American Association of Motor Vehicle Administrators

AAMVA

Testimony of

Linda R. Lewis
President & CEO

American Association of
Motor Vehicle Administrators

Driver's License Security Issues

Submitted to the
Senate Finance Committee

Washington, DC

September 9, 2003

Good Morning, Chairman and distinguished Members of the Senate Finance Committee. My name is Linda Lewis and I am the president & CEO of the American Association of Motor Vehicle Administrators or AAMVA. Thank you for the opportunity to testify on behalf of AAMVA to discuss the vulnerabilities in the driver's license application process and the document itself, its impact on highway safety, identity fraud and national security and a comprehensive approach needed to fix the driver's licensing system.

AAMVA is a state-based, non-profit association representing motor vehicle agency administrators and senior law enforcement officials in the United States and Canada. Our members are the recognized experts who administer the laws governing motor vehicle operation, driver credentialing, and highway safety enforcement. AAMVA plays an integral role in the development, deployment and monitoring of both the commercial driver's license (CDL) and motor carrier safety programs. The Association's members are responsible for administering these programs at the state and provincial levels.

We believe this hearing will generate critical public discourse about the urgent public policy issue of building more integrity into the driver licensing process.

BACKGROUND

After reading the GAO report, neither I, nor any of my members, are surprised by the findings of the investigation. In fact, we believe this investigation is long overdue. This report, conducted under Congressional oversight, only adds to the mounting evidence that ***we need to fix*** our driver licensing process. As technical, hands-on authorities in this field, ***we can tell you*** that the report has, unfortunately, revealed only fragments of the problems that exist in driver licensing.

Why is this happening? Our current licensing structure and the credential that we issue were designed for another time and today's system is, at best, antiquated. The U.S. has more than 240 different, valid forms of passenger car driver's licenses and ID cards in circulation. Each state and D.C. has different practices for issuing licenses and reporting convictions. Individuals looking to undermine the system, whether a problem drinker, underage drinker, identity thief or terrorist shop around for licenses in those states with the weakest practices. Unfortunately, over-the-counter computer software and hardware is making it easier for individuals to produce counterfeit licenses and fraudulent breeder documents.

In addition, the lack of standard security features on a license allows individuals to exploit the system. This makes it difficult for law enforcement to verify the validity of a license from another state — not to mention the identity of the person holding it. This situation is worsened by the availability of counterfeit licenses and fraudulent breeder documents over the Internet and on the underground market.

AAMVA commends the Senate Finance Committee, for its focus on defining and showing the vulnerabilities with the driver's license and identification card. For over 70 years, the AAMVA membership has worked toward uniformity in driver licenses practices. Our members have accepted that the driver's license—a credential, intended to provide the privilege to drive—has become America's most widely accepted form of ID within the past few decades.

Many of our members have taken steps to improve the driver's license issuance process within their own state borders. However, until we all share uniform practices, the process will remain fragmented and vulnerable … as a result, we increase the opportunities for identity theft and put at risk our nation's national security and highway safety.

Shortly after September 11th, AAMVA members came together to develop a comprehensive solution to enhancing the licensing process. Note that I say comprehensive … fixing one aspect of the problem ***will not*** make a difference.

This comprehensive approach addresses:

- tightened application requirements for obtaining a driver's license,
- real-time verification of an applicant's driver history and breeder documents,[1]
- improved processes and procedures for issuance, including internal audit controls and training for employees, and
- increased penalties for those that commit credential fraud.

Vulnerabilities & Comprehensive Approach

The events of September 11th, caused a radical shift in the perception of risk and the use of a driver license or ID card. In October 2001, the AAMVA Executive Committee developed and passed a resolution establishing the Special Task Force on Identification Security. The Task Force concluded that there were a number of common issues needing to be addressed: administrative processing, verification/information exchange, the need for a unique identifier, the format of the driver's license/ID card, fraud prevention and detection, residency, and enforcement and control of standards. Based on the recommendations of the Task Force, AAMVA brought together knowledge, experience and expertise from across jurisdictional boundaries, federal agencies and stakeholder organizations to establish uniform identification practices and procedures to aid in the prevention of fraudulently issued driver licenses and identification cards.

[1] Breeder documents are defined as those documents used to confirm identity such as birth certificates,
Social Security cards or immigration documents.

The objective, with participation and recommendations from states and provinces, was to provide a guide to jurisdictions that would help standardize the process of identifying applicants in the 21st century. AAMVA divided the issues surrounding identification security into 14 subtopics, each subtopic being addressed by a task group.

AAMVA has identified and targeted the areas to fix what we believe are the problems with the current system. Let's look at the vulnerabilities in driver licensing. And more importantly, the steps needed to tighten the system.

First, individuals can apply for and obtain a license in more than one state, which the GAO investigators illustrated by using the same fictitious name and fraudulent documents in seven of the eight states. At this time, DMVs do not have an electronic method to verify whether a person has been issued a license in another state. We need to establish an information system that will ensure each driver has only one driver's license and one driver history record.

Currently, motor vehicle agencies use the National Driver Register/Problem Driver Pointer System (NDR/PDPS) maintained by National Highway Traffic Safety Administration (NHTSA). PDPS helps prevent the issuance of a driver's license to drivers whose licenses have been withdrawn or denied. States are supposed to query PDPS before issuing a license to an applicant to determine whether or not a given driver's license applicant has revocations, suspensions, denials or cancellations anywhere in the country. As illustrated by the GAO investigators, PDPS does not help DMVs determine whether a license has been issued by another state especially if the individual is presenting fraudulent documents and a fictitious name.

In the mid-1990s, AAMVA began exploring the possibility of having a system similar to the Commercial Drivers License Information System (CDLIS) for all drivers within the United States in order to better monitor the problem driver population. States need more effective tools to manage the driving records *we already maintain*. Problem drivers, who obtain multiple licenses, spread their bad driving history across the states. As a result, they avoid detection, penalties and punishment. By 1999, Congress recognized the potential benefits of such an information system and directed NHTSA and FMCSA to study the IT issues and costs associated with developing and operating this system. The report concluded an all-driver pointer system is feasible.[2]

[2] National Highway Traffic Safety Administration in conjunction with Federal Motor Carrier and AAMVA, "*Report to Congress: Evaluation of Driver Licensing Information Program and Assessment of Technologies,"* 2001. (http://www.aamva.org/drivers/drv_AutomatedSystemsDRIVerS.asp#Tech Assessment)

We have witnessed the success of such a system through the use of CDLIS, which kept more than 871,000 potential dangerous truck drivers from obtaining a commercial driver's license between 1992 and 1996.[3] CDLIS is designed as a pointer system for commercial drivers. CDLIS limits commercial drivers to **one and only one** commercial driver's license and it has worked well for this purpose. Before CDLIS, it was possible for a commercial driver to apply for and obtain a commercial driver's license in a new state without acknowledging having an existing license in another state. This had serious implications for highway safety, since hiding the existence of another license could also hide a dangerous driving record.

We need an all-pointer driver system that will direct one state where to find and accurately verify someone's driving histories in other states for all drivers, commercial and non-commercial. DMVs already exchange driver history on commercial vehicle drivers through CDLIS. An all-driver pointer system will help prevent identity theft and strengthen national security by limiting a driver to one license and one driving history.

Second, the use of false breeder documents to obtain an authenticate driver's license or identification card runs rampant within the application process. <u>DMVs must adopt a uniform resource list for acceptable identification documents</u>, which will narrow down the numerous documents, relied on for issuing a license or identification card. After much research, AAMVA has recently concluded and issued the Acceptable Verifiable ID Resource List and Administrative Procedures.[4] By utilizing the lists, its procedures and future fraudulent document recognition training, motor vehicle employees should be able to verify that the applicant in front of them is who they are claiming to be and that documents presented are reliable. The use of the resource lists also promotes uniformity, identification reciprocity between jurisdictions, and helps protect the customer's personal information.

In addition, <u>DMVs must provide adequate fraudulent document training to their employees.</u> We need to give them the tools to recognize and appropriately handle fraudulent documents. The use of fraudulent documents has caused enormous economic losses in both the U.S. and Canada. The use of fraudulent documents to obtain driver's licenses/identification cards has grown exponentially in recent years. AAMVA in conjunction with the Federal Motor Carrier Safety Administration (FMCSA), the National Highway Traffic Safety Administration (NHTSA), the U.S. Secret Service (USSS), the Royal Canadian Mounted Police (RCMP) and the Canadian Council of Motor Transport Administrators (CCMTA) has developed a comprehensive model training program for Fraudulent Document Recognition (FDR)**.**

[3] Federal Highway Administration, Office of Motor Carrier Research & Standards Driver Division, *"Commercial Driver License Effectiveness Study,"* page 11, September 1998.

[4] American Association of Motor Vehicle Administrators, *Status Report to AAMVA Membership--Attachment 1 Acceptable Verifiable Resource Lists and Procedures*, July 2003,(http://www.aamva.org/Documents/idsAttach1StatReportJuly03.pdf).

The three-level FDR program is designed to assist states and provinces with the formal training of motor vehicle and law enforcement personnel in the recognition/detection of fraudulent identification documents. Level I address basic training needs for frontline employees and law enforcement officials. Level II addresses advanced training needs for motor vehicle supervisors, document examiners, law enforcement officials and fraud investigators. Level III addresses training at a forensic level and is slated for future development, if deemed necessary. Level I and Level II training materials were showcased during the 2003 AAMVA regional meetings. Formal Level I and Level II train-the-trainer sessions, designed to train jurisdictional fraud trainers, will be held between October 2003 and February 2004. Based on available funding, future development may include training videos, educational brochures, self-study materials and computer-based and/or Web-based training. AAMVA will establish a maintenance program to update the materials on a regular basis. We invite members of the committee to attend any of the upcoming training sessions.

Furthermore, we must ensure motor vehicle agencies have the ability, preferably electronically, to verify the validity of source documents with issuing agencies, such as the Social Security Administration, Immigration and Naturalization Services, vital records agencies and other DMVs. Currently, 25 states are electronically verifying Social Security Numbers with the Social Security Administration. But that verification process needs improvement. Too frequently SSA's automated system indicates that a number does not match, when in reality, after manual investigation, it is a match. This situation is deterring other states from using the SSA system. Congress must direct the Social Security Administration to improve their system so that this unnecessary, labor-intensive process can be eliminated. Each check of the system should also reference SSA's death records to ensure that a state does not issue a driver's license or identification card to an individual presenting personal information of a deceased person.

AAMVA is working cooperatively with the state and the Federal Motor Carrier Safety Administration (FMCSA) to pilot test three on-line verification systems:

- Online Verification of Driver Licenses – this allows states and third parties, such as airports and banks, to electronically verify that a license presented to them was actually issued by the state shown on the face of the license. Once rolled out nationwide, this effort will greatly inhibit a criminal's ability to use counterfeit driver licenses.

- Interstate Digital Image Exchange – this allows states to exchange digital driver photos so that they can compare the picture to the individual standing in front of the clerk applying for a license. Once rolled-out nationwide, this will inhibit imposters from obtaining licenses and ID cards under another person's identity.

- Online Verification of Birth Certificates – this allows the states to electronically interact with the National Association for Public Health Statistics and Information Systems (NAPHSIS) to check state vital statistics records to determine the validity of a birth certificate being used to establish identity as part of the driver licensing program. Once rolled-out nationwide, this will inhibit the criminal's ability to use counterfeit birth certificates to obtain a driver license or ID card.

These are very worthy efforts and, on behalf of the states, AAMVA thanks Congress and FMCSA for providing the seed money to get them going. But they are not fully effective unless all of the data is available and all of the states are participating. The states need the help and support of Congress to get these programs rolled-out nationwide.

Third, the driver's license document is easily counterfeited. The current variety of documents and lack of uniform security features makes it easy for criminals to alter a real document or create a counterfeit. We must provide fraudulent document training to not only DMV employees but stakeholders to thwart acceptance of fake documents. The GAO investigators showed how easy it was to create and alter a driver's license and breeder documents using inexpensive commercial available software and hardware. Also, motor vehicle agencies must establish better procedures for removing fraudulent documents when an employee realizes the documents are fraudulent. We cannot afford to give the fraudulent documents back to the perpetrator and law enforcement needs to be notified without endangering the DMV employee. However in some instances, DMV employees inform individuals that produce fraudulent documents to obtain a driver's license or ID card the correct procedure to apply for a document. There is a delicate balance between customer service, safety and security.

Additionally, motor vehicle agencies need to adopt minimum, uniform card design and security specifications for the driver license document. To secure jurisdiction-issued driver's license/ID card credentials, the association examined card functionality, visible data and card layout, machine-readable data elements, machine-readable technology (MRT), document security features, and other card design elements and considerations. AAMVA, working with a wide variety of stakeholders, has developed those minimum specifications and they are now available for use by the states.

Fourth, we are all human. For some, this comes with the vulnerability to criminal behavior, which can result in stolen DMV equipment and inventory and the acceptance of bribes. Daily, individuals are breaking into DMV's, stealing equipment and inventory to produce documents. AAMVA is developing model procedures for security and inventory controls. DMVs and all identity issuing agencies need an information system to post alerts when equipment or inventory is stolen. Currently, through AAMVA's Web site, the association posts alerts regarding official federal, international or state documents and equipment that is stolen.

We must provide online verification of the driver license and ID card. This will render stolen equipment and inventory useless. Any driver licenses or ID cards created on stolen equipment would be rejected in the verification process because the state's database would not contain information pertaining to those cards.

Unfortunately, individuals bribe DMV clerks to issue driver's license or ID cards. It is a lucrative business. We want to stop criminal behavior on both sides of the counter. However, we need to implement stronger internal controls and auditing procedures that detect this behavior and prevent it from spreading. And, we must implement stiffer penalties and enforcement for those who choose to break the law.

Fifth, we must protect an individual's personal privacy while trying to bring the driver's license system into the 21st century. DMVs adhere to some of the strongest privacy laws on the books – the Driver's Privacy Protection Act. DPPA prohibits DMVs from selling your driver record information for commercial purposes without your prior consent. We'd like to make them stronger. The AAMVA Board of Directors passed a resolution stating that the association does not support the practice of collecting people's personal information from a driver's license for the purposes of marketing or building customer databases— without the full knowledge and consent of the license holder. We advocate that people or organizations scan the driver's license only to verify and not to capture information. Furthermore, in May 2003, the AAMVA Board endorsed eight privacy principles based on the Global Privacy Design Principles.[5] The principles address openness, individual participation, collection limitation, data quality, use, disclosure limitation, security, and accountability. Therefore, AAMVA is assessing the impact of DL/ID security improvement on personal privacy and will develop best practices and model guidelines for motor vehicle agencies to inform citizens of personal information protection.

CONCLUSION

These problems exist and are **interstate** in nature. The only way to ensure that the proper fixes have been applied is for all states to follow the same roadmap. Inconsistent remedies from state to state will leave open the loopholes that exist today. The solution:

- must be implemented as a package and not as a piecemeal fix.
  - will reduce identity theft and enhance homeland security and highway safety.
  - can be accomplished ***without*** sacrificing an individual's personal privacy.
  - can only be achieved with a federal-state partnership. Without a federal-state partnership to implement the solutions, this comprehensive approach is little more than a best practice.

[5] American Association of Motor Vehicle Administrators, *Status Report to AAMVA Membership –Attachment 4 Privacy Principles*, July 2003, (http://www.aamva.org/Documents/idsAttach4StatReportJuly03.pdf)

Firsthand, you have witnessed the vulnerabilities of the current process. Congress, we need your help. AAMVA has submitted three proposals to Congress for authorization and funding to help implement this comprehensive approach through the reauthorization of the Transportation Equity Act for the 21st Century (TEA-21). We have asked for funding to implement an all-driver pointer system, interstate digital image exchange and online verification of birth and death records.

Now I ask you to take the first step in supporting the changes that must take place to reduce identity theft, enhance our national security and to save lives on our highways.

Thank you. I've concluded my testimony and welcome any questions from the subcommittee.