Testimony of

Barry J. Goleman

Vice President, Public Sector

American Management Systems, Inc.

United States Senate

Committee on Governmental Affairs

Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia

"A License to Break the Law? Protecting the Integrity of Driver's Licenses"

April 16, 2002

I would like to thank Chairman Durbin, the Ranking Member, and the other members of this committee for the opportunity to appear here today.

I am a vice president in the Public Sector Group at American Management Systems. AMS is a business and information technology consulting firm with international headquarters located in Fairfax, Virginia. In 2001, AMS had revenues of $1.18 billion. We employ more than 7,000 people in 51 offices worldwide. Our business is equally split between the public and private sector, with about one-half of our public sector work serving state and local governments. Our clients have included more than 90 percent of U.S. federal civilian agencies, all U.S. military and major defense agencies, 41 U.S. state governments, and eight of the top 10 U.S. cities.

AMS specializes in the intelligent application of information technology. Our size and balanced business portfolio give us the agility to work across the public and private sector, introducing innovative solutions and best practices across industries and government.

I have been involved in the issuance of driver's licenses, and the information systems to support that process, for more than 29 years—first as a driver's license examiner for the State of California and later as the president of the American Association of Motor Vehicle Administrators (AAMVA) information technology subsidiary, AAMVAnet. In my capacity as an examiner, I was presented with counterfeit documents to obtain a license, I stopped people from stealing identities for the purpose of cashing stolen checks, and I was offered bribes to issue false identification. I come here today in support of your efforts to strengthen the integrity of the driver's license because I know what work needs to be done, and I know that this work can be done—if state and federal agencies and the technology industry will work together to make it happen.

Senator Durbin, I commend your committee for its thoughtful approach to this challenging task. It is obvious, especially in the wake of our nation's new homeland security imperative, that the problems of identity theft and fraud must be addressed quickly. Prior to September 11, driver's license fraud and identity theft often were viewed as financial crimes or teenage pranks. According to research conducted by the Yankee Group, during the year 2000, the Financial Crimes Division of the Secret Service made 10,000 arrests involving identity theft or fraud. Such crimes can have as many as 750,000 victims and cost consumers tens of millions of dollars annually. As you know, the investigation subsequent to September 11 has placed the problems of identity theft in a whole new light. We learned that terrorists, bent on destroying the American way of life, used our state motor vehicle agencies to create identities that allowed them entry into our economic and transportation systems. They were able to accomplish this because the driver's license, or state-issued identification card, is the de facto identification used by Americans to prove their identity within our borders.

This recognition of the driver's license as a trusted form of identification has grown out of its use in everyday American life: retailers use it for check cashing, banks for account verification, and airports for security access. One of my own encounters with how much trust is placed in the driver's license occurred when I was required to present documents proving my American citizenship to be employed by a federal agency. I provided my naturalization papers, as I was born outside the United States to American parents. Instead of using my secure naturalization papers to verify my identity, the personnel clerk asked to see my driver's license. You may remember that 6 of the 19 hijackers on September 11 used stolen identities. The terrorists obtained multiple IDs because they knew that the driver's license was a trusted form of identification, and these terrorists were able to leverage the weaknesses in our state identification systems with devastating consequences. Therefore, it is imperative that we improve the integrity of the driver's license so that it can live up to its reputation as a trusted personal identification document.

To address this critical homeland security threat, state and federal agencies should develop a strategy that takes advantage of rapid evolution. By that, I mean adapting and expanding existing technology, relatively quickly, and capitalizing on existing infrastructure. We do not need to reinvent the wheel here. Existing state-based assets can be used to create a more secure identification to combat the problem of identity fraud and theft.

Some have called for a new national identification system, built essentially from scratch, but this proposed solution is neither feasible nor quick to implement. States already have an extensive, functioning infrastructure through their motor vehicle agencies. It is essential to capitalize on the existing information assets maintained by these state agencies.

Identification fraud, also known as identity theft, is exacerbated by the 50 states issuing a confusing array of state licenses that use a range of security features and rely on easily forged or counterfeit documents. Law enforcement experts estimate that there are more than 240 valid driver's license formats in circulation. As we have seen, identity theft is a security breach with enormous consequences. New state-issued and controlled secure personal ID cards, based on national standards, are an essential component of maintaining our nation's security. To issue personal identification documents that ensure the highest level of security, national standards should be developed around the following processes:

- Verification of source documents prior to their acceptance as proof of identification
- Issuance of a new, secure, tamperproof driver's license or other personal ID document
- Authentication of the ID with visual and machine-readable features

The most persuasive argument for turning to state motor vehicle agencies for improved personal ID verification processes is that these agencies are already in the identification business. This enormous, functioning infrastructure can be adapted by providing national standards and enhanced technologies to verify identification and detect fraud.

Many proponents of a secure personal ID system will tell you about the value of biometrics and smart-card technologies, and clearly these technologies can provide substantial benefit. To provide maximum security, these next-generation ID documents must adhere to standard security features using the highest level of tamper-resistant technologies available. Biometrics, for example, can complete a positive one-to-one authentication of the person to the card. In addition, smart cards can make the driver's license a carrier for important data such as including the biometric identifier right on the card itself or other optional data that individuals may wish to add, such as emergency medical information or digital government access.

These new technologies are an important part of our future, but if they are used without improved verification technologies, they will be useless as secure, reliable forms of identification. As you draft new legislation to improve the integrity of the driver's license, I urge you to consider new technologies that can be used to verify identity. This will ensure that people with counterfeit or false IDs won't receive better, more secure ID documents.

The first step in securing identification is a thorough verification of the individual's identity before enrolling them in the system. To accomplish this verification, state examiners must have access to the data backing up these documents, such as birth records and immigration data. Databases are more difficult to falsify than paper documents

The second step is addressing privacy concerns by ensuring that the data is verified but not copied or aggregated into a consolidated personal identification database. Today's Web services technologies can exchange data between these databases and secure personal data from unintended disclosure. The simple fact is that if you don't do a better job of establishing an individual's identity before you issue a new, secure driver's license, you will not have achieved your goal of making the driver's license a more trustworthy document.

For example, technology is available to assist driver's license examiners make better identification decisions. These tools can be used to verify data from the driver's license application (name, address, Social Security number, etc.) by leveraging existing public consumer databases. The examiner can quickly check and confirm the applicant's information, validate the identity, and identify fraudulent information during the driver's license transaction. Discrepancies can be resolved by requesting additional documentation from the applicant or, in some cases, no license will be issued until further checks are made at the central office. States and federal governments are in the process of testing solutions like this in an effort to improve the basis for making identification decisions.

The third step in developing a secure ID system is the prevention or deterrence of employee fraud. Just as I was occasionally offered bribes of cash or sexual favors in exchange for issuing driver's licenses, today's examiners have their integrity challenged when criminals seek any path to obtain a valid state license. (For the record, let me assure you that I refused these attempted bribes.) Unfortunately some have not resisted these kinds of temptations, and the resulting scandal and corruption are well documented. Effective employee fraud deterrence by a responsible licensing administrator must include internal auditing and business intelligence tools.

There is tremendous power and sophistication in software already in use in the commercial sector. This technology underlies millions of everyday transactions in the marketplace and enables a more rigorous approach to auditing and decision support. These same tools can be used to monitor driver's license transactions and highlight behaviors and patterns that warrant further investigation. For example, it takes about 45 minutes to complete a commercial driver's license test administered according to Federal Motor Carrier Safety Administration rules. As a supervisor, I would want to investigate an examiner that issued commercial licenses in 10 minutes. Sadly, today many state motor vehicle agencies are unaware of these fraudulent activities until agency co-workers or the public report suspected activity. This is an example of the application of proven technology from the business sector.

All of these steps are achievable with federal, state and private-sector cooperation. From my experience working with state and federal agencies to improve motor vehicle systems, I can assure you that the application of best practices in the state issuance process—supported by robust and effective information technology—can result in a secure and trustworthy means of personal identification.

The IT industry uses sophisticated technology and management know-how to open doors to better efficiency, productivity, and prosperity however, we must be willing to work in a public-private partnership to close doors that will keep out those who want obtain false identification and move freely about our commercial, financial, and transportation systems.

I am sad to say that, in the aftermath of September 11, we've learned that the terrorists obtained multiple driver's licenses and ID cards from state motor vehicle agencies with ease—some using fraudulent documents or bribes. Despite this breach in security, there is encouraging news: this is a problem that we can fix. With technology that exists today, we can stop the fraud and counterfeiting of state licenses. The states and federal government worked cooperatively from 1987 to 1992 to implement the requirements of the Commercial Motor Vehicle Safety Act. Federal grants were made available to states to implement new strict standards that were developed in cooperation with state licensing experts. That cooperative effort serves as an example of how to solve problems by employing technology and leveraging the combined strengths of federal and state agencies. Working together, again, we can solve this homeland security problem.

Senator Durbin, we at AMS believe that this committee is on exactly the right track by holding this hearing and advocating the development of a more secure driver's license. We believe technology can advance identification security while preserving our personal freedoms.

Thank you. I look forward to your questions.

Attachment: AMS White Paper, "Establishing a National System for State-Issued Secure Personal Identification"