the Secret Service investigate and how successful have these efforts been?

- What is your assessment of how well existing criminal laws in this area work, whether additional legislation is needed, and what type of personnel and budgetary resources would help in prosecuting and convicting identity theft criminals?

- How well does the federal-state task force enable federal and state law enforcement to work together to apprehend identity thieves?

- What special issues and concerns exist to make identity theft crimes harder or easier to prosecute than other types of fraud?

Ms. Tamara Blair, Assistant Special Agent in Charge, and Mr. Leroy Hendricks, Special Agent, of the Baltimore Field Office spoke to the task force.

Federal legislation enacted in 1982 and 1984 provided the Secret Service authority for the investigation of access device fraud, including credit and debit card fraud, and parallel authority with other law enforcement agencies in identity crime cases. The mission has evolved dramatically in recent years. In 2006, the Secret Service arrested over 3,400 suspects for identity theft crimes, representing almost $500 million in actual fraud. It is expected the crime statistics will be higher in 2007. A recent trend is the use of computers and the Internet to launch cyber attacks against citizens and financial institutions. Cyber criminals steal victims' personal information by phishing, account takeovers, malicious software, hacking, and network intrusions. Stolen information is often sold in bulk quantities on the Internet, often to criminals operating overseas. The Secret Service has modified investigative techniques to meet these challenges. It has established a national network of Financial Crimes Task Forces to combine resources of the private sector and other law enforcement agencies to combat these and other financial crimes. The Baltimore Field Office is the base of operations for two different task forces: the Financial Crimes Task Force and the Electronic Crimes Task Force. The Secret Service educates consumers and provides training to law enforcement personnel. The Secret Service consults with the Federal Trade Commission to support and encourage use of the Identity Theft Data Clearinghouse.

In response to questions from task force members, agents Blair and Hendricks were unable to provide statistics on Nigerian email scams but advised that the Secret Service maintains two databases on identity theft cases. They also advised that the Secret Service is establishing training centers for local law enforcement officers to learn how to better investigate economic crime, and that members of the task force have full access to all data kept by the Secret Service, except information deemed classified. Cases brought to the task force are prosecuted vigorously without regard for jurisdiction. The Secret Service does not generally pursue fraudulent mortgage cases unless there are elements of identity theft involved.

## Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) was asked to provide the following information to the task force:

- What is the prevalence of identity theft in Maryland and nationally?
- What work does the FBI do in the area of fighting identity theft and participating in the federal-state task force on financial crimes?
- What types of identity theft cases do the FBI investigate and how successful have these efforts been?

- What is your assessment of how well existing criminal laws in this area work, whether additional legislation is needed, and what type of personnel and budgetary resources would help in prosecuting and convicting identity theft criminals?

- How well does the federal-state task force enable federal and state law enforcement to work together to apprehend identity thieves?

- What special issues and concerns exist to make identity theft crimes harder or easier to prosecute than other types of fraud?

Mr. David Musgrove, Supervisory Special Agent, Baltimore Field Office, provided testimony on behalf of the FBI.

Agent Musgrove advised that identity theft has been a major focus of the FBI in recent years. The Internet Crime Complaint Center (known as IC3) was established as a partnership between the FBI and the National White Collar Crime Center to serve as a means to receive Internet-related criminal complaints and to further research, develop, and refer criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation they deem to be appropriate. The IC3 was intended to serve the broader law enforcement community and includes federal, as well as state, local, and international agencies, which are combating Internet crime and, in many cases, participating in Cyber Crime Task Forces. Since its inception, the IC3 has received complaints crossing the spectrum of cyber crime matters, to include online fraud in its many forms including intellectual property rights matters, computer intrusions (hacking), economic espionage (theft of trade secrets), online extortion, international money laundering, identity theft, and a growing list of Internet facilitated crimes. Since June 2000, it has become increasingly evident that, regardless of the label placed on a cyber crime matter, the potential for it to overlap with another crime is substantial. Therefore, the former Internet Fraud Complaint Center was renamed the IC3 in October 2003 to better reflect the broad character of such matters having an Internet, or cyber, nexus, and to minimize the need for one to distinguish "Internet fraud" from other potentially overlapping cyber crimes.

## Maryland State Police

The Maryland State Police were asked to provide information in the following areas:

- What is the prevalence of identity theft in Maryland?

- What is the level of resources allocated to identity theft crimes, given other departmental priorities, and the circumstances which dictate whether the department will become involved in an investigation?

- What work does the State Police do in the area of fighting identity theft and participating in the federal-state task force on financial crimes?

- How does the federal-state task force on identity theft identify cases to investigate and what advantages arise from collaboration?

- What is your assessment of how well existing criminal laws in this area work, whether additional legislation is needed, and what type of personnel and budgetary resources would help in prosecuting and convicting identity theft criminals?

- What special issues and concerns exist to make identity theft crimes harder or easier to prosecute than other types of fraud?

First Sergeant Robert Smolek of the Department of State Police and a member of the task force presented testimony. He is the supervisor of the Computer Crimes Unit, a specialized investigative unit of the State Police.

As there is no common database for complaint or case information in this area among the 160 jurisdictions in Maryland, statistics are difficult to acquire. There is no formal federal-state task force on identity theft in which the Department of State Police participates. Investigations in these cases are assigned to the 23 State Police barracks or the Criminal Investigation Division. The troopers generally work with federal partners on a case-by-case basis as resource needs dictate. The crime of identity theft has shifted the traditional criminal investigation paradigm in which the criminal act, the police, the victim, and the suspect are often in the same jurisdiction. With identity theft, victims, local police, and suspects often operate from geographically disparate locations. The logistical and budgetary problems with investigating, making arrests, producing witnesses, etc., are significant. First Sergeant Smolek advised that current Maryland law in the area of identity theft is sound and recent changes have made prosecutions for this crime more effective. For example, allowing prosecution of cases in the jurisdiction of the victim is very helpful. The following objectives should be achieved:

- Law enforcement personnel must be properly trained and informed about this type of crime.
- Law enforcement agencies should be appropriately staffed with criminal investigators to conduct the in-depth and lengthy investigations required of this type of crime.
- The public needs to be educated to protect themselves and they need information on the steps to be taken once victimized.

First Sergeant Smolek recommended that witness affidavits would make prosecutions of these cases easier.

## Baltimore County Office of the State's Attorney

The Baltimore County State's Attorney's Office was asked to provide testimony to the task force in the following areas:

- What resources does the Baltimore County State's Attorney's Office allocate to the prosecution of identity theft?

- What is the prevalence of identity theft crimes from the perspective of your office, and how successful has the prosecution been of such offenders?

- What is your assessment of how well existing criminal laws in this area work, whether additional legislation is needed, and what type of personnel and budgetary resources would help in prosecuting and convicting identity theft criminals?

- What are the circumstances under which federal, State, and local prosecutors and law enforcement work together to apprehend, extradite, and ultimately prosecute identity thieves?

- Are there any special issues or concerns that make identity theft crimes harder or easier to prosecute than other types of fraud?

Mr. Scott D. Shellenberger, the State's Attorney for Baltimore County and Ms. Marsha Russell, Chief, Baltimore County State's Attorney's Office Identity Theft Unit, spoke with the task force.

Given the steady increase in identity theft crimes, the office created an Identity Fraud Unit to identify cases as soon as they were charged so that a prosecutor with particular expertise could review them and ensure what evidence needs to be gathered for court. The unit is staffed with a senior trial assistant and a full-time paralegal who make initial determinations as to whether a case is filed in the District Court or circuit court. Since 2005, the unit has reviewed 513 identity fraud cases. In 2006 the office initiated 213 prosecutions, and won 136 convictions. Of the 77 cases not resulting in a conviction, the vast majority were resolved with a guilty plea in another case. The office also assists people who have been wrongly charged with a crime due to stolen identities. Approximately 99 such people are assisted each year. The ability under Maryland law to prosecute such crimes in the jurisdiction in which the victim resides is a useful tool to prosecutors. Changes in two areas of the law were recommended:

- The allowance of use of sworn affidavits of victims of the identity fraud statute rather than their in-court appearance which is now required (modeled after § 8-214.1 of the Criminal Law Article).

- Raise the penalty for identity fraud involving more than $500 to imprisonment up to 15 years (from 5 years) to correspond with the penalty for use of stolen credit cards.

Mr. Shellenberger also recommended additional public education on the problem. Brochures distributed by the office explaining how to protect oneself before or after such crimes are useful and popular. Public service announcements urging people to place locks on their mailboxes and to shred personal information would also help. Consumers should be made aware of the option in Maryland of freezing credit reports. Ms. Russell stated that helping victims unravel their lives is the most stressful aspect of identity theft. The consumer who monitors credit reports and shreds his/her personal information can still be victimized if the businesses the consumer patronizes do not adequately secure that personal information.

In response to questions, Mr. Shellenberger acknowledged the need to provide training for law enforcement officers who take reports from victims of identity theft. Time and budgetary resources for prosecuting such cases are often stretched since these cases often require substantial documentary evidence and the appearance of witnesses from out-of-state. The office is aware of the investigative thresholds of crimes in which the FBI can be called in, usually a minimum of fraud involving at least $150,000.

## Baltimore County Police Department

### Economic Crimes Unit

The Economic Crimes Unit of the Baltimore County Police Department was asked to advise the task force on the following:

- What prompted your department to allocate specific resources to economic crimes, including identity theft?

- What is the prevalence of such crimes from your perspective and how successful has the apprehension of identity theft criminals been?

- What is your assessment of how well existing criminal laws in this area work, whether additional legislation is needed, and what type of personnel and budgetary resources would help in prosecuting and convicting identity theft criminals?

- Are there any special issues or concerns that make identity theft crimes harder or easier to prosecute than other types of fraud?

Lt. Douglas McManus, Commander; Det. Cpl. Morgan Hassler, Supervisor; and Greg Hebding, Detective presented testimony on behalf of the Baltimore County Police Department's Economic Crimes Unit.

The economic crimes team has grown over the past few years from 5 detectives to a total of 2 sergeants, 1 corporal, and 10 detectives whose sole responsibility is the investigation of financial crimes with an emphasis on identity theft. The department was very supportive of the recent change in Maryland law allowing prosecution of such crimes in the jurisdiction in which the victim resides. The reports of identity theft the department has received has grown from 314 in 2002 to over 1,100 in each of the past two years. These numbers, however, do not include credit card misuse and other fraud crimes that are not originally reported as identity theft but do include those crime elements. The methods which identity thieves use change on a daily basis, and examples of such cases were provided to the task force. Several examples were presented to the task force demonstrating that many identity thieves, even when caught, are made to pay an amount of fines and restitution that represents only a fraction of the assets which they fraudulently acquired. Therefore, the department has previously urged and recommends that the General Assembly adopt seizure and/or forfeiture laws for identity fraud crimes so that all assets of such criminals, such as the home, vehicle, or monies obtained through the crime can be frozen during the investigation of such crimes and forfeited upon conviction.

The department has not been able to obtain any federal funding to assist in the investigation and prosecution of identity theft cases and is in need of additional equipment, including cars and cell phones. In addition to a seizure and forfeiture law, the department would support legislation, introduced last session, to increase penalties for identity fraud repeat offenders (House Bill 1044/07) and expungement of false criminal records of victims of identity theft (House Bill 931/07). The department also supports allowing affidavits to be used in lieu of forcing the appearance of a witness victim in identity theft cases.

## U.S. Postal Inspection Service

The U.S. Postal Inspection Service was asked to provide the task force with the following information:

- What is the prevalence of mail fraud in Maryland?

- What is the impact of mail fraud on identity theft and has focusing on mail fraud helped to apprehend identity thieves?

- What is your assessment of how well existing criminal laws in this area work, whether additional legislation is needed, and what type of personnel and budgetary resources would help in prosecuting and convicting identity theft criminals?

- How well does the federal-state task force enable federal and state law enforcement to work together to apprehend identity thieves?

- What special issues and concerns exist to make identity theft crimes harder or easier to prosecute than other types of fraud?

The U.S. Postal Inspection Service provided testimony to the task force by Postal Inspectors John Schick, Burt Foster, and Michael Blackman. Detective Mark Coulter of the Prince George's County Police Department also testified with this panel. As the law enforcement arm of the United States Postal Service, the U.S. Postal Inspection Service has full police powers to investigate and apprehend criminals that adversely affect or fraudulently use the U.S. Mail and postal system.

The panel noted that identity "fraud" and "theft" while used interchangeably are different. "Theft" is taking personal information without the owner's consent. "Fraud" occurs when stolen personal information is used to get material gain without the owner's consent. Mail theft rings are the agency's biggest concern. While the Federal Trade Commission has reported that only 4 percent of identity theft victims cite stolen mail as the source of the stolen information, postal inspectors take this threat seriously. In the past three years, postal inspectors arrested on average 3,000 suspects annually for identity theft schemes. In the past few years, the inspection service has increased the resources devoted to the identity theft problem by 38 percent. One problem is that thieves have turned to this crime from other types of crime (*e.g.*, guns and drugs) because it is considered relatively safe and easier to accomplish. Postal inspectors have the ability to force the forfeiture of criminal's assets in these cases. The panel recommended that Maryland consider passing a law that makes the mere unauthorized possession of another's mail a State crime, since mail theft is often a predicate offense to identity fraud. Minnesota passed a law that was similar to House Bill 293, introduced in the Maryland General Assembly during the 2007 session. More law enforcement resources should be assigned to investigate these crimes within each jurisdiction, and multi-jurisdiction task forces should investigate and share information and resources on a statewide basis. The panel also recommended that postal inspectors have "peace officer" status so that they can execute search warrants without using local law enforcement.

Detective Coulter testified that the Prince George's County Police deals with victims, witnesses, and suspects from all over the country in identity theft cases. Requiring appearances from out-of-state witnesses in these cases is very difficult. Education, training, and networking among law enforcement agencies and the public are the keys to prevention of identity theft. Stiffer penalties for these criminals (who have a high recidivism rate) would also be helpful. The number of victims affected by an identity theft incidence should be considered when sentences are imposed.

## Maryland Association of Bank Security

The Maryland Association of Bank Security (MABS) was asked to provide information to the task force about MABS's efforts to combat identity theft. Robert Smetzer, President of

MABS, and a fraud investigator for PNC Bank, and Michelle Stutheit, MABS member and security coordinator for SunTrust Bank presented information to the task force.

MABS, originally organized in 1972, has 175 members. MABS officers donate their time to the association. MABS serves as an alert system which allows members to share information and put together cases against those who perpetuate fraud and robberies on Maryland financial institutions. Hundreds of thousands of dollars are lost to identity theft each year. Many criminals are believed to be operating overseas, making prosecution difficult. The U.S. Patriot Act has helped in many ways, including precluding a lawsuit by a criminal against a financial institution for taking reasonable steps to prevent fraud and capture criminals. While victims are usually made financially whole, they often face the significant aggravation of putting personal finances back together and overcoming the feeling of being almost physically violated by the assault on their identity.

## Session V – Tuesday, November 13, 2007

The task force held its fifth session on November 13, 2007, on the topics of "REAL ID Act and the Impact on Identity Theft" and "Local Government Information Security Practices" and then held a work session to discuss possible recommendations for the report of the task force.

### REAL ID Act and the Impact on Identity Theft

#### American Civil Liberties Union of Maryland

Appearing on behalf of the American Civil Liberties Union of Maryland (ACLU) to discuss the REAL ID Act was Cynthia Boersma, the Legislative Director.

Ms. Boersma's presentation was entitled "The REAL ID Act: A Nightmare for Privacy and Identity Theft Prevention." The REAL ID Act, passed by Congress in 2005, sets standards for state driver's licenses and identity cards. To enforce the uniform standards, proposed federal regulations would prevent the use of noncompliant IDs for airline flights, access to federal facilities, and other purposes set by the Department of Homeland Security (DHS). According to Ms. Boersma, the REAL ID Act's mandated standards include:

- card data elements and security features;
- a "machine readable zone" (MRZ);
- a 50-state interlinked database;
- "breeder document" standards (breeder documents are those source documents that must be reviewed before an identification document is issued);

- breeder documents must be scanned and stored; and
- facial image capture.

The card is required to include the full legal name, date of birth, gender, license or identity card number, digital photograph, principal residence, signature, physical security features, and an MRZ. The breeder documents must indicate identity, date of birth, proof of SSN or noneligibility, proof of residential address, and proof of lawful status or citizenship. No foreign documents are to be accepted except passports. The cost to the states to implement this new system is estimated to be $14.6 billion. So far, the federal government has only provided about $40 million in funding. It is estimated that the REAL ID Act's implementation will increase licensing costs to individuals by $7.62 billion and drive the cost of a license to $100 a person. The ACLU made the following arguments:

- A "national ID" would be a "one-stop shop" for ID thieves – easy to steal and hard to repair.

- Identity documents would be too easy to replicate under the REAL ID Act.

- The requirement of a single 50-state, interlinked database is unprecedented – and would make comprehensive and unique personal data assessable to every motor vehicle administration employee in the country.

- The MRZ called for in the new ID has no encryption requirement – making personal data readable by the private sector, with no limitations on use or access.

Ms. Boersma cited a number of computer and privacy organizations, including DHS's own Data Privacy and Integrity Committee that has criticized the unaddressed policy, privacy, and security issues of the REAL ID Act. Ms. Boersma also stated that DHS appears to be backing away from the compliance mandate by indicating that those people with noncompliant identification will not be turned away from federal courthouses or airplanes. It is now unclear how the REAL ID Act standards will be enforced. She said that nine states have officially refused to implement the REAL ID Act.

The ACLU urges the task force to make the following recommendations:

- Maryland should pass comprehensive legislation protecting data privacy and data security in both government agencies and the private sector, independent of REAL ID Act status.

- The General Assembly should delete funds for the REAL ID Act implementation until acceptable data privacy and data security standards have been enacted.

- The General Assembly should reject the REAL ID Act implementation until acceptable data privacy and data security standards have been enacted and federal funding provided to comply with standards.

In response to questions from the task force, Ms. Boersma testified that the REAL ID Act's regulations do not provide for how a state is to respond to a security breach of the REAL ID system. The time required to implement the REAL ID Act has been receding as states have made objections. She said there is still time for state governments to take a comprehensive approach to implementation if they decide to go forward with implementation. The National Governor's Association and the National Conference of State Legislatures (NCSL) have both proclaimed that the REAL ID Act must be fixed and funded or repealed. Since funding has not been forthcoming, the NCSL is expected to announce in January 2008 that it now supports the REAL ID Act's repeal.

## Motor Vehicle Administration

The Motor Vehicle Administration (MVA) was asked to provide testimony to the task force on the implementation of the REAL ID Act and issues relating to its impact on protecting Maryland from identity theft. Mr. John T. Kuo, task force member and the MVA Administrator, and Mr. Marshall Rickert, a consultant to MVA on best business practices, spoke.

Mr. Kuo began by reminding the task force that MVA, since its inception in 1910, has regularly developed and implemented special programs mandated by government, including, for example, programs in support of child support enforcement, arrest warrant enforcement, speed cameras, and truancy prevention. MVA is one of the most monitored agencies in the State and is regulated audited for compliance by both federal and State agencies.

Mr. Rickert agreed with Ms. Boersma's list of the REAL ID Act's requirements for driver's licenses and identity cards but emphasized that each element is already required in current identification issued by MVA, including full legal name, gender, driver's license or identification number, digital photo, principle address, signature, physical security features designed to prevent tampering, counterfeiting, or duplication, and a common machine-readable technology. Mr. Rickert pointed out that some people have raised concerns about the ability to read REAL ID compliant data with radio-frequency identification (RFID) technology. He said that RFID technology is not required under the REAL ID Act or recommended by DHS or MVA.

The REAL ID Act requires the following documentation from an applicant: photo identity document, date of birth, proof of SSN or verification of noneligibility, and proof of residency. New work rules required by the REAL ID Act include background checks for MVA employees, document retention and scanning, electronic verification of documents with the original issuer, and information sharing through a national network linking state databases. Information sharing with other states and agencies, which already occurs, is in the form of

"yes/no" queries. If a negative answer is received to a question on data in an application, the customer is refused a new card until the customer can provide confirmable information. There is no transfer of actual documentary information. Mr. Rickert testified that, once the REAL ID Act is implemented, MVA will produce all licenses and ID cards at a central facility and mail them to the customers. This will provide shorter transaction times in MVA offices, cost savings, and an additional fraud check. Although the customer would not leave the local MVA office with a driver's license, a temporary receipt confirming renewal may be provided. Mr. Rickert said that the cost estimates for implementation of the REAL ID Act that some have provided are "worst case scenarios." Most of the costs are driven by time deadlines for implementation rather than new work requirements. Therefore, many of the regulations are being modified and new regulations that ease the deadlines are expected to be issued soon. Mr. Rickert said that there are implementation problems with the REAL ID Act, but the problems can be corrected and no data storage system is perfect.

In response to questions from task force members, Mr. Rickert testified that the mailing of the new cards from a central facility should not present an additional security issue, because a stolen card would have the wrong picture, higher security elements, and no additional information about the customer than what the current license contains. Mr. Rickert testified that statistics have shown that when other motor vehicle agencies have changed to central issuance jurisdictions, fraud attempts have dropped. Mr. Kuo said that if there is an error on a newly issued card (like the wrong photo), a customer would have to return to MVA to correct the problem. MVA is not required to use standardized software under the REAL ID Act, just software that can interface with "yes/no" queries. Requiring a correct SSN should preclude the mix-up among customers with the same or similar names.

Senator Kelley stated that the most recent audit of MVA indicates significant concerns with the ability of MVA to adequately secure the personal information that it has custody of at this time. Implementation of the REAL ID Act would be overwhelming for MVA, and, given the problems cited in the audit, should not continue.

## Local Government Information Security Practices

### Maryland Association of Counties

The Maryland Association of Counties, Inc. (MACo) was asked to provide testimony to the task force on the following issues:

- What policies and practices govern when and how SSNs and other personal information are requested from the public and your employees?

- What policies and practices govern the personnel who have access to SSNs and other personal information and under what circumstances are these individuals permitted access?

- What procedures and practices ensure that access to SSNs and other personal information are limited to only those personnel who need the information to perform their job duties?

- What policies and practices govern how long SSNs and other personal information are kept and how the information is disposed of when no longer needed?

- How could policies, procedures, and practices be improved to protect SSNs and other personal information and limit or prevent unauthorized disclosure?

Mr. Leslie Knapp, MACo Associate Director, spoke with the task force.

As an overview, Mr. Knapp explained that there are three key policies to a county government maintaining security of personal information including (1) human resources; (2) information technology; and (3) compliance with federal and State law. With regard to human resources, counties must limit the use of SSNs; have clear policies regarding the disclosure, retention and destruction of personal information; require employees to sign written confidentiality agreements; and secure hard copies of all documents containing personal information. In the information technology area, counties need to limit access to electronic research; avoid the use of laptops; and, if laptops need to be used, protect information with data encryption and password-only access. Finally, with regard to legal compliance, counties must have staff that keep current with changes in the law and applicable regulations; and make sure that legitimately public information remains public. Mr. Knapp offered specific examples of how these policies are implemented in Anne Arundel County, Baltimore City, Frederick County, and Harford County.

**Maryland Municipal League**

The Maryland Municipal League (MML) was asked to provide testimony to the task force on the following issues:

- What policies and practices govern when and how SSNs and other personal information are requested from the public and your employees?

- What policies and practices govern the personnel who have access to SSNs and other personal information and under what circumstances these individuals are permitted access?

- What procedures and practices ensure that access to SSNs and other personal information is limited to only those personnel who need the information to perform their job duties?

- What policies and practices govern how long SSNs and other personal information are kept and how the information is disposed of when no longer needed?

- How could policies, procedures, and practices be improved to protect SSNs and other personal information and limit or prevent unauthorized disclosure?

Mr. Thomas C. Reynolds, Manager, Research and Information Management, provided information to the task force on behalf of MML. There are 157 municipalities in Maryland, with a wide range in the numbers of population and employees, some quite small. Credit card use has traditionally been rare. The former collection of SSNs of employees was maintained in locked files with limited access. By and large this has ceased, and employees are given unique employee identification numbers. Some of the large municipalities are now accepting credit card payment. When such transactions are taken over the phone, all information placed on paper is destroyed on completion of the transaction. In response to increasing concern over the threat of identity theft, MML has begun to explore the possibility of creating educational sessions for members and articles for its monthly magazine to better develop awareness.

**Maryland Chamber of Commerce**

The task force received written testimony from the Maryland Chamber of Commerce (the "chamber") offering comments regarding identity theft. In a letter dated November 12, 2007, the chamber's Vice-President of Governmental Affairs, Ronald W. Wineholt, cited three recent news accounts of lost or stolen computer laptops or data drives from county and State agencies. Mr. Wineholt urged the task force to recommend to the General Assembly that State and local agencies be required to "abide by many of the same security breach and Social Security number standards that have been applied to Maryland businesses." Specifically, the chamber suggested:

- The exemption for State and local government agencies from the Social Security Number Privacy Act (CL, § 14-3301) could be repealed.

- State agencies could be prohibited from requiring the submission of SSNs unless specifically authorized by State or federal law.

- State agencies could be added to the Maryland Person Information Protection Act (CL, §§ 14-3504 – 14-3508) (MPIPA) that requires reasonable steps be taken when destroying the personal information of customers.

- State agencies could be added to the security breach provisions of the MPIPA, requiring that specified actions be taken when a security breach has occurred.

## Work Session

After receiving testimony, the task force spent the remainder of the session discussing possible recommendations to include in the final report. At the direction of Co-chairman Kelley, staff presented a list of suggested recommendations that the task force had received from prior testimony and some recommendations inferred from questions raised in prior sessions by task force members to witnesses. Senator Kelley suggested that the focus be put on the recommendations received from many witnesses for improvements in law enforcement, including:

- witness affidavit in lieu of personal testimony;
- authorizing forfeiture of proceeds from identity fraud crime on conviction;
- unauthorized possession of another's mail becomes crime;
- increase penalties for the identity theft offense to make comparable to credit card fraud crimes;
- expungement of criminal records for those falsely accused due to identity theft;
- admissibility of business records, including faxes and e-mails, by account holders, in addition to record custodians;
- training on identity theft record and case development for local police departments and State's Attorney's offices by the Office of the Attorney General – allowing training and materials to be provided via the Internet to reduce costs; and
- prohibiting the unauthorized possession of "skimmers" (portable devices that read and store credit card numbers or other personal data).

Task force member Steve Sakamoto-Wengel suggested that the task force should also consider adopting a new Social Security Number Protection Act and a statute similar to one in Minnesota that limits the length of time a retailer may hold onto transaction information. Task force member A. Marie Day suggested that the task force be given copies of the language of the legislation suggested by Mr. Sakamoto-Wengel before discussing them further. Senator Kelley added that the task force should consider endorsing the ACLU's suggestion that Maryland refrain from implementation of the REAL ID Act until provided with assurances of security regulations and proper federal funding. Senator Kelley suggested that, if the task force does decide to recommend specific legislation, that such bills be identified as "task force bills."

After a distribution of sample legislation, Senator Kelley asked if the task force was supportive of the recommendations that (1) rules of evidence be amended to allow a witness affidavit be used in an identity theft prosecution in lieu of personal testimony; and (2) to allow business records, including faxes and e-mails, to be admissible on testimony by account holders, in addition to record custodians. A show of hands indicated unanimous support by members. Senator Kelley suggested that the two ideas be joined in a single bill. Task force member A. Marie Day asked on a procedural point whether a dissenting member could register dissent if

the majority of the task force made a recommendation of which the dissenter did not approve. Senator Kelley responded that dissent could be freely given.

Senator Kelley then asked for comments on the proposal to authorize forfeiture of proceeds from identity fraud crime on conviction. Task force member Jeffrie Zellmer cautioned that similar legislation failed in the House Judiciary Committee last session because of various concerns, like when assets could be frozen and what to do with funds obtained from the forfeiture. It was suggested that assets only be frozen at indictment and not forfeited until conviction. There was a general discussion concerning the difficulty encountered in fairly dividing a lending institution's interest and that of the identity thief in a real estate forfeiture, and other issues relating to the idea. Senator Kelley appointed a subcommittee of task force members to review and discuss the proposal and report back to the full task force at the next meeting. The subcommittee consisted of task force members A. Marie Day, Henry Greenberg, Steven Hannan, Sarah Bloom Raskin, and Steve Sakamoto-Wengel.

A discussion was then held on the proposal to increase penalties for identity theft crimes. After a wide ranging discussion on various issues and possibilities, it was suggested that an ID theft of over $500 should have a penalty of 15 years, instead of only 5 years. It was also suggested that ID thefts by fiduciaries, repeat offenders, in cases of multiple victims or where the victim is a "vulnerable adult" also be treated as a 15 year penalty. Senator Kelley requested that a workable definition of "fiduciary" be included in the draft under consideration.

Finally, a discussion was held on the proposal to make the unauthorized possession of another's mail a crime. House Bill 293 of 2007 was reviewed and discussed. Delegate McComas advised that creating such a crime might be an additional weapon in the arsenal between an aggrieved couple in a domestic or divorce dispute. Delegate McComas also expressed concern that a person could get into trouble for picking up another's mail as a favor. Various ideas to amend the bill were discussed, including setting a threshold of requiring the offender to have three or more unrelated persons' mail, or requiring that the intent to commit the crime of identity theft be an element that must be proven to get a conviction. The idea of setting thresholds or providing an intent requirement was criticized as making the bill ineffective. It was noted that the bill as written requires that the possession be unauthorized. The task force agreed to endorse the bill without amendments and leave it for the General Assembly to amend, if it decides to do so.

## Session VI – Tuesday, December 6, 2007

The task force held its sixth and final work session on December 6, 2007, to discuss and vote on possible recommendations for the report of the task force.

## Increased Penalties

Co-chairman Lee began by asking staff to present a draft of a bill containing increased penalties for identity fraud which had received support from the members of the task force at the previous work session. Staff presented a draft bill (LR1088/1089) that increases the penalty for felony identity fraud from a maximum of 5 to 15 years imprisonment and from a $25,000 to a $50,000 fine. The draft bill also provides the same penalty to a person who commits identity fraud while serving as a "fiduciary" for the victim, or if a person commits identity fraud against a "vulnerable adult." Definitions for the terms "fiduciary" and "vulnerable adult" were provided (and are from other sections of the Maryland Code). Finally, the bill provides for a similarly enhanced penalty for a person convicted of identity fraud who has been convicted of identity fraud on a prior occasion not arising from the same incident. The task force members discussed the language of the bill and no objections to the draft were raised. It was noted that draft bills receiving support from the task force would be co-sponsored by the legislator-members of the task force and the "Maryland Task Force to Study Identity Theft" and cross-filed in both houses. A motion was made to endorse the bill as drafted. The motion was seconded. The motion was passed unanimously.

## Unauthorized Possession of Mail

Delegate Lee then asked the task force members to consider a bill that had been discussed at the previous work session prohibiting a person from knowingly and willfully removing, taking, possessing, obtaining, or receiving mail under certain circumstances without the permission of the United States Postal Service or the intended recipient, similar to House Bill 293 which had been introduced in the 2007 session. A draft bill was reviewed by the members (LR1127/1128) and discussed. A motion was made to endorse the bill as drafted. The motion was seconded. The motion was passed unanimously.

## Forfeiture

Co-chairman Lee then asked for the report of the subcommittee that had been asked to discuss possible legislation to provide for the seizure and forfeiture of property that a person convicted of identity fraud had taken from the offense. The chairman of the subcommittee, Ms. A. Marie Day, reported that the subcommittee had met twice since the previous task force meeting and had substantive discussions about various issues, including what would be involved in ordering property to be "frozen" and/or seized before trial, how to protect secured and other innocent third parties, and whether and in what fashion victims of identity fraud should receive restitution from forfeited property.

Subcommittee Chairman Day reported that the subcommittee was generally supportive of calling for the forfeiture of property from criminals convicted of identity fraud but had not reached full agreement on the details of a specific bill. With Co-chairman Lee's permission, the task force heard a presentation from Mr. Bob Enten of the Maryland Bankers Association

(MBA), on the history and mechanics of the current Maryland drug forfeiture statute. Mr. Enten suggested that a bill patterned on that statute, which he thought adequately protects "lien holders," might partially serve the purposes of the General Assembly, should it agree to establish forfeiture for identity fraud. The proceeds from the drug forfeiture law, however, go to the prosecuting law enforcement agency, and various task force members suggested that a distribution of at least some of the proceeds to the victims of identity theft would be a better use of those funds. It was noted that as part of the sentence, a Maryland court can currently order a criminal to make restitution to an identity theft crime victim, but that such payments rarely make the victim "whole." How the proceeds from forfeiture would be distributed was then generally discussed by task force members, with some suggesting that victims receive a liquidated amount, and others urging that any amount be tied to actual damages. It was also suggested that it would be helpful to victims if the court could provide a form that could be used as a "proof of claim." A motion was made to recommend that a forfeiture draft be developed which reflects the concepts expressed by task force members after the General Assembly conducts further study on these issues. The motion was seconded. The motion was passed unanimously.

## REAL ID

Co-chairman Lee then asked the members to discuss whether to take a position on the REAL ID Act, on which the task force had received testimony. Co-chairman Lee pointed out that the Motor Vehicle Administration (MVA) had recently received an audit with an unsatisfactory rating and raised a question as to whether the agency would be able to handle the additional responsibilities that would be required under REAL ID. Co-chairman Lee also pointed to testimony that REAL ID would costs almost $50 million for Maryland to implement, with no reimbursement expected from the federal government. Finally, Co-chairman Lee reminded the task force of the testimony it received concerning the increased danger to the security of personal information under REAL ID and the lack of safeguards under the Act.

The task force representative for MVA responded that a hearing has been scheduled by the Joint Audit Committee to review the audit. MVA expected to report that many of the concerns had already been addressed. The representative emphasized that there has never been an actual breach of security at MVA and that, if anything, implementation of REAL ID would increase security at the agency. Co-chairman Lee responded that REAL ID apparently lacks security standards and the interconnectivity of the databases with other states is a real concern. Co-chairman Kelley described the audit as an "F" for MVA and pointed to instances of failure to encrypt personal information from bank checks and the issuance of driver's licenses to individuals who were actually dead. Co-chairman Kelley reported that she had recently attended a conference sponsored by the National Conference of State Legislatures. The Secretary of the Department of Homeland Security had given a speech in which he indicated that, in response to the many concerns that had been raised, new regulations would be forthcoming within two months. Details of the revised regulations, however, were unavailable.

Co-chairman Kelley proposed that the task force report indicate that the General Assembly should delay the implementation of REAL ID at this time due to the deficiencies in

security standards and because it represents an unfunded mandate by the federal government that Maryland cannot afford at this time. The MVA representative stated that MVA has been assured by the Department of Homeland Security that the concerns about information security have been taken seriously. Many of the current requirements that led to the high cost estimates for implementation are expected to be less onerous. The representative cautioned, however, that the consequences of a refusal to implement the REAL ID program will mean that Maryland driver's licenses will no longer be valid for a variety of federal purposes. Co-chairman Kelley suggested that the task force certainly could not endorse implementation of the REAL ID Act at this time but should recommend that the General Assembly decide this issue. A motion was made that the task force caution the General Assembly to delay action on the implementation of the REAL ID Act until the new regulations are promulgated and the relevant standing committees have had the opportunity to be briefed and to review them. The motion was seconded. The motion was passed with one dissenting vote made by the MVA representative.

## State Agencies

Co-chairman Lee then opened the floor for motions concerning recommendations the task force might make regarding the handling of personal information by State and local governmental agencies. Co-chairman Kelley reviewed testimony that the task force had taken about the varying standards for information security that are employed, depending on the agency. Co-chairman Kelley reminded the task force that mandating security standards for State agencies would require additional expenditures that could be of concern considering the current budget problems affecting the State. A motion was made to recommend that the General Assembly study the feasibility of establishing additional standards for State and local agencies regarding personal information security including further review of what information is collected and the purposes for which it is collected. The motion was seconded and passed unanimously.

## Limits on the Storage of Transaction Information by Retailers

Co-chairman Lee asked task force member Steve Sakamoto-Wengel to discuss a proposal to recommend that the General Assembly consider legislation similar to that passed recently in Minnesota requiring retailers to refrain from retaining personal information taken from credit and debit cards any longer than required to process the transaction. Mr. Sakamoto-Wengel provided task force members a copy of the Minnesota legislation and noted that the National Retail Federation had indicated support for the new law. Task force member Eric Ellman indicated that he had not seen the legislation before, but that his understanding was that retailers would not support the concept. Mr. Ellman pointed out that the Minnesota law could interfere with the contractual relationship between the card processor and the retailer. Also, if a consumer wanted to dispute a charge, but the retailer has no record of the transaction, it may be more difficult for the consumer to resolve the dispute. Task force member Jeffrie Zellmer added that the Maryland Retailers Association was not supportive. Mr. Enten (who was given permission by the chairmen to stand in for A. Marie Day, who was excused from the remainder of the meeting) pointed out that only one state had apparently passed this type of law, and that MBA had not had

time to evaluate it. Task force member Delegate Susan McComas asked if such legislation could be viewed as an unfunded mandate on business. Task force member Mr. Sakamoto-Wengel responded that it could also be an unfunded mandate for businesses to be required to hold onto transaction data for a year or more and be responsible for setting up adequate security to protect the information from unauthorized access. Co-chairman Kelley suggested that the task force did not know enough about the legislation and suggested it called for further study. A motion was made to inform the General Assembly that the issue of mandating an optimum time that retailers were authorized to retain transaction information had been raised, but that no action was taken by the task force. The motion was seconded and passed unanimously.

## Expungement

Co-chairman Lee then asked for a discussion on the issue of recommending legislation to assist victims of identity fraud with expungement of criminal records, similar to House Bill 931 from the 2007 session. How the bill had been previously viewed by the House Judiciary Committee was discussed. Co-chairman Kelley thought that the bill was a good idea. Mr. Zellmer said that his organization had supported the bill. Mr. Sakamoto-Wengel cautioned that the Office of Attorney General (OAG) was concerned about being required to administer expungements on behalf of identity fraud victims. Co-chairman Kelley responded that administering expungement on a statewide basis made more sense than letting the various courts handle the issue in their own fashion. Delegate McComas stated that the opportunity for expungement is greater if the mistake is discovered earlier in the criminal justice process. Task force member Steve Hannan stated that expunging a criminal record is very labor intensive and a program to do to this for victims would require funding. If OAG was required to manage the program, it would need to subcontract out much of the background checks that would be required. Mr. Sakamoto-Wengel asked task force member Isabel Mercedes Cumming if a judge could be asked to order expungement of the victim's record as part of its disposition of a criminal case. Ms. Cumming responded that this was a good idea. Delegate McComas noted that expunging aliases from police files is difficult and could make it more difficult to track the criminals who use aliases. Co-chairman Kelley reminded the task force that victims are often unsophisticated about taking the right steps to proceed on issues like getting expungement of false criminal records. It was suggested that consideration of how expungement could be accomplished through a task force or other vehicle would be a good idea. The study should include input from the courts, the police, prosecutors, and others. However, no motion was made and the discussion ended on this issue.

## Credit Card Skimming Devices and Reencoders

Co-chairman Lee then asked the task force to discuss a proposal to recommend legislation to the General Assembly making the unauthorized possession and use of certain devices known as "skimmers" and "reencoders" illegal. Delegate McComas introduced a bill draft prepared by staff for review (LR1170). The bill would prohibit the unauthorized possession and use of skimming devices that access, read, memorize, or otherwise obtain

payment device numbers or personal identifying information. The bill would also prohibit the use of a reencoder to place information encoded on the magnetic strip or stripe of a credit card onto the magnetic strip or stripe of a different credit card or use any other electronic medium that allows such a transaction to occur without the consent of the individual authorized to use the credit card. Penalties would be the same as those currently established for other identity fraud, *i.e.*, if the amount stolen has a value of over $500, the offense would be a felony with the possibility of 5 years imprisonment or a $25,000 fine or both and, if less than $500, a misdemeanor, with the possibility of 18 months imprisonment or a fine of $5,000 or both. Delegate McComas advised that similar legislation had been enacted in 28 states. A motion to endorse the legislation was made and seconded, and received a unanimous vote from the task force members.

## Identity Theft Training of Local Law Enforcement Agencies by Office of Attorney General

A motion was made to recommend that OAG develop and provide training in identity theft record and case development to local police departments and State's Attorney's offices. The task force agreed that such training could be provided via the Internet to reduce costs. The motion was seconded and received unanimous support from the members of the task force.

## Witness Affidavits and Admissibility of Business Records

The task force then reviewed a draft bill (LR1172) that combined two evidentiary reforms that had received unanimous support during the prior work session. The bill would (1) make personal bank records, business bank records, personal credit card reports, business credit card reports, personal credit card statements, business credit card statements, personal credit card notices, and business credit card notices admissible as evidence and presumed to be authentic if the account holder testifies as to their authenticity in a judicial or administrative proceeding; and (2) add the crime of identity fraud to the list of offenses for which an affidavit sworn to by a lawful credit cardholder may be introduced as substantive evidence that the credit card or credit card number was taken, used, or possessed without the authorization of the credit cardholder. The affidavit would be allowed if, at least 10 days before a proceeding at which the State intends to introduce the affidavit, notice is given to the defendant and the defendant fails within 5 days of the proceeding to make a written demand to require the presence of the affiant as a prosecution witness. A motion was made to recommend the bill to the General Assembly. The motion was seconded and received unanimous support.

Hearing no further motions, Co-chairmen Kelley and Lee thanked the task force and staff for their work.

# Appendices

- Task Force Meeting Agendas
- Legislation Recommended by the Task Force
  - Criminal Law – Mail Theft – Penalty
  - Identity Fraud – Personal and Business Documents and Cardholder Affidavits – Evidence
  - Identity Fraud – Prohibition of Unauthorized Skimming and Reencoding Devices
  - Identity Fraud – Felony or Repeat Offender, Fiduciary, or Vulnerable Adult – Penalties
    - NCSL Summary of Credit Skimming Laws
- Disclosure of Social Security Numbers Under Maryland Law
- NCSL Summary of Use of Social Security Numbers by States
- Custody and Use of Social Security Numbers – State Agency Responses to Questionnaire
  - Department of Health and Mental Hygiene
  - Department of Human Resources
  - Maryland Department of Transportation, Motor Vehicle Administration
  - Office of the Comptroller
  - University System of Maryland
  - Maryland Independent Colleges and Universities
  - Maryland Association of Community Colleges
  - Department of Budget and Management
    - Additional Follow-up Information
- Additional Testimony Submitted to the Task Force
  - Office of the State's Attorney for Baltimore City
  - Office of the Public Defender
  - Maryland Criminal Defense Attorneys' Association
  - Maryland Bankers Association
- Additional Information
  - Storage of Credit Information by Retailers
  - Consumers Union Model Legislation – Protection of Social Security Numbers

MARYLAND GENERAL ASSEMBLY
TASK FORCE TO STUDY IDENTITY THEFT

***Senator Ralph M. Hughes, Co-Chairman***
***Delegate Susan C. Lee, Co-Chairman***

# Agenda

Wednesday November 15, 2006
2:00p.m.
Judiciary Committee hearing room (Room 100, House Office Building)

---

**Call to Order and Opening Statements**
Senator Ralph M. Hughes, Co-Chairman
Delegate Susan C. Lee, Co-Chairman

**Introduction of Task Force Members and Staff**

**A Review of the Authorizing Legislation for the Task Force**
John J. Joyce
Task Force Staff

**Legislative Responses to Identity Theft**
Karen D. Morgan
Task Force Staff

**Presentation of Draft Interim Report and Proposed Legislation to Extend the Task Force**
John J. Joyce
Task Force Staff

**Adjournment**



Room 110 Legislative Services Building · 90 State Circle · Annapolis, Maryland 21401-1991
410-946-5350 · Fax 410-946-5395 · TDD 410-946-5401
301-970-5350 · Fax 301-970-5395 · TDD 301-970-5401

MARYLAND GENERAL ASSEMBLY
TASK FORCE TO STUDY IDENTITY THEFT

***Senator Delores G. Kelley, Co-Chairman***
***Delegate Susan C. Lee, Co-Chairman***

# Agenda

Wednesday, August 22, 2007
1:00 p.m.
Judiciary Committee Hearing Room (Room 100, House Office Building)

---

- **Department of Health and Mental Hygiene**

  Mr. Jim Johnson
  Deputy Secretary of Operations

  Ms. Geneva Sparks
  Deputy State Registrar
  Vital Records Administration

  Mr. Charles Lehman
  Executive Director, Office of Operation and Eligibility
  Medicaid Administration

- **Department of Human Resources**

  Mr. Brian Wilbon
  Deputy Secretary

- **Maryland Department of Transportation**
  **Motor Vehicle Administration**

  Ms. Christine Nizer
  Associate Administrator for Driver and Vehicle Policies and Programs



Room 110 Legislative Services Building · 90 State Circle · Annapolis, Maryland 21401-1991
410-946-5350 · Fax 410-946-5395 · TDD 410-946-5401
301-970-5350 · Fax 301-970-5395 · TDD 301-970-5401

- **Maryland Department of Transportation**
  **Motor Vehicle Administration – (continued)**

  Ms. Sandy Pinder
  Associate Administrator for Information Resources

  Ms. Rose Bianco
  Internal Investigator

- **Office of the Comptroller**

  Ms. Linda Tanton
  Deputy Comptroller

- **University Systems of Maryland**

  Dr. Donald Z. Spicer
  Associate Vice-Chancellor and CIO

  Mr. Lennox Brown
  Manager, Information Systems Audit

- **Maryland Independent College and University Association**

  Ms. Tina Bjarekull
  President

- **Maryland Association of Community Colleges**

  Dr. Deborah Cruise
  Vice President for Student Development and Institutional Effectiveness
  Harford Community College

  Ms. Lori Rounds
  Chief Technology Officer
  Frederick Community College

- **Department of Budget and Management**

  Ms. Becky Burner
  Legislative Liaison

MARYLAND GENERAL ASSEMBLY
TASK FORCE TO STUDY IDENTITY THEFT

***Senator Delores G. Kelley, Co-chair***
***Delegate Susan C. Lee, Co-chair***

# Agenda

Tuesday, September 18, 2007
1:00 p.m.
Judiciary Committee Room, House Office Building, Room 100

---

Consumers and Businesses: Dealing With Identity Theft

Welcome and Opening Remarks
Senator Delores Kelley, Senate Chair
Delegate Susan Lee, House Chair

*Consumers and Consumer Representatives*

Federal Trade Commission
Ms. Betsy Broder
Assistant Director
Division of Privacy and Identity Protection

Other Consumer Representatives

Mr. Evan Hendricks
Founder, Editor, Publisher
Privacy Times

Sonya Smith-Valentine, Esq.
The Valentine Legal Group, LLC
Consumer Advocate

Michael Worsham, Esq.
Private Practice Attorney and Consumer Advocate

Dr. Edward C. Papenfuse
State Archivist and Commissioner of Land Records
Maryland State Archives



Room 110 Legislative Services Building · 90 State Circle · Annapolis, Maryland 21401-1991
410-946-5350 · Fax 410-946-5395 · TDD 410-946-5401
301-970-5350 · Fax 301-970-5395 · TDD 301-970-5401

Citizen Consumer Panel

Mr. Warren Gatewood
Ms. Ginny Shelp
Ms. Cindi Curtis
Mr. Michael Johnson

*Business Representatives*

Banking Panel

Ms. Kathleen Murphy
President and Chief Executive Officer
Maryland Bankers Association

Mr. Kevin Smith
Senior Vice President and Corporate Security Director
Chevy Chase Bank
Chairman of the Maryland Bankers Association Security Committee

Ms. Eartha Morris
Senior Vice President of Management of Consumer Information
Provident Bank

Ms. Michael W. Briggs
Legal Counsel, Gordon, Feinblatt, Rothman, Hoffberger and Hollander

Ms. Mindy Lehman
Vice President of Government Affairs
Maryland Bankers Association

Credit Card Company

Mr. Mark MacCarthy
Senior Vice President, Public Policy
Visa USA, Inc.

Retail Panel

Mr. Damien Walter
Investigator, Loss and Prevention
Target Corporation

Mr. Jeffrie Zellmer
Legislative Director
Maryland Retailers Association

MARYLAND GENERAL ASSEMBLY
TASK FORCE TO STUDY IDENTITY THEFT

***Senator Delores G. Kelley, Co-chair***
***Delegate Susan C. Lee, Co-chair***

# Agenda

Tuesday, October 2, 2007
1:00 p.m.
Judiciary Committee Room, House Office Building, Room 100

---

Prince George's County Office of State's Attorney

Delegate Doyle L. Niemann
Assistant State's Attorney

Isabel Mercedes Cumming
Assistant State's Attorney

Montgomery County Office of State's Attorney

Robert Hill
Assistant State's Attorney

U.S. Secret Service

Tamara Blair
Assistant Special Agent in Charge
Baltimore Field Office

Federal Bureau of Investigation

David Musgrove
Supervisory Special Agent
Baltimore Field Office

Department of State Police

First Sgt. Robert Smolek



Room 110 Legislative Services Building · 90 State Circle · Annapolis, Maryland 21401-1991
410-946-5350 · Fax 410-946-5395 · TDD 410-946-5401
301-970-5350 · Fax 301-970-5395 · TDD 301-970-5401

Baltimore County Office of State's Attorney

Scott Shellenberger
State's Attorney

Marsha Russell
Assistant State's Attorney

Baltimore County Police Department
Economic Crimes Unit

Lt. Douglas McManus
Commander

Det. Cpl. Morgan Hassler
Supervisor

Greg Hebding
Detective

Legal Division

Greg Rothwell
Acting Director

U.S. Postal Inspection Service

John Schick
Supervisory Postal Inspector

Burt Foster
Postal Inspector

Michael Blackman
Postal Inspector

Mark Coulter
Detective
Prince George's County Police Department

Maryland Association of Bank Security

Robert Smetzer
President, Maryland Association of Bank Security
Fraud Investigator, Greater Maryland Region, PNC Bank

Michelle Stutheit
Member, Maryland Association of Bank Security
Security Coordinator, SunTrust Bank

MARYLAND GENERAL ASSEMBLY
TASK FORCE TO STUDY IDENTITY THEFT

***Senator Delores G. Kelley, Co-chair***
***Delegate Susan C. Lee, Co-chair***

# Agenda

Tuesday, November 13, 2007
1:00 p.m.
Judiciary Committee Room, House Office Building, Room 100

---

REAL ID Act and the Impact on Identity Theft

John Kuo, Administrator
Motor Vehicle Administration

Cynthia Boersma, Legislative Director
American Civil Liberties Union

Local Government Information Security Practices

Michael Sanderson, Legislative Director
Leslie Knapp, Associate Director
Maryland Association of Counties

Tom Reynolds
Manager, Research and Information Management
Maryland Municipal League

Work Session

Adjournment



Room 110 Legislative Services Building · 90 State Circle · Annapolis, Maryland 21401-1991
410-946-5350 · Fax 410-946-5395 · TDD 410-946-5401
301-970-5350 · Fax 301-970-5395 · TDD 301-970-5401

MARYLAND GENERAL ASSEMBLY
TASK FORCE TO STUDY IDENTITY THEFT

***Senator Delores G. Kelley, Co-chair***
***Delegate Susan C. Lee, Co-chair***

# Agenda

Thursday, December 6, 2007
10:00 a.m.
Senate Finance Committee Room
3 East, Miller Senate Office Building

---

## Work Session

- Review of Legislative Drafts for Task Force Consideration
  - Expungement of False Criminal Record
  - Mail Theft Possession
  - Enhanced Identity Theft Penalties
  - Possession and Use of Skimmers
  - Affidavits and Document Authentication
  - Use of Social Security Numbers
  - Storage of Credit Information by Retailers
- Report of Subcommittee on Proposed Forfeiture Legislative Draft
- Discussion of Other Recommendations and Ideas
- Discussion of Final Report
- Adjournment



Room 110 Legislative Services Building · 90 State Circle · Annapolis, Maryland 21401-1991
410-946-5350 · Fax 410-946-5395 · TDD 410-946-5401
301-970-5350 · Fax 301-970-5395 · TDD 301-970-5401

E1
HB 293/07 – JUD

8lr1127
CF 8lr1128

Bill No.: _____

Drafted by: Joyce

Requested: _____

Committee: _____

By: **Delegates Niemann, Lee, and McComas (Maryland Task Force to Study Identity Theft)**

A BILL ENTITLED



AN ACT concerning

**Criminal Law - Mail Theft - Penalty**

FOR the purpose of prohibiting a person from knowingly and willfully removing, taking, possessing, obtaining, or receiving mail under certain circumstances without the permission of the United States Postal Service or the intended recipient; providing penalties for a violation of this Act; repealing a prohibition against opening a letter without permission; providing that a person who violates this Act is subject to a certain statute of limitations; defining certain terms; and generally relating to the theft of mail.

BY repealing
Article – Criminal Law
Section 3–905
Annotated Code of Maryland
(2002 Volume and 2007 Supplement)

BY adding to
Article – Criminal Law
Section 7–106.1
Annotated Code of Maryland
(2002 Volume and 2007 Supplement)

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.
[Brackets] indicate matter deleted from existing law.

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

**Article – Criminal Law**

[3–905.

(a) A person may not take and break open a letter that is not addressed to the person without permission from the person to whom the letter is addressed or the personal representative of the addressee's estate.

(b) A person who violates this section is guilty of a misdemeanor and on conviction is subject to imprisonment for 6 days and a fine of $15.]

**7–106.1.**

(A) (1) IN THIS SECTION THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.

(2) "MAIL" MEANS A LETTER, POSTAL CARD, PACKAGE, BAG, OR OTHER SEALED ARTICLE.

(3) "MAIL CARRIER" MEANS A PERSON OR ENTITY THAT DELIVERS MAIL ON BEHALF OF THE POSTAL SERVICE.

(4) "MAIL DEPOSITORY" MEANS A MAILBOX, LETTER BOX, OR RECEPTACLE IN WHICH MAIL IS DEPOSITED OR STORED; A POST OFFICE OR STATION OF A POST OFFICE; A MAIL ROUTE; OR A VEHICLE USED BY THE POSTAL SERVICE FOR THE DELIVERY OF MAIL.

(5) "POSTAL SERVICE" MEANS THE UNITED STATES POSTAL SERVICE OR ANY OF ITS SUBSIDIARIES OR CONTRACTORS.

(B) A PERSON MAY NOT KNOWINGLY OR WILLFULLY AND WITHOUT PERMISSION FROM THE POSTAL SERVICE OR THE INTENDED RECIPIENT:

(1) REMOVE MAIL FROM A MAIL DEPOSITORY;

(2) TAKE MAIL FROM A MAIL CARRIER;

(3) OBTAIN CUSTODY OF MAIL BY INTENTIONALLY DECEIVING A MAIL CARRIER, OR OTHER PERSON WHO RIGHTFULLY POSSESSES OR CONTROLS THE MAIL, WITH A FALSE REPRESENTATION THAT IS KNOWN TO BE FALSE, MADE WITH INTENT TO DECEIVE;

(4) TAKE MAIL, OR THE CONTENTS OF MAIL, THAT HAS BEEN LEFT FOR COLLECTION OR DELIVERY ON OR NEAR A MAIL DEPOSITORY; OR

(5) RECEIVE, POSSESS, TRANSFER, BUY, OR CONCEAL MAIL OBTAINED BY ACTS DESCRIBED IN PARAGRAPHS (1) THROUGH (4) OF THIS SUBSECTION KNOWING OR HAVING REASON TO KNOW THE MAIL WAS OBTAINED ILLEGALLY.

(C) A PERSON WHO VIOLATES THIS SECTION IS GUILTY OF A MISDEMEANOR AND ON CONVICTION IS SUBJECT TO IMPRISONMENT NOT EXCEEDING 3 YEARS OR A FINE NOT EXCEEDING $5,000 OR BOTH.

(D) A PERSON WHO VIOLATES THIS SECTION IS SUBJECT TO § 5–106(B) OF THE COURTS ARTICLE.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2008.

E2, I4

8lr1172
CF 8lr1320

Bill No.: _____

Requested: _____

Committee: _____

Drafted by: Morgan



By: **Senators Kelley and Jones (Task Force to Study Identity Theft)**

A BILL ENTITLED

AN ACT concerning

**Identity Fraud – Personal and Business Documents and Cardholder Affidavits – Evidence**

FOR the purpose of providing that certain personal and business documents are admissible as evidence and presumed to be authentic if a certain person testifies as to their authenticity in any judicial or administrative proceeding; providing that a certain affidavit by a lawful credit cardholder may be introduced as evidence in a certain criminal or juvenile proceeding; and generally relating to the admissibility personal and business documents and affidavits as evidence.

BY adding to

Article – Commercial Law

Section 24–101 to be under the new title "Title 24. Authentication of Documents"

Annotated Code of Maryland

(2005 Volume and 2007 Supplement)

BY repealing and reenacting, with amendments

Article – Criminal Law

Section 8–214.1

Annotated Code of Maryland

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.

(2002 Volume and 2007 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

**Article – Commercial Law**

**TITLE 24. AUTHENTICATION OF DOCUMENTS.**

**24–101.**

**THE FOLLOWING DOCUMENTS ARE ADMISSIBLE AS EVIDENCE AND PRESUMED TO BE AUTHENTIC IF THE ACCOUNT HOLDER TESTIFIES TO AS TO THEIR AUTHENTICITY IN ANY JUDICIAL OR ADMINISTRATIVE PROCEEDING:**

**(1) PERSONAL BANK RECORDS;**

**(2) BUSINESS BANK RECORDS;**

**(3) PERSONAL CREDIT CARD REPORTS;**

**(4) BUSINESS CREDIT CARD REPORTS;**

**(5) PERSONAL CREDIT CARD STATEMENTS;**

**(6) BUSINESS CREDIT CARD STATEMENTS;**

**(7) PERSONAL CREDIT CARD NOTICES; AND**

**(8) BUSINESS CREDIT CARD NOTICES.**

**Article – Criminal Law**

8–214.1.

(a) In a criminal case or juvenile proceeding involving a violation of § 8–204, § 8–205, § 8–206, § 8–207, § 8–208, § 8–209, § 8–210, [or] § 8–214, **OR § 8–301** of this subtitle, an affidavit sworn to by a lawful credit cardholder may be introduced as

substantive evidence that the credit card or credit card number was taken, used, or possessed without the authorization of the credit cardholder.

(b) (1) At least 10 days before a proceeding in which the State intends to introduce into evidence an affidavit as provided under this section, the State shall provide written notice to the defendant that the State intends to:

(i) rely on the affidavit; and

(ii) introduce the affidavit into evidence at the proceeding.

(2) On written demand of a defendant filed at least 5 days before the proceeding described in subsection (a) of this section, the State shall require the presence of the affiant as a prosecution witness.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2008.

E1 8lr1170
CF 8lr1321

Drafted by: Morgan

Bill No.: _____

Requested: _____

Committee: _____

By: **Delegates McComas, Lee, and Niemann (Task Force to Study Identity Theft)**

A BILL ENTITLED



AN ACT concerning

**Identity Fraud – Prohibition of Unauthorized Skimming and Reencoding Devices**

FOR the purpose of prohibiting the unauthorized possession and use of certain devices that access, read, memorize or otherwise obtain a payment device number or personal identifying information; providing certain penalties; defining certain terms; and generally relating to the unauthorized use or possession of certain devices.

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

**Article – Criminal Law**

BY repealing and reenacting, with amendments,
Article – Criminal Law
Section 8–301
Annotated Code of Maryland
(2002 Volume and 2007 Supplement)

8–301.

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.
[Brackets] indicate matter deleted from existing law.

(a) (1) In this section the following words have the meanings indicated.

(2) "Payment device number" has the meaning stated in § 8–213 of this title.

(3) "Personal identifying information" includes a name, address, telephone number, driver's license number, Social Security number, place of employment, employee identification number, mother's maiden name, bank or other financial institution account number, date of birth, personal identification number, credit card number, or other payment device number.

**(4) "REENCODER" MEANS AN ELECTRONIC DEVICE THAT PLACES ENCODED PERSONAL IDENTIFYING INFORMATION OR A PAYMENT DEVICE NUMBER FROM THE MAGNETIC STRIP OR STRIPE OF A CREDIT CARD ONTO THE MAGNETIC STRIP OR STRIPE OF A DIFFERENT CREDIT CARD OR ANY ELECTRONIC MEDIUM THAT ALLOWS SUCH A TRANSACTION TO OCCUR.**

**(5) "SKIMMING DEVICE" MEANS A SCANNER, SKIMMER, READER, OR ANY OTHER ELECTRONIC DEVICE THAT IS USED TO ACCESS, READ, SCAN, OBTAIN, MEMORIZE, OR STORE, TEMPORARILY OR PERMANENTLY, PERSONAL IDENTIFYING INFORMATION OR A PAYMENT DEVICE NUMBER ENCODED ON THE MAGNETIC STRIP OR STRIPE OF A CREDIT CARD.**

(b) A person may not knowingly, willfully, and with fraudulent intent possess, obtain, or help another to possess or obtain any personal identifying information of an individual, without the consent of the individual, in order to use, sell, or transfer the information to get a benefit, credit, good, service, or other thing of value in the name of the individual.

(c) A person may not knowingly and willfully assume the identity of another:

(1) to avoid identification, apprehension, or prosecution for a crime; or

(2) with fraudulent intent to:

(i) get a benefit, credit, good, service, or other thing of value; or

(ii) avoid the payment of debt or other legal obligation.

**(D) A PERSON MAY NOT KNOWINGLY, WILLFULLY, AND WITH FRAUDULENT INTENT TO GET A BENEFIT, CREDIT, GOOD, SERVICE OR OTHER THING OF VALUE, USE:**

**(1) A REENCODER TO PLACE INFORMATION ENCODED ON THE MAGENTIC STRIP OR STRIPE OF A CREDIT CARD ONTO THE MAGNETIC STRIP OR STRIPE OF A DIFFERENT CREDIT CARD OR USE ANY OTHER ELECTRONIC MEDIUM THAT ALLOWS SUCH A TRANSACTION TO OCCUR WITHOUT THE CONSENT OF THE INDIVIDUAL AUTHORIZED TO USE THE CREDIT CARD FROM WHICH THE PERSONAL IDENTIFYING INFORMATION OR PAYMENT DEVICE NUMBER IS BEING REENCODED; OR**

**(2) A SKIMMING DEVICE TO ACCESS, READ, OBTAIN, MEMORIZE OR STORE PERSONAL IDENTIFYING INFORMATION OR A PAYMENT DEVICE NUMBER ON THE MAGNETIC STRIP OR STRIPE OF A CREDIT CARD, WTIHOUT THE CONSENT OF THE INDIVIDUAL AUTHORIZED TO USE THE CREDIT CARD.**

**(E) A PERSON MAY NOT KNOWINGLY, WILLFULLY, AND WITH FRAUDULENT INTENT, POSSESS, OBTAIN, OR HELP ANOTHER POSSESS OR OBTAIN A REENCODER OR SKIMMING DEVICE FOR THE UNAUTHORIZED USE, SALE OR TRANSFER OF PERSONAL IDENTIFYING INFORMATION OR A PAYMENT DEVICE NUMBER.**

[(d)] **(F)** A person may not knowingly and willfully claim to represent another person without the knowledge and consent of that person, with the intent to solicit, request, or take any other action to otherwise induce another person to provide personal identifying information or a payment device number.

[(e)] **(G)** (1) A person who violates this section where the benefit, credit, good, service, or other thing of value that is the subject of subsection (b) [or] (c) **OR (D)** of this section has a value of $500 or greater is guilty of a felony and on conviction is subject to imprisonment not exceeding 5 years or a fine not exceeding $25,000 or both.

(2) A person who violates this section where the benefit, credit, good, service, or other thing of value that is the subject of subsection (b) [or] (c) **OR (D)** of this section has a value of less than $500 is guilty of a misdemeanor and on conviction is subject to imprisonment not exceeding 18 months or a fine not exceeding $5,000 or both.

(3) A person who violates this section under circumstances that reasonably indicate that the person's intent was to manufacture, distribute, or dispense another individual's personal identifying information without that individual's consent is guilty of a felony and on conviction is subject to imprisonment not exceeding 5 years or a fine not exceeding $25,000 or both.

(4) A person who violates subsection (c)(1) [or (d)] **(E) OR (F)** of this section is guilty of a misdemeanor and on conviction is subject to imprisonment not exceeding 18 months or a fine not exceeding $5,000 or both.

(5) When the violation of this section is pursuant to one scheme or continuing course of conduct, whether from the same or several sources, the conduct may be considered as one violation and the value of the benefit, credit, good, service, or other thing of value may be aggregated in determining whether the violation is a felony or misdemeanor.

[(f)] **(H)** A person described in subsection [(e)] **(G)**(2) or (4) of this section is subject to § 5–106(b) of the Courts Article.

[(g)] **(I)** In addition to restitution under Title 11, Subtitle 6 of the Criminal Procedure Article, a court may order a person who pleads guilty or nolo contendere or who is found guilty under this section to make restitution to the victim for reasonable costs, including reasonable attorney's fees, incurred:

(1) for clearing the victim's credit history or credit rating; and

(2) in connection with a civil or administrative proceeding to satisfy a debt, lien, judgment, or other obligation of the victim that arose because of the violation.

[(h)] **(J)** A sentence under this section may be imposed separate from and consecutive to or concurrent with a sentence for any crime based on the act or acts establishing the violation of this section.

[(i)] **(K)** Notwithstanding any other law, the Department of State Police may initiate investigations and enforce this section throughout the State without regard to any limitation otherwise applicable to that department's activities in a municipal corporation or other political subdivision.

[(j)] **(L)** (1) Notwithstanding any other law, a law enforcement officer of the Maryland Transportation Authority Police, the Maryland Port Administration

Police, the park police of the Maryland–National Capital Park and Planning Commission, or a municipal corporation or county may investigate violations of this section throughout the State without any limitation as to jurisdiction and to the same extent as a law enforcement officer of the Department of State Police.

(2) The authority granted in paragraph (1) of this subsection may be exercised only in accordance with regulations that the Department of State Police adopts.

(3) The regulations are not subject to Title 10, Subtitle 1 of the State Government Article.

(4) The authority granted in paragraph (1) of this subsection may be exercised only if an act related to the crime was committed in the investigating law enforcement agency's jurisdiction or if the complaining witness resides in the investigating law enforcement agency's jurisdiction.

[(k)] **(M)** If action is taken under the authority granted in subsection (j) of this section, notification of an investigation:

(1) in a municipal corporation, shall be made to the chief of police or designee of the chief of police;

(2) in a county that has a county police department, shall be made to the chief of police or designee of the chief of police;

(3) in a county without a police department, shall be made to the sheriff or designee of the sheriff;

(4) in Baltimore City, shall be made to the Police Commissioner or the Police Commissioner's designee;

(5) on property owned, leased, or operated by or under the control of the Maryland Transportation Authority, the Maryland Aviation Administration, or the Maryland Port Administration, shall be made to the respective chief of police or the chief's designee; and

(6) on property owned, leased, or operated by or under the control of the Maryland–National Capital Park and Planning Commission, to the chief of police of the Maryland–National Capital Park and Planning Commission for the county in which the property is located.

[(l)] **(N)** When acting under the authority granted in subsection (i) or (j) of this section, a law enforcement officer:

(1) in addition to any other immunities and exemptions to which the officer may be entitled, has the immunities from liability and exemptions accorded to a law enforcement officer of the Department of State Police; but

(2) remains an employee of the officer's employing agency.

[(m)] **(O)** (1) A State's Attorney or the Attorney General may investigate and prosecute a violation of this section or a violation of any crime based on the act establishing a violation of this section.

(2) If the Attorney General exercises authority under paragraph (1) of this subsection, the Attorney General has all the powers and duties of a State's Attorney, including the use of a grand jury in any county or Baltimore City, to investigate and prosecute the violation.

[(n)] **(P)** Notwithstanding any other provision of law, the prosecution of a violation of this section or for a violation of any crime based on the act establishing a violation of this section may be commenced in any county in which:

(1) an element of the crime occurred; or

(2) the victim resides.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2008.

E1

8lr1088
CF 8lr1089

Bill No.: _____

Requested: _____

Committee: _____

Drafted by: Joyce



By: **Senators Kelley and Jones (Maryland Task Force to Study Identity Theft**

A BILL ENTITLED

AN ACT concerning

**Identity Fraud – Felony or Repeat Offender, Fiduciary, or Vulnerable Adult – Penalties**

FOR the purpose of increasing the penalty for a person who commits identity fraud where the benefit, credit, good, service, or other thing of value that is the subject of the offense has a value of $500 or greater; increasing the penalty for a person who commits identity fraud under circumstances that reasonably indicate that the person's intent was to manufacture, distribute, or dispense another individual's personal identifying information without that individual's consent; providing an enhanced penalty for a person who commits identity fraud while serving as a fiduciary for the victim; providing an enhanced penalty for a person who commits identity fraud in circumstances in which the victim is a vulnerable adult; providing an enhanced penalty for a person convicted of the crime of identity fraud who has been convicted of identity fraud on a prior occasion not arising from the same incident; defining terms; and generally relating to penalties for identity fraud.

BY repealing and reenacting, without amendments,
Article – Criminal Law
Section 8–301(b), (c), (d), and (h)
Annotated Code of Maryland
(2002 Volume and 2007 Supplement)

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.
[Brackets] indicate matter deleted from existing law.

BY repealing and reenacting, with amendments,
Article – Criminal Law
Section 8–301(a) and (e)
Annotated Code of Maryland
(2002 Volume and 2007 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

**Article – Criminal Law**

8–301.

(a) (1) In this section the following words have the meanings indicated.

**(2) "FIDUCIARY" MEANS A PERSONAL REPRESENTATIVE, TRUSTEE, AGENT ACTING UNDER A POWER OF ATTORNEY, OR OTHER PERSON AUTHORIZED TO ACT AS A FIDUCIARY WITH RESPECT TO THE PROPERTY OF ANOTHER PERSON.**

**[**(2)**]** **(3)** "Payment device number" has the meaning stated in § 8–213 of this title.

**[**(3)**]** **(4)** "Personal identifying information" means a name, address, telephone number, driver's license number, Social Security number, place of employment, employee identification number, mother's maiden name, bank or other financial institution account number, date of birth, personal identification number, credit card number, or other payment device number.

**(5) "VULNERABLE ADULT" HAS THE MEANING STATED IN § 3–604 OF THIS ARTICLE.**

(b) A person may not knowingly, willfully, and with fraudulent intent possess, obtain, or help another to possess or obtain any personal identifying information of an individual, without the consent of the individual, in order to use, sell, or transfer the information to get a benefit, credit, good, service, or other thing of value in the name of the individual.

(c) A person may not knowingly and willfully assume the identity of another:

(1) to avoid identification, apprehension, or prosecution for a crime; or

(2) with fraudulent intent to:

(i) get a benefit, credit, good, service, or other thing of value; or

(ii) avoid the payment of debt or other legal obligation.

(d) A person may not knowingly and willfully claim to represent another person without the knowledge and consent of that person, with the intent to solicit, request, or take any other action to otherwise induce another person to provide personal identifying information or a payment device number.

(e) (1) A person who violates this section where the benefit, credit, good, service, or other thing of value that is the subject of subsection (b) or (c) of this section has a value of $500 or greater is guilty of a felony and on conviction is subject to imprisonment not exceeding **[**5**]** **15** years or a fine not exceeding **[**$25,000**]** **$50,000** or both.

(2) A person who violates this section where the benefit, credit, good, service, or other thing of value that is the subject of subsection (b) or (c) of this section has a value of less than $500 is guilty of a misdemeanor and on conviction is subject to imprisonment not exceeding 18 months or a fine not exceeding $5,000 or both.

(3) A person who violates this section under circumstances that reasonably indicate that the person's intent was to manufacture, distribute, or dispense another individual's personal identifying information without that individual's consent is guilty of a felony and on conviction is subject to imprisonment not exceeding **[**5**]** **15** years or a fine not exceeding **[**$25,000**]** **$50,000** or both.

**(4) A PERSON WHO VIOLATES THIS SECTION WHILE SERVING AS A FIDUCIARY FOR THE VICTIM IS GUILTY OF A FELONY AND ON CONVICTION IS SUBJECT TO IMPRISONMENT NOT EXCEEDING 15 YEARS OR A FINE NOT EXCEEDING $50,000 OR BOTH.**

**(5) A PERSON WHO VIOLATES THIS SECTION IN CIRCUMSTANCES IN WHICH THE VICTIM IS A VULNERABLE ADULT IS GUILTY OF A FELONY AND ON CONVICTION IS SUBJECT TO IMPRISONMENT NOT EXCEEDING 15 YEARS OR A FINE NOT EXCEEDING $50,000 OR BOTH.**

**[**(4)**]** **(6)** A person who violates subsection (c)(1) or (d) of this section is guilty of a misdemeanor and on conviction is subject to imprisonment not exceeding 18 months or a fine not exceeding $5,000 or both.

**[**(5)**]** **(7)** When the violation of this section is pursuant to one scheme or continuing course of conduct, whether from the same or several sources, the conduct may be considered as one violation and the value of the benefit, credit, good, service, or other thing of value may be aggregated in determining whether the violation is a felony or misdemeanor.

**(8) ON CONVICTION OF A VIOLATION OF THIS SECTION, A PERSON WHO HAS BEEN CONVICTED ON A PRIOR OCCASION NOT ARISING FROM THE SAME INCIDENT OF A VIOLATION OF THIS SECTION IS SUBJECT TO IMPRISONMENT NOT EXCEEDING 15 YEARS OR A FINE NOT EXCEEDING $50,000 OR BOTH.**

(h) A sentence under this section may be imposed separate from and consecutive to or concurrent with a sentence for any crime based on the act or acts establishing the violation of this section.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2008.


## Credit Card Skimming Laws and Legislation

Last Updated: November 19, 2007

NCSL Contact: Heather Morton (Denver)

| State: | Statutory Citation: | Penalties: |
|---|---|---|
| **Arizona** | Ariz. Rev. Stat. Ann. §13-2110 | Unlawful possession or use is a class 6 felony |
| **Arkansas** | Ark. Stat. Ann. §5-37-227 | Classified as Financial Identity Fraud - a class C felony. A violation is also classified as an unfair and deceptive trade practice which is a class A misdemeanor. The attorney general may also file suit to recover civil damages |
| **California** | Cal. Penal Code §502.6 | Any person who possesses and uses a scanning and/or re-encoding device with the intent to defraud will be guilty of a misdemeanor punishable by no more than one year in county jail and/or a fine not in excess of $1,000 |
| **Connecticut** | Conn. Gen. Stat. §53-388a | Class A misdemeanor |
| **Delaware** | Del. Code Ann. tit. 11, §903A | Any person who possesses and/or uses a scanning or reencoding device for the purpose of willfully, knowingly and with the intent to defraud will be guilty of a class D felony |
| **Florida** | Fla. Stat. §817.625 | A person who unlawfully uses a scanning or re-encoding device with the intent to defraud will be guilty of a third degree felony punishable by no more than five years imprisonment for first offense. For second and subsequent offenses the individual is guilty of a second degree felony punishable by no more than 15 years imprisonment. |
| **Idaho** | Idaho Code §18-2415 | A person who uses a scanning or re-encoding device to intentionally defraud is guilty of Grand Theft felony punishable by not less than one year and no more than 14 years imprisonment and/or a fine no more than $5,000 |
| **Illinois** | Ill. Rev. Stat. ch. 750, §5/17-25<br><br>Ill. Rev. Stat. ch. 750, §5/16G-14 | A person who unlawfully uses a scanning or re-encoding device with the intent to defraud is guilty of a class 4 felony for first offense, class 3 felony for second and subsequent offenses.<br><br>A person who unlawfully uses a financial transaction device to capture, copy or transmit or otherwise obtain personal information without the consent of the person will be guilty of a class A misdemeanor. |
| **Indiana** | Ind. Code §35-43-5-4.3 | Unlawful possession of a card skimming device under subdivision (1) or (2) is a Class D felony. Unlawful possession of a card skimming device under subdivision (3) is a Class C felony. |
| **Iowa** | Iowa Code §715A.10 | Use of scanning and/or re-encoding device for the purpose of defrauding the authorized user: First offense - class D felony; second and subsequent offenses - class C felony |
| **Kansas** | Kan. Stat. Ann. §21-4019 | Violation is a severity level 6, nonperson felony |
| **Kentucky** | Ky. Rev. Stat. §§434.675 and 434.730 | Possessing or misusing a scanning or reencodeing device - First offense: class D felony; Second and subsequent offenses: class C felony |
| **Louisiana** | La. Rev. Stat. Ann. §14:67.4 | Violations result in imprisonment, with or with out hard labor, for not more than five years and/or fines not more than $5,000. If the use of the scanning or reencoding devise was used with the |

| | | |
|---|---|---|
| | | intent to defraud the penalty is imprisonment, with or with out hard labor, for not more than 10 years and/or fines not more than $10,000. The court may also impose restitution. |
| **Maine** | Me. Rev. Stat. Ann. tit. 17-A, §905-B | Misuse of a scanning or reencoder device is a class D crime. |
| **Michigan** | Mich. Comp. Laws §750.539k | A person who unlawfully uses a devices to capture personally identifiable information will be guilty of a misdemeanor punishable by imprisonment of no more than one year and/or a fine no more than $1,000 |
| **Mississippi** | Miss. Code Ann. §97-45-31 | Violation is a felony punishable by no more than five years in prison and/or fines not to exceed $10,000 |
| **Missouri** | Mo. Rev. Stat. §407.433 | A person who unlawfully uses a scanning or re-encoding device with the intent to defraud will be guilty of a class A misdemeanor. |
| **Nevada** | Nev. Rev. Stat. §§205.605 and 205.606 | An individual who unlawfully possesses a scanning or re-encoding device is guilty of a class C felony. An individual who unlawfully uses a scanning or re-encoding device is guilty of a class B felony punishable by no less than one year and no more than 20 years in prison and/or a fine of $100,000. In addition, the unlawful use may also result in the repayment of any or all monies to the harmed individual in the amount caused by the unlawful use including but not limited to attorney's fees, the cost to correct credit and any debts incurred as a result of the misuse. |
| **New Hampshire** | N.H. Rev. Stat. Ann. §638:29 | The unlawful use of a scanning or re-encoding device is: (1) a class B if the person has one or more prior convictions in New Hampshire or any other state for this crime; (2) a class B felony if the individual has used a scanning or re-encoding device two or more times to defraud the authorized user; (3) a misdemeanor in all other instances. |
| **New Jersey** | N.J. Rev. Stat. §2C:21-6.1 | A crime in the third degree if the intent was to defraud the rightful own of the card through the use of a scanning or re-encoding device. A crime in the fourth degree if one knowingly possesses a device with the intent to defraud. |
| **Oregon** | Or. Rev. Stat. §165.074 | A person who unlawfully uses a scanning device is guilty of a class C felony. If an individual has one or more convictions under the section, guilty of a class B felony. |
| **South Dakota** | S.D. Codified Laws Ann. §§22-30A-8.3 and 22-30A-8.4 | The use of a scanning or re-encoding device to intentionally defraud the authorized user is punishable as a class 6 felony. |
| **Texas** | Tex. Business and Commerce Code Ann. §35.60 | A class B misdemeanor and violator may additionally be prosecuted under any other applicable provision of law. |
| **Utah** | Utah Code Ann. §76-6-506.7 | A person who unlawfully uses a scanning or re-encoding device is guilty of a third degree felony. If the individual has a prior conviction under this section they are guilty of a second degree felony for the second and subsequent offenses. |
| **Virginia** | Va. Code §18.2-196.1 | The use of a scanning or re-encoding device with malicious intent is a Class 1 misdemeanor. Use of a device and selling of the information and/or the information is used in the commission of another crime is a Class 6 felony. |
| **Washington** | Wash. Rev. Code §9A.56.290 | A person who unlawfully uses a scanning or re-encoding device for the purpose to defraud is guilty of a class C felony for the first offense and a class B felony for second and subsequent offenses. |
| **West Virginia** | W. Va. Code §61-3-56 | An individual who uses a scanning or reencodeing device for unlawful purposes will be guilty of:<br>First offense - a misdemeanor punishable by confinement in county or regional jail for no more than a year and/or a fine no more than $1,000;<br>Second and subsequent offenses - a felony punishable by no less than a year and no more than three years in state jail and/or a fine no more than $5,000. |
| **Wyoming** | Wyo. Stat. §6-3-803 | First conviction: no more than five years in prison and/or fines no more than $10,000. Second and subsequent convictions: no more than 10 years in prison and/or fines no more than $25,000. |

MARYLAND GENERAL ASSEMBLY
TASK FORCE TO STUDY IDENTITY THEFT

# Maryland Laws
# Disclosure of Social Security Numbers

---

- A person may not knowingly, willfully, and with fraudulent intent possess, obtain, or help someone else to possess or obtain another's Social Security number (SSN) without that person's consent, in order to use, sell, or transfer the SSN to get a benefit, credit, good, service, or other thing of value in the name of that person.
  - *§ 8-301 of the Criminal Law Article*

- With certain exceptions, a person may not:
  - publicly post or display another's SSN;
  - print another's SSN on a card required for that person to access products or services;
  - require another to transmit their SSN or initiate the transmission of another's SSN over the Internet unless the connection is secure or the SSN is encrypted;
  - require an individual to use their SSN to access a website, unless an authentification device is also required; or
  - (unless required by law), print an individual's SSN on material mailed to the individual, include a person's SSN in material electronically transmitted to the individual (unless the connection is secure and the SSN encrypted), or transmit an individual's SSN to the individual by fax.
  - *§ 14-3401, et seq. in the Commercial Law Article ("The Social Security Number Privacy Act")*

- The State may not print or have printed a State employee's SSN on an identification card.
  - *§ 1-202 in the State Personnel and Pensions Article*

- A local government may not print or have printed a local government employee's SSN on an identification card.
  - *§ 1-109 of Article 24, Annotated Code of Maryland*



Room 110 Legislative Services Building · 90 State Circle · Annapolis, Maryland 21401-1991
410-946-5350 · Fax 410-946-5395 · TDD 410-946-5401
301-970-5350 · Fax 301-970-5395 · TDD 301-970-5401

- An employer (including a governmental unit) may not print or cause to be printed an employee's SSN on the employee's wage payment check, on an attachment to the check, on a notice of direct deposit of the wage, or on a notice of credit of the wage to a debit card or card account.
  - *§ 3-502 of the Labor and Employment Article*

- A public institution of higher education may not print or have printed an employee's or a student's SSN on identification cards.
  - *§ 15-110 of Education Article*

- The State Superintendent, a county board, or a county superintendent may not print or have printed a teacher's or other employee's SSN on an identification card.
  - *§ 6-114 of the Education Article*

- A public school may not print or have printed a student's SSN on an identification card.
  - *§ 7-113 in the Education Article*

- An applicant for a driver's license must provide SSN or certify that applicant does not have one.
  - *§ 16-106 of the Transportation Article*

- The custodian of the record shall deny public inspection of marriage license applications or recreational licenses that contain SSNs with certain exceptions.
  - *§ 10-617 of State Government Article*

- The SSN of each party is required for a marriage application but may not be disclosed as part of the public record, with certain exceptions.
  - *§ 2-402 of the Family Law Article*

- The Department of Natural Resources requires applicant for recreational license to provide SSN if the applicant has one but may not disclosed the SSN as part of the public record, with certain exceptions.
  - *§ 4-205 of the Natural Resources Article*

NATIONAL CONFERENCE *of* STATE LEGISLATURES

*The Forum for America's Ideas*

**Donna D. Stone**
*State Representative*
*Delaware*
*President, NCSL*

**Sharon A. Crouch Steidel**
*Director, Information Systems*
*Virginia House of Delegates*
*Staff Chair, NCSL*

**William T. Pound**
*Executive Director*

August 20, 2007

The Honorable Delores G. Kelley
State Senator
Senate Chair, Task Force to Study Identity Theft
Maryland General Assembly

The Honorable Susan C. Lee
State Delegate
House Chair, Task Force to Study Identity Theft
Maryland General Assembly

Dear Senator Kelley and Delegate Lee and Members of the Task Force:

My name is Heather Morton, and I am a Program Principal with the National Conference of State Legislatures. I cover the issues of banking and financial services, financial privacy and identity theft and I am pleased to have the opportunity to submit written testimony regarding the use of Social Security numbers as identifiers and state legislatures' efforts to regulate the use of these numbers. To begin, I will describe the current landscape of regulation and recent state legislation.

Established in 1936 by the Social Security Administration, Social Security numbers (SSNs) were originally used to track earnings and eligibility for Social Security benefits. Recognizing the universal nature of SSNs, Congress enacted several laws that require the use of SSNs for purposes other than Social Security, such as food stamps, Temporary Assistance for Needy Families, and child support



**Denver**
*7700 East First Place*
*Denver, Colorado 80230*
*Phone 303.364.7700 Fax 303.364.7800*

**Washington**
*444 North Capitol Street, N.W. Suite 515*
*Washington, D.C. 20001*
*Phone 202.624.5400 Fax 202.737.1069*

*Website www.ncsl.org*

enforcement, as well as the Commercial Driver's License Information System and the Internal Revenue Service.

To address concerns regarding the availability of personal information, Congress enacted the Privacy Act of 1974. The Act is primarily directed at federal agencies, but Section 7 (5 U.S.C. §552a note) also applies to state and local governmental agencies. It provides that: "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number." Sec. 7(a)(1). The Privacy Act and other acts amending it do provide several exceptions for states' use of SSNs, including the use of SSNs "in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law within its jurisdiction." (*See* Tax Reform Act of 1976, 42 U.S.C. §405(c)(2)(C)(i), (iv) (2000).) Other exceptions include the state issuance of birth certificates and the enforcement of child support orders.

The Privacy Act of 1974 also provides that "Any Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it." Sec. 7(b). Further, the Social Security Act Amendments of 1990 bars the disclosure of SSNs by federal, state and local governments collected pursuant to any laws enacted on or after October 1, 1990.

These federal laws provide a patchwork of regulation, but there is no one law that governs the use of SSNs. Because the laws governing the use of SSNs focus on specific uses by governmental

agencies, SSNs have been used extensively to identify individuals by businesses and other organizations and agencies. The SSN is a unique personal identifier that does not tend to change, unlike a person's name or address. SSNs have been widely available and, until recently, states have printed them on driver's licenses, health care organizations have used them on insurance identification cards and SSNs often appear on financial documents and court records.

Concerns continue that the availability of SSNs is helping facilitate identity theft and fraud. Studies have shown that identity thieves often use valid SSNs to commit their crimes. To combat identity theft, state legislators have introduced legislation to restrict the availability and use of SSNs, but these actions are not without controversy.

## Use as Identifier by Government Agencies

Since 2002, all 50 state legislatures and the District of Columbia have introduced legislation addressing the use of SSNs in various ways and at least 47 states have enacted legislation. Arizona, Kentucky, Maryland, Michigan, Nevada and Texas limited the use of SSNs on marriage licenses. Eighteen states[1] have limited SSNs as identifiers for students and for access to health insurance and other benefits. In 2003, Arkansas and North Dakota eliminated the use of SSNs on driver's licenses; Virginia eliminated the optional use of SSNs as driver's license numbers, and Hawaii and West Virginia eliminated SSNs on commercial driver's licenses. In 2005, Delaware prohibited displaying an individual's SSN on the driver's license or identification card document in either printed form or electronically recorded in the bar code. In contrast, Oregon passed a law that requires state agencies, boards and commissions to record an applicant's SSN for application for and renewals of driver's licenses, certifications and permits. However, the law also prohibits the state department of

transportation from disclosing SSNs from motor vehicle records. In 2006, South Dakota prohibited the display of SSNs on driver licenses and nondriver's identification cards.

## Use in Public Records

More than 20 states[2] limit the use and disclosure of SSNs in documents filed in court proceedings and through clerk and recorder offices. In 2006, Indiana required county recorders to redact SSNs from documents filed with the county recorder. In 2007, the Arizona Legislature required county recorders in counties with a population greater than 800,000 to redact references to SSNs that were recorded after December 31, 1985 and are posted on the recorder's Web site. At least 25 states[3] passed laws that protect the confidentiality of military discharge paperwork, which usually contains veterans' SSNs.

## Use by Government Agencies

Indiana prohibits state agencies, boards, commissions, or other state entities from requiring a person to provide a SSN to the agency against the person's will, absent federal requirements to the contrary. In Arizona, state agencies, except the state department of revenue and law enforcement agencies, are prohibited from using an individual's entire SSN, with certain exceptions. The Arizona state agencies may use the last four numbers. In 2004, California prescribed that only the last four digits of a governmental employee's SSN may be printed on a paycheck after January 1, 2008. Florida exempted a voter's SSN and signature from the state's public records laws, while Hawaii allowed only the last four digits of a registered voter's SSN on nomination papers filed on behalf of a candidate. And, Illinois required the state department of revenue to notify an individual if the department discovers or reasonably suspects that another person has used that individual's SSN. In

2007, Utah authorized the state department of workforce services to disclose to an individual the suspected misuse of the individual's personal identifying information and allows the department to report the suspected misuse to the appropriate law enforcement agencies for investigating identity theft violations.

**Use by Businesses**

To protect consumers' privacy, several states have addressed SSN use by businesses. For example, Arizona, California, Colorado, Hawaii, Illinois, Minnesota, New Jersey, North Carolina and Virginia prohibit mailing documents or parcels where an individual's SSN can be seen through the packaging. Colorado now prohibits recording a SSN or credit card number when a person is accepting a check from a consumer. New Mexico enacted the Privacy Protection Act, which regulates the collection and disclosure of SSNs. Under this new law, companies that acquire SSNs must adopt internal policies that limit access to authorized employees who need the information to perform their duties. The law holds those employees responsible if the SSNs are released to unauthorized persons. Maine prohibits the denial of goods or services to an individual if the individual refuses to give a SSN, but it does not prevent the collection of SSNs when provided for in law. Michigan makes the act of requiring a consumer to disclose a SSN as a condition to selling goods or providing a service to the consumer an unlawful trade practice, unless the purchase, provision, payment or transaction included an application for or an extension of credit to the consumer or the disclosure was required or authorized by law. And, Rhode Island enacted a law that prohibits a person, firm, corporation or other business entity from requiring a person to furnish a SSN or motor vehicle operator's license in order to apply for a consumer discount card for purchases.

Michigan created the Social Security Number Privacy Act, which prohibits disclosing or publicly displaying all or any part of the SSN of an employee, student, or other individual without the individual's consent in writing, or the disclosure is authorized by law. Under Michigan's Social Security Number Privacy Act, the law applies to individuals, partnerships, corporations, schools and other government or legal entities. And, Arizona passed a law that governs the use of SSNs by people and business entities. For example, individuals cannot be required to provide a SSN over the Internet unless the connection is secure or the SSN is encrypted or transmit a SSN to access a Web site unless a password or unique identification is also required to access the Internet site. In 2005, Texas prohibited the collection of identifying information from a consumer for use in compiling or tracking their returns of merchandise and granted authority to the attorney general, or the county attorney, to bring suit to recover a civil penalty of up to $500 for each violation. In 2006, Maryland prohibited an employer from printing an employee's SSN on a wage payment check or other specified wage payment documents.

In summary, state legislatures have taken many steps to protect the privacy and financial security of citizens by regulating the way both government and businesses may use Social Security Numbers. Unfortunately the on-going problem of identity theft indicates there is work still to be done to safeguard Social Security numbers. Thank you for the opportunity to provide testimony on this issue and I would be happy to provide additional information if needed.

Sincerely,

Heather Morton
Program Principal
National Conference of State Legislatures
7700 East First Place
Denver, CO 80230
(303) 364-7700 extension 1475
(303) 364-7800 fax
heather.morton@ncsl.org

## Notes

[1] Arizona, Arkansas, California, Colorado, Delaware, Georgia, Illinois, Michigan, New Jersey, Oregon, Pennsylvania, Tennessee, Texas, Utah, Virginia, Washington, West Virginia and Wisconsin

[2] Arizona, Arkansas, California, Colorado, Delaware, Hawaii, Illinois, Kentucky, Louisiana, Missouri, Nebraska, New Hampshire, New Jersey, Ohio, Oregon, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, Wisconsin and Wyoming

[3] Arizona, Arkansas, California, Connecticut, Florida, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Minnesota, New Mexico, North Carolina, Ohio, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Virginia, Washington, West Virginia and Wyoming

STATE OF MARYLAND
DHMH

Maryland Department of Health and Mental Hygiene
201 W. Preston Street • Baltimore, Maryland 21201
Martin O'Malley, Governor – Anthony G. Brown, Lt. Governor – John M. Colmers, Secretary

August 21, 2007

The Honorable Delores G. Kelley
Chair, Task Force to Study Identity Theft
James Senate Office Building, Rm. 302
Annapolis, MD 21401

The Honorable Susan C. Lee
Chair, Task Force to Study Identity Theft
House Office Building, Rm. 414
Annapolis, MD 21401

Dear Senator Kelley and Delegate Lee,

Thank you for the opportunity to participate in the Task Force to Study Identity Theft's hearing about State Agency Custody and Use of Social Security Numbers. DHMH provides a variety of public services that require Department personnel to collect personal information. Examples of programs containing personal information requirements or Social Security Numbers are listed in the chart below:

| **DHMH Administration** | **Number of Records** |
|---|---|
| Breast and Cervical Cancer Diagnosis and Treatment Program | 34,720 |
| Breast and Cervical Cancer Screening Program | 61,723 |
| Division of Reimbursements | 70,000 |
| Division of Vital Records | 10,320,0000 |
| Epidemiology and Disease Control Program | 2,200,000 |
| General Accounting | 12,000 |
| Maryland Cancer Registry | 350,000 |
| Medicaid | 2,001,256 |
| Mental Hygiene Administration | 125,000 |
| Developmental Disabilities Administration | 36,939 |
| AIDS Administration | 57,000 |

DHMH has taken numerous measures to protect personal information and Social Security Numbers. Measures related to the physical security of facilities and the security of Information Technology systems have been implemented and continue to be upgraded when warranted. Additionally, DHMH has an Information Assurance Policy (COMAR 02.01.06) that provides high-level policy and procedural direction on custody of protected health and proprietary information. A Privacy Officer position was created within the Office of the Inspector General to regularly train and monitor employee compliance with the DHMH Information Assurance Policy, Federal Privacy Act, Maryland Medical Records Privacy Act, and the Health Insurance Portability and Accountability Act (HIPAA).

Physical security at DHMH facilities has increased by requiring the use of a government issued ID prior to entry. Access restrictions and controls are in place in high security identified areas. A comprehensive access control and video observation system at all building access points has been installed in our headquarters facility, selected internal high-risk locations, and through out the DHMH lab tower. Additionally, equipment cannot be removed without prior permission and documentation must be presented to security upon exiting the building.

The security of personal information and social security numbers has also been strengthened through the use of Information Technology policies and procedures. Critical data equipment has been removed from multiple locations at our headquarters facility and remote sites. The equipment has been relocated to a highly secured and monitored data center. Additionally, data is password protected and the Department has instituted a policy regarding the physical or electronic transfer of protected data.

Retention of personal information and Social Security Numbers differs among programs. Schedules differ based on audit requirements that are often drive by outside agents such as the Courts or the federal government.

In addition to the efforts previously referenced, DHMH has a Department wide workgroup that meets monthly to address combined security interests of personnel, physical security, safety, and information and communications security. The Department also participates in statewide information security and privacy workgroups sponsored by the Department of Budget and Management, and works closely with other State agencies on data sharing and protection issues.

DHMH has proactively tried to secure all personal information and Social Security Numbers collected by Department programs. The Division of Vital Records, which collects, maintains and certifies records for all births, deaths, fetal deaths, marriages and divorces occurring in Maryland, presents the biggest challenge to the security of personal information in that 10 million records are on paper and additional records are maintained on microfilm or other media. Records are stored under lock and key, only accessible to supervisory staff. DVR is in need of an electronic vital records system that would serve to better secure the information and allow DVR to provide better service to the public through an expedited search process.

Additional efforts to improve security should be considered, starting with a baseline review of major data collection systems to determine if they meet current privacy requirements and prevailing standards. The creation of a DHMH database of all employees with access to MMIS and other systems containing private data could be reviewed and evaluated, and used to validate approvals and denials for access to systems. The most valuable improvement would be to convert to electronic systems for the maintenance of personal information.

Again, thank you for the opportunity to participate in this afternoon's hearing. Please find attached individual responses to the six Task Force questions provided to the Department prior to the hearing. If you have any questions or would like additional information regarding the Department's efforts to secure personal information and Social Security Numbers, please contact Anne Hubbard, Director of Governmental Affairs, at 410-767-6481.

Very truly yours,

James P. Johnson
Deputy Secretary of Operations

**Department of Health and Mental Hygiene**
**Responses to Task Force to Study Identity Theft Questionnaire**
**August 22, 2007**

**1. How many records containing SSN or other personal information are maintained? For what purpose is the information collected and used?**

Breast and Cervical Cancer Diagnosis and Treatment Program
There are 34,720 individual records that contain a Social Security number and other personal information in the BCC_DHMH database which is utilized by the Program for administrative and reimbursement purposes.

There are approximately 23,328 individual medical records that contain a Social Security number in locked file cabinets on the unit. The keys to the cabinets are kept in the locked office of the Program Manager. These records are archived every two years to remove individuals that are deceased or have not participated in the Program since the last record archive. The archived records are boxed and sent to Jessup for storage for 10 years. After 10 years the files are destroyed by the Jessup facility.

There are 689,409 tables (all containing social security numbers) stored on the electronic claims management system (eCMS) at the present time. These are transactions and represent several iterations of the same information that is used during the various phases of claims processing. The Program is required to keep a record of all transactions.

There are 3,664 individual records stored on the Medical Assistance (MA) Recoup file. The BCCDT is required to keep a record of monies reimbursed providers during a time when the patients were deemed eligible for MA.

Breast and Cervical Cancer Screening Program
The Breast and Cervical Cancer Program database has 61,723 records with social security numbers. The database contains records on all women who receive a screening service through the BCCP.

This Social Security Number is collected to match the BCCP database with the Maryland Cancer Registry database. Both programs BCCP and the MCR receive federal funds. A condition of the federal funds is to conduct a database match of patients with cancer in both databases to verify the cancer stage and tumor size. Social Security numbers are used because they are the only unique patient field. There are patients that have the same name and same date of birth making it hard to perform a one-to-one match. The purpose of the match is to obtain missing cancer stage and tumor size information that is required to be reported by the Breast and Cervical Cancer Program. The information collected is also used to match BCCP patients with BCCDT patients to determine numbers of clients in both program and diagnostic costs for BCCP clients.

Community Health Administration
Several hundred paper records are maintained connected with the Harmful Algal Blooms (HAB) program; these are paper and were collected in connection with HAB surveillance activities.

Division of Reimbursements

The Division of Reimbursements (DOR) has an estimated 70,000 + paper files containing patient financial information, employee personnel data and timesheets, and remittance advices. Additionally DOR maintains dozens of data printouts containing SSN and other pertinent patient financial and medical data. The purpose of the collection of this information is to conduct a financial investigation in order to establish a billing for the cost of care provided in the DHMH hospital facilities and for the recovery of said cost for the State's general fund as mandated by the Annotated Code of Maryland (H-G 16-101 – 16-407) and COMAR (10.02.01.05 and .06).

Division of Vital Records

The Division of Vital Records (DVR) collects, maintains and certifies records for all births, deaths, fetal deaths, and marriages occurring in Maryland. DVR also provides verification of absolute divorces occurring in Maryland. DVR maintains approximately 10,320,000 paper records (7,630,000 birth; 1,710,000 death; 680,000 marriage, and 300,000 divorce) within its office. Additional records are maintained on microfilm and other media. DVR issues approximately 470,000 certified copies of vital records each year with an additional 200,000 certified copies of birth and death records issued through the local health departments.

*Birth Records*

The Division of Vital Records registers approximately 70,000 births annually. Birth records are available for births occurring since 1898. Birth record information for births occurring prior to 1898 is available through the Maryland State Archives. Social security numbers are collected for both parents and appear on the confidential portion of the birth record. Social security numbers are not shown on certified copies of birth certificates. The confidential portion of the birth record is used for health statistics purposes, and copies of documents that must be printed for this purpose are promptly shredded.

*Death and Fetal Death Records*

The Division of Vital Records registers approximately 45,000 deaths annually. Death records are available for deaths occurring after 1969. Death records for deaths prior to 1969 are available though the Maryland State Archives. Social security numbers are collected for the deceased and appear on certified copies of death certificates. Social security numbers from death certificates are reported to the Social Security Administration to assist them in determining termination of or eligibility for social security benefits.

*Marriage Records*

The Division of Vital Records registers approximately 40,000 marriages annually. Marriage records are available for marriages occurring after 1990. Marriage records prior to 1990 are available through the circuit court in the jurisdiction where the marriage took place or through the Maryland State Archives. Social security numbers are collected at the time a couple applies for a marriage license; however, this information is maintained in the circuit courts and does not appear on marriage certificates.

*Divorce Verifications*

The Division of Vital Records records approximately 20,000 divorces annually. Divorce verifications are available for absolute divorces occurring after 1992. The Division of Vital Records is only able to verify that a divorce occurred; actual divorce decrees must be obtained through the circuit court in the jurisdiction where the divorce took place or through the Maryland

State Archives. Social security numbers are shown on absolute divorce decrees, but are not shown on divorce verifications.

Epidemiology and Disease Control Program
It is estimated that approximately 2.2 million EDCP records (paper or electronic) contain one or more items of personal information, including a fraction which contain SSNs.

Division of General Accounting
General Acounting processes expense accounts with SSN and address. SSN is designated key for financial system's (FMIS) vendor file. Address is needed in FMIS for payment purposes. Payroll reports contain SSN.

Maryland Cancer Registry
The Maryland Cancer Registry (MCR) maintains a database with 350,290 consolidated records containing the cancer incidence for the years 1992-2004. This database contains 342,460 records containing social security numbers and 350,072 containing first and last names. This consolidated database is derived from abstracted records from individual clinics that contain confidential information. These files are kept on password protected network drives. Demographic information is collected for matching purposes-as a unique identifier for patients. Federal Public Law 102-515 enacted October 24, 1992 indicates that demographic information is to be collected.
The MCR contracts with Macro International to manage the cancer reports received from facilities. These reports may be in electronic form or hard copy form. The personnel at Macro International are required to follow the same confidentiality guidelines as personnel at the MCR.

Medicaid
The Maryland Medicaid program has total of 2,001,256 open and closed records on MMIS as of 8/8/07.

Mental Hygiene Administration
As of today, there are just over 125,000 records stored in the HMIS system (since 1987) and slightly more than 17,000 of these records have blank or unknown values for social security number. The main reason for collecting social security numbers in the HMIS is for the purpose of billing third party entities (viz., Social Security, Medicaid etc.) as well as providing DHMH managers with data to facilitate operation of each hospital center.

Office of Human Resources
The OHR maintains numerous records that contain SSN and other personal information. These include personnel files, the on-line MS 310 system, the payroll and timekeeping system, on-line timesheets, applications for recruitments, disciplinary action forms, retirement and health benefit forms, and criminal background check forms. The SSN is used as the identifying factor on all forms. The MS 310 system provides employment data for each employee by their SSN. All on-line systems are accessed through the SSN.

Maryland Board of Physicians
MBP currently maintains electronic and paper records for over 40,000 licensed practitioners. The MBP has the authority to license physicians and other health care providers such as physician assistants, medical radiation technologists, radiation oncology therapy technologists, nuclear medicine technologists, respiratory care practitioners, psychiatrist assistants and

polysomnographers to practice in Maryland. The MBP also disciplines licensees who violate the Maryland Medical Practice Act.

**2. What policies and practices govern when and how SSN are requested from the public and your employees?**

Breast and Cervical Cancer Diagnosis and Treatment Program
The Social Security number is used by the Program for administrative and reimbursement purposes. The Program is required to check the MA eligibility files at the time an application is received to make sure that the patient does not already receive MA. If the applicant is MA eligible, the application is rejected. The Program is also required to remove a participant and recoup any monies reimbursed during a time when MA has made the participant eligible. The eCMS runs every claim file against the MA eligibility file and rejects claims for Program patients found MA eligible. The Social Security number appears on all claims. The Social Security number is the one common element that allows the Program to perform these requirements and functions.

Breast and Cervical Cancer Screening Program
Social security numbers are requested of all patients accessing a service through the Breast and Cervical Cancer Screening Program.

Community Health Administration
SSN is not requested for any purposes from the public. SSN is requested of successful applicants to the Department's Preventive Medicine Residency Program, for the purpose of verifying credentials associated with their previous training.

Division of Reimbursements
The records are needed to carry out responsibilities under two statutes: H-G 16-202 and S-G 10-617(f).

Division of Vital Records
The Division of Vital Records has procedures in place to protect the integrity of Maryland's vital records. However, DVR recognizes its vulnerability in ensuring the safety of those records in light of its lack of automation in its record keeping systems. Ideally, DVR should be a paperless system maintaining all records and files electronically with safeguards and firewalls in place to protect record confidentiality. At present, DVR must retain all paper copies of records, with the majority of these records stored in a secure vault. Access to the vault is restricted to DVR staff only and it is not accessible to anyone else (including maintenance and janitorial staff) unless under close supervision of a DVR staff member.

*Obtaining a Copy of a Vital Record*
As outlined under COMAR 10.03.01.07, the Division of Vital Records restricts access to certificates and related records. In the case of birth records, a direct and tangible interest shall be evidenced by a request from:

- The subject of the vital record;
- A parent named on the birth certificate;
- The subject of the vital record's legal guardian; or
- An authorized representative of the subject of the vital record.

- A confidential intermediary authorized by the Director of the Social Services Administration of the Department of Human Resources; or
- The Director of the Social Services Administration of the Department of Human Resources.

In the case of death or fetal death records, a direct and tangible interest shall be evidenced by a request from:

- Surviving relatives;
- An authorized representative;
- A person who is a beneficiary of the deceased;
- An individual who wishes to establish an estate in the name of the deceased;
- A person who paid to the deceased while the deceased was alive or who has paid to or is trying to pay to the deceased's beneficiaries insurance benefits, pension benefits, welfare benefits, or other benefits;
- A person who demonstrates to the Secretary that the individual is trying to carry out a legal duty that was the responsibility of the deceased;
- A person who presents a subpoena that commands that a copy of the record be produced, if the subpoena is issued by:
    - A court,
    - An administrative body empowered by statute to issue a subpoena, or
    - A person empowered by statute to issue a subpoena;
- A person who is a party or who represents a party in litigation in which there is an issue as to whether the subject of the record is deceased;
- A person who needs to prove that a beneficiary who is the subject of the record is deceased;
- A person who needs to prove that the subject of the record is deceased so that a piece of property may be transferred with a clear title;
- A person who is a creditor of the deceased; or
- A government official who requests a death certificate in order to carry out the duties or functions of the official's office.

In the case of marriage records, the direct and tangible interest shall be evidenced by a request from:

- The married parties; or
- An authorized representative.

In the case of information regarding divorce, a direct and tangible interest shall be evidenced by a request from:

- The divorced parties; or
- An authorized representative.

In order to receive a certified copy of a certificate on the day of application (same day service), an applicant will be required to present valid, unexpired, government-issued photo identification. The identification must have a date issued and an expiration date.

Applicants who are unable to supply valid photo identification must present two pieces of alternative documentation. At least one of these documents must contain the applicant's current mailing address. Applicants who cannot provide valid photo identification do not receive the

birth certificate the same day. Their certificates must be mailed to the address displayed on the document(s) provided for identification. Acceptable documents are:

- Social security card
- Pay stub
- Current car registration
- Bank statement
- Letter from a government agency requesting a vital record
- Lease/rental agreement
- Utility bill with current address
- Copy of income tax return/W-2 form

The Division of Vital Records accepts a social security card as an alternate form of identification when requesting copies of vital records. Copies of the identification are not made nor are copies maintained by Vital Records. When individuals submit the social security card as a form of identification when ordering records by mail or fax, the documentation is shredded once the order is filled. Information is verified by a visual inspection of the presented identification. Customers are not asked to provide social security numbers on any DVR application forms.

Due to logistic limitations and the volume of records and applications received annually, there are some applications that cannot be stored within the vault. These applications are secured within DVR offices and are not accessible by the general public. Due to its lack of a paperless, automated system, DVR must maintain copies of all applications for a minimum of two years for audit purposes.

It is the goal of DVR goal to establish a paperless system once an electronic system is in place, which will eliminate many of the potential hazards intrinsic in a paper-based system. DVR envisions information being input electronically and stored on electronic media with access limited to those with identified and approved needs. Any paper received would be scanned and stored electronically, and original copies would be shredded or returned to the customer. Logon IDs would give DVR staff access to only those records necessary to complete their specified duties.

Epidemiology and Disease Control Program

EDCP does not (as a program) request such data from employees. Certain Human Resources and Payroll forms do ask for such information. EDCP does not (as a program) mandate collection of SSN information from the public, e.g., for cases of reportable diseases.

Division of General Accounting

General Accounting processes expense accounts with SSN and address. SSN is designated key for financial system's (FMIS) vendor file. Address is needed in FMIS for payment purposes. Payroll reports contain SSN.

Maryland Cancer Registry

Release of confidential data is governed by the Health—General Code annotated Sections 18-203-204 and Code of Maryland Regulations 10.14.01. Sections of the Health General Code (§4-102) pertaining to the MCR indicate that: 1) Each confidential record shall remain in the custody and control of the Secretary or an agent or employee of the Secretary, if the Secretary assembled or obtained the confidential record, 2) The confidential record may be used only for the research and study for which it was assembled or obtained, 3) A person may not disclose any confidential

record to any person who is not engaged in the research or study project. Violation of this code is considered a misdemeanor. Cancer reports are to include social security numbers per the Federal Public Law (102-515 ).

Medicaid
The Maryland Medicaid program does not release such confidential information to the general public. Employees have access to such information only to the extent that it is necessary to perform their job.

Mental Hygiene Administration
Current Policy and procedures governing the use and disclosure of all Protected Health Information (PHI) in the HMIS are State and Federal (HIPAA) laws specifically written for these purposes. The Federal HIPAA regulations are very explicit in terms of releasing any information that identifies individuals (e.g., Social Security numbers). Mechanisms have been implemented in the last three years that record all accesses to the 'PHI' data and all users of the system must be authorized by management with specific roles that limit what data can be viewed by specific staff. No public requests for data are granted unless the authorization from DHMH management is documented in writing. A recent example of this process is the gun permit queries performed by the Maryland State Police to determine prior Psychiatric hospitalizations over 30 days.

Office of Human Resources
The Department of Budget & Management requires the use of the SSN for all personnel transactions.

Maryland Board of Physicians
Licensure, Compliance and document receiving staff require the use of SSN to enter, update or track transactions through the MBP electronic data systems.

**3. What policies and practices govern the personnel who have access to SSN and other personal information and under what circumstances these individuals are permitted access?**

Breast and Cervical Cancer Diagnosis and Treatment Program
Access to records is limited by job function. Only those whose job requires the need to know are allowed access.

Breast and Cervical Cancer Screening Program
Access to the records is limited by job function. Access to the records is restricted by three different security levels: Windows authentication security to the folder containing the database, file level security to the database, and application level security.

Community Health Administration
Only the Director of the Environmental Health Coordination Program has access to the locked office and locked files associated with the HAB program. Only the Director of the Preventive Medicine/Public Health Residency Program (PMPHR) and the Administrator of the PMPHR have access to the locked files where resident information is kept.

Division of Reimbursements
All DOR employees have access to all data in the performance of their job duties as they relate to the billing and recovery of the cost of care provided to patients by the DHMH hospital facilities and other providers. HIPAA and State, Federal and Departmental privacy laws and regulations govern access to information.

Division of Vital Records
The Division of Vital Records follows the guidelines established by the Department's Office of Human Resources, with all new hires fingerprinted for criminal background checks. The Office of Human Resources alerts DVR if questionable information is found. Though its systems are not fully automated, DVR does maintain electronic indexes for death, marriage, and divorce records to more easily locate a specific vital record. A limited number of birth records are available electronically and social security numbers are not a part of this system. Staff members are assigned individual logon identification codes and system access is limited to those areas essential to performing his or her function.

Many positions within DVR are contractual, and staff are often hired under contract. This results in a high turnover of staff since employees leave as soon as they can find a permanent position with benefits. DVR recognizes that this turnover compromises its security and would prefer to limit hiring of contractual staff to emergencies only rather than making this a standard practice.

Epidemiology and Disease Control Program
Generally EDCP staff sign a confidentiality agreement, as well as an agreement to use State information systems for lawful purposes relating to their job duties. Also, only those individuals with a need for access are given the passwords, IDs, and trainings about how to access records.

Division of General Accounting
General Accounting employees need access to records as part of their job duties. Electronic access is limited based on job duties. Paper documents with SSN and address are stored in locked file cabinets.

Maryland Cancer Registry
All personnel who deal with confidential records are required to read and sign the Maryland Department of Health and Mental Hygiene Confidentiality Agreement of the Maryland Cancer Registry. Included in this agreement are the following requirements:

- I will avoid action that will provide confidential information to any unauthorized individual or agency.
- I will not make copies of any confidential records or data except as specifically authorized.
- I will not remove confidential identifying information from my place of employment except as authorized in the performance of my duties.
- I will not discus in any manner, with any unauthorized person, information that would lead to identification of individuals described in confidential files or data.
- I will use confidential files and data only for purposes for which I am specifically authorized.
- I will not provide any computer password or file access codes which protect these data to unauthorized person.

- If I observe unauthorized access or divulgence of confidential data or records to other person, I will report it immediately to the MCR. I understand that failure to report violations of confidentiality by others is just as serious as my own violation and may result in civil or criminal penalties and termination of current and future access to confidential data.

Medicaid

Division Security Monitors and Supervisors/Managers request in writing access to DHR/DHMH systems. Final approval goes through Agency Security Monitors established by DHR/DHMH rules and regulations. In addition, all employees accessing confidential information must follow HIPAA privacy standards as shown on the DHMH website.

Mental Hygiene Administration

Based upon a users assigned 'role' group within the HMIS system, the specific functions are clearly defined and 'locked in'. In other words the IBM level 40 (object Level) security software prevents users from viewing any data they are not allowed to access by management. Most users of the system are defined in terms of facility specific Medical Record functions, Billing functions, Quality Assurance functions, system operation functions or management/technical functions. The federal HIPAA law is a good example of how users are restricted to the electronic personal data records and for what purposes.

Office of Human Resources

DHMH Policy 02.01.06 "Policy to Assure Confidentiality, Integrity, and Availability of DHMH Information", the DHMH "Information Assurance Guidelines", and DHMH Policy 01.03.06 "Policy on Administrative and Organizational Requirements for Privacy of Health Information" govern access to confidential information. COMAR 17.04.14.01 "Maintenance and Inspection of Records" governs access by members of the public. All OHR employees sign a confidentiality statement annually acknowledging their responsibility for adhering to strict standards of confidentiality where employees' personal information is concerned.

Maryland Board of Physicians

All personnel that require access to electronic records sign a Supervisor Sign-up Sheet that denotes rights or privileges to data that is pertinent to their job duties. In addition, all personnel sign IRMA confidentiality forms to ensure their knowledge of State and DHMH policy concerning confidentiality of protected information.

**4. What procedures and practices ensure that access to SSN and other personal information is limited to only those personnel who need the information to perform their job duties?**

Breast and Cervical Cancer Diagnosis and Treatment Program

Access to records is limited by job function. It is provided by the network administrator via a request voucher signed by the unit director and the security officer.

Breast and Cervical Cancer Screening Program

Access to the records is limited by job function. Access to the records is restricted by three different security levels: Windows authentication security to the folder containing the database, file level security to the database, and application level security.

Community Health Administration
The Administrator of the PMPHR and the Director of the PMPHR discuss confidentiality and security of records on a periodic basis. They are the only two individuals with keyed access to the files.

Division of Reimbursements
Employees have total access to all paper files and documents (with the exception of personnel and timekeeping materials). Employees have limited access to the data maintained on the Hospital Management Information System (HMIS) based on their job function.

Division of Vital Records
In order to provide optimal customer service, staff at both the main office in Baltimore and in the local health departments are often responsible for more than just one function and require access to multiple types of records and/or systems. Although DVR screens employees and provides training on maintaining confidentiality of records, it is impossible to be 100% certain that a staff member is only accessing those records necessary for his or her job. The volume of requests for certificates precludes more security over a paper-based system. As previously noted, an electronic system would more accurately track which records are accessed and by whom to better determine if there are any security breaches.

Epidemiology and Disease Control Program
Supervisory staff ensure during initial and subsequent training which EDCP personnel need access to certain data sets, depending on job function. Such access is rescinded when an employee leaves EDCP.

Division of General Accounting
General Accounting employees need access to records as part of their job duties. Electronic access is limited based on job duties. Paper documents with SSN and address are stored in locked file cabinets.

Maryland Cancer Registry
Supervisory personnel in the Maryland Cancer Registry request access for MCR staff through the FHA network administration. All network drives are password protected. Printouts are labeled as confidential and shredded. Other computer files with SSN derived from the source databases are noted as confidential and subject to the same policies.

Medicaid
Currently access to CARES/MMIS files are limited per DHR/DHMH employee as is the level of security. The level of security is based on the responsibilities or job functions of each individual DHR/DHMH employee.

Many Medicaid employees work in areas that are secured from the general public. Those who do not are instructed on how to keep personal information from being seen by the general public.

Mental Hygiene Administration
The system security software currently enabled (IBM Level 40 Object level security features) prevents all unauthorized access to the HMIS electronic "PHI' data. Management is required to put in writing all requests to add or delete all users from the system.

Office of Human Resources
OHR's practice is to secure all paperwork that contains SSN under lock and key. Electronically, OHR has two dedicated servers that are firewall protected. The Annapolis Data Center is controlled by the Department of Budget and Management security procedures. Procedures contained in DHMH Policy 02.01.06, DHMH "Information Assurance Guidelines", Policy 01.03.06, and COMAR 17.04.14.01 govern access to this information.

Maryland Board of Physicians
All data and network access is scrutinized by senior level staff for appropriateness via signature on the Supervisor Sign-up Sheets. Network and data privilege levels are based upon this authorization.

**5. What policies and practices govern how long SSN and other personal information are kept and how the information is disposed of when no longer needed?**

Breast and Cervical Cancer Diagnosis and Treatment Program
Paper participant records are kept on file as long as the patient remains active. Inactive patient records are picked up by the Department of General Services personnel and shipped to Jessup on a routine basis to be kept for ten years from the date on the record schedule. The Jessup facility has the responsibility to destroy these records via their approved policy. Participant claims files are also sent to Jessup on a routine basis and destroyed after six years from the last date on each box which corresponds to the date the claims were processed.
Electronic records are not destroyed. Some files are archived electronically.

Breast and Cervical Cancer Screening Program
All records with social security numbers are electronic on a secure server. Cumulative electronic records are kept forever.

Community Health Administration
Information on previous residents is maintained so that their status as graduates of the program can be verified. This is governed by policies related to DHMH former employees, as well as policies of the Accreditation Council for Graduate Medical Education (ACGME). Other records (such as HAB-related records) are governed by DHMH record retention policies.

Division of Reimbursements
The Division maintains a Record Retention and Disposal Schedule. The Division also follows the Departmental Records regulations and Federal records requirements where appropriate and also follows procedures as set forth by HIPAA Security Regulations. The Division destroys records in accordance with these policies. Some materials (print outs, etc.) are maintained until completion of audits and then destroyed.

Division of Vital Records
Social security numbers are part of both birth and death records and these original records are kept indefinitely either at DVR or at the Maryland State Archives. Any copies of supporting documentation that contain social security numbers are shredded prior to disposal. Applications for certificates do not contain social security numbers, but applications do contain other identifying information such as names, birth dates, and addresses. For audit purposes, DVR maintains these documents for a minimum of two years.

Ideally, DVR envisions maintaining all vital records information electronically, with the elimination of paper. This will not be possible until the Department completes development and implementation of a system that will store records, allow supporting documentation to be maintained electronically and prepare certified copies of records for issuance. While there are always chances for security breaches with electronic systems, the availability of firewalls, limited and approved system access, and other controls in electronic systems provide much better security for confidential records than paper systems.

Epidemiology and Disease Control Program
EDCP's Record Retention policy dictates how long records are kept; State policies on archiving information or purging electronic files prescribe the manner of disposal.

Division of General Accounting
General Accounting maintains financial records for a total of 5 years, with records usually transferred off grounds after 2 years. All records containing personal information disposed of by General Accounting are shredded.

Maryland Cancer Registry
The files are kept for the life of the registry (some in the db are into the 1980s) on computer. The files are kept at the MCR vendor until the contract changes, then purged from that vendor and transferred to the next vendor.

Medicaid
As of today, records are kept on MMIS for an indefinite amount of time. DHR-CARES records are archived after 3 years.

Mental Hygiene Administration
All HMIS electronic 'PHI' data are stored indefinitely (starting in 1987) on the IBM mini computers that support 16 State operated hospital centers for centralized billing and distributed patient management functions.

Office of Human Resources
DHMH Policy 02.10.02 "Policy on the Management of Records"

Maryland Board of Physicians
Licensure and Compliance data must be accessible throughout the lifetime of licensed medical practitioners and is thus kept indefinitely in various forms, including: electronic, paper and microfiche.

**6. How could policies, procedures and practices be improved to protect SSN and other personal information and limit and prevent unauthorized disclosure?**

Breast and Cervical Cancer Diagnosis and Treatment Program
The Program has ordered and will install software which will monitor those individuals who access the eCMS and patient database. It will allow an independent reviewer the ability to identify unlawful entry into the system and database and to take remedial action quickly.

Breast and Cervical Cancer Screening Program
The BCCP program is exploring ways to limit the view of the Social Security Number field.

Community Health Administration
Facilitation of conversion to fully electronic records would be helpful in this regard. No other policy changes appear to be indicated at this time.

Division of Reimbursement
To effectively and efficiently perform their job duties, DOR employees must have immediate access to all patient financial data. To protect that data from unauthorized use by persons other than employees at field locations, most offices are locked after hours. The exception being the offices located at the Walter P. Carter Center, which share space with other Carter Center employees. Some field offices have a limited number of locking file cabinets, so once access is gotten to the office area patient data files may be readily accessible.

At the central billing office of DOR (300 West Preston Street) there are locks on the doors off of the elevator areas, but there are no locks on the patient file storage areas within the office space, nor are there any lockable file cabinets to protect the patient files. Access to HMIS is controlled by logons and passwords. In order to provide greater security for the patient files, either locking lateral file cabinets would have to be acquired to replace the existing non lockable units or a select number combination keypad door locks should be added to entrance doors and to file room doors to protect the contents of those areas from unauthorized access.

Division of Vital Records
Until an electronic vital records system is implemented, DVR does not have a better solution for protecting social security numbers and other personal information. Space limitations within its current offices prevent all records from being stored in the vault. In order to provide good customer service, staff must have access to all records. While some customers apply for a single type of certificate, others request a combination of birth, death, or marriage certificates or divorce verification. Often they request multiple types with multiple copies of each. Providing the high-quality level of customer service DVR customers have come to expect requires staff to quickly locate and generate the records requested. Staff have been trained to issue records and information only to those entitled to it, and also on the proper and necessary forms of identification customers can provide. It is through staff members' awareness that fraudulent documents have been identified and records protected. In a recent case, DVR staff identified fraudulent documents that were deemed acceptable in another state. DVR was instrumental in preventing more perpetration of fraud by this individual, who was prosecuted and convicted for the offense.

The office is currently set up so that entry to the area where records are stored and staff work is accessible only by swipe card or by admitted entry by the receptionist. Keys are held by a small number of supervisory staff only. Mall personnel do not have access to vital records office space unless accompanied or supervised by vital records staff. Last year at Vital Records' request, mall security began providing a full time guard to the public area during office hours.

Epidemiology and Disease Control Program
Upgrades of technology over time, to protect against inappropriate access to DHMH data systems, records, or files, should be funded as needed. Otherwise, based on track record of experience with millions of EDCP records for more than a decade, no additional specific suggestions seem reasonable. Continued monitoring of data access by supervisory staff, based on current confidentiality guidelines, can be expected.

Division of General Accounting
General Accounting regularly reviews electronic protocols to identify potential problems to improve the security of records.

Maryland Cancer Registry
The MCR does not release SSNs. If a researcher with IRB approval sends the MCR a list of SSN for matching, the MCR uses the SSN that they have sent us and may confirm it if it matches our database, but the MCR never releases SSNs.

We are unaware of any confidential personal information having been disclosed in an unauthorized fashion. We believe our policies are as tight as possible.

Medicaid
Below is a list of items of initiatives that could be implemented to improve the current system:

a. Create a database of all DHR/DHMH employees having access to MMIS. This database would be reviewed and evaluated by Security Monitors on a regular basis.

b. Validate approvals and denials for access to the MMIS system.

c. Conduct unannounced spot checks of employee log-ons.

d. Conduct periodic purging of inactive MMIS records after a certain amount of time. (5 years). All purged records can be copied to a CD and archived. These archived records can be retrieved if necessary.

Mental Hygiene Administration
At rest data encryption (i.e., automatic encryption of data stored on hard drives or back-up medium) would be an ideal add on to 'harden' data security against unauthorized data access on the IBM servers.

Office of Human Resources
There have been no instances of unauthorized disclosure of personal information by OHR staff. The SSN is a unique identifier. It is our understanding that it may legally be used in the payroll and benefits process. We are not aware of any better methods to protect personal information than the ones that we currently use.

Maryland Board of Physicians
A periodic review of data access practices may uncover previously undetected systemic breakdowns or risk points. Elimination or "masking" of SSN and other sensitive data from general view screens can also reduce the risk associated with identity theft.

# TESTIMONY PRESENTED BY
# BRIAN WILBON, DEPUTY SECRETARY FOR OPERATIONS
# MARYLAND DEPARTMENT OF HUMAN RESOURCES
# BEFORE THE
# TASK FORCE TO STUDY IDENTITY THEFT

Wednesday, August 22, 2007, 1:00 p.m.
House Office Building, Room 100, Annapolis, MD

Good Afternoon, Chairwoman Kelley and Chairwoman Lee. My name is Brian Wilbon and I am the Deputy Secretary for Operations in the Maryland Department of Human Resources. I am delighted to represent the Department at this Task Force and to explain to you how we maintain the confidentiality of Social Security numbers. I have with me today staff from the Department to answer specific questions regarding specific programs.

In responding to your questions sent to the Department on August 6, 2007, I will give a general overview about how many Social Security numbers are collected as well as how those Social Security numbers and other personal information are maintained. Attached to the testimony is a packet of policies and procedures which is program and office specific and details how those programs and offices collect and maintain personal information.

**How many records containing Social Security numbers and other personal information are maintained?**

The Department collects and maintains about 2.7 million active records with Social Security numbers in our automated data bases. We collect approximately 50,000

Social Security numbers in our personnel office which includes current staff, contractual staff, and applicants. The Inspector General collects another 2 million Social Security numbers for the purpose of investigating allegations of public assistance, employee, and vendor fraud; and for audits of the 24 local departments of social services.

**For what purpose is the information collected and used?**

Each Administration within the Department has a variety of rules for what information is collected and how it used. For those programs where we are providing direct services to the community do require Social Security numbers. Those programs include: The Family Investment Administration (FIA), The Child Support Enforcement Administration (CSEA), The Social Services Administration (SSA) and The Community Services Administration (CSA).

For example FIA uses Social Security numbers as a tool to determine eligibility for services including Temporary Cash Assistance, Food Stamps and Medicaid. Use of the numbers is required by the federal government in order to match and track individuals and in most cases there is corresponding state law and state regulation. Additionally FIA uses Social Security numbers to match with employment records with the Department of Labor Licensing and Regulation to insure accuracy of payments and to avoid overpayments. The Child Support program is also required by the federal government to collect Social Security numbers to interface with various State and federal agencies to establish paternity, locate parents and collect support, and to ensure payments.

**What policies and practices govern when and how Social Security numbers are requested from the public and your employees?**

The policy and practice of giving Social Security numbers to the public is governed by state and federal law and regulations. Social Security numbers are shared by programs and only released if directed by the court, by a federal or state government or with contractors doing business with the state who have a valid contract and by law need the Social Security numbers for program activity, which may include automation, matching and tracking individuals as stated above or to assist in fraud or criminal investigations or as required to determine eligibility.

In the course of doing business with the public and providing services to the public Social Security numbers are requested by employees when that information is needed to meet State or federal requirements that govern operation of our programs. Specifically the Child Support program must request Social Security numbers of parents or risk fiscal sanction by the federal government. Forms which are used in our Human Resources Development and Training Office which handles all of the Department's personnel matters must include Social Security numbers as required by the Department of Budget and Management.

**What policies and practices govern the personnel who have access to Social Security numbers and other personal information and under what circumstances these individuals are permitted access?**

With regard to program activity, the Department maintains stringent policies to grant restrict and terminate access to our computer systems where all program functions are maintained. Levels of access are requested and granted based on classification and job function. The Department's data security unit reviews requests for access to ensure appropriateness. Passwords are routinely changed and must meet minimum standards in terms of length and characters to minimize the likelihood that a password could be cracked by a hacker or others with malicious intent. Passwords are protected to prevent malware from compromising the password files, and security and virus patches.

The Department also maintains paper records with Social Security numbers. Those files are kept in locked filing cabinets. Access is limited to the staff of the unit as required by their job function. Employees are governed by COMAR 07.01.07 Confidentiality of Records, and there are civil and or criminal penalties if an employee violates those policies and procedures.

**What procedures and practices ensure that access to Social Security numbers and other personal information is limited to only personnel who need the information to perform their job duties?**

A computer and paper file where personal information is stored is protected by strict guidelines and policies. Employees are only granted access to those functions and files needed to perform his or her job. Access is monitored by supervisors, managers and administrators.

**What policies and practices govern how Social Security numbers and other personal information are kept and how the information is disposed of when no longer needed?**

Retention schedules are set by the Program Administrations. All program schedules follow state and federal law and data could be retained beyond that if there is an audit or legal requirement. For example, adoption records are maintained for 75 years based on federal law and are stored in Jessup. In Child Protective Services, ruled out cases are retained for 120 days and then destroyed. In Child Support cases, information is maintained for as long as the case is active. Once the case is closed, the information is stored in our computer system. Hard copy files are destroyed three years after case closure by shredding or incineration. Any information stored electronically is encrypted. Information on magnetic tapes is overwritten during back-up processes. When the tape reaches its useful life, the tape is destroyed by shredding.

**How could policies, procedures and practices be improved to protect Social Security numbers and other personal information and limit or prevent unauthorized disclosure?**

Numerous policies and procedures are in place currently to mitigate the risks associated with maintaining personally identifiable information in technological and paper environments. We do have a few recommendations including:

- Standardize the transportation of documents when transferring closed records.
- Develop a policy on electronic exchange of personal information which would include blackberries, thumb drives, laptops and personal hand held devices.

- Review and revise standard procedures securing paper records
- Consistently enforce policy and procedures, physical safeguards and IT security
- Review our security policies as part of the biennial review by our Inspector General
- Annual staff training and certification and acknowledgement of security procedures

# Motor Vehicle Administration

## Presentation to the Identity Theft Task Force

August 22, 2007

IDENTITY THEFT TASK FORCE 8.22.07

**1. How many records containing Social Security numbers (SSN) and other personal information are maintained? For what purpose is this information collected and used?**

The MVA currently has 6,095,608 records containing SSNs. The purpose for collection of the SSNs for driver's license applicants is to comply with federal and state statute and state regulations.

FEDERAL LAW
- 42 USC 405(c)(2)(c)(i) provides authorization for the use of the SSN as identification for driver licensing purposes.
- 42 USC 666 requires states to collect the SSN of any driver's license applicant for improving collection in child support enforcement.

STATE LAW
- TR § 16-106(b)-(c) requires the MVA to collect a driver's license applicant's SSN or a self-certification that the applicant is not eligible for a social security number. For commercial driver's licenses, a SSN is required by TR § 16-810.

- COMAR 11.17.12. governs the disclosure of an individual's SSN. This section also limits the use of a SSN to: Identification purposes (to match a number with a name), collection of debts (specifically vehicle registration debts, insurance compliance fines, excise tax collections, and child support), and verification of driver records with other databases.

See attachment "A" for full copy of the aforementioned laws.

**2. What policies and practices govern when and how SSNs are requested from public and your employees?**

There are statutory protections to protect a driver license applicant's SSN and all personal information. Personal information maintained by the MVA is closed to the public under the federal Driver Privacy Protection Act of 1994, codified in Maryland as SG 10-616(p) (attachment "A").

See attachment "B" for a copy of MVA Policy regarding collection of SSN.

**3. What policies and practices govern the personnel who have access to SSNs and other personal information and under what circumstances these individuals are permitted access?**

Access to confidential data and information is tightly controlled and approved only for legitimate job related purposes. There is a security access form MVA employees must fill out and have approved for access to the database. Management must approve

the level of access based on job classification and responsibilities. Additionally, all employees must sign a security advisory statement acknowledging prohibited information disclosure.

Regarding SSNs, access is more restricted with very few employee classifications having access. This restriction is already in place with most mainframe functions to mask the Social Security number except for the last 4 digits. All other MVA programs will be updated by the end of 2007 to also have this masking restriction.

See attachment "C" for a copy of the MVA Security Advisory Form.

**4. What procedures and practices ensure that access to SSNs and other personal information is limited to only those personnel who need the information to perform their job duties?**

A password policy prevents unauthorized use of computers. All terminals use biometric physical security to ensure proper use. The password policy requires 12 characters and must be changed every 45 days.

Whenever a driving record is accessed, the Security Access Program (SAP) makes a record of the transaction. This record includes what username and terminal the changes were made from and both the date and time of the change. This SAP record is stored indefinitely.

For Quality Control employees, the Driving Record Automated Transmission System (DRATS) produces a daily report of any changes made. The supervisors of the Quality Control Unit audit 5% of these records for accuracy.

The Social Security Administration conducts periodic audits of how the MVA handles the SSNs that are collected. The last audit concluded in the fall of 2006.

**5. What policies and procedures govern how long SSNs and other personal information are kept and how the information is disposed of when no longer needed?**

It is important to understand that the MVA does not keep written records of SSNs. This information is only stored electronically in our secure database. This database encompasses several security features.

The records are never purged or disposed of. When a person dies, their record is appropriately marked but kept in the database to prevent misuse.

**6. How could policies, procedures, and practices be improved to better protect SSNs and other personal information and limit or prevent unauthorized disclosure?**

The Maryland Department of Transportation is in the planning phase of encrypting data currently stored on the mainframe as well as the tapes that go off-site for backup.

In September the MVA will begin a "V" indicator program. After a victim files a police report and signs the authorization form, this program permits an identity theft victim to have a "V" placed on their driving record and license to alert law enforcement personnel. For instance, if someone attempts to use a victim's name or identifying information in a traffic stop and does not physically have the driver's license, the officer will be alerted from the "V" code contained on their driving record that the person has been a victim of identity theft. The officer should attempt to further verify the identity of the individual. At a recent American Association of Motor Vehicle Administrators meeting this program was mentioned as one of the first identity theft programs in the country.

By the end of 2007, MVA will also finish masking SSNs in all systems.

# Attachment "A"

## Federal Law

### 42 U.S.C. Section 405(c)(2)(c)(i). Evidence, procedure, and certification for payments.

It is the policy of the United States that any State (or political subdivision thereof) may, in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law within its jurisdiction, utilize the social security account numbers issued by the Commissioner of Social Security for the purpose of establishing the identification of individuals affected by such law, and may require any individual who is or appears to be so affected to furnish to such State (or political subdivision thereof) or any agency thereof having administrative responsibility for the law involved, the social security account number (or numbers, if he has more than one such number) issued to him by the Commissioner of Social Security.

### 42 U.S.C. Section 666. Requirement of statutorily prescribed procedures to improve effectiveness of child support enforcement.

Requirement of statutorily prescribed procedures to improve effectiveness of child support enforcement

(13) Recording of social security numbers in certain family matters. — Procedures requiring that the social security number of—

(A) any applicant for a professional license, driver's license, occupational license, recreational license, or marriage license be recorded on the application;
(B) any individual who is subject to a divorce decree, support order, or paternity determination or acknowledgment be placed in the records relating to the matter; and
(C) any individual who has died be placed in the records relating to the death and be recorded on the death certificate.

For purposes of subparagraph (A), if a State allows the use of a number other than the social security number to be used on the face of the document while the social security number is kept on file at the agency, the State shall so advise any applicants.

## Maryland State Law and Regulations

### Transportation Article, §16–106. Application for license – In general.

(b) The application shall state:

(4) Subject to the provisions of subsection (c) of this section, the applicant's Social Security number; and

(c) (1) Subsection (b)(4) of this section applies only to an applicant who has a Social Security number.

(2) If an applicant does not have a Social Security number, the applicant shall certify in the application that the applicant does not have a Social Security number.

(d) The applicant shall sign the application and certify that the statements made in it are true.

## Transportation Article, § 16-810. Application for license.

(a) Each application for a commercial driver's license or commercial driver's instructional permit shall be made on the form the Administration requires.

(b) In addition to the information specified by § 16-106 of this title, each application shall contain:

(1) The applicant's Social Security number;

(c) Under penalty of perjury, the applicant shall sign the application and certify that the statements made are true and correct to the best of his knowledge, information, and belief.

## State Government Article, § 10-616. General Right to Information – Specific Records.

(p) (1) Except as provided in paragraphs (2) through (5) of this subsection, a custodian may not knowingly disclose a public record of the Motor Vehicle Administration containing personal information.

(2) A custodian shall disclose personal information when required by federal law.

(3) (i) This paragraph applies only to the disclosure of personal information for any use in response to a request for an individual motor vehicle record.

(ii) The custodian may not disclose personal information without written consent from the person in interest.

(iii) 1. At any time the person in interest may withdraw consent to disclose personal information by notifying the custodian.

2. The withdrawal by the person in interest of consent to disclose personal information shall take effect as soon as practicable after it is received by the custodian.

(4) (i) This paragraph applies only to the disclosure of personal information for inclusion in lists of information to be used for surveys, marketing, and solicitations.

(ii) The custodian may not disclose personal information for surveys, marketing, and solicitations without written consent from the person in interest.

(iii) 1. At any time the person in interest may withdraw consent to disclose personal information by notifying the custodian.

2. The withdrawal by the person in interest of consent to disclose personal information shall take effect as soon as practicable after it is received by the custodian.

(iv) The custodian may not disclose personal information under this paragraph for use in telephone solicitations.

(v) Personal information disclosed under this paragraph may be used only for surveys, marketing, or solicitations and only for a purpose approved by the Motor Vehicle Administration.

(5) Notwithstanding the provisions of paragraphs (3) and (4) of this subsection, a custodian shall disclose personal information:

(i) for use by a federal, state, or local government, including a law enforcement agency, or a court in carrying out its functions;

(ii) for use in connection with matters of:

1. motor vehicle or driver safety;
2. motor vehicle theft;
3. motor vehicle emissions;
4. motor vehicle product alterations, recalls, or advisories;
5. performance monitoring of motor vehicle parts and dealers; and
6. removal of nonowner records from the original records of motor vehicle manufacturers;

(iii) for use by a private detective agency licensed by the Secretary of State Police under Title 13 of the Business Occupations and Professions Article or a security guard service licensed by the Secretary of State Police under Title 19 of the Business Occupations and Professions Article for a purpose permitted under this paragraph;

(iv) for use in connection with a civil, administrative, arbitral, or criminal proceeding in a federal, state, or local court or regulatory agency for service of process, investigation in anticipation of litigation, and execution or enforcement of judgments or orders;

(v) for purposes of research or statistical reporting as approved by the Motor Vehicle Administration provided that the personal information is not published, redisclosed, or used to contact the individual;

(vi) for use by an insurer, insurance support organization, or self-insured entity, or its employees, agents, or contractors, in connection with rating, underwriting, claims investigating, and antifraud activities;

(vii) for use in the normal course of business activity by a legitimate business entity, its agents, employees, or contractors, but only:

1. to verify the accuracy of personal information submitted by the individual to that entity; and

2. if the information submitted is not accurate, to obtain correct information only for the purpose of:

A. preventing fraud by the individual;

B. pursuing legal remedies against the individual; or

C. recovering on a debt or security interest against the individual;

(viii) for use by an employer or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under the Commercial Motor Vehicle Safety Act of 1986 (49 U.S.C.A. § 2701 et seq.);

(ix) for use in connection with the operation of a private toll transportation facility;

(x) for use in providing notice to the owner of a towed or impounded motor vehicle;

(xi) for use by an applicant who provides written consent from the individual to whom the information pertains if the consent is obtained within the 6-month period before the date of the request for personal information;

(xii) for use in any matter relating to:

1. the operation of a Class B (for hire), Class C (funeral and ambulance), or Class Q (limousine) vehicle; and

2. public safety or the treatment by the operator of a member of the public;

(xiii) for a use specifically authorized by the law of this State, if the use is related to the operation of a motor vehicle or public safety; and

(xiv) for use by a hospital to obtain, for hospital security purposes, information relating to ownership of vehicles parked on hospital property.

(6) (i) A person receiving personal information under paragraph (4) or (5) of this subsection may not use or redisclose the personal information for a purpose other than the purpose for which the custodian disclosed the personal information.

(ii) A person receiving personal information under paragraph (4) or (5) of this subsection who rediscloses the personal information shall:

1. keep a record for 5 years of the person to whom the information is redisclosed and the purpose for which the information is to be used; and

2. make the record available to the custodian on request.

(7) (i) The custodian shall adopt regulations to implement and enforce the provisions of this subsection.

(ii) 1. The custodian shall adopt regulations and procedures for securing a person in interest's waiver of privacy rights under this subsection when an applicant requests personal information about the person in interest that the custodian is not authorized to disclose under paragraphs (2) through (5) of this subsection.

2. The regulations and procedures adopted under this subparagraph shall:

A. state the circumstances under which the custodian may request a waiver; and

B. conform with the waiver requirements in the federal Driver's Privacy Protection Act of 1994 and other federal law.

(8) The custodian may develop and implement methods for monitoring compliance with this section and ensuring that personal information is used only for purposes for which it is disclosed.

## COMAR TITLE 11

## SUBTITLE 11 – MOTOR VEHICLE ADMINISTRATION – ADMINISTRATIVE PROCEDURES

### 11.11.01.02 Use of the Social Security Number.

A. The Administration may use the Social Security number obtained under Regulation .01 of this chapter for the following purposes:

(1) The administration and enforcement of Maryland's vehicle registration and driver licensing laws;
(2) Verifying the identity of a person to whom a vehicle is registered;
(3) Any purpose authorized under COMAR 11.17.12; or
(4) The collection of any debts owed as a result of the owner's failure to pay:
    (a) Fees owed by the owner for the registration of any vehicle,
    (b) Penalties owed by the owner under Transportation Article, § 17-106, Annotated Code of Maryland,
    (c) Fees owed by the owner for the issuance of an identification document, as defined in COMAR 11.17.12.01, and
    (d) The excise tax owed for the titling of any vehicles owned by the owner.

B. The Administration may not utilize the Social Security number for any purpose not authorized under this regulation or COMAR 11.17.12.

C. Except as provided in this regulation and COMAR 11.17.12, the Administration may not disclose an individual's Social Security number.

## SUBTITLE 17 – MOTOR VEHICLE ADMINISTRATION – DRIVER LICENSING AND IDENTIFICATION DOCUMENTS

### 11.17.09.04 Proof of Residence, Age, Identity, and Name Change.

A. Initial and Duplicate Licenses.

D. Identifying Document List.
(1) The following sources of identification are considered primary sources of identification:

(b) Actual Social Security card;

### 11.17.09.06 Fraud and Misrepresentation.

A. The Administration may not accept as proof of identity or a Maryland residence address any document which it has reason to believe has been altered, has been fraudulently obtained, or is misrepresentative.

B. Notwithstanding any provision of this chapter or of COMAR 11.17.12, the Administration may require additional documentation, including an actual Social Security card, if it suspects that fraudulent, altered, or misrepresented documents have been submitted.

### 11.17.12.02 Disclosure.

A. The Administration shall request the social security number of each applicant for an original, renewed, duplicate, or corrected driver's license or identification document.

B. An applicant for a driver's license shall disclose the applicant's social security number as required by 42 U.S.C. §666. If the applicant does not have a social security number, the applicant shall certify in the application that the applicant does not have a social security number.

C. The administration shall deny the issuance of a driver's license for failure to disclose the required social security number or to certify that the applicant does not have a social security number.

D. The disclosure of the social security number is voluntary for applicants for an identification document.

### 11.17.12.03 Use of the Social Security Number.

A. The Administration may use the social security number for the following purposes:

(1) Verifying driver records through:
(a) The National Driver's Registry,

(b) Other states' motor vehicle agencies, and
(c) The Commercial Driver's License Information System;
(2) Verifying out-of-State driving convictions;
(3) Verifying the identity of a person when two individuals have the same name and the same date of birth;
(4) Identifying a person who has changed that person's name as permitted under the Maryland Vehicle Law and the Motor Vehicle Administration's regulations;
(5) Assisting law enforcement agencies in identifying a person who is the subject of an investigation regarding that person's driver's license or motor vehicle registration;
(6) Providing the Administration with access to a person's driving or vehicle registration records when the purpose for which access is sought is permitted by State and federal laws;
(7) Identifying an individual for driver licensing and vehicle registration purposes as long as a disclosure of the social security number conforms with State and federal laws;
(8) The administration and enforcement of Maryland's vehicle registration and driver licensing laws;
(9) Verifying the identity of a person to whom a vehicle is registered;
(10) The collection of any debts owed as a result of the applicant's failure to pay:
(a) Fees owed by the applicant for the issuance of a driver's license or an identification document,
(b) Fees owed by the applicant for the registration of any vehicles owned by the applicant,
(c) Penalties owed by the applicant under Transportation Article, §17-106, Annotated Code of Maryland, and
(d) Excise tax owed for the titling of any vehicles owned by the applicant; or
(11) Assisting in the enforcement of child support orders as required by State and federal laws.
B. The Administration may not utilize the social security number for any purpose not authorized under this regulation, COMAR 11.11.01.02, or COMAR 11.17.09.

## 11.17.12.02 Disclosure.

A. The Administration shall request the social security number of each applicant for an original, renewed, duplicate, or corrected driver's license or identification document.

B. An applicant for a driver's license shall disclose the applicant's social security number as required by 42 U.S.C. §666. If the applicant does not have a social security number, the applicant shall certify in the application that the applicant does not have a social security number.

C. The administration shall deny the issuance of a driver's license for failure to disclose the required social security number or to certify that the applicant does not have a social security number.

D. The disclosure of the social security number is voluntary for applicants for an identification document.

## 11.17.12.03 Use of the Social Security Number.

A. The Administration may use the social security number for the following purposes:

(1) Verifying driver records through:

(a) The National Driver's Registry,
(b) Other states' motor vehicle agencies, and
(c) The Commercial Driver's License Information System;

(2) Verifying out-of-State driving convictions;

(3) Verifying the identity of a person when two individuals have the same name and the same date of birth;

(4) Identifying a person who has changed that person's name as permitted under the Maryland Vehicle Law and the Motor Vehicle Administration's regulations;

(5) Assisting law enforcement agencies in identifying a person who is the subject of an investigation regarding that person's driver's license or motor vehicle registration;

(6) Providing the Administration with access to a person's driving or vehicle registration records when the purpose for which access is sought is permitted by State and federal laws;

(7) Identifying an individual for driver licensing and vehicle registration purposes as long as a disclosure of the social security number conforms with State and federal laws;

(8) The administration and enforcement of Maryland's vehicle registration and driver licensing laws;

(9) Verifying the identity of a person to whom a vehicle is registered;

(10) The collection of any debts owed as a result of the applicant's failure to pay:

(a) Fees owed by the applicant for the issuance of a driver's license or an identification document,
(b) Fees owed by the applicant for the registration of any vehicles owned by the applicant,
(c) Penalties owed by the applicant under Transportation Article, §17-106, Annotated Code of Maryland, and
(d) Excise tax owed for the titling of any vehicles owned by the applicant; or

(11) Assisting in the enforcement of child support orders as required by State and federal laws.

B. The Administration may not utilize the social security number for any purpose not authorized under this regulation, COMAR 11.11.01.02, or COMAR 11.17.09.

## 11.17.12.04 Display of Social Security Number.

A. Except as provided in Regulation .03, COMAR 11.11.01.02, and COMAR 11.17.09, the Administration may not disclose a person's social security number.

B. A social security number may not be disclosed in a person's public driving record or displayed on a person's identification document, except when required by federal law.

# Attachment "B"

**TOPIC:** **Mandatory Social Security Number Collection**
**Originator:** **Driver Services Division**

I. **Effective Date:** October 1, 2003

II. **Description:**

This policy describes the standards the Motor Vehicle Administration (MVA) will follow in requiring customers to provide their Social Security Number (SSN) during certain MVA transactions.

**Applicants self-certifying they are not eligible / do not have a SSN are not required to provide a SSN on the application (See Section V., #7 below).**

III. **Legislative Authority:**

1. Title 42, United States Code, §666. Requirements for statutorily prescribed procedures to improve effectiveness of child support enforcement. Mandates that an applicant for a driver's license shall disclose the applicant's SSN.

2. COMAR 11.17.12. Social Security Number – Requires individuals to submit a SSN when applying for a driver's license in the State of Maryland.

IV. **Relationship to MVA's Mission:**

This policy is consistent with MVA's mission of providing excellence in customer service. By collecting and verifying SSN's, the MVA is improving the accuracy and integrity of driver records pertinent to child support enforcement and the general security of the public.

V. **Policy Statements:**

1. The Motor Vehicle Administration (MVA) shall request and verify the Social Security Number (SSN) of each applicant for an original, renewed, duplicate, or corrected driver's license. This includes commercial (CDL) and non-commercial, temporary, and provisional licenses, and learner's permits.

2. **Disclosure of the SSN for Identification Cards (ID Cards) and moped permits is voluntary**. However, the MVA still shall request the SSN of such applicants. If a SSN is either not provided or provided but not verifiable, the MVA will use a generic number to complete the application, same as when an applicant does not have a SSN due to ineligibility (See # 7 below).

**TOPIC:** **Mandatory Social Security Number Collection**
**Originator:** **Driver Services Division**

3. Applicants are required to provide a verifiable SSN as a condition of obtaining an original, renewed, duplicate, or corrected driver's license. If the MVA determines a SSN is not verifiable, the MVA may deny issuance.

4. If the MVA denies a driver's license for SSN reasons, the MVA may issue a temporary non-commercial driver's license according to standard procedures (for example, same as when an applicant fails the eye test). The purpose is to afford applicants time to obtain, correct or otherwise provide a verifiable SSN. Temporary issuance is not allowed for CDL holders unless the MVA's SSN verification system is down (See #10 b. below).

5. The MVA shall verify SSNs electronically with the Social Security Administration (SSA). The MVA shall confirm the SSN with the applicant before it is sent for verification. If a SSN sent for verification is returned not verifiable, the MVA may allow the applicant to re-confirm or correct the SSN and may re-send it for verification.

6. In instances of alleged errors with SSA records, it is incumbent upon the applicant to pursue error correction through the SSA. The MVA shall provide applicants with contact information for the SSA. The MVA may issue a temporary license in such instances (See #4 above).

7. A SSN is not required if the applicant certifies by signature on the application that he/she is ineligible and does not have an SSN but is otherwise eligible for a driver's license. For example, a foreign national temporarily residing in this country who presents the required primary documents evidencing proof of residence in the United States.

8. Anyone eligible for a SSN must provide a verifiable SSN as a condition of obtaining an original, renewed, duplicate, or corrected driver's license. Exceptions shall not be allowed on religious, cultural, political or any other grounds other than SSN ineligibility (See #7 above).

9. Once a SSN is verified applicants still are required to disclose their SSN at future driver's license transactions. If the SSN provided at future transactions matches the verified SSN on the MVA record, the MVA shall consider it still verified. If a different and verifiable SSN is provided, MVA shall update the record accordingly. If a different and not verifiable SSN is provided, the MVA may deny an original, renewed, duplicate, or corrected driver's license.

**TOPIC:** **Mandatory Social Security Number Collection**
**Originator:** **Driver Services Division**

10. If the MVA's electronic SSN verification system is down:

    a. For Non-Commercial Applicants - The MVA may issue an original, renewed, duplicate, or corrected non-commercial driver's license without immediate SSN verification. Upon restored electronic verification, the MVA shall verify all outstanding SSNs. Instances where the MVA determines a SSN is not verifiable may result in cancellation of a driver's license according to standard procedures.

    b. For CDL Applicants – The MVA shall not issue an original, renewed, duplicate, or corrected CDL if electronic verification is down. The MVA may issue a temporary license to CDL applicants subject to later verification and cancellation as warranted. If later verification is successful, the MVA shall issue the CDL to the applicant.

11. In accordance with standard MVA procedures, if the MVA acts to cancel a driver's license for SSN reasons, written notification to include a future effective date for the cancellation shall be provided to the applicant. If the applicant provides a verifiable SSN before the effective date, the MVA may halt license cancellation and issue a corrected license. After the cancellation effective date, the applicant may re-apply for a license.

## VI. Purpose/Background:

Previously the MVA collected SSNs during transactions on a voluntary basis. The result was a driver record database containing some missing or inaccurate SSNs. In 1997 in compliance with federal law the MVA began exchanging records with the Child Support Enforcement Administration (CSEA) which uses the SSN as its primary record key. The MVA's mandatory collection and verification of SSNs will improve the MVA's capability to match records with the CSEA. It also brings the MVA into compliance with federal law requiring individuals to disclose their SSN when applying for a driver's license for the purpose of enhancing child support enforcement.

## VII. Definitions: Not Applicable.

## VIII. Procedures:

For operational procedures for MVA Branch Offices on mandatory SSN collection and verification, refer to applicable DLS procedures.

**TOPIC:** **Mandatory Social Security Number Collection**
**Originator:** **Driver Services Division**

## IX. Reference Material:

1. *Memorandum of Agreement between the State of Maryland Motor Vehicle Administration and the Social Security Administration*, approved October 13, 2000. Establishes the conditions for the SSA to provide verification services to the MVA.

## X. Alternatives Considered but Not Selected:

The alternative to this policy is to continue collecting SSNs on a voluntary basis and without verification. This alternative is not viable because it would neither improve the MVA's ability to match records with the CSEA nor bring the MVA into compliance with federal law.

## XI. Similarities with Other States:

According to an AAMVA email survey conducted by the MVA in September 2002, the following states require applicants for commercial and non-commercial driver's licenses to disclose SSN: CA, CT, DE, FL, IL, IA, KY, MO, NJ, NY, ND, OH, OK, SD, TN, TX, UT, VA, WA, WV, and WI.

## XII. Quality Control Methods:

The quality control methods for this policy will include the SSN being a required field in DLS and electronic verification of SSNs with the Social Security Administration.

## XIII. Performance Measure:

The performance measure for this policy will be the percentage of records matching with CSEA by SSN. Increased matching by SSN indicates increased accuracy of SSNs in the MVA database.

## XIV. Endorsement:

Administrator - Signature on file in the Office of Driver & Vehicle Policy.

## XV. Change History:

| Adopted | Brief Description |
|---|---|
| 2003/24/10 | Omit references to temporary license time frame; omit incorrect sentence on entering a generic SSN for ineligible applicants – the field is left blank. |

# Attachment "C"

# Maryland Department of Transportation
# Office of Transportation Technology Services

## SECURITY ADVISORY FORM

This ADVISORY is initiated for INFORMATIONAL purposes only. The following paragraphs shall in no way be construed as a waiver by the undersigned of the rights and protections provided by COMAR (Code of Maryland Regulations) Volume XII Title II Transportation, if applicable, and/or by law or regulation.

The Office of Transportation Technology Services, its client agencies and their customers adhere to state data processing security policies as set forth in Executive Order 01.01.1983.18 (Privacy and State Data System Security); Md. Ann. Code, art. 27 §§ 45A (falsification of public records) and 146 (unauthorized access); Md. Code Ann., State Gov't §§ 10-611, 10-616 and 10-626 (Maryland Public Information Act); Md. Code Ann., Transp. II §§ 12-111 to 12-113 (Motor Vehicle Administration Records); and, as published by the Secretary of the Department of Budget and Management from time to time under Md. Code Ann., State Fin. & Proc. § 3-403.

Federal laws affecting access to and use of computer information include, but are not limited to, the following: 15 U.S.C.S. § 271, 40 U.S.C.S. § 759 (Computer Security Act of 1987); 23 U.S.C.S. § 401 (National Driver Register Act); 5 U.S.C.S. § 552 (Freedom of Information Act); 5 U.S.C.S. § 552a (Privacy Act of 1974); 18 U.S.C.S. § 1001 (Computer Fraud and Abuse Act of 1986); § 17 U.S.C.S. § 109 (Computer Software Rental Amendments Act of 1990); 15 U.S.C.S. § 1681 (Fair Credit Reporting Act); and, 18 U.S.C.S. §§ 2721 et seq. (Driver's Privacy Protection Act of 1994).

Specifically **PROHIBITED ACTS** include, but are not limited to:

1. Unauthorized access to or use of a computer, data or software.
2. Unauthorized copying or disclosure of data or software.
3. Obtaining unauthorized confidential information.
4. Unauthorized modification or altering of data or software.
5. Introduction of false information (public records).
6. Disruption or interruption of the operation of a computer.
7. Disruption of government operations or public services.
8. Denying services to authorized users.
9. Taking or destroying data or software.
10. Creating/altering a financial instrument or fund transfer.
11. Misusing or disclosing passwords.
12. Breaching a computer security system.
13. Damaging, altering, taking or destroying computer equipment or supplies.
14. Devising or executing a scheme to defraud.
15. Obtaining or controlling money, property, or services by false pretenses.

Authorized access to, including **INTERNET** and **INTRANET**, and use of information and computer resources is limited to the **PURPOSE** for which these privileges are granted. All authorized users during the term of their access and thereafter, shall hold in strictest confidence and not willfully disclose to any person, firm or corporation without the express authorization of the Director, OTTS, any information related to security, operations, techniques, procedures or any other security matters. Any breach of security will be promptly reported to the Director, Office of Transportation Technology Services, designee or security officer.

I acknowledge that I have read and understand the foregoing security advisory.

Date: _____ Name: _____
(Please print or type)

EIN: _____ _____
(Signature)

Badge _____ Logonid _____

COMPTROLLER of MARYLAND
*Serving the People*

# Testimony of the Comptroller of Maryland before the Task Force to Study Identity Theft

Thank you for this opportunity to discuss with the Task Force members the Comptroller's Office use and protection of social security numbers and other personal information of Maryland's taxpayers.

We currently have 8.3 million active social security numbers on our income tax file, 690,000 accounts on our Central Registration file where we capture the social security number of responsible officers for withholding tax purposes, 157,000 active social security numbers on our payroll file and 1.3 million federal employer identification numbers or social security numbers on the R*STARS system that pays the State's bills. The Central Payroll Bureau also maintains annual payroll summary information in the form of W-2 files that go back to 1986. Holders of unclaimed property often include social security numbers of owners when they report abandoned property to the Comptroller and we currently have 245,000 social security numbers on that file. Our Field Enforcement agents have access to the Criminal Justice Information System (CJIS) and utilize social security numbers to access information for enforcement purposes. Social security numbers are also used to a more limited extent in other areas of the agency. The identifying numbers and names and addresses of individuals and businesses are invariably used by our agency for tax administration and criminal justice administration.

Social security numbers are requested from the public strictly for the administration of our various programs, and the requirement to provide these numbers is often mandated by statute. For instance, Section 6109 of the Internal Revenue Code sets forth the requirement that taxpayers include their social security number on each return and Maryland has adopted that requirement Section 15-102 of the State Finance and Procurement Article of the Annotated Code of Maryland specifically requires a contractor submitting an invoice for a procurement contract to include the contractor's federal employer's identification number or social security number on the invoice. The W-2 files that are maintained by the Central Payroll Bureau are used in the generation of Wage and Tax Statements as required by the Social Security Act of 1935.

Section 13-202 of the Tax General Article of the Annotated Code of Maryland provides that "Except as otherwise provided in this subtitle, an officer, employee, former officer, or former employee of the State or of a political subdivision of the State may not disclose, in any manner, any tax information." The exceptions to this rule are extremely narrow and a violation of this provision carries criminal penalties. The Comptroller's Office endeavors to protect this information. Every employee in the agency must sign a Certificate of Confidentiality (see Attachment No. 1) the first day of employment. In addition, contractors and vendors working on our behalf are required by contract to sign this form. Every time an employee signs on to CICS (our mainframe transaction server) to begin to access our various systems, a screen appears (see Attachment No. 2) warning that browsing in taxpayer files is unlawful and describes the potential consequences for doing so, both disciplinary and criminal. Access to our buildings in Annapolis is strictly controlled to prevent unauthorized parties from obtaining confidential information. In Baltimore we have installed keypad access to the three floors in the State Office Building complex that houses our offices.

Each individual employee's job description and the various divisions' operating manuals govern whether each employee has access to any of our systems and, if so, which ones. Some employees are granted inquiry access only and others may require update capability to perform their job functions. This is accomplished utilizing access control software(ACF2) that (1) identifies users by means of a Logon ID and a password, (2) based on the access rules established for each user, allows access only to authorized files, and (3) produces audit logs showing which Log On IDs have accessed what files and produces security violation reports. Each Division within the agency has a security officer who periodically coordinates the management review of the system access reports to determine if access for each employee continues to be appropriate for the employee's job duties. The Legislative Auditor's Office also includes reviews of security as part of their fiscal/compliance audits with our agency. Finally, employees are provided periodic training regarding the protection of confidential information and the consequences, both civil and criminal, for violations of confidentiality. We also have a Disclosure Officer from the Internal Revenue Service participate in this training.

In the administration of the Agency's function, various divisions also have access to federal tax information and information in the Maryland Criminal Justice Information System (CJIS). As a result of this access, the agency is audited periodically by the Internal Revenue Service and by CJIS to ensure that we are maintaining our files pursuant to their procedures, that we have limited access to the information, and that only those employees with a job that requires access are, in fact, accessing the information.

To further protect taxpayers from identity theft, over the last several years our office has moved from printing the full social security number on our notices and payroll stubs to printing only the last 4 digits of the social security number, unless the full social security number is required.

The Comptroller's Office has, in the last year, installed encryption software on all our notebook personal computers that are used in the field to prevent access to the information on the personal computer by any unauthorized party in the event of loss or theft. In addition, we are moving to install encryption software on our mainframe computer tape drives so that data on tapes stored offsite could not be accessed by unauthorized parties. In most cases, we use encryption software when we electronically transmit information from our agency to a third party, whether it is the IRS, a bank, or another state. We use specialized software to encrypt e-mail correspondence to taxpayers and for e-mail attachments sent to partners in the Suspicious Filers Exchange Program. All internet applications involving sensitive data use SSL (Secure Socket Layer) encryption and data bases are protected from attempts to access them from the internet.

When a personal computer is designated as surplus property by our agency, the hard drive is "scrubbed" to remove all information on it. When tapes are disposed of by the agency, they are burned.

While we feel that we have a number of controls in place to protect confidential information, we continually work to improve our procedures and controls. For instance, over the next year, we plan to continue to work with our exchange partners to implement encryption software for all remaining data exchanges. In addition, we plan to review the R*STARS procedures to remind State agencies of the controls they need to exercise over the confidential information in the R*STARS reports that are generated and stored in each agency.

Linda L. Tanton
Deputy Comptroller
Comptroller of Maryland
410 260 7806
ltanton@comp.state.md.us

Attachment #1

COMPTROLLER of MARYLAND
*Serving the People*

# CERTIFICATE OF CONFIDENTIALITY FOR EMPLOYEES OF THE COMPTROLLER OF MARYLAND

**Part 1**

I understand that under federal and Maryland state law it is illegal for me:

- To disclose any information from *any* tax return, report, or document filed with *any* division of the Comptroller's Office;
- To willfully and without authorization alter, deface, destroy, remove, or conceal any public records; and
- To willfully and without authorization access *any* part of any computer system in the Comptroller's Office.

I will not examine any return, report, or document filed with the comptroller unless my supervisor and/or superior tell me to do so, and then I will only examine those documents assigned to me.

I will hold any and all information I see in the strictest of confidence. I will not use it against any taxpayer for any personal reason nor will I use it to obtain special treatment or favors from any taxpayer.

I understand that the comptroller has the authority to adopt this certificate of confidentiality to carry out his administrative duties and that I must abide by its provisions during as well as after my employment with the Comptroller's Office.

I understand that if I violate any of these provisions, I will be subject to criminal prosecution and to disciplinary action under the law and the regulations of the state personnel system.

The issue of confidentiality of tax data is addressed in:
Maryland Tax-General Article, §13-201, 202, 203, 204, 205, 206 and 1018
Maryland Criminal Law Article, §7-302 and 8-606
44 *Opinions of the Attorney General* 350 (1959)
Internal Revenue Code, 26 USC 6103, 7213, 7213A and 7431

**Part 2**

Have you had any criminal convictions other than minor traffic violations?

☐ No.

☐ Yes If yes, explain: _____

_____

_____

**Part 3**

Signed this _____ day of _____ , _____

_____ _____

Witness Employee signature

COM/OC-144 Rev. 1/07

Attachment # 2

# WARNING

## BROWSING IN TAXPAYER FILES IS UNLAWFUL

THE BROWSING OF TAXPAYER RECORDS IS PROHIBITED BY COMPTROLLER'S OFFICE POLICY. EMPLOYEES MAY NOT ACCESS THE TAX INFORMATION OF ANY TAXPAYER, INCLUDING THEIR OWN TAX INFORMATION, UNLESS THAT ACCESS IS DIRECTLY RELATED TO THEIR ASSIGNED DUTIES. UNAUTHORIZED ACCESS IS SUBJECT TO SEVERE DISCIPLINARY ACTION UNDER THE STATE PERSONNEL SYSTEM.

IN ADDITION, FEDERAL LAW APPLIES CRIMINAL SANCTIONS FOR THE WILLFUL, UNAUTHORIZED DISCLOSURE OR INSPECTION OF IRS TAX RETURN INFORMATION. THE LAW APPLIES NOT ONLY TO FEDERAL EMPLOYEES BUT ALSO TO EMPLOYEES OF STATE TAX AGENCIES AND THEIR CONTRACTORS HAVING CUSTODY OF FEDERAL TAX INFORMATION. VIOLATORS WILL FACE A PENALTY OF UP TO $1000 AND/OR IMPRISONMENT FOR UP TO ONE YEAR. IN ADDITION, THE TAXPAYER HAS THE RIGHT TO BRING A CIVIL SUIT AGAINST AN EMPLOYEE IN THE FEDERAL DISTRICT COURT FOR AN UNAUTHORIZED DISCLOSURE OR INSPECTION.

TO CONTINUE, PLEASE ENTER YOUR TRANSACTION AT THE TOP OF THE SCREEN

**UNIVERSITY SYSTEM OF MARYLAND**
**Written Testimony**
**Task Force to Study Identity Theft**

**August 22, 2007**

## BACKGROUND AND CONTEXT

The University System of Maryland (USM) is a system of 13 public, four-year and graduate/professional, universities in Maryland. Eleven are degree-granting institutions and two are research centers. In the fall of 2005, the USM institutions had a collective headcount of 92,977 undergraduate students, 3,520 professional students, and 31,928 graduate students. Also, in the fall term of 2005, the USM employed 11,929 faculty, 5,995 teaching assistants, and 15,082 staff. Thus our community consists of approximately 160,000 individuals. These numbers represent largely those living in Maryland, although we have several worldwide programs that involve students and faculty outside of Maryland.

### Data Privacy vs. Data Security

To discuss activities that enhance data protection and reduce the risk of identity theft within the USM, a brief examination of the relationship between "privacy" and "security" is warranted. The terms are often used interchangeably in discussions of data protection, and some say that you can't have the former without the latter. However, there is a distinction between the two frequently complementary, interdependent principles.

For organizations such as colleges and universities, privacy involves the policies, procedures, and other controls that determine which personal information is collected, how it is used, with whom it is shared, and how individuals who are the subject of that information are informed and involved in this process

Information security, on the other hand, includes processes for protecting data from accidental or intentional misuse by people inside or outside the organization. Although information security is by no means strictly a technical problem, its technical aspects (e.g., firewalls, encryption) are important.

### Privacy Legislation and Standards

To a large extent, the USM's efforts to protect information are guided by privacy legislation and related standards that impact higher education.

The Family Educational Rights and Privacy Act of 1974 (FERPA) is the fundamental guidance followed by university administrators regarding the privacy

of student records. Upon its passage, those university officials charged with safeguarding student information privacy began to rethink the nature of how student records were released to the public. In addition to the passage of FERPA, society in general was changing and the need for more stringent personal security became more and more evident. In the early 80s and 90s, there was less concern for safeguarding the social security number. The balance between security and the convenience of having a truly unique identifier fell on the side of convenience. Yet even then, policies were in place regarding access to private information and those policies were stringently enforced. Today, however, with identity theft on everyone's mind, protection of personally identifiable information is critical and the efforts by USM institutions to protect that information are extensive.

Within the last 10 years, all USM institutions have moved away from the public display of SSNs on class lists, rosters, official and unofficial transcripts, and student ID cards. Our library system has always used a bar code number without displaying the SSN. With the advent, subsequent to 1999, of the new Student Information Systems from Oracle/PeopleSoft on most USM campuses, the institutions took advantage of the opportunity to move from using SSNs as the primary key to student records and now use a computer generated number system that is not derived from the student's SSN. Those institutions not using PeopleSoft have also modified their systems to remove SSN as the principal key to the record. Searches for student records are by computer generated ID or simply by a name search, eliminating the need to ask the student to provide the SSN.

The law does require that in certain instances institutions must collect and store a student's Social Security Number. When a student seeks financial aid or is employed by the institution in any way, SSNs must be reported to the federal and state governments as part of the payroll and aid disbursement processes. Additionally, SSNs are required for processing fees related to certain student services as well as for a limited number of business processes. Where the SSN is carried on the record, it is not displayed publicly in any setting and access to those SSN records is very tightly controlled on a need-to-know basis.

FERPA continues to be a major framework for protecting the student's personally identifiable information. Each institution has in place training programs for faculty and staff focused on what information can or cannot be released. The most intensive training is given to staff of the offices where information is routinely sought: Admissions, Registrar and Records, Health Services, and Student Services offices. However, institutions also have programs in place to provide fundamental information to faculty and other staff regarding the basic principles of FERPA. These training programs are often formally conducted in person with knowledgeable staff delivering instruction in departmental meetings; or at faculty orientation programs; or through required web-based learning tools. Some campuses utilize a web-based training program that requires all faculty and staff

to read a set of FERPA instructions and answer a set of test scenarios correctly before they are able to receive access to any student information. Under FERPA guidelines, all institutions publish their policies on what student information is considered public, again under the direction of FERPA interpretations from the federal government.

Also, all of our institutions come under the Gramm-Leach-Bliley Act of 1999 (GLB) for the protection of financial information. Additionally, many of our institutions come under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), since the institutions run health services and/or mental health counseling services.

In addition to the federal laws cited, the credit card industry established the PCI Data Security Standards to provide baseline expectancy for how vendors, or any entity that handles credit card transactions or data, should protect data to ensure it is not stolen or compromised.

These federal laws, industry security standards and the State *Information Technology Security Policy and Standards* inform our approach to IT Security and the protection of personal information. Since the State *Information Technology Security Policy and Standards* was not developed with the special needs of higher education institutions in mind, we established a USM IT Security Taskforce in 2000, consisting of the Security Officers and security personnel from all USM institutions. This group spent more than a year in developing higher education specific guidelines for IT security, based on the State policy and standards. These guidelines (cf. http://www.usmd.edu/usm/adminfinance/itcc/ITSecResource.html) have been vetted with the Maryland Legislative IT auditors and are now the basis of IT legislative audits for our institutions. Additionally, by USM Board of Regents policy, each institution must report to the USM Chief Information Officer annually on the status of implementation of these guidelines. Among the guidelines, and particularly relevant to the issues of this task force, are policies and procedures for protection of nonpublic information; access controls; network security; physical security; and microcomputer/pc/laptop security. A standard for encryption of sensitive information is currently being developed.

Finally, in cooperation with other higher education institutions in Maryland, the USM helps organize an annual Maryland Higher Education IT Security Day, which has been a forum for sharing best practices and discussion of common issues in the field. The issues related to protection of personal information as well as incident response and reporting have been regular topics at these sessions.

## RESPONSES TO QUESTIONS FROM THE TASK FORCE

In its August 6th letter to Chancellor Kirwan, the task force requested information on policies and practices for protecting social security numbers and other personal information. The following are responses to the task force's questions:

1. **How many records containing Social Security numbers and other personal information are maintained? For what purpose is this information collected and used?**

*Collectively, the USM institutions manage more than 2,000,000 records containing social security numbers and other personal information for students, faculty, staff, and affiliates.*

*Social security numbers are collected to comply with federal reporting requirements, including payroll processing and reporting, Department of Labor Statistics, federal student financial aid processing, federal certifications for handling hazardous materials, and a few others. USM institutions do not use social security numbers as a primary key to access student, faculty, staff, and affiliate information.*

2. **What policies govern when and how Social Security numbers are requested from students, prospective students, and university employees?**

*USM employees are required to provide their social security numbers, as mandated by the IRS. Students and prospective students have the option of providing their social security numbers, but are not required to provide this information.*

*However, to participate in federal financial aid programs or avail of certain services, students are required to provide their social security numbers. In these cases, the social security numbers are used for processing purposes, but are not publicly displayed. For example, if students need to submit FAFSA applications for federally funded financial aid or borrow materials from the library.*

*An example institutional policy is the University of Maryland, College Park's (UMCP) Policy on the Collection, Use and Protection of ID Numbers, which is available at: (http://www.oit.umd.edu/units/dataadmin/Policies/Policy_on_Collection_Use_Protection_of_ID_Numbers.pdf).*

3. **What policies and practices govern the personnel who have access to Social Security numbers and other personal information and under what circumstances these individuals are permitted access?**

*Employees are permitted access to social security numbers and personal information only if their job functions require such access, as determined and approved in writing by the department head. The USM institutions have also made significant efforts to remove social security numbers as the primary key for administrative systems, limiting the number of employees with access to this information. In addition, internal controls such as strong password management practices and departmental and role-based security as well as data management councils enable restricting access to sensitive information to only authorized individuals.*

*As examples, UMCP's Policy on Institutional Data Management (cf. http://www.president.umd.edu/policies/vi2200a.html) and Policy on Data Management Structure and Procedures (cf. http://www.president.umd.edu/policies/vi2300a.html) address policies and practices for personnel access to social security numbers and other personal information.*

4. **What procedures and practices ensure that access to Social Security numbers and other personal information is limited to only those personnel who need the information to perform their job duties?**

*As outlined in the response to the previous question, department or unit heads must approve, in writing, the access privileges that are accorded to employees. These access privileges are regularly reviewed and audited, as an additional control to limit access to social security numbers and personal information to only those personnel who need the information to perform their job responsibilities.*

5. **What policies and practices govern how long Social Security numbers and other personal information are kept and how the information is disposed of when no longer needed?**

*In general, retention of source documents is determined by federal audit guidelines and by audit policies of the State Legislative Auditors. When disposed, paper documents containing social security numbers and other personal information are shredded.*

*State-of-the-art security processes are used for protecting electronic data that are retained indefinitely. These data are retained so as to be able to provide student transcripts and other required reports. Electronic media such as disk*

*drives and tape media are typically degaussed and then physically destroyed or made unusable prior to disposal.*

*UMCP's Records Retention and Disposal Schedule, as an example, is available at: http://www.dbs.umd.edu/records_forms/schedule.php.*

**6. How could policies, procedures, and practices be improved to protect Social Security numbers and other personal information and limit or prevent unauthorized disclosure?**

*Potential areas for improvement include:*

- *Increased education for employees and students in policies and practices*
- *New technologies for encrypting data to add another layer of security*
- *Policy to address the classification of data, for example, as public, internal, and confidential*
- *Enhanced assessments of compliance with policy by audit staff (see the Audit and Compliance section below)*
- *Examination of the holistic flow of data. In some instances USM institutions must collect, store, and transmit personal information, such as SSNs, due to the needs of processes downstream in the cycle from the institution.*

## AUDIT AND COMPLIANCE PROCEDURES

As observed in the Background section, there is a distinction between "data privacy" and "data security". Internal Audit is responsible for assessing policies, procedures and their implementation relating to both issues. With regard to data privacy, the work of Information System Audit in the higher education environment to a large extent is guided by privacy legislation that impacts higher education. With regard to security, Information System Audit is responsible for performing reviews to ensure the integrity and security of sensitive data, at rest and in transit.

### Audit activities in the area of Information Security.

At the network level, Internal Audit initially performs network vulnerability assessments. This involves evaluating the controls that are put in place to protect the network perimeter. In this regard, routers and firewall configuration are reviewed for vulnerabilities (flaws). In addition, audit evaluates the existence of security appliances like Intrusion Detection System (IDS) and Intrusion Protection System (IPS).

The periodic network vulnerability assessments have resulted in the introduction of continuing "Self-Audit". Institutions are now required to run vulnerability scans at least quarterly to identify vulnerabilities on their network and submit results to audit to monitor corrective actions taken.

At the server level, network vulnerability scans are run against the servers to identify vulnerabilities that could be exploited by hackers to gain access to data on an institution's servers. Also, host vulnerability scanners are run on the servers themselves to identify vulnerabilities and improper configurations that could allow hackers access.

At the application level, Internal Audit reviews the effectiveness of access controls implemented to prevent unauthorized access to data. Guidance on password polices and associated administration is documented in the USM document: ***Guidelines in Response to the State IT Security Policy*** (cf. http://www.usmd.edu/usm/adminfinance/itcc/ITSecResource.html).

Internal Audit has begun security reviews of databases that store application data from PeopleSoft modules (Human Resource Management System, Financials and Student Information Systems). A secure database reduces the risk of data theft if application security is bypassed and hackers attempt to extract data directly from the database.

**Audit activities in the area of Data Privacy**

Access control reviews are regularly performed by both Internal and Legislative Auditors. These reviews ensure that access privileges assigned to personnel are appropriate for the job functions performed, reducing the risk of unauthorized access to data.

Internal Audit has also performed a Health Insurance Portability and Accountability Act (HIPAA) Security Standard Readiness Review. The purpose of the review was to determine the extent to which the University System of Maryland institutions complied with the security component of HIPAA.

Privacy audits entailing reviews of institutional privacy procedures have been planned for the current audit cycle. These audits will provide an assessment of USM institutions' compliance with federal and state privacy laws and regulations as well as each institution's ability to reduce the risk of identity theft.

Among other factors, the privacy audits will evaluate the controls and risks related to:

- Privacy policy and associated control framework elements
- Compliance with the privacy policy

- Controls for protecting personal information, including collection, usage, retention, and disposal
- Procedures for identifying the types of personal information collected, controlling access to the information and protecting the stored data
- Governance structures related to privacy compliance.
- Institutional compliance monitoring processes
- Incident response plans.
- Education in privacy awareness, data handling, and information security

MICUA

**Maryland Independent College and University Association**
**Tina M. Bjarekull, President**

**Task Force to Study Identify Theft**
**August 22, 2007**

The Maryland Independent College and University Association (MICUA), representing 18 independent institutions of higher education in Maryland, supports efforts to protect personal information about their students, employees, alumni, and other constituents. The theft of personal information and the breach of database security systems have raised concerns across the country. Clearly, these are issues that governments, businesses, and non-profits take seriously and deal with on a daily basis.

MICUA institutions, as well as public senior and two-year colleges and universities, maintain a range of personal records such as: personnel information; academic records; student financial aid and loan information; and medical data. There are numerous State and federal laws that regulate the retention, protection, and distribution of this personal data. In contrast, there are also State and federal laws requiring colleges and universities to release certain personal information to regulatory agencies. For example, Maryland's colleges and universities are required to share specific student unit record data with the Maryland Higher Education Commission (MHEC), and postsecondary educational institutions that participate in federal student aid programs must submit personal information to the Integrated Postsecondary Education Database System, administered by the U.S. Department of Education. Additionally, all students applying for federal financial aid must complete the Free Application for Federal Student Aid (FAFSA), which includes a Social Security number to match the student with information from the U.S. Citizenship and Immigration Services and the Social Security Administration. For the most part, the Federal Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act (HIPPA) regulate how these records are collected, protected, and released.

FERPA applies to all colleges and universities that receive funds under an application program of the U.S. Department of Education, which includes all MICUA member institutions. FERPA provides that an educational agency or institution may not have a policy or practice of disclosing education records, or personally identifiable information from education records, without the prior written consent of a parent or eligible student. FERPA also applies to ID numbers that the college or university assigns to and maintains on any individual who is or has been in attendance as a student. In short, colleges and universities must have written permission from eligible students in order to release any information from a student's education record. In addition, FERPA stipulates that students have the right to inspect and review the student's education

records maintained by the school. The law also states that students have the right to request that a school correct records which they believe to be inaccurate or misleading.

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" (GLB), regulates higher education institutions that act as financial institutions and offer financial products or services to individuals, such as loans, financial or investment advice, or insurance. GLB includes provisions to protect consumers' personal financial information held by financial institutions. GLB gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to "financial institutions," which include not only banks, securities firms, and insurance companies, but also non-traditional "financial institutions" such as colleges and universities. The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information to control the ways that financial institutions deal with the private information of individuals. The Act consists of three sections: The Financial Privacy Rule, which regulates the collection and disclosure of private financial information; the Safeguards Rule, which stipulates that financial institutions must implement security programs to protect such information; and the Pretexting provisions, which prohibit the practice of pretexting (accessing private information using false pretenses). The Act also requires these regulated institutions to give customers written privacy notices that explain their information-sharing practices.

Additionally, some offices or departments at MICUA member institutions take measures to protect personally-identifiable information to comply with HIPAA. HIPAA requires that all units that provide medical services or conduct medical research (such as health centers, counseling centers, medical schools, pharmacy schools, etc.) protect private information by only releasing information with the consent of the patient and with specific provisions for the release of information to insurance companies for payment processing. HIPAA requires institutions to create administrative, physical, and technical safeguards to ensure privacy. Among the requirements, institutions must develop written policies and procedures to track and secure information, develop a classification system to restrict employee access to data, develop procedures to address security breaches, create physical barriers to restrict access to medical records and computer systems, protect computer systems from intrusion through encryption or a closed network, and verify a patient's identity.

MICUA was asked to respond to six questions concerning the policies, procedures, and practices of its member institutions related to the custody, use, disclosure, and distribution of Social Security numbers and other personal information. These questions and answers are provided below:

1. *How many records containing Social Security numbers and other personal information are maintained by member organizations? For what purpose is the information collected and used?*

   MICUA-member institutions collect and maintain Social Security numbers for all faculty, staff, and students at the institution. The MICUA member institutions enroll about 50,000 students annually and employ about 36,000 workers on a full- or part-time basis. Furthermore, the colleges and universities maintain records on hundreds of thousands of



60 West Street, Suite 201 • Annapolis, MD 21401 • Phone 410-269-0306 • Fax 410-269-5905 • www.micua.org

graduates and students who have taken courses on their campuses. In addition, some institutions collect Social Security numbers from prospective students, workforce applicants, human research subjects, medical patients, security officials, and professional drivers.

As an example, Goucher College enrolls about 2,300 students annually and employs 500 workers. At this time, 85,354 records in the College's information system contain Social Security numbers. An institution such as Johns Hopkins University maintains over four million records that contain Social Security numbers. Some of these records are duplicative and the count is complicated by the university/hospital distinction. In short, it is safe to assume that the MICUA member institutions maintain well over five million records with Social Security information.

For faculty and staff, Social Security numbers are used for employment eligibility/verification of citizenship as well as withholding of federal, State, and local taxes. Social Security numbers are also used for faculty and staff benefits, including retirement accounts and insurance products. Some colleges and universities conduct criminal background checks for staff in sensitive positions and collect Social Security numbers for that process. For students, Social Security numbers are required for federal financial aid processing, such as the Federal Pell Grant Program, the Federal Family Education Loan (FFEL) program, the William Ford Direct Loan program, and Veterans benefits. In other cases, the Social Security number is needed to ensure accurate transfer of academic credit. The NCAA collects Social Security numbers from all prospective collegiate student athletes who register with the Clearinghouse. For persons affiliated with an institution (such as medical patients or donors) the collection of Social Security numbers is required for business practices (e.g., insurance claims) or required federal/state reporting (usually for tax purposes).

Additionally, MHEC requires colleges and universities to use a Social Security number as the unique identifier for mandatory reporting on enrollment, degrees, and financial aid. All MICUA member institutions that receive Sellinger grants are required to participate in this data collection effort.

Several MICUA member institutions also participate in the Student Outcome and Achievement Report (SOAR). The Maryland General Assembly passed legislation in 1988 requiring MHEC "to improve information to high schools and local school systems concerning the performance of their graduates at the college level." In response to this mandate, MHEC established SOAR. All public two- and four-year institutions in Maryland and eleven state-aided independent institutions participate in SOAR. Using Social Security numbers, MHEC collects data from participating institutions on the performance of new high school graduates. In addition, information about the students' high school experience is collected from the College Board. This information is matched with the SOAR data collected from participating institutions. The SOAR report is provided to county superintendents and high school principals as an indication of how well their graduates are performing at the college level. The data is used as a tool to help



60 West Street, Suite 201 • Annapolis, MD 21401 • Phone 410-269-0306 • Fax 410-269-5905 • www.micua.org

local educators with the evaluation of high school preparatory programs, curriculum development, and counseling.

2. *What policies and practices govern when and how Social Security numbers are requested from students, prospective students, and employees?*

   Because Social Security numbers are required for financial aid processing, employment verification, and federal and State tax reporting, MICUA member institutions usually collect Social Security numbers at the first contact with the student or staff member. For students, the federal government requires that Social Security numbers be reported for financial aid processing. For staff, the federal and State government requires the use of Social Security numbers for the employment of U.S. Citizens or authorized non-residents. In both cases, students and staff would not be able to enroll in classes or commence employment without reporting a valid Social Security number.

   During the 2005 Legislative Session, the Maryland General Assembly passed legislation restricting the use of Social Security numbers. The law prohibits a person from (1) publicly posting or displaying an individual's Social Security number; (2) printing an individual's Social Security number on a card required to access products or services provided by the person providing the card; (3) requiring an individual to transmit the individual's Social Security number over the Internet unless a secure connection and encryption protection exists; (4) initiating the transmission of an individual's Social Security number over the Internet unless there is a secure connection and encryption protection; (5) requiring an individual to use the individual's Social Security number to access an Internet web site; or (6) unless required by law, printing an individual's Social Security number on any material mailed to the individual, including an individual's Social Security number in material that is electronically transmitted to the individual without a secure connection or encryption protection.

   In compliance with this law, colleges and universities no longer use Social Security numbers as unique identifiers for campus transactions. Most institutions use computer systems to generate unique numbers that serve as the primary identifier. These systems generate numbers that have no real meaning or value off campus. However, as stated earlier, campuses must use Social Security numbers for certain transactions, primarily due to external requirements from State and federal governments and insurance companies.

   Furthermore, all institutions conduct training sessions on the protection and use of personal information. Attached to this testimony are excerpts of the policies adopted by Johns Hopkins University concerning the protection and use of student Social Security numbers, electronic information classification, and FERPA.



60 West Street, Suite 201 • Annapolis, MD 21401 • Phone 410-269-0306 • Fax 410-269-5905 • www.micua.org

3. *What policies and practices govern the personnel who have access to Social Security numbers and other personal information and under what circumstances are these individuals permitted access?*

Release of private information (including Social Security numbers) is governed and restricted through FERPA, and all member institutions have developed policies to comply with that law. Typically, access to computers containing Social Security records is restricted to a few offices, such as human resources, financial aid, and the registrar. Only full-time employees whose job responsibilities require record validation have access to Social Security numbers and other personal information. In accordance with federal law, institutions have developed written policies governing the release of personal information (i.e., information cannot be released by staff without the student's permission or a court order); all staff who have access to personal information are required to attend training sessions on the protection of data.

Colleges and universities use information technology security systems to protect personal information. These security systems are capable of generating unique student identifiers that are used for most campus activities. Access to personal information is limited to staff on a need-to-know basis. For example, individual accounts on systems containing personal information are restricted to the assigned job functions. Only those data elements necessary for the employee to complete job functions are accessible. Department supervisors must provide written documentation to the information technology department regarding the needs of staff members to access Social Security numbers and other personal information. Each employee who has access to personal information must read and sign the institution's policy on the protection and security of personal information as well as FERPA regulations. At some colleges, staff that have access to personal information are required to acknowledge their agreement to operate under FERPA guidelines every time they sign on to the computer system.

As with any secure computer system, colleges assign a login ID and an initial password to authorized staff. This password must be changed periodically. For example, Washington College requires each employee to change his/her password every 30 days, the password must be at least 6 characters, the same password cannot be used again for four cycles, and the password cannot be changed for two weeks. In addition, some computer data systems have the capacity to track users who access files containing personal information and to log the date, time, and information accessed.

4. *What procedures and practices are in place to ensure that access to Social Security numbers and other personal information is limited to only those personnel who need the information to perform their job duties?*

Most colleges have developed computer systems that segregate Social Security numbers from other academic and staff records so that only staff authorized to view the numbers have access. Computer systems are typically designed so that every member of the staff has an individual user name and password with permission set in their account to only access records for to which they are authorized based on their job responsibilities.

Access to paper files is restricted. Files containing personal information are locked in fire-proof cabinets in a secure environment and a secure location. As a further precaution, some institutions have installed computer monitor privacy screens that prevent others from seeing data displayed on monitors unless the viewer is directly aligned with the computer monitor.

In addition, some colleges and universities hire outside security companies to perform information technology security audits. These audits include an internal and external network assessment to identify vulnerabilities to ensure that the college's security policies and procedures are complete and appropriate. These audits are typically conducted every two years.

5. *What policies and practices govern how long Social Security numbers and other personal information are kept and how the information is disposed of when no longer needed?*

Most MICUA-member institutions follow the policies recommended by the American Association of Collegiate Registrars and Admissions Officers on the retention and destruction of personal information. Institutional policy on how and who will destroy documents are varied, but most shred paper documents containing personal information on a given schedule in-house or through an authorized shredding company. Staff records are destroyed in a range from seven to ten years. Some student records are destroyed after a period of time ranging from five to seven years. However, the majority of student transcript records are retained forever. These records are usually maintained electronically or on microfilm and are stored in secured and locked locations. Colleges must retain this data for historical analysis, to generate transcripts, and to allow students to enroll in future classes.

Information technology departments destroy all sensitive electronic data from hard drives, flash drives, floppies, and removable drives by overwriting it several times with carefully selected patterns. For example, College of Notre Dame of Maryland uses the data destruction method defined in the National Industrial Security Program Operating Manual of the U.S. Department of Defense. Files are overwritten with pseudorandom data. When hard drives are discarded, they are damaged beyond use after data has been erased.

6. *How could policies, procedures, and practices be improved to protect Social Security numbers and other personal information and limit or prevent unauthorized disclosure?*

Multiple institutions responded that reducing the reporting requirements to State and federal governments would reduce the need for records containing Social Security numbers because institutions have phased out the use of Social Security numbers as identifiers and on transcripts. Many member institutions recommended using secure technology to protect sensitive data. Some institutions already have or are in the process of establishing a position dedicated to information security. This position helps to

identify and maintain proper policies towards campus-wide data standards for information security and integrity, manipulation, and removal of data from core systems. Additionally, some colleges have conducted security audits.

In general, colleges and universities should continue on the current path of consolidation, education, and awareness. There has been significant progress and considerable investments in personal information security.

As stated earlier, there are numerous federal laws and regulations that govern the collection, retention, and distribution of personal information maintained by colleges and universities. Furthermore, colleges and universities have a moral obligation to their workers, students, alumni, and associations to secure and protect personal information. Over the past several years, the MICUA member institutions have invested millions of dollars in information technology to improve their data collection and retention efforts and to ensure that personal information is secure. Securing personal information is a constant and evolving challenge due to the rapid change in technology and the unsavory efforts of would-be hackers. Those who secure personal information must keep abreast of all of these developments. MICUA and its member institutions are aware of these challenges and are committed to maintaining the security and integrity of the personal information that we collect and store.



60 West Street, Suite 201 • Annapolis, MD 21401 • Phone 410-269-0306 • Fax 410-269-5905 • www.micua.org

**Appendix 1**

# Johns Hopkins University
# Policy on Student Social Security Number Protection and Use

December 8, 2006

## BACKGROUND

In 2003 JHU issued to its faculty and staff specific guidance for the protection and use of the student SSN. This policy statement clarifies and extends that prior guidance. University-wide implementation of this policy, which applies to the entire JHU community, is guided by the following objectives and needs:

1. Broaden awareness about the confidential, protected nature of the student SSN.

2. Reduce reliance on the student SSN for identification purposes.

3. Establish consistent University-wide and divisional student SSN protection and use policies and practices.

4. Increase student confidence surrounding handling of their SSN.

## POLICY

Johns Hopkins University (JHU) is committed to ensuring privacy and proper handling of confidential information it collects and maintains on faculty, staff and students, including the Social Security Number (SSN) which is required for state and federal government reporting purposes. It is the policy of JHU to protect the privacy of the student SSN and to place appropriate limitations on its use throughout admission, financial aid, billing and registration processes — both within and outside of JHU information systems. The collection, use and dissemination of student SSNs or any part thereof for other purposes is strongly discouraged.

This policy outlines acceptable use of the student SSN, limits use to business purposes only and establishes procedures to assure that University employees and students are aware of and comply with the Family Educational Rights and Privacy Act of 1974, the Maryland Social Security Number Privacy Act and other applicable laws and regulations.

1. JHU considers the student SSN or any part thereof to be "personally identifiable information" under the Family Educational Rights and Privacy Act of 1974 (FERPA).

2. No part of a student SSN may be publically displayed or released (e.g., via e-mail to multiple students, student rosters, bulletin boards, etc).

3. The student SSN may be collected as part of the application process and required for registration at JHU. The student SSN is also generally required for certain

government reporting and as part of applying for financial aid, billing and employment.

4. The risk of unauthorized disclosure of the student SSN increases with each additional electronic or paper copy of the SSN. Divisional leadership is responsible for ensuring that the number and scope of physical and electronic repositories of SSN are kept to the minimum necessary.

**GENERAL REQUIREMENTS**

The following requirements apply to paper and electronic records.

1. Authorization. Only individuals with a "need to know" are authorized to access the student SSN. These individuals are to receive appropriate on-line privacy training and sign a confidentiality statement prior to receiving the student SSN.

2. Document Handling and Storage. Documents containing the student SSN are not to be distributed to or viewed by unauthorized individuals. Such documents are to be stored in secured cabinets and locations. In high traffic areas, such documents are not be left on desks or other visible areas.

3. Disposal. The student SSN stored in either documentary or electronic formats are to be destroyed (e.g., shredding papers, wiping electronic files, etc) prior to disposal.

4. Current and Future Records. JHU will insert in all student records in the new information systems (ISIS and HopkinsOne) new primary identifiers. Until those numbers are available it is acceptable to use the last four digits of the student SSN as a secondary identifier.

5. Historical Records. The student SSN is included in archived databases and in imaged documents. Such historical records cannot be altered. All records and files containing student SSN data are to be considered sensitive information and must be handled and stored accordingly.

6. Acceptable Release to Third Parties. JHU may release a student SSN to third parties as allowed by law, when authorization is granted by the individual student, when the Office of the General Counsel has approved the release (e.g. subpoenas) or when the authorized third party is acting as JHU's agent and when appropriate security is guaranteed by the agreement (e.g., National Student Loan Clearinghouse, financial institutions providing student loans or other financial services to students, and student- designated entities receiving a student academic transcript).

**REQUIREMENTS FOR ELECTRONIC DATA**

"SSN Data" include any aggregation or collection of JHU student SSN stored, processed or transmitted in an electronic format. Examples of these include: enterprise databases, small databases such as MS Access, Web pages, e- mail, spreadsheets, and tables or lists in word processing documents.

1. Student SSN Transmission by E-Mail, FTP, Instant Messaging, Etc. SSN Data may not be transmitted (e.g., e-mail, FTP, instant messaging) to parties outside JHU

▶Social Security Number Privacy Act, Sec. 14-3401 of the Maryland Commercial Law Code

## Appendix 2

## Excerpt from Johns Hopkins Information Technology Policies

### 2. ELECTRONIC INFORMATION CLASSIFICATION

Electronic information covered by these Policies falls into one of three classifications below:

1. *Restricted* -- includes *Confidential* and *Internal-use-only*

a. *Confidential.* This includes information required by statutory or common law a high level of protection against unauthorized disclosure, modification, destruction, and use. Confidential information includes, without limitation, the following:

i. Patient medical or billing records and Plan Member records including those covered by the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA)

ii. Student records, including those protected under the Family Educational Rights and Privacy Act (FERPA)

iii. Financial information, including that covered under the Gramm-Leach-Bliley Act (GLBA) and credit card numbers

iv. Employment records, including pay, benefits, personnel evaluations and other staff records

v. Research data involving human subjects that are subject to the Common Rule (Federal Policy for the Protection of Human Subjects, 46 CFR 101 et seq)

vi. Social Security Numbers.

b. *Internal-use-only.* This includes information that requires protection against unauthorized use, disclosure, modification and/or destruction. Internal-use-only information includes, without limitation, the following:

i. Certain sensitive research data, including information related to a forthcoming or pending patent application

ii. Johns Hopkins operations, finances, legal matters, audits, or other business or academic activities of a sensitive nature

iii. Sensitive information related to donors and potential donors

iv. Information security data, including passwords and information about security-related incidents occurring at Johns Hopkins

v. Internal memos, correspondence, and other documents or information whose distribution is limited as intended by the author and/or administrator.

2. *Unrestricted.* This classification covers information that can be disclosed to any person inside or outside Johns Hopkins. Although security mechanisms are not needed to control disclosure and dissemination, they may still be required to protect against unauthorized modification and destruction of information.

Not all IT Resources require the same level of security or protection mechanisms. Even within the categories of Restricted and Unrestricted information, appropriate security can vary. Security controls must be commensurate with the sensitivity and value of the information resources and actual threats to those resources. Members of the Johns Hopkins community should exercise discretion and judgment when determining how to protect information for which they have responsibility, subject to legal or other obligations of Johns Hopkins. Standards and practices are meant to be flexible enough to change with circumstances.

**Appendix 3**

## University Policy on Family Educational Rights and Privacy

The following policy has been adopted and promulgated by The Johns Hopkins University in compliance with the Family Educational Rights and Privacy Act of 1974, as amended:

1. Each year the university will inform students of their rights under the Family Educational Rights and Privacy Act of 1974 (P.L. 93-380, sec. 513), as amended (P.L. 93-568, sec. 2) (FERPA), as well as their rights under regulations promulgated thereto, and relevant university policy.

2. It is the policy of Johns Hopkins University to permit students to inspect and review their education records to the extent permitted by applicable law and regulations.

3. The following exceptions and exclusions shall apply to the general policy permitting inspection and review of education records:

a) Persons will not be permitted to inspect and review their education records maintained by a school or division in which they have not been in attendance;

b) Students will not be permitted to inspect financial records or statements of parents or any information thereof;

c) Students will not be permitted to inspect confidential letters and confidential statements of recommendation which were placed in the education records prior to Jan. 1, 1975, provided that (i) they were solicited with a written assurance of confidentiality, or sent and retained with a documented understanding of confidentiality, and (ii) they were used only for the purposes for which they were specifically intended.

d) Students will not be permitted to inspect confidential letters and confidential statements of recommendation which were placed in the education records of the student after Jan. 1, 1975, respecting admission to an educational institution, respecting an application for employment or respecting the receipt of an honor or honorary recognition, provided that the student has waived the right to inspect and review those letters and statements of recommendation.

e) The university will not disclose documents which do not come within the statutory and regulatory definition of the term "education records" as, for example,

i) Records of instructional, supervisory and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker and are not accessible or revealed to any other individual except as a substitute

ii) Records of a university law enforcement unit which are maintained apart from a student's education record solely for law enforcement purposes and are not disclosed to individuals other than law enforcement officials of the same jurisdiction

iii) Records relating to an individual who is employed by the university which are made and maintained in the normal course of business, relate exclusively to that individual's capacity as an employee and are not available for use for any other purpose though this exclusion does not apply to records relating to a student in attendance at the university, who is employed as a result of his or her status as a student. This means that records of student employees relating to their capacity as an employee can be disclosed

iv) Records which are created or maintained by a physician, psychiatrist, psychologist or other recognized professional or para-professional acting in a professional capacity, which are created, maintained or used only in connection with the provision of treatment to the student and which are not disclosed to anyone other than individuals providing the treatment although they may be personally reviewed by a physician or other appropriate professional of the student's choice

v) Records containing only information relating to a person subsequent to attendance at the university

4. Parents of students and students desiring to inspect and review the education records of the student should address a written request to the registrar of the school which the student attends or has attended. FERPA requires that requests from parents of non-dependent students must be accompanied by a written letter of permission from the student whose record is requested. For dependent students, it is the University policy that requests from parents should be accompanied by a written letter of permission from the student whose record is requested, unless the University decides to release records without consent of the student pursuant to Section 9(i) of this Policy. In the event that the records requested are not in the registrar's custody, the registrar shall direct the request to the appropriate custodian.

5. The university shall attempt to respond to requests for access to records as expeditiously as practicable, and within 45 days of the receipt of the written request. Records may be inspected by students only in the presence of the custodian or other such persons as the custodian designates and in no event shall a student be permitted to remove records from the office where they are maintained. The opportunity to inspect and review education

records will be confined to normal business hours on the days when that office is open.

6. The university reserves the right to decline to make copies of education records when the parent of a student and/or a student lives within a normal commuting distance from the school and when the task of preparing copies presents itself as unduly burdensome or interferes with the normal duties and operations of personnel.

7. Students may obtain copies of education records, other than a transcript, by paying upon delivery a charge of $.50 a page. Copies of transcripts may be secured with payment of any applicable fee. The university reserves the right to decline to furnish a copy of a transcript from another educational institution which is a part of a student's education record unless the student demonstrates that it is otherwise unavailable. All copies of transcripts furnished a student shall bear a conspicuous legend indicating that the copy has been delivered directly to the student.

8. Education records are maintained on each student by the registrar of the school in which the student is or has been enrolled. (School of Health Services academic records are in the Medical Archives of the Johns Hopkins Medical Institutions.) Education records on students also may be maintained by departments within the school as well as in the offices of the appropriate departments. A complete listing of the departments within the school, the location of each department and the location of each dean is in the university's telephone directory and on the University website. Following is a listing of other education records maintained by the university and their locations.

Zanvyl Krieger School of Arts and Sciences/Whiting School of Engineering Homewood Student Accounts, 31 Garland Hall; Student Financial Services, 146 Garland Hall; Student Health and Wellness, Alumni Memorial Residences II; Full- time Arts and Sciences students academic records, 322 Garland Hall; Full-time Engineering students academic records, 126 New Engineering Building; Advanced Academic Programs in Arts and Sciences students academic records, 1717 Mass Ave, Suite 101, Washington, D.C., 20036; Part- time Programs in Engineering and Applied Science students records, Dorsey Center, 6810 Deerpath Road, Suite 200, Elkridge, MD, 21075; Academic records of both schools, Homewood Registrar's Office, 75 Garland Hall, 3400 N. Charles Street, Baltimore, MD, 21218.

School of Professional Studies in Business and Education (formerly School of Continuing Studies) Student account records from summer 1998 to the present, 6740 Alexander Bell Drive, Suite 110, Columbia, MD 21046; student account records for dates prior to summer 1998, Room 4, Shriver Hall, Homewood campus; financial aid, student loan and academic records are located in the offices of Financial Aid and Records and Registration, 6740 Alexander Bell Drive, Suite 110, Columbia, MD 21046.

Bloomberg School of Public Health Student Accounts Office, Suite W1101, Business Office; health records, University Health Service (UHS), 136 Carnegie; Johns Hopkins Hospital; student loan records, Suite B200, Johns Hopkins at Eastern, academic records and financial aid records, Suite E1002, Student Affairs.

School of Medicine Academic Records, Suite 147, Broadway Research Building; Student account records, Office of Financial Affairs/Business Office, Suite 131, Broadway Research Building; financial aid records, Suite 137, Broadway Research Building; health records, University Health Service, 1 Carnegie; student loan records, Suite B200, Johns Hopkins at Eastern.

School of Nursing Student account records, Room 336, 525 N. Wolfe St.; Student Financial Services, Room 127, 525 N. Wolfe St.; admissions records, Office of Admissions and Student Services, Room 113, 525 N. Wolfe St.; academic records, Office of the Registrar, Room 127, 525 N. Wolfe St.; health records, Alumni Memorial Residence, Homewood campus.

SAIS Student account records, Room N310, Business Office; financial aid records, Room N314, Financial Aid Office; placement records, Room N212, Career Services; student loan records, Room N314, Financial Aid Office.

Peabody Student account records, Business Office, ground floor, Leakin Hall; financial aid records, ground floor, Leakin Hall; placement records, 105 Conservatory; health records, Peabody Student Health Services at Maryland General Health Care, 1501 W. Mt. Royal Ave. (active files) and JHU Student Health Clinic at Homewood (archived files for students enrolled prior to July 1, 1994); student loan records, Suite B200, Johns Hopkins at Eastern, and ground floor, Leakin Hall; academic records, Office of the Registrar, Room 233, New Building.

9. It is the policy of the university to refrain from disclosing personally identifiable information from the education records of a student without the prior written consent of the student, except that:

a) The university reserves the right to disclose personally identifiable information without the prior consent of the student to university and school officials, including teachers, who in the opinion of the university are determined to have legitimate educational interests.
i) The term "university and school officials" refers to administrators, staff members of the university, third party contractors, specifically, the National Student Clearinghouse and school(s) in which the student is or has been enrolled.

ii) The term "legitimate education interest" refers to, for example, any action or interest affecting the academic and administrative situation of a student who is the subject of the education record and any action or interest relating to the planning, execution and evaluation of academic and administrative

programs of the university and organizations and institutions with which the university is affiliated or which are utilized by the university.

b) The university may disclose as directory information the following categories of personally identifiable information:
i) The name of a student who is in attendance or who has been in attendance

ii) The local, home and e-mail addresses of a present or former student

iii) The telephone number of a present or former student

iv) The date and place of birth of a present or former student

v) Names of parents and spouse

vi) The major field of study of a present or former student

vii) Participation of a student or former student in officially recognized activities and sports

viii) Dates of attendance

ix) Degrees and awards received and pertinent dates

x) Honors

xi) Photograph

xii) Classification and level of study

A student may refuse to permit the designation as directory information of any or all of the categories of personally identifiable information with respect to that student by delivering a written request to the registrar within the first two weeks of the fall, spring, or summer terms or anytime thereafter.

c) The university may disclose personally identifiable information without the prior consent of the student to officials of another school or school system in which the student seeks or intends to enroll.

d) The university may disclose personally identifiable information without the prior consent of the student to authorized representatives of

i) The U.S. comptroller general

ii) The secretary of the U.S. Department of Education

iii) The attorney general of the United States

iv) State and local educational authorities

v) Third party contractors, specifically, the National Student Clearinghouse

e) To the extent permitted by law, the university may disclose personally identifiable information without the prior consent of the student in connection with financial aid for which a student has applied or which a student has received.

f) The university may disclose personally identifiable information without the prior consent of the student to state or local officials or authorities to whom information may be specifically required to be reported or disclosed pursuant to state statute adopted prior to Nov. 19, 1974.

g) To the extent permitted by law, the university may disclose personally identifiable information without the prior consent of the student to organizations conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating or administering predictive tests, administering student aid programs and improving instruction.

h) The university may disclose personally identifiable information without the prior consent of the student to accrediting organizations in order to enable them to carry out their accrediting functions.

i) The university may disclose personally identifiable information without the prior consent of the student to parents of a dependent student, as defined in section 152 of the Internal Revenue Code of 1986.

j) The university may disclose personally identifiable information without the prior consent of the student to comply with a judicial order or lawfully issued subpoena; however, the university will make a reasonable effort to notify the student of the order or subpoena in advance of the compliance therewith.

k) The university may disclose personally identifiable information without the prior consent of the student in a health or safety emergency, subject to the conditions set forth in applicable law and regulations.

l) The university may disclose to the parent of a student under the age of 21 the student's violation of any federal, state or local law, or of any rule or policy of the university governing the use or possession of alcohol or a controlled substance, where the university determines that the student has committed a disciplinary violation.

m) The university may disclose:

i) to the victim of an alleged perpetrator of a crime of violence or a nonforcible sex offense, the final results of the disciplinary proceeding conducted by the university with respect to that crime or offense;

ii) the final results of a disciplinary proceeding, where the university determines as a result of that disciplinary proceeding that a student alleged to be a perpetrator of a crime of violence or a nonforcible sex offense has committed a violation of university rules or policies with respect to the allegation made against him or her.

For purpose of paragraph 9 (m) (i) and (ii): 1) The term "crime of violence" means arson, assault offenses, burglary, criminal homicide, destruction/damage/vandalism of property, kidnapping/abduction, robbery and forcible sex offenses, as those terms are defined in 29 CFR § 99.39; 2) The term "non-forcible sex offense" means statutory rape or incest; and 3) the term "final results" means a decision or determination made by any entity or individual authorized to resolve disciplinary matters. Disclosure of final results may include name of the student who is the alleged perpetrator, any violation committed and any sanction imposed (including description of disciplinary action, date imposed and the sanction's duration).
10. The university will maintain a record of disclosures of personally identifiable information from the education records of a student, as required by law, and will permit a student to inspect that record.

11. The university will provide a student who believes that information contained in his or her education records is inaccurate or misleading or violates his or her privacy or other rights with an opportunity to seek the correction of the education records.

a) A student may seek to amend an education record by submitting a written request to the registrar explaining the basis for the request. A student whose request is denied may request a hearing before the registrar.

b) The dean's designate will hold a hearing within 14 days of the receipt of a written notice of the hearing's time and place. The hearing will be closed to all except the university's representative(s), student, his or her representative or attorney, and witnesses. The student will be afforded a full opportunity to present evidence relevant to the issue of whether information contained in his or her education records is inaccurate, misleading or violates his or her privacy or other rights.

c) The student will be informed in writing of the university's decision.

d) If, as a result of the hearing, the dean's designate decides that the information is not inaccurate, misleading or otherwise in violation of the privacy or other rights of the student, the student may place in the education record a statement commenting upon the information in the education

records and/or setting forth any reason for disagreeing with the university's decision.

MACC Maryland Association of Community Colleges

# MACC Testimony
# Maryland General Assembly Task Force to Study Identity Theft
# August 22, 2007

Protecting the personal and confidential information of students enrolled at colleges has been a key interest to colleges for many years, primarily related to and in support of FERPA (Family Educational Rights and Privacy Act). In addition to the general culture of student privacy embedded at the Maryland community colleges through compliance with FERPA, the community colleges are quite well versed in the issues of identity theft, addressing it from the perspectives of the technology infrastructure and security, implementing secure procedures and practices, and educating both students and employees on continually assessing and improving their use and handling of confidential and personal information, including SSN (Social Security Number). The following describes policies, procedures, and practices relating to the custody, use, disclosure, and distribution of SSN and other personal information at Maryland community colleges:

1. **How many records containing SSN and other personal information are maintained by member community colleges? For what purpose is this information collected and used?**

   - The actual number of records containing SSN varies from college to college, depending on enrollment size, numbers of employees, and institutional policies and practices regarding data collection and record keeping.

   - Colleges are required to keep a permanent record of every student who ever earned credit at the college. This requirement is also moving toward inclusion of specific non-credit workforce development programs. These records include SSN and other personal information used for identity verification purposes.

   - The community colleges are also employers, and as such, are required to maintain employment records, following state and federal regulations and professional standards.

   - All of the community colleges have either moved away from or are in the process of moving away from using the SSN as the Student ID #. Colleges now create a unique/randomly assigned Student ID # for each student. Under no circumstances do colleges print the SSN on any form of student ID card per SSN Privacy Act.


MARYLAND ASSOCIATION OF COMMUNITY COLLEGES • 60 WEST STREET, SUITE 200 • ANNAPOLIS, MD 21401
Phone: 410-974-8117 • Fax: 410-263-6425 • Web Site: mdacc.org

- The SSN is collected and recorded by the colleges for a variety of purposes including:
    - completing required state and federal reporting,
    - coordinating between state funding agencies,
    - student federal financial aid applications,
    - student 1098-T earned income statements,
    - state collections referrals,
    - student transcripts,
    - student VA benefits,
    - National Clearinghouse data requests,
    - NJCAA intercollegiate athletics eligibility/applications,
    - employment eligibility (I-9 forms),
    - employee payroll and benefits,
    - workers compensation claims, and
    - other required reports and transactions.

2. **What policies and practices govern when and how SSN are requested from students, prospective students, and employees?**

    - There are no standardized policies and practices established for community colleges except for the legislation governing the required retention of some records for designated periods of time with proper disposal upon expiration of that time period.

    - Established internal office or college procedures govern when and how SSN is requested. For example, in a face-to-face transaction, in most colleges students are no longer asked to state their SSN – they are asked for their Student ID #.

    - Offices follow all state and federal regulations and guidelines, as well as standards established by external professional organizations such as AACRAO (Admissions and Registrars), NACUBO (Business Offices), NACADA (Academic Advising).

    - HR offices follow House Bill 56/Senate Bill 280 privacy of SSN

3. **What policies and practices govern the personnel who have access to SSN and other personal information and under what circumstances these individuals are permitted access?**

    - Personnel with a legitimate "need to know" in completing their job duties are granted access to confidential information and only for the purpose of completing their assigned work.

    - FERPA training sessions, which address the confidentiality of all student records including SSN, are provided for all employees and are required at most community

colleges. Employees are required to follow all established policies and procedures, including those protecting the confidentiality of student records and information.

- College computer network systems require employees to change their passwords regularly.
- Enterprise applications are accessed through a secure password-protected intranet.
- Data is stored inside a secure data center – not on PCs or portable storage devices (e.g., flash drive).
- Personnel violating access and usage rules are subject to disciplinary action up to and including termination of employment.

4. **What procedures and practices ensure that access to SSN numbers and other personal information is limited to only those personnel who need the information to perform their job duties?**

   - The need to access SSN and other personal information is defined by the employee's job classification.
   - Paper copy records are kept in secure, locked storage areas, accessible only to the employees in that office area who have a need for the information.
   - Electronic records through the colleges' computer information systems are only available to employees who are provided security levels allowing access to those records. Access is granted according to employee's job assignment.
   - Procedures exist for granting approval of access rights; access rights are granted and relinquished based upon an employee's current status and responsibilities.
   - Many colleges offer identity theft awareness and prevention information to faculty, staff and students.

5. **What policies and practices govern how long SSN and other personal information are kept and how the information is disposed of when no longer needed?**

   - Colleges keep a permanent record of every student who ever earned credit at the college. Some records are on paper and some are electronic and they include SSN. This requirement is also moving toward inclusion of specific non-credit workforce development programs.
   - Colleges' records and retention practices are governed by the need for compliance with institutional policy and state and federal law.

- Colleges comply with COMAR and FERPA regulations and AACRAO guidelines regarding retention and disposal of records.

- Disposal of confidential records varies from college to college. Some colleges incinerate records and some shred records, all according to their own institutional policy/practice.

6. **How could policies, procedures, and practices be improved to protect SSN and other personal information and limit or prevent unauthorized disclosure?**

   - Diligence of each employee at each college to follow internal office policies and practices can help to protect sensitive student/employee information.

   - For students, colleges could consider removing SSN from all student forms and paperwork except the initial application to the college, from which SSN would be extracted and entered into the college's computer information system to be accessible only to those employees with a need to know the SSN.

   - Require transmission of any personal identifiable information to be conducted over secure (https) IP systems.

   - To minimize risk of identity theft, each College could establish an Identity Theft Task Force to examine the elements of its current structure, culture, policies and operations that could create or increase the risk of identity theft. This group could lead the effort to establish an incident response process and post-incident review process.

   - Each College could conduct an annual review of data policies for needed updates and compliance to laws and new threats to address these three areas related to data security:
     - Physical layer (access)
     - Logical layer (anti-virus, firewalls)
     - Administrative layer (people)

   - Records retention policies and procedures could include standard for destruction of records such as shredding standards for paper-based PII documents (1/4 cut, cross-cut, etc), discarding of PC's and servers, and handling of data on remote PC or portable storage device.

   - Educate faculty, staff and students on ways to deter, detect and defend against identity theft.
     - Communicate efforts to prevent identity theft to the entire College community through campus television, flyers, student newspaper, professional development

  - Raise awareness that sensitive data can exist on any electronic device or paper media, not just PCs and file servers.
  - Include a section on identity theft in annual security awareness training.
  - Offer Continuing Education seminars in identity theft awareness and prevention.
  - Educate credit and non-credit students on the importance of knowing and using their Student ID# instead of their SSN for transactions at their college.

- College security could conduct routine/random social engineering audit for 'user error' that could lead to identity theft.
- College could encrypt all backup tapes, drives, laptops and portable storage devices.
- Purchasing office could require that vendor contracts include identity theft clause.

MARYLAND
DEPARTMENT OF
BUDGET & MANAGEMENT

*MARTIN O'MALLEY*
Governor

*ANTHONY BROWN*
Lieutenant Governor

*T. ELOISE FOSTER*
Secretary

September 17, 2007

The Honorable Delores G. Kelley, Co-Chairman
Task Force to Study Identify Theft
302 James Senate Office Building
Annapolis, MD 21401-1991

The Honorable Susan C. Lee, Co-Chairman
Task Force to Study Identity Theft
414 House Office Building
Annapolis, Maryland 21401-1991

Dear Senator Kelley and Delegate Lee:

At the Wednesday, August 22 meeting of the Task Force on Identity Theft, I was asked to get back to the Task Force regarding the role of the Chief of Information Technology in enforcing the Statewide IT Security Policy and Standards and to provide additional information regarding the State's notification policy in the event the security of personal information is breached.

As I explained during the August 22 meeting, the State Information Technology Security Policy is a broad and encompassing policy, but is considered to be the minimum standard for State agencies. The primary focus of the policy is to safeguard against security breaches and attempts to hack or infect State networks. State agencies can and have adopted additional requirements to meet their specific operations, especially if there are laws or federal guidelines that cover their agencies. Each agency has a designated chief information officer and is required to do an annual self assessment to document their compliance with the State IT security policy. In some instances agencies have taken the additional step of contracting an independent third party to audit their IT security. These annual self assessments are reviewed and examined by the Office of Information Technology. The office does not physically audit every agency because the staff and resources are not available. However, the Division of Legislative Audits in the Department of Legislative Services does audit the agencies for IT security compliance -- including the Department of Budget and Management, which was audited last year, and the Governor's office, which is being audited this year.

If an instance occurs where non-public identification information has been released, then State agencies are required to promptly notify the individuals who could potentially be impacted by the inadvertent release of this information.



~Effective Resource Management~
*45 Calvert Street • Annapolis, MD 21401-1907*
*Tel: (410) 260-7041 • Fax: (410) 974-2585 • Toll Free: 1 (800) 705-3493 • TTY Users: call via Maryland Relay*
*http://www.dbm.maryland.gov*

I hope that this information is helpful to the members of the Task Force in its deliberations. Mr. Ellis Kitchen, the State Chief of Information Technology, and I are available to assist you in any recommendations and proposals that the Task Force may be considering. Please do not hesitate to contact me at 410-260-6397 or at bburner@dbm.state.md.us if we can be of further assistance.

Sincerely,

Rebecca F. Burner
Legislative Director
Department of Budget and Management

cc: Mr. Sean Malone, Governor's Legislative Office
Mr. Kevin Hughes, Governor's Legislative Office
Mr. Ellis Kitchen, Statewide Chief of Information Technology, DBM

MICUA

September 24, 2007

The Honorable Delores G. Kelley
Maryland State Senate
James Senate Office Building, Room 302
11 Bladen St., Annapolis, MD 21401

Dear Senator Kelley:

On behalf of the Maryland Independent College and University Association (MICUA), thank you again for the opportunity to appear before the Task Force to Study Identify Theft on August 22, 2007. MICUA strongly supports efforts to protect personal information about their students, employees, alumni and others, and we appreciate the opportunity to work with the Task Force and the State to seek ways to enhance the protection of personal information.

During the hearing a question was raised specific to Johns Hopkins University, referencing an incident that occurred in late December 2007 when computer tapes being sent to a contractor that contained names, addresses and other sensitive, personal information for Johns Hopkins University employees, former employees and retirees were not returned to the institution. The question focused on how Johns Hopkins was able to identify who was possibly impacted by the lost computer tapes. The answer is that the computer tapes that Johns Hopkins believes was inadvertently incinerated were backup computer tapes that were being transferred to microfiche. Johns Hopkins University still had possession of the original computer tapes and was able to contact those individuals that had possibly been impacted.

Should you need further information from MICUA regarding this issue or the work of the Task Force, please do not hesitate to contact me at (410) 269-0306.

Sincerely,

Bret Schreiber

Cc: Karen D. Morgan
John J. Joyce



Maryland Independent College and University Association

60 West Street, Suite 201 ◆ Annapolis, Maryland 21401 ◆ Phone 410 269 0306 ◆ Fax 410 269 5905 ◆ www.micua.org

**Maryland Department of Transportation**
**The Secretary's Office**

**Martin O'Malley**
Governor

**Anthony G. Brown**
Lt. Governor

**John D. Porcari**
Secretary

**Beverley K. Swaim-Staley**
Deputy Secretary

August 23, 2007

Ms. Karen D. Morgan
Maryland General Assembly
Task Force Staff
Legislative Services Building, Room 110
90 State Circle
Annapolis MD 21401-1991

Dear Ms. Morgan:

Thank you for your letter regarding the Task Force to Study Identity Theft and requesting information regarding the Maryland Motor Vehicle Administration's (MVA) handling of social security numbers and other personal information. Mr. Milt Chaffee, Chief Deputy Administrator of the MVA, attended the hearing on August 22, 2007. Nonetheless, I hope the following information will be helpful to you.

The MVA makes every effort to protect confidential information. Personal information maintained by the MVA is closed to the public under the authority of the Driver Privacy Protection Act of 1994 (DPPA). Both federal and state privacy laws prohibit the disclosure of personal information, unless the individual consents to the disclosure in writing or the records are released for authorized purposes provided for in federal and state laws.

All MVA employees are required to sign a security advisory statement prior to having access to confidential information. Furthermore, access to confidential information is tightly controlled and approved for legitimate job-related purposes. All MVA offices containing confidential records are secured via cipher locks and/or security key badge entry.

Pursuant to both federal and state laws, an applicant for a driver's license is required to provide the applicant's social security number or certify that the applicant does not have one. The disclosure of a social security number is voluntary for applicants for an identification card. This information is used to verify the identity of the individuals applying for a Maryland product, access driving records, and other purposes covered in COMAR 11.17.12.03. Currently, there are approximately 6,095,608 MVA records containing social security numbers.

Maryland law requires the MVA to keep a record of each driver's license application received and each driver's license issued. These records are maintained in an automated format, microfilm, microfiche, or hard copies for an indefinite period of time. Documentation requiring disposal, such as duplicate copies of records, are shredded or placed in a locked recycling bin. Although the MVA's policies and procedures currently require the strict handling and destruction of sensitive information, we will continuously evaluate our policies and practices and make improvements.



My telephone number is 410-865-1000
Toll Free Number 1-888-713-1414 TTY Users Call Via MD Relay
7201 Corporate Center Drive, Hanover, Maryland 21076

Thank you again for your letter and interest in MVA's practices regarding sensitive information. If you have any questions, please contact Mr. Chaffee at 410-768-7281 or via email at mchaffee1@mdot.state.md.us, or you may also contact Mr. John T. Kuo, Administrator, MVA, at 410-768-7274 or via email at jkuo@mdot.state.md.us. Mr. Chaffee and Mr. Kuo will be pleased to assist you.

Sincerely,

John D. Porcari
Secretary

cc: Mr. John T. Kuo, Administrator, MVA
Mr. Milt Chaffee, Chief Deputy Administrator, MVA

OFFICE OF THE STATE'S ATTORNEY
FOR
BALTIMORE CITY

208 THE CLARENCE M. MITCHELL, JR. COURTHOUSE
BALTIMORE, MARYLAND 21202

PATRICIA C. JESSAMY
STATE'S ATTORNEY

PHONE:
443-984-2992

November 8, 2007

Senator Delores G. Kelley, Co-Chair
Delegate, Susan C. Lee, Co-Chair
Maryland Identity Theft Task Force
90 State Circle
Annapolis, Maryland 21401

Dear Senator Kelley and Delegate Lee,

According to FBI statistics, identity theft is currently our nation's fastest growing Crime; and in 2006, for the 7th year in a row, identity theft topped the Federal Trade Commission's (FTC) consumer complaints. Additionally, a survey conducted by the FTC in 2003, reported that 27.3 million Americans had been victims of some form of identity theft since 1997.

To address this ever-growing issue, and to ease the burden on identity theft victims in Baltimore City, the Office of the State's Attorney for Baltimore City (BCSAO) combined resources in 2003 with the Maryland Motor Vehicle Administration (MVA) and the Baltimore City Police Department (BPD), to begin an identity theft initiative. The main goals of the initiative are to assist victims, primarily in District Court, rectify their criminal and/or driving record when they have been wrongfully implicated in a matter due to another's use of their name, and to aid in the prosecution of persons charged in Baltimore City with crimes associated with identity theft.

The initiative is mainly comprised of three members, one BCSAO funded investigator, one MVA funded investigator, and one BPD funded officer. All work jointly to respond to referrals from identity theft victims, the courts, law enforcement, Judges, and other governmental agencies. Their duties often include, but are not limited to, investigating allegations of identity theft, providing a mechanism for protecting professional licenses, housing, employment, educational opportunities, etc., for those that have been compromised by an identity thief, and preparing documents and testimony to be used during court proceedings.

Statistics of actions directly taken by the BCSAO member of the identify theft initiative from 2003 - 2006 are as follows:

| Action | Total |
|---|---|
| Appointments with victims | 2,191 |
| Identity theft related arrests reviewed | 427 |
| Criminal charges filed with the commissioner | 127 |
| Letters written to employers, housing, other agency, etc | 897 |
| Criminal record expungement requests made | 247 |

The members of the initiative have received the Governor's Victim's Assistance Award for the past 2 years in recognition of outstanding service to the victims of identity theft. Their efforts have resulted in numerous individuals being able to gain, restore, or continue their employment, housing, and education. Despite these accomplishments, legal barriers to fully assist identity theft victims still remain. Our recommendations to eliminate some of those barriers are enclosed with this letter.

Victims lose precious time and financial resources while attempting to rectify the damage caused by the identity theft. Due to the nature of the crime, perpetrators are difficult to locate and/or bring to justice. We need stronger laws to not only aid in the prosecution of identity thieves and address the root causes of identity theft, but to also provide law enforcement with the tools they need to assist victims in restoring their good names. I am willing to support any action taken by this task force that moves in that direction, and am available to assist in any way I can.

Sincerely,

Patricia C. Jessamy

Patricia C. Jessamy
State's Attorney for Baltimore City

Enclosure

# The Office of the State's Attorney for Baltimore City
# Identity Theft Legislative Suggestions

**1. Expand CR § 9-502 Entitled: "False Statement- to law enforcement officer when under arrest" to include statements made during the investigation of a traffic offense.**

The majority of identity theft cases originate during a traffic stop when the driver falsely gives the name and DOB of a friend or family member. §9-501 includes only those statements prior to the commencement of an investigation, and §9-502 includes statements only after arrest. This narrow change would significantly augment charging tools and fill the legislative gap between §9-501 and §9-502 by addressing the time period between the beginning of the investigation and after or in the absence of an arrest.

**2. Expand the statute of limitations period to 5 years from the date of offense, or date of discovery, for certain identity theft misdemeanor offenses.**

This should include but is not limited to:

- CR § 9-502 Currently entitled: "False statement to law enforcement officer- when under arrest" (Limitations period currently 1 year)
- TR § 16-301 Entitled: "Unlawful application for or use of license" (Limitations period can be either 1 or 2 years depending upon the offense)
- Any traffic offense that is related to an identity theft offense.
    - CR § 8-301, the primary identity theft statute in MD, has an unlimited limitations period. Similarly, related offenses should have an expanded limitations period to allow for delayed discovery which commonly occurs in identity theft crimes. (For example, fraudulently opened credit accounts may not be discovered until several years later.)

**3. Expand CR § 7-302 to prohibit copying or possessing computer data obtained by unauthorized access to a computer database.**

Identity thieves often hack into computer databases and steal vast amounts of identity related data. § 7-302 currently prohibits altering, damaging, and unauthorized access to a computer database, but does not prohibit copying or possessing the data.

STATE OF MARYLAND

MARTIN O'MALLEY
GOVERNOR

OFFICE OF THE PUBLIC DEFENDER
ADMINISTRATION
WILLIAM DONALD SCHAEFER TOWER
6 SAINT PAUL STREET, SUITE 1400
BALTIMORE, MARYLAND 21202
*Ph. (410) 767-8460 Fax (410) 333-8496*
*Toll Free: 1 (877) 430-5187*

NANCY S. FORSTER
PUBLIC DEFENDER

MICHAEL R. MORRISSETTE
DEPUTY PUBLIC DEFENDER

November 15, 2007

**Via Facsimile: (410) 946-5395**

Karen D. Morgan
Principal Analyst
Maryland General Assembly
Legislative Services Building, Room 110
90 State Circle
Annapolis, MD 21401-1991

Dear Ms. Morgan:

Thank you for the opportunity to provide input to the Task Force to Study Identity Theft. The responses to your questions follow. Preliminarily, please note that identity theft is of great concern to the Office of the Public Defender. OPD clients may be charged with crimes they did not commit because they are the victims of identity theft. Additionally, OPD clients may be accused of committing identity theft. This causes difficulty at the intake stage and, of course, may create a conflict within our offices, requiring that cases be sent to panel attorneys.

Please also note that several of the submitted questions involve possible future legislation. It is difficult, if not impossible, to comment on legislation without the actual language of the bill. Accordingly, the following comments are an attempt to give the task force an idea of the legal issues presented. A representative of the Public Defender is available to assist in drafting and commenting on all drafts of proposed legislation.

***1. Has the OPD had to allocate any specific resources to the defense of persons charged with identity crimes?***

As noted above, the crime of identity theft often causes conflicts within the OPD. In addition, OPD attorneys report that investigating allegations of identity theft are difficult and expensive because, *inter alia*, discovery is

often incomplete and the alleged victim's credit reports are inaccessible.

More problematic are cases where the defendant is charged with a crime because his or her identity was stolen and used by another. It is reported that these cases require extensive investigations, subpoenas, and trial preparation.

***2. What are your views about allowing an identity theft victim to submit an affidavit relating to the use of his/her credit or account information without consent, rather than making a personal court appearance to provide the same testimony?***

The Office of the Public Defender adamantly opposes any procedure which allows the victim of identify theft to submit an affidavit in lieu of sworn testimony for the following reasons:

Primarily, the issue presented by this question involves the constitutional right of a criminal defendant to confront witnesses and evidence presented against him or her in a court of law. That is, the Sixth Amendment to the Constitution of the United States and Article 21 of the Maryland Declaration of Rights implements the right of the accused to face his or her accuser(s) in court. Generally, this excludes statements from admission in court if the witness does not appear and the statements he would give are not subject to cross-examination by the defendant.

The U. S. Supreme Court wrote a landmark opinion in the case of *Crawford v. Washington*, 541 US 36 (2004), reaffirming and reinforcing the supremacy of the confrontation clause in criminal prosecutions. The Court wrote "Our cases have thus remained faithful to the Framers' understanding: Testimonial statements of witnesses absent from trial have been admitted only where the declarant is unavailable, and only where the defendant has had a prior opportunity to cross-examine." *Crawford*, 541 U.S. at 59, 124 S.Ct. at 1369. The Court continued, "the Clause's ultimate goal is to ensure reliability of evidence... It commands...that reliability be assessed in a particular manner: by testing in the crucible of cross-examination." *Id.* at 61, 124 S.Ct. at 1370. Accordingly,

permitting the admission of evidence not subject to cross-examination is inconsistent with the requirements of the confrontation clause.

Additionally, aside from violating constitutional protections, there are also possible unintended consequences to permitting the use of an affidavit. There is often a "race to the commissioner" for persons who wish to file charges to retaliate against someone who they believe has wronged them, and not necessarily in a criminal sense. Unfortunately, some people are all too willing to use the criminal justice process to harass, annoy, and embarrass others. Often, these charges are dismissed because the complainant fails to appear for trial. They realize that filing charges is quite easy and painless. However, swearing in a court of law to tell the truth and facing questioning, especially cross-examination, exposes a person to being seen as incredible and possibly face perjury charges.

"Trial by affidavit" suffers from the flaw that an alleged victim might never have to appear for trial, compounding the possibility of abuse of process. Further, it could certainly result in scenarios where a ringleader of an ongoing fraud, sensing either that he might be charged or wishing to cut his cohorts out of the profits, goes to a commissioner or notary and swears-out an affidavit painting himself as a victim and disavowing any knowledge. Again, he would never have to appear for trial, but could cause great harm to others while using and occupying the process to avoid detection himself. Thus, permitting use of an affidavit could unwittingly give scam artists a new tool to prolong their schemes and avoid prosecution.

Moreover, allegations of identity theft often hinge on the credibility of the accuser. Personal appearance, testimony, and cross-examination are crucial to any credibility determination. "Trial by affidavit" makes it impossible for the trier of fact to make this crucial determination.

***3. What are your views about a change in Maryland laws to allow police to seize the items that are subject of an identity fraud investigation and to allow for forfeiture of those items after a defendant has been found guilty?***

Absent specific language, commenting on a possible forfeiture law is particularly difficult. Such laws must be narrowly written to ensure that "innocent property" is not subject to forfeiture. Furthermore, the issues of burdens of proof, presumptions, and exclusions must be precisely established within the language of such a law.

For instance, consider a case where a young man is engaged in identity fraud in his grandparents' basement. The grandparents are unaware of this activity. They keep a large sum of cash in a safe near where their grandson makes "false identity" documents, in violation of the identity theft laws. Imprecise language may result in a presumption that the cash is to be forfeited despite the fact that the grandparents did not know about the criminal activity and that the defendant actually had no access to the money in the safe.

***4. Is additional legislation needed to assure a fair defense to defendants that have been charged with identity fraud?***

OPD attorneys raised the issue of credit repair. Is the Task Force considering legislation to make it easier to repair falsely damaged credit?

In order to determine injury to an alleged victim, defense counsel should have access to the alleged victim's credit report.

***5. Has your office encountered any issues or concerns that make it harder (or easier) to develop a defense for a person who has been charged with identity fraud?***

Several jurisdictions report that it is very difficult to get proper discovery from the State.

It is always more difficult to defend a client when his or her right to due process or right to a fair trial is

compromised. Permitting "trial by affidavit" would severely compromise these constitutional protections and make defending a client much more difficult.

I appreciate the opportunity to provide the views of the Office of the Public Defender and would welcome working with the Task Force in the future.

Sincerely,

Nancy S. Forster
Public Defender

NSF/jps

cc: Michael R. Morrissette
Laurel Albin

# Maryland Criminal Defense Attorneys' Association



November 15, 2007

Karen Morgan
Task Force to Study Identity Theft
Department of Legislative Services
Room 209
90 State Circle
Annapolis, MD 21401

Dear Ms. Morgan,

Thank you for the opportunity to submit responses to the questions posed by the Task Force. I note that there is not a representative from the criminal defense bar on the Task Force. The Maryland Criminal Defense Attorneys Association is interested in issues relating to the defense and prosecution of identity theft and I would be happy to have the Association play an increased role in the work of the Task Force either by providing live testimony or nominating an association member to become a member of the Task Force.

1. *What are your views about allowing an identity theft victim to submit an affidavit about the use of his/her credit or account information without consent, rather than making a personal court appearance to provide the same testimony?*

The Maryland Criminal Defense Attorneys Association strongly opposes allowing an alleged identity theft victim to submit an affidavit in lieu of appearing in court and being subjected to cross-examination. The right of confrontation afforded to criminal defendants under both the Constitution of the United States and the Maryland Declaration of Rights is central to ensuring a fair trial for those accused of a crime.

2. *What are your views about allowing police to seize the items that are the subject of an identity fraud investigation and to allow forfeiture of those items after a defendant has been found guilty?*

In order to preserve due process, forfeiture laws must be narrowly and precisely drawn. Absent the ability to view the specific language of a proposed forfeiture statute, it is impossible to comment on any forfeiture procedure.

3. *Is additional legislation needed to assure a fair defense to defendants that have been charged with identity fraud?*

Identity theft cases are complex and require a significant amount of preparation and careful examination of documents in both the pretrial and pre-sentencing stages of the prosecution. Legislation that addresses specific discovery obligations of the prosecution in identity theft prosecutions, including but not limited to access to the alleged victim's credit reports would be useful in ensuring a fair defense to defendants.

4. *Have defense attorneys encountered any issues or concerns that make it harder (or easier) to develop a defense for a person who has been charged with identity fraud?*

As noted in the response to question number 3, prompt and full access to discovery would make it easier to develop a defense for a person who has been charged with identity theft.

Sincerely,

Maureen Essex
President, Maryland Criminal
Defense Attorneys Association

720 Light Street • Baltimore, MD 21230 • Phone: 410-752-3318
• Fax: 410-752-8295 • mcdaa@assnhqtrs.com • www.mcdaa.org

**Maryland Bankers Association**

To: Senator Delores Kelley, Co-Chair
Delegate Susan Lee, Co-Chair

Cc: Members, Identity Theft Task Force

From: Kathleen Murphy, MBA President and CEO

Date: December 6, 2007

RE: Identity Theft Task Force December 6, 2007 - MBA Position Statement

---

Several issues have been raised during recent Identity Theft Task Force deliberations that deal with changes to Maryland's forfeiture and social security number laws. These are complex issues which merit careful consideration. The banking industry has several specific concerns that we believe are important to share with Task Force members. This document outlines MBA's position on forfeiture and social security laws. Please contact me or Mindy Lehman, MBA's Vice President of Government Affairs, with any questions. Our contact information is: Kathleen Murphy (phone: 443-837-1601 / kmurphy@mdbankers.com) and Mindy Lehman (phone: 443-837-1613 / mlehman@mdbankers.com). Thank you for your consideration of our concerns. We look forward to working with the Task Force on these important issues.

**Forfeiture**

The Maryland Bankers Association has a process for considering proposed legislation which includes review by members of its Government Relations Council. The Association has not had the opportunity to take an official position on the identity theft forfeiture issue because the issue has come up very quickly. As members of the MBA, Bank of America and Provident Bank believe it is critical that the industry have the opportunity and time to review this issue.

With that said, the MBA agrees that individuals should not benefit from proceeds derived from identity theft and is therefore not necessarily opposed to amending Maryland's *existing* seizure and forfeiture law to encompass identity theft. We are aware of one state, Tennessee, which has taken this approach. Tennessee added identity theft to the list of crimes which could trigger forfeiture and provided that the proceeds from a sale, after payment of the costs and distribution to lien holders and other persons with an interest in the property, go to the victim rather than the State. In a similar fashion, the current Maryland law could be amended to allow for forfeiture of property attained through identity theft. We also believe the change in Maryland law in this area could include an allowance for the distribution of *net* proceeds to compensate victims if they can document losses associated with repairing their stolen identity and to others, such as banks and credit card companies, which can demonstrate losses associated with deposit account and credit card fraud resulting from the identity theft.

The MBA is strongly opposed to the creation of a *new* seizure/forfeiture law.

**Social Security Numbers**

Maryland currently has an extensive social security number law in effect. This legislation was based on California law and represents the hard work of many interest groups including industry and consumer protection representatives. If there are specific provisions which consumer advocates believe should be added to Maryland's existing law, they should bring them forth for discussion. However, identity theft, according to a recent study, is decreasing as more states enact laws to address the issue and businesses, as well as the public sector, take steps to protect everyone's identity. The banking industry, and I believe the business sector in general, feel that changes to current law (House Bill 56) are not necessary.

Current Maryland SSNs Use and Data Security Law Address Identity Theft Concerns

House Bill 56 was enacted by the Maryland General Assembly in 2005 and became effective on January 1, 2006. This issue was first given serious consideration by the General Assembly in 2004 and legislation was passed in that year, but was vetoed by Governor Erhlich. After the veto, interested parties met repeatedly with the result that House Bill 56 passed the General Assembly in 2005 with little or no opposition. While there were groups at the time which wished the legislation had gone further, there were also groups which thought it went too far. However, everyone supported the final version of House Bill 56. The bill passed both the House and the Senate unanimously. No floor amendments were offered in either chamber. This bill was carefully crafted to provide necessary protections for individuals without unnecessarily restricting secure business activities that require the use of a social security number.

Specifically Maryland (2005) Md. Code Ann., Com. Law § 14- 3301 et seq.4, prohibits any person or entity, except government entities, from:

(1) Publicly displaying or posting an individual's SSN;
(2) Printing an individual's SSN on any card required to receive products or services;
(3) Requiring an individual to transmit his or her SSN over the Internet unless the number is encrypted or the connection is secure;
(4) Initiating the transmission of an individual's SSN unless the connection is secure;
(5) Requiring the use of a SSN to access an Internet Web site unless a password or other security device is used;
(6) Printing an individual's SSN on any material to be mailed to the individual, unless the inclusion of the SSN is required by law;
(7) Electronically transmitting an individual's SSN unless the connection is secure or the SSN is encrypted; and (8) faxing an individual's SSN to that individual.

In short, HB 56 accomplishes what the Consumers Union Model's fact sheet refers to as "meaningful SSN protections." HB 56 also covers what the Consumers Union Model identifies as "what more can be done:"

- prevents (unless required by law) placing SSN's on identification and membership cards
- Posting, displaying, or making SSNs available to the general public
- Using the SSN as a password or access code for goods and services unless it is encrypted
- Inviting input of the SSN on the web for unencrypted transmission.

Maryland data breach legislation passed in 2007 address additional concerns raised by the Consumers Union: specifically requiring all types of companies holding SSNs to safeguard that data.

Differences between Maryland Law and Consumers Union's Position

There are also provisions the Consumers Union recommends that Maryland law, after careful consideration, did not implement.

- Reduce the appearance of SSNs in public records
- Reducing government agency use of SSNs
- Stop most requests for, collection of, and mailing of SSN's by private businesses for purposes beyond credit, taxes, employment, new bank accounts, child support and criminal record checks unless the SSN is required by law
- Restricting the practices of database companies that sell information about individuals including or using SSNs

The first two bullet points are examined as part of the 2007 Identity Theft Task Force's charge. MBA does not have a position on these issues. The third bullet point is not prohibited specifically by law, but from a practical perspective, current law discourages the requests for SSN's in this manner. Legislation is not needed in this area.

**MBA has strong concerns about the fourth bullet point which has the effect of prohibiting the sale of SNNs in a business transaction**. The Minnesota legislation passed in 2005 prohibits the sale of Social Security numbers obtained from individuals in the course of business. It is our understanding that this provision caused extensive problems for the credit bureaus and the banking industry. Credit bureaus "sell" individual social security numbers as a part of transactions that take place when a lender requests an individual's credit report. The SSN is a critical part of this financial information. In addition, mortgage documents include SSNs as a part of the legal paperwork. Under this provision, banks and mortgages would be swept up into this provision when a mortgage is sold into the secondary market. This provision has caused serious complications for the Minnesota law and resulted in two delayed effective dates. Minnesota has extended the delayed effective date until 2008.

186 Duke of Gloucester Street • Annapolis, Maryland 21401
phone: (410) 269-5977 • fax: (410) 269-1874) • www.mdbankers.com

# News

*Data Security*

## Retail Federation Seeks Credit Card Sales Data Storage Changes to Ease ID Theft Risk

Retailers should not be forced to store account information for credit card companies while also facing increased liability for data security breaches involving just such data, the National Retail Federation said in an Oct. 2 letter.

In the letter to the Payment Card Industry Data Security Standards Council, NSF argued that the rules place consumers at "unnecessary risk."

"The bottom line is that it makes more sense for credit card companies to protect their data from thieves by keeping it in a relatively few secure locations than to expect millions of merchants scattered across the nation to lock up their data for them," David Hogan, NRF senior vice president and chief information officer, said in the letter.

Credit card issuing companies such as Visa and MasterCard typically require retailers to store credit card numbers anywhere from one year to 18 months in order to satisfy card company retrieval requests, according to NRF.

**Limited Data Storage Proposed.** Instead, Hogan said that credit card companies and their banks should provide merchants with the option of keeping nothing more than the authorization code provided at the time of sale and a truncated receipt. Neither would contain the full account number, and therefore would be of no value to a potential identity thief, he said.

According to a credit card industry source, retailers may already store truncated account numbers in lieu of the full account number.

The recommendation from NRF comes as retailers face increased pressure to take steps to secure sensitive customer data. The industry has been criticized because of major data security breaches in recent years.

In January, retailer TJX Companies Inc. announced that its computer network that handles customer transactions for some 2,500 retail stores was hacked into, and personal credit, debit, and driver's license information was stolen (6 PVLR 107, 1/22/07). Information on over 46 million credit and debit cards was breached.

Hogan acknowledged that there have been numerous instances of hackers targeting retail computer systems and stealing credit card data in order to commit fraud. He said the retail industry is investing "hundreds of millions" of dollars annually in systems and procedures to better protect credit data. "Much of this spending has gone toward making retailers compliant with the standards put forth by the Payment Card Industry Security Standards Council," he said.

**Companies Subject to Fines.** The Payment Card Industry Data Security Standards (PCI DSS), which were initially developed by MasterCard and Visa and began taking effect June 2005, require merchants and credit card transaction processors to build and maintain a secure computer network, maintain a vulnerability management program, and regularly monitor and test networks. The standard includes requirements for restricting access to data, encrypting sensitive data transmitted over public networks, the use of firewalls, current virus software, and other data security measures.

Covered entities that fail to comply with the standard run the risk of fines and increases in the transaction fees charged by card issuers, and potentially, of losing their business relationship with credit card companies.

Among the largest retailers who process the greatest volume of credit card transactions, 40 percent have been certified as being compliant with PCI DSS. An additional 50 percent have submitted their initial validation or are otherwise on the way to achieving compliance, Hogan said.

Still, he said, customer data will continue to be at risk until the credit card industry decides to limit the amount of information that retailers are required to maintain.

Bob Russo, general manager of the PCI Security Standards Council, said the council will respond to NRF's letter after reviewing the group's request in further detail.

"However, it must be recognized that the payment brands—and not the council—operate the systems underlying the payments process, as well as the compliance programs," Russo said. "Because of this, Mr. Hogan should be directing his concerns to those individual brands."

**State Card Data, Retailer Liability Law.** In the wake of the TJX data breach incident, some states considered taking legislative action to make merchants liable for the costs associated with breaches of credit and debit card information.

Minnesota this year enacted legislation to limit the types of payment card transaction data which may be retained and to set data retention time limits (6 PVLR 848, 5/28/07). Under the legislation, H.F. 1758, banks could file lawsuits to recover from retailers the costs they incur, such as for consumer notification and card replacement, as a result of a breach of card data stored in violation of the law.

Similar retailer liability bills did not make it out of legislatures this year in Connecticut (6 PVLR 920, 6/11/07), Massachusetts (6 PVLR 1167, 7/23/07) and Texas (6 PVLR 878, 6/4/07).

But a merchant credit card data breach liability measure in California, A.B. 779, passed the Legislature Sept. 10 (6 PVLR 1467, 9/17/07). The bill was sent Sept. 18 to Gov. Arnold Schwarzenegger (R). Under state law, Schwarzenegger had until Oct. 14 to act on the legislation. As of press time, he had not taken action on the



PVLR ISSN 1538-3423

bill or indicated whether he intended to sign A.B. 779 into law.

In addition, retailer breach liability bills are still alive during the 2007 legislative sessions in Illinois and New Jersey (6 PVLR 1058, 7/2/07).

A NRF spokesman told BNA Oct. 10 that state laws are unnecessary because the contracts between retailers and the credit card companies already make the merchants liable for data breach costs, such as expenses related to reissuing credit cards.

Meanwhile, TJX Oct. 9 announced that it had revised its proposed settlement of consumer class action litigation filed to offer either a store voucher or cash to consumers who were affected by the hacking breach that exposed their personal and financial information (*see related report in this issue*).

BY ALEXEI ALEXIS

*Full text of the NRF's letter is available at http://op.bna.com/pl.nsf/r?Open=dapn-77tj7z.*

Sunday, August 05, 2007

## New ID Theft Law in Minnesota

To determine how well my state helps protect me from ID theft, I look at what other states have done. On July 31, 2007 the Caveat Emptor blog wrote:

> "Starting tomorrow, a new law takes effect in Minnesota that will prohibit merchants from storing a customer's PIN, CVV security code, or magnetic stripe information for more than 48 hours. In another year, the penalty provisions of the law kick in, which allow a banks to sue merchants for security breaches. The law essentially gives teeth to security standards already put in place by Visa, MasterCard, and American Express."

This Minnesota law helps prevent payment fraud where an ID thief has stolen a customer's credit card information. Retailers can still retain the customer's card number, expiration date, and card name. My impression is that this new law was facilitated by the TJX breach.

There are some good comments by readers on The Consumerist blog about the advantages and disadvantages of this new law. One reader commented:

> "In order to settle with the card companies and handle disputes, retailers have to retain this data [name, card number, and expiration date]. Mastercard allows 12 months for disputes, Visa 18 months, and AmEx 24 months. Your data will be retained for some period, I guarantee it. If it was not retained, then card fraud would increase dramatically and costs would go up even more. The problem is keeping unnecessary data and not controlling properly the usage, retention, and storage. Security requirements (known as the PCI DSS) mandated by Visa, Mastercard, Discover, and AmEx already prohibit storage of the information mandated in this law. Not that MOST merchants are compliant. Maybe this will help. Maybe. What this will do is help the merchant banks, card issuers, and card companies further push liability for breaches to merchants. This is NOT necessarily a good thing, although there is a certain amount that needs to happen. I don't want to debate here the extent that a company should go to to protect personal data. The bar needs to be higher than it already is, but regulation in this area will ultimately only lead to INNEFECTIVE and EXPENSIVE security controls, instead of useful ones."

Another reader commented:

> "For a receipt lookup, a store could easily get away with storing just the last 4 of the card number and expiration date and then doing a match in their database with that and the UPC. Store the cardholder's name too, so in the one-in-a-gajillion chance someone else with the same last 4 and same expiration date bought the exact same item as you, the cashier can just ask you for the name on the card and match it up."

I wonder which other states provide a law similar to this new one in Minnesota.

To me, a law like this is a step in the right direction. A better law would have been to limit retailers to storing only the last 4 digits of the consumer's credit card number. Regardless, this new law is good news since it, a) clarifies who is responsible for what (e.g., the retailer vs. the credit card company; b) specifies what personal data should be retained vs. destroyed and *by when*; and c) provides consumers with greater protection against identity theft.

However, this new legislation is limited in that it seems to focus on retail data breaches. The Privacy Rights Clearinghouse has compiled since 2005 a list of data breaches, which documents both retailer and employer data breaches. Hence, effective legislation needs to focus on both retailer and employer breaches: a ) how long employers can retain unnecessary personal data about former employees, b) the personal data employers are allowed to retain, c) the personal data employers must delete and by when, and d) penalties for violators.

In a prior blog entry, I discussed how IBM updated my 16-year-old personal data; an update approach it probably did for many other former employees, too. What do you think?

**Next entry:** Fun with ID Theft

Posted on Sunday, August 05, 2007 at 04:33 PM in Government | Permalink | Comments (1)
Digg This | Save to del.icio.us

Friday, August 03, 2007

## CHAPTER 108–H.F.No. 1758

*An act relating to commerce; regulating access devices; establishing liability for security breaches; providing enforcement powers; proposing coding for new law in Minnesota Statutes, chapter 325E.*

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. **[325E.64] ACCESS DEVICES; BREACH OF SECURITY.**

Subdivision 1. **Definitions.** (a) For purposes of this section, the terms defined in this subdivision have the meanings given them.

(b) "Access device" means a card issued by a financial institution that contains a magnetic stripe, microprocessor chip, or other means for storage of information which includes, but is not limited to, a credit card, debit card, or stored value card.

(c) "Breach of the security of the system" has the meaning given in section 325E.61, subdivision 1, paragraph (d).

(d) "Card security code" means the three-digit or four-digit value printed on an access device or contained in the microprocessor chip or magnetic stripe of an access device which is used to validate access device information during the authorization process.

(e) "Financial institution" means any office of a bank, bank and trust, trust company with banking powers, savings bank, industrial loan company, savings association, credit union, or regulated lender.

(f) "Microprocessor chip data" means the data contained in the microprocessor chip of an access device.

(g) "Magnetic stripe data" means the data contained in the magnetic stripe of an access device.

(h) "PIN" means a personal identification code that identifies the cardholder.

(i) "PIN verification code number" means the data used to verify cardholder identity when a PIN is used in a transaction.

(j) "Service provider" means a person or entity that stores, processes, or transmits access device data on behalf of another person or entity.

Subd. 2. **Security or identification information; retention prohibited.** No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of

the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

Subd. 3. **Liability.** Whenever there is a breach of the security of the system of a person or entity that has violated this section, or that person's or entity's service provider, that person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders, including but not limited to, any cost incurred in connection with:

(1) the cancellation or reissuance of any access device affected by the breach;

(2) the closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts;

(3) the opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach;

(4) any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and

(5) the notification of cardholders affected by the breach.

The financial institution is also entitled to recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity that has violated this section. Costs do not include any amounts recovered from a credit card company by a financial institution. The remedies under this subdivision are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.

**EFFECTIVE DATES; APPLICATION.** Subdivisions 1 and 2 are effective August 1, 2007. Subdivision 3 is effective August 1, 2008, and applies to breaches of the security of a system occurring on or after that date.

Presented to the governor May 18, 2007

Signed by the governor May 21, 2007, 2:58 p.m.

DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value



DigitalTransactionsNews

## Retailers Challenge the Networks' Card-Data Storage Requirements

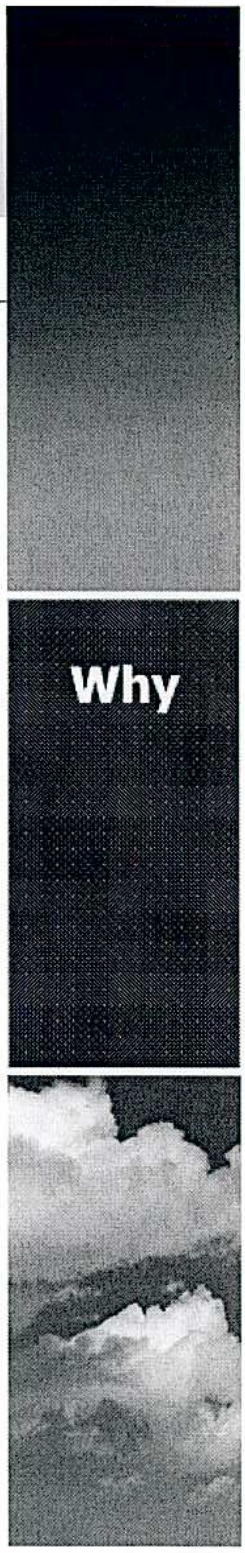
(October 4, 2007) A leading retailer trade group on Thursday called for the payment card networks to stop forcing merchants to store credit card numbers, in effect challenging banks and the networks to take more responsibility for preventing data thefts.

In a letter to the PCI Security Standards Council, an organization the networks created last year to oversee and update the Payment Card Industry data-security standard, or PCI, National Retail Federation senior vice president and chief information officer David Hogan says the networks' requirement that merchants store card numbers for possible retrieval long after a card transaction creates undue fraud risk. Merchants are then required to reduce that risk by adhering to PCI, according to the NRF. Depending on the merchant's size, computer systems, and point-of-sale hardware and software, PCI compliance can be a multimillion dollar expense. PCI contains a dozen main mandates and scores of dependent requirements ranging from data encryption to scans, tests, firewalls, passwords, and anti-virus programs as well as data storage.

While noting that retailers invest "hundreds of millions" of dollars annually to improve credit card data security, Hogan also says in the letter PCI compliance alone won't be enough to protect consumers. A better solution, according to Hogan, would be to permit retailers to store only an authorization code generated at the time of the sale, and a truncated receipt. Those items would suffice for settling disputed sales would remove retailers from the crosshairs of computer hackers looking for card data they can use fraudulently, according to the NRF.

"With this letter, we are officially putting the credit card industry on notice," says Hogan in an NRF news release. "Instead of making the industry jump through hoops to create an impenetrable fortress, retailers want to eliminate the incentive for hackers to break into their systems in the first place."

Hogan addressed his letter to PCI Council general manager Robert M. Russo Sr., who wasn't available for an interview. In a statement, the Council punted to the networks. "The Council will respond to the letter in kind after reviewing the request in further detail," the statement says. "However, it must be recognized that the payment



brands—and not the Council—operate the systems underlying the payments process, as well as the compliance programs. Because of this, Mr. Hogan should be directing his concerns to those individual brands." The statement goes on to say that the Council welcomes input from the NRF, which it notes is a registered participating organization.

A spokesperson for Visa USA, the largest card network, said Visa won't comment on the letter but notes that Visa on Aug. 27 issued a notice about what's permitted and not permitted in storing card data.

According to the NRF and sources familiar with card security, the bank card networks require merchants to store 16-digit account numbers, names, and expiration dates for possible retrieval, including chargeback resolution, for as long as 18 months after a card sale. They do not permit the storage of full magnetic-stripe data, including PIN blocks (encrypted debit card personal identification numbers) and the three-digit validation codes printed on the back of bank cards and used for further security in card-not-present sales. The issue of payment-card data storage has been in the headlines almost constantly for the past two years because of data breaches that resulted in thefts of millions of payment card numbers and other personal financial data. The biggest breach was the intrusion into TJX Cos. Inc.'s computer system that compromised nearly 46 million cards (Digital Transactions News, Sept. 24).

Speaking to Digital Transactions News, Hogan says "PCI wouldn't go away," but that the NRF's proposal is a simpler solution that would make retailers a smaller target for hackers while easing the financial burden of PCI compliance. "The path we have been going down, PCI mandates, 225-plus sub-requirements, is not the path to go down," he says. He adds that the NRF estimates all merchants have spent more than $1 billion over the past three years on PCI compliance, an expense that will be ongoing because of required periodic system scans and audits. All that effort won't deter hackers if they know a retailer may be storing thousands or millions of card numbers, according to Hogan. "We build a firewall, and they come in with a taller ladder," he says.

The NRF's proposal seemingly wouldn't correct the problem posed by some older POS software systems, which automatically record and store magnetic-stripe data, one of the biggest security weaknesses PCI supporters are trying to correct. But Hogan says that with most large retailers having already achieved or being close to full PCI compliance, those problems primarily affect smaller merchants usually ignored by hackers.

The NRF's letter partially confirmed some analysts' claims that PCI places too much of the data-security burden on merchants. "Strategically [the letter] is a brilliant move, and long overdue," says Avivah Litan, a vice president at Stamford, Conn.-based technology research firm Gartner Inc. who has advocated that banks, processors, and the card networks use other methods, such as one-time transaction identifiers, to secure data.

Adil Moussa, a payments analyst at Boston-based Aite Group LLC,

said in a statement that PCI compliance is "very hard on merchants financially," and that the NRF's proposal "make sense." It needs to be expanded, however, he said. "Storing the authorization number is not a viable solution as those six-digit numbers can be easily recycled and a merchant might have the same authorization number twice," Moussa said. "It makes more sense to use a unique transaction code to identify the transaction and keep that record for ulterior processing of chargebacks if they happen. After going the route of enforcing PCI, I feel it will be difficult for [card] associations to change the course, but it might be something to consider."

---

Consumers Union

To: State Legislators and Activists Interested in Reducing Identity Theft.
From: Gail Hillebrand, Financial Services Campaign Manager, Consumers Union, 415-431-6747, ghillebrand@consumer.org
Date: August 6, 2007
Re: Social Security Number Protection Legislation for States

## SUMMARY

- Reducing the collection, printing, mailing, and display of Social Security numbers (SSNs) is a key element in reducing identity theft.

- Companies put individuals at heightened risk of identity theft when they ask for SSNs they do not need, places the SSN on identification cards and cards used to access goods or services, print the SSN on documents such as pay stubs, mail documents containing the SSN, or require individuals to transmit an SSN over the Internet.

- A thief who gets a consumer's name and SSN can open new accounts unless the consumer has placed a security freeze to bar access to his or her credit reporting files. The Social Security number has been called the "magic key" for identity thieves, by George Washington University law school professor Daniel Solove. He also said: "Anyone can easily find it [the Social Security number] out...It's used everywhere, and it's really hard to change if it falls in the wrong hands. How could you come up with a worse system?"[1]

- It is time for a change in the use of SSNs. Part of that change is reducing the private collection, display, and mailing of SSNs.

The SSN has evolved beyond its intended purpose to become a near-universal identifier used by private and public sector entities.[2] The widespread use of the SSN has made it a valuable target for identity thieves. According to a U.S. Government Accountability Office report released June 2007, "SSNs are a key piece of information used to create false identities for financial misuse or to assume another individual's identity."[3] A Federal Trade Commission survey from 2003 found that approximately 10 million Americans were victims of some form of ID theft within the prior year.[4] Consumers Union estimates that this is 27,000 new U.S. victims of identity theft every day.[5] Consumers who experienced new account ID theft in 2006 spent an average of 40 hours resolving the problem.[6] Identity theft costs U.S. businesses and consumers about $50 billion a year.[7]

## WHAT HAS ALREADY BEEN DONE?

States across the country have enacted laws to restrict the printing and display of SSNs on identification cards, the mailing of SSNs, and requirements to send SSNs on the Internet. Two states have gone further, and made it illegal for a business to require an SSN as a condition of the purchase or lease of goods or services.

Many states have enacted laws to restrict the printing on cards, mailing, display and Internet use of SSNs. For example, California enacted legislation in 2001 that generally prohibited businesses from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs, mailing documents that display SSNs before the document is opened, printing SSNs on cards necessary for accessing products or services, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.[8] Twenty one states have passed laws similar to California's—Arizona, Arkansas, Colorado, Connecticut, Georgia, Hawaii, Illinois, Maryland, Michigan, Minnesota, Missouri, New Jersey, New Mexico, New York, North Carolina, Oklahoma, Pennsylvania, Rhode Island, Texas, Utah, and Virginia.[9] Kansas and New Mexico have gone further and restricted the collection of SSNs.[10]

The following states have passed these meaningful SSN protections:[11]

- States that restrict the printing of SSNs on ID cards required to access products or services:
    - Arizona
    - Arkansas
    - California
    - Colorado
    - Connecticut
    - Hawaii
    - Illinois
    - Michigan*
    - Minnesota
    - New Jersey
    - New York
    - North Carolina
    - Pennsylvania
    - Rhode Island
    - Texas
    - Vermont
    - Virginia

- States that restrict intentionally communicating SSNs to the public and/or intentional public posting and display:
    - Arizona
    - Arkansas
    - California
    - Colorado
    - Connecticut
    - Georgia
    - Missouri
    - New Jersey†
    - New Mexico
    - New York
    - North Carolina
    - Pennsylvania

* The Michigan prohibition applies to the printing of all or more than 4 sequential digits of an SSN on any ID badge or card, membership card, or permit or license. The statute does not refer specifically to cards required to access products or services, but these should be covered as membership cards.

† The New Jersey prohibition applies regardless of whether the posting/display is intentional.

- Hawaii
- Illinois
- Michigan
- Minnesota
- Rhode Island
- Texas
- Vermont
- Virginia

- States restrict mailing of SSNs within the mailing envelope:[‡]
  - Arizona
  - California
  - Colorado
  - Hawaii
  - Illinois
  - Michigan
  - Minnesota
  - New Jersey
  - New Mexico
  - New York
  - North Carolina
  - Pennsylvania
  - Rhode Island
  - Texas
  - Vermont

## What More Can Be Done?

**The remaining states can act to get the SSN out of the wallet, out of the mailbox, off the Internet, and to stop the solicitation of SSNs when they are not required by law or required for certain specific purposes.** States can start to clean up the SSN mess by following the 17 states that restrict the printing of the SSN on identification cards, the 20 states that restrict the intentional communicating/ public posting/ display of SSNs, and the 15 states that restrict the mailing of documents containing an SSN. States can also enact legislation prohibiting the private collection of SSNs except where required by law or for the specific purpose of credit, taxes, employment, or investment.

The Consumers Union Model State SSN Protection Law will:

- **Stops most requests for, collection of, and mailing of the SSN.** Stops collection of the SSN by private businesses for purposes beyond credit, taxes, employment, investment, new bank accounts, child support and criminal record checks unless the SSN is required by law.

- **Stops these practices unless required by law:**
  - **Placing SSNs on identification and membership cards**
  - **Posting, displaying, or making SSNs available to the general public**
  - **Using the SSN as a password or access code for goods and services.**
  - **Inviting input of the SSN on the web for unencrypted transmission.**

[‡] States have a variety of exemptions to this prohibition. There are also other states that restrict the mailing of materials in such a way that the SSN is visible on the outside of the mailed material.

- **Tailors exceptions for true need.** Some of the early state laws restricting SSN use included a variety of exceptions. Too many exceptions will undermine the usefulness of a state law restricting SSN collection and use.

This simple measure focuses on a going-forward basis on reducing the risk of identity theft from stolen SSNs by reducing the instances in which SSNs can be requested, collected, mailed, printed on wallet cards, used as passwords, and solicited over the Internet without encryption.

There are also additional areas for further work on SSNs. These additional areas include reducing the appearance of SSNs in public records, reducing government agency use of SSNs, requiring all types of companies holding SSNs to safeguard that data, restricting the practices of database companies that sell information about individuals including or using SSNs, and restricting the internal uses and sharing of SSNs by private companies. Consumers Union is ready to work with states who wish to tackle these additional issues.

---

[1] Krim, Jonathan. "Net Aids Access to Sensitive ID Data." Washington Post. April 4, 2005. Accessed June 21, 2007: www.washingtonpost.com/ac2/wp-dyn/A23686-2005Apr3?language=printer

[2] United States Government Accountability Office, *GAO-07-1023T, Social Security Numbers: Use is Widespread and Protection Could Be Improved* (June 2007), available at http://www.gao.gov/new.items/d07752.pdf

[3] Ibid.

[4] http://www.ftc.gov/os/2003/09/synovatereport.pdf Accessed 6/27/07

[5] www.consumersunion.org/campaigns/financialprivacynow/2007/04/fact_sheet_about_id_theft_1.html

[6] Javelin Strategy & Research, *2007 Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance Necessary*, February 2007.

[7] Ibid.

[8] Cal. Civil Code § 1798.85 (West 2001).

[9] See Arkansas (Ark. Code Ann. § 4-86-107 (2005)); Arizona (Ariz. Rev. Stat. § 44-1373 (2004)); Colorado (Colo. Rev. Stat. § 6-1-715(2006)); Connecticut (Conn. Gen. Stat. § 42-470 (2003)); Georgia (Ga. Code Ann. § 10-1-393.8 (2006)); Hawaii (Haw. Rev. Stat. § 487J-2 (2006)); (Illinois (815 Ill. Comp. Stat. 505/2QQ (2004)); Maryland (Md. Code Ann., Com. Law § 14-3301 et seq. (2005)); Michigan (Mich. Comp. Laws § 445.81 et seq. (2004)); Minnesota (Minn. Stat. § 325E.59 (2005)); Missouri (Mo. Rev. Stat. § 407.1355 (2003)); New Jersey (NJ Stat. Ann. § 56:8-164 (West 2005)); New Mexico (NM Stat. Ann. § 57-12B-4 (2005)); New York (N.Y. Gen. Bus. Law § 399-dd (2006)); North Carolina (N.C. Gen. Stat. § 75-62 (2005)); (Oklahoma (Okla. Stat. tit. 40, § 173.1 (2004)); Pennsylvania (74 Pa. Stat. Ann. § 201 (West 2006); Rhode Island (R.I. Gen. Laws § 6-48-8 (2006)); Texas (Tex. Bus. & Com. Code Ann. 35.58 (2003)); Utah (Utah Code Ann. § 31A-21-110 (2004)); and Virginia (Va. Code Ann. § 59.1-443.2 (2005)).

[10] Kansas recently passed legislation stating that businesses shall not "solicit, require or use for commercial purposes an individual's social security number unless such number is necessary for such person's normal course of business and there is a specific use for such number for which no other identifying number may be used." Kan. Stat. Ann § 75-3520 (2006).

New Mexico also limits the collection of SSNs: "No business shall require a consumer's social security number as a condition for the consumer to lease or purchase products, goods or services from the business." (NM Stat. Ann. § 57-12B-3). This law permits businesses to require SSNs, however, "if the number will be used in a manner consistent with state or federal law or as part of an application for credit or in connection with annuity or insurance transactions" or "if the consumer consents to the acquisition or use." (NM Stat. Ann. § 57-12B-3).

[11]Other states have comprehensive restrictions that only pertain to specific industries. For example, Oklahoma's SSN law only binds health benefit plan employers, while Utah's law restricts SSN use by insurance companies.

The Consumers Union/U.S. PIRG Model State SSN Protection Law

- **Stops most requests for, collection of, and mailing of the SSN.** Stops collection of the SSN by private businesses for purposes beyond credit, taxes, employment, investment, new bank accounts, child support and criminal record checks unless the SSN is required by law.

- **Stops these practices unless required by law:**
  - **Placing SSNs on identification and membership cards**
  - **Posting, displaying, or making SSNs available to the general public**
  - **Using the SSN as a password or access code for goods and services.**
  - **Inviting input of the SSN on the web for unencrypted transmission.**

- **Tailors exceptions for true need.** Some of the early state laws restricting SSN use included a variety of exceptions. Too many exceptions will undermine the usefulness of a state law restricting SSN collection and use.

This simple measure focuses on a going-forward basis on reducing the risk of identity theft from stolen SSNs by reducing the instances in which SSNs can be requested, collected, mailed, printed on wallet cards, used as passwords, and solicited over the Internet without encryption. There are other areas for further work on SSNs. These other areas include reducing the appearance of SSNs in public records, reducing government agency use of SSNs, requiring all types of companies holding SSNs to safeguard that data, restricting the practices of database companies that sell information about individuals including or using SSNs, and restricting the internal uses and sharing of SSNs by private companies. Consumers Union is ready to work with states who wish to tackle these additional issues.

## SPECIFIC LANGUAGE OF MODEL STATE SSN LAW ON PRIVATE COLLECTION, MAILING AND CERTAIN USES OF SSNS

1. A person doing business in this State may not request, collect, or mail to the individual the Social Security number of an individual residing in this State unless one of the following exceptions applies.

(a) The SSN is expressly required by federal, state, or local law or regulation.

(b) The SSN is requested, collected or mailed in connection with a request for credit or a credit transaction initiated by the consumer or in connection with a lawful request for a consumer credit report.

(c) The SSN is requested, collected or mailed in connection with the opening of a deposit account or in connection with an investment.

(d) The SSN is requested, collected or mailed for purposes of employment, including in the

course of the administration of a claim, benefit, or procedure related to the individual's employment by the person, including the individual's termination from employment, retirement from employment, injury suffered during the course of employment; or to check on an unemployment insurance claim of the individual.

(e) The SSN is requested, collected or mailed for purposes of tax compliance.

(f) The SSN is requested, collected, or mailed for the purpose of: interaction with a governmental law enforcement agency; the collection of child or spousal support; or to determine whether an individual has a criminal record.

(g) Nothing in this section or section 2(d) prohibits a person from including his or her own Social Security number on materials sent through the mail. Nothing in this Act applies to the mailing of a copy of a public record which contains a Social Security number.

2. A person doing business in this State may not do any of the following with the Social Security number of an individual residing in this State unless expressly required to do so by federal, state, or local law or regulation:

(a) Place the Social Security number of an individual on any card, tag, badge, or other device issued or used for identification or membership, or on other any card, tag or device issued to an individual, including one issued for the purpose of providing access to products or services. This section includes printing, embedding, encoding within a magnetic strip or on a chip, and any other means of placing the Social Security number on a card, tag, badge, or other device issued for identification or membership.

(b) Solicit or require the use of the SSN as a password for computerized service, telephone customer service, or an Internet web site, or require that an individual provide his or her SSN as a condition to access goods, services, or a website.

(c) Solicit or require an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted, and the request or collection of the Social Security number is otherwise permitted under section (1).

(d) Where mailing of a Social Security number is otherwise permitted under section (1), the Social Security number may not be printed on a postcard or other mailer that does not require an envelope, or in any other manner that makes the Social Security number visible on the envelope or without the envelope being opened.

(e) Publicly post or display, or otherwise make available to the general public, including by sale to the general public, the Social Security number of another individual.

(3) Definitions. For purposes of this Act, the following terms have the following meanings:

(a) "Social Security number" means any portion of three or more consecutive digits of a Social Security number.

(b) "Person" means any individual, firm, partnership, association, corporation, limited liability company, organization or other entity, but does not include the state or any political subdivision of the state, or any agency thereof.

(4) Penalties for violations of this Act.

(a) A person who violates this section is responsible for the payment of a civil fine of not more than $3,000 per violation.

(b) A person who knowingly violates this section is guilty of a misdemeanor punishable by imprisonment for not more than 60 days or a fine of not more than $3,000 or both.

(c) A person who violates this section is liable to each person whose Social Security number is treated in violation of this Act for all of the following: $5,000 per person, actual damages, and reasonable court costs and attorney's fees to a prevailing plaintiff.

(5) The provisions of this act are severable. If any phase, clause, sentence, provision or section is declared to be invalid or preempted in whole or in part by any federal law or regulation, the validity of the remainder of this Act shall not be affected.